Н. А. Молдовян

ПРАКТИКУМ ПО КРИПТОСИСТЕМАМ С ОТКРЫТЫМ КЛЮЧОМ

- *Математический минимум*
- *Алгоритмы электронной цифровой подписи*
- *Новые схемы ЭЦП*
- *Задачи с решениями по анализу и синтезу ЭЦП*
- *Задания для курсовых работ*

УЧЕБНОЕ ПОСОБИЕ

bhv

Н. А. Молдовян

ПРАКТИКУМ ПО КРИПТОСИСТЕМАМ С ОТКРЫТЫМ КЛЮЧОМ

Санкт-Петербург
«БХВ-Петербург»
2015

УДК 681.3
ББК 32.81
М75

Молдовян Н. А.

М75 Практикум по криптосистемам с открытым ключом. — СПб.: БХВ-Петербург, 2015. — 304 с.: ил.

ISBN 978-5-9775-3524-3

Приведено краткое изложение математических результатов, используемых при синтезе и анализе криптосистем с открытым ключом, и ряда классических и новых криптосистем этого типа, включая достаточно большое число схем электронной цифровой подписи (ЭЦП). Основная часть книги содержит материалы для проведения практических занятий: формулировки заданий для курсовых работ и проектов и большое количество оригинальных задач, связанных с новыми схемами ЭЦП или вопросами, касающимися синтеза и анализа последних. Все задачи сопровождаются подробными указаниями и решениями.

Для преподавателей, студентов и аспирантов инженерно-технических вузов

УДК 681.3
ББК 32.81

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Компьютерная верстка	*Сергея Матвеева*
Корректор	*Наталия Першакова*
Дизайн обложки	*Игоря Цырульникова*
Зав. производством	*Николай Тверских*

Формат 70×100$^{1}/_{16}$. Усл. печ. л. 24,51. Доп. тираж 20 экз.
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Отпечатано в типографии ООО "Супервэйв Групп"
193149, РФ, Ленинградская область, Всеволожский район, пос. Красная Заря, д. 15

ISBN 978-5-9775-3524-3

Содержание

Введение **5**

Глава 1. Понятия и результаты теории чисел **7**

1.1. Сравнения: некоторые свойства и теоремы 7
1.2. Показатели и первообразные корни 9
1.3. Индексы по модулям p^{α} и $2p^{\alpha}$ 10
1.4. Теоремы о числе классов с заданным показателем 11
1.5. Теоремы о числе решений степенных сравнений 13

Глава 2. Алгоритмический минимум **15**

2.1. Вычисление наибольшего общего делителя и его линейного представления 15
2.2. Китайская теорема об остатках 16
2.3. Алгоритм быстрого возведения в степень по модулю 17
2.4. Нахождение первообразных корней 19
2.5. Нахождение чисел, относящихся к заданному показателю 20
2.6. Генерация простых чисел 21
2.7. Детерминистическая генерация больших простых чисел 23
2.8. Извлечение квадратных корней по простому модулю 26
2.9. Извлечение корней степени $n > 2$ по простому модулю 32
2.10. Факторизация B-гладкого модуля RSA 37
2.11. Метод дискретного логарифмирования 39

Глава 3. Краткий обзор классических криптосистем с открытым ключом **45**

3.1. Открытое распределение ключей 45
3.2. Открытое шифрование 46
3.3. Системы электронной цифровой подписи 48
3.4. Слепая подпись 54
3.5. Схемы ЭЦП с восстановлением сообщения 55
3.6. Экзистенциальная подделка подписи и потайные каналы в системах ЭЦП 58

Глава 4. Схемы ЭЦП с новым механизмом формирования подписи 63

4.1. Схемы с формированием подписи на основе решения системы сравнений 63
4.2. Схемы с подписью вида (k, S) 67
4.3. Схемы с RSA-модулем 70
4.4. Применение простого модуля в схемах, основанных на сложности факторизации 75
4.5. Схемы с восстановлением сообщения 79
4.6. Новые схемы ЭЦП с сокращенной длиной подписи 86
4.7. Новый подход к уменьшению размера подписи до 160 бит 92

Глава 5. Варианты заданий для курсового проектирования 99

5.1. Схемы ЭЦП на основе сложности дискретного логарифмирования 101
5.2. Схемы ЭЦП на основе сложности факторизации RSA-модуля 108
5.3. Схемы ЭЦП с восстановлением сообщения 115
5.4. Схемы ЭЦП с сокращенным размером подписи 121
5.5. Задания повышенной сложности 130
5.6. Генерация числовых примеров 134

Глава 6. Задачник 139

6.1. Элементы теории чисел 139
6.2. Схемы ЭЦП 149

Глава 7. Ответы, решения и пояснения 181

7.1. Элементы теории чисел 181
7.2. Схемы ЭЦП 213

Заключение 291

Список литературы 293

Введение

В настоящее время проблематика и методы криптографии входят в ряд курсов по подготовке специалистов в области защиты информации и информационных технологий в целом. К настоящему моменту появилось достаточно большое число книг на русском языке, затрагивающих вопросы классической и современной криптографии. Среди этих книг имеются справочники, монографии, учебные пособия и учебники, написанные зарубежными и российскими авторами. Благодаря этому студенты, аспиранты и молодые специалисты имеют достаточно широкие возможности по выбору теоретического материала, однако материал для практических занятий в имеющихся книгах проработан недостаточно. В частности, отсутствует материал для подготовки заданий к курсовым работам и проектам, а приводимые для самопроверки вопросы и задачи не снабжены достаточно подробными указаниями и решениями. Целью данной книги является восполнение этого пробела по отношению к криптосистемам с открытым ключом. Она является дополнением к учебному пособию Н. А. Молдовяна и А. А. Молдовяна «Введение в криптосистемы с открытым ключом» (БХВ-Петербург, 2005) и включает следующий материал:

- краткий перечень основных понятий и результатов теории чисел, используемых при построении и анализе двухключевых криптосистем;
- краткий обзор классических криптосистем с открытым ключом;
- алгоритмический минимум, дающий возможность получить представление, как организуются вычисления в двухключевых криптосистемах;
- описание некоторых новых систем с открытым ключом, расширяющих набор конструктивных механизмов, которые использованы для разработки вариантов курсовых заданий и при составлении задач;
- около 200 вариантов заданий для выполнения курсовых работ и проектов;

- список задач по элементам теории чисел, необходимым для понимания вычислительных процедур, лежащих в основе криптосистем с открытым ключом;
- список задач по двухключевой криптографии, который, в частности, охватывает тематику анализа и синтеза систем электронной цифровой подписи различного типа;
- решения, указания и ответы ко всем задачам, число которых составляет около 300.

При этом преобладающую часть объема книги занимает рассмотрение курсовых заданий и задач.

Данное учебное пособие ориентировано в первую очередь на студентов и преподавателей вузов, аспирантов и молодых специалистов, работа и исследования которых затрагивают вопросы криптографии.

ГЛАВА 1

Понятия и результаты теории чисел

Более полно с результатами теории чисел и их доказательствами можно ознакомиться в работах [1, 2, 3].

Простым числом называется число, которое делится без остатка только на единицу и само на себя. Иными словами, простым называется число $p \geq 3$, которое не делится без остатка ни на одно из следующих чисел 2, 3, ..., $p-1$. Число 2 также является простым.

Взаимно простыми называются два целых положительных числа, наибольший общий делитель которых равен 1.

1.1. Сравнения: некоторые свойства и теоремы

Два числа a и b называются сравнимыми по некоторому модулю n, если разность $a-b$ делится на n без остатка. Сравнимость можно определить также и следующим образом: два числа a и b называются сравнимыми по некоторому модулю n, если остатки от деления a на n и b на n равны между собой. Если принять второе определение, то первое является следствием, и наоборот.

Утверждение 1

Если НОД$(a, n) = 1$ и $(a \times b) \equiv (a \times c) \bmod n$, то $b \equiv c \bmod n$.

Утверждение 2

Для любого целого числа $a > 0$, взаимно простого с модулем n, существует обратное по mod n число, обозначаемое знаком a^{-1}, такое что $a \times a^{-1} \equiv 1 \bmod n$. Число a^{-1} называется мультипликативно обратным по модулю n.

Следствие 1

Если модуль p является простым числом, то для любого числа $0 < a < p$ существует мультипликативно обратный элемент по модулю p.

Утверждение 3

Пусть для целых положительных чисел a и b имеем $a > b$ и НОД$(a, b) = d$, тогда для остатка r от деления a на b выполняется равенство НОД$(b, r) = d$.

Данное утверждение лежит в основе алгоритма Евклида, позволяющего эффективно вычислять наибольший общий делитель (НОД) двух натуральных чисел.

Теорема Ферма

Теорема Ферма утверждает следующее: для любого простого числа p и любого положительного числа a, которое не делится на p, выполняется сравнение

$$a^{p-1} \equiv 1 \bmod p.$$

Функция Эйлера обозначается символом $\varphi(n)$ и определяется как число положительных целых чисел, которые меньше натурального числа $n > 1$ и являются взаимно простыми с n. По определению $\varphi(1) = 1$. Функция Эйлера является мультипликативной функцией, т. е. для двух взаимно простых чисел a и b выполняется соотношение $\varphi(ab) = \varphi(a) \times \varphi(b)$. Произвольное число n может быть представлено в виде произведения, содержащего только взаимно простые сомножители вида p^s, где $s \geq 1$ и p — простое число. Для числа p^s имеем:

$$\varphi(p^s) = p^{s-1}(p-1).$$

Теорема Эйлера

Для любых взаимно простых чисел a и n выполняется сравнение

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Обобщенной функцией Эйлера называется функция $L(n)$, определенная для всех натуральных чисел следующим образом: $L(1) = 1$, а при $n > 1$

$$L(n) = \text{НОК}\left[p_1^{\alpha_1 - 1}(p_1 - 1); p_2^{\alpha_2 - 1}(p_2 - 1); \ldots; p_k^{\alpha_k - 1}(p_k - 1)\right],$$

где $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ и НОК — наименьшее общее кратное.

Обобщенная теорема Эйлера

Если НОД$(a, n) = 1$, то $a^{L(n)} \equiv 1 \bmod n$.

1.2. Показатели и первообразные корни

Определение

Пусть НОД$(a, n) = 1$. Наименьшее из чисел γ, для которых выполняется сравнение $a^{\gamma} \equiv 1 \bmod n$, называется ***показателем***, которому число a принадлежит по модулю n.

Утверждение 4

Если a по модулю n принадлежит показателю δ, то числа $a^0, a^1, \ldots, a^{\delta-1}$ по модулю n несравнимы.

Утверждение 5

а) Если a по модулю n принадлежит показателю δ, то $a^{\gamma} \equiv a^{\gamma'} \bmod n$ тогда и только тогда, когда $\gamma \equiv \gamma' \bmod \delta$.

б) Если $\gamma = 0$, то имеем сравнение $a^{\gamma} \equiv 1 \bmod n$, которое выполняется тогда и только тогда, когда γ делится на показатель δ.

Следствие 2

Показатели, которым числа a принадлежат по модулю n, являются делителями $\varphi(n)$.

Действительно, пусть a по модулю n принадлежит показателю δ. Из $a^{\varphi(n)} \equiv 1 \bmod n$ следует, что $\varphi(n)$ делится на δ. Наибольший из этих делителей есть само $\varphi(n)$.

Утверждение 6

Если число a по модулю n принадлежит показателю $\varepsilon'\varepsilon$, то $a^{\varepsilon'}$ принадлежит показателю ε.

Утверждение 7

Если a по модулю n принадлежит показателю u, а b — показателю v, причем НОД$(u, v) = 1$, то ab принадлежит показателю uv.

Интересен вопрос о существовании чисел, принадлежащих показателю $\varphi(n)$. Такие числа существуют и называются первообразными корнями по модулю n. В теории чисел доказываются теоремы о существовании первообразных корней по модулю p, по модулю p^k и по модулю $2p^k$, где p — простое нечетное число и k — произвольное положительное целое число.

Утверждение 8

Существуют первообразные корни по модулю p, где p — простое нечетное число.

Утверждение 9

Пусть g — первообразный корень по модулю простого числа p. Можно указать t с условием, что u, определяемое равенством $(g + pt)^{p-1} = 1 + pu$,

не делится на p. Соответствующее $g + pt$ будет первообразным корнем по модулю p^{α} при любом $\alpha > 1$.

Утверждение 10

Пусть $\alpha \geq 1$ и g_1 — первообразный корень по модулю p^{α}, где p — нечетное простое число. Нечетное из чисел g' и $g' + p^{\alpha}$ будет первообразным корнем по модулю $2p^{\alpha}$.

Утверждение 11

Пусть $q_1, q_2, \ldots, q_k$ — различные простые делители функции Эйлера $\varphi(n)$ от числа n. Для того чтобы число g, взаимно простое с n, было первообразным корнем по модулю n, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений:

$$g^{c/q_1} \equiv 1 \bmod n,\ g^{c/q_2} \equiv 1 \bmod n,\ \ldots,\ g^{c/q_k} \equiv 1 \bmod n.$$

1.3. Индексы по модулям p^{α} и $2p^{\alpha}$

По отношению к первообразным корням g вводится понятие индекса (при основании g) по модулю.

Утверждение 12

Пусть p — простое нечетное число; $\alpha \geq 1$; n — одно из чисел p^{α} и $2p^{\alpha}$; $c = \varphi(n)$; g — первообразный корень по модулю n. Если γ пробегает наименьшие неотрицательные вычеты $\gamma = 0, 1, \ldots, c-1$ по модулю c, то g^{γ} пробегает приведенную систему вычетов по модулю n.

Для чисел a, взаимно простых с n, рассматривается понятие об индексе (дискретном логарифме), представляющее аналогию понятия о логарифме. Если $a \equiv g^{\gamma} \bmod n$ (предполагается, что $\gamma \geq 0$), то γ называется индексом числа a по модулю n при основании g и обозначается символом $\gamma = \operatorname{ind}_g a$ (или просто $\gamma = \operatorname{ind} a$). Из утверждения 12 следует, что всякое a, взаимно простое с n, имеет некоторый единственный индекс среди чисел ряда $\gamma = 0, 1, \ldots, c-1$. Зная γ', такое что $\gamma' = \operatorname{ind}_g a$, мы можем указать все индексы числа a: это будут все неотрицательные числа класса $\gamma \equiv \gamma' \bmod c$. Действительно, имеем $a \equiv g^{\gamma} \bmod n$ и $a \equiv g^{\gamma'} \bmod n$, поэтому $g^{\gamma - \gamma'} \equiv 1 \bmod n$, и поскольку g относится к показателю $c = \varphi(n)$, то $c \mid (\gamma - \gamma')$, т. е. $\gamma \equiv \gamma' \bmod c$.

Из определения индекса непосредственно следует, что числа с данным индексом γ образуют класс чисел по модулю n. Индексы обладают следующими свойствами:

$$\operatorname{ind}_g ab\ldots l \equiv \operatorname{ind}_g a + \operatorname{ind}_g b + \ldots + \operatorname{ind}_g l \pmod c,\ \operatorname{ind}_g a^n \equiv n \operatorname{ind}_g a \pmod c.$$

1.4. Теоремы о числе классов с заданным показателем

Обозначим число классов, относящихся к показателю δ, через $\psi(\delta)$. Если δ не делит $\varphi(n)$, то такое δ не может быть показателем ни для какого числа, поэтому в этом случае имеем $\psi(\delta) = 0$. Показатель числа a будем обозначать как $P(a)$.

Теорема 1

Сравнение степени k по простому модулю p с коэффициентом при старшем члене, не делящемся на p, может иметь не больше чем k решений.

Теорема 2

В последовательности $a, a^2, a^3, \ldots$ все числа принадлежат $P(a)$ классам, представителями которых являются числа $a, a^2, a^3, \ldots, a^{P(a)}$, где $P(a)$ есть показатель числа a по некоторому модулю n.

Теорема 3

$P(a^l) = P(a)$ тогда и только тогда, когда НОД$(l, P(a)) = 1$.

Теорема 4

Если по модулю n $P(a) = k$, то классы $\overline{a}, \overline{a^2}, \ldots, \overline{a^k}$ представляют собой различные решения сравнения $x^k \equiv 1 \bmod n$. (В общем случае указанные классы не охватывают *всех* решений данного сравнения.)

Теорема 5

Если по простому модулю p $P(a) = k$, то классы $\overline{a}, \overline{a^2}, \ldots, \overline{a^k}$ представляют собой *все* решения сравнения $x^k \equiv 1 \bmod p$.

Теорема 6

Количество классов, относящихся к какому-либо показателю по модулю n, равно функции Эйлера $\varphi(n)$ от модуля:

$$\sum_{\delta|\varphi(n)} \psi(\delta) = \varphi(n).$$

Теорема 7

По простому модулю p для любого целого $\delta \geq 1$ имеет место неравенство

$$\psi(\delta) \leq \varphi(\delta).$$

Теорема 8

По простому модулю p при $\delta | p - 1$ имеет место равенство $\psi(\delta) = \varphi(\delta)$.

Теорема 9

По любому простому модулю p существует $\varphi(p-1)$ первообразных корней.

Теорема 10

Первообразные корни по модулю n существуют тогда и только тогда, когда либо 1) $n = p^{\alpha}$ или $n = 2p^{\alpha}$, где p — любое нечетное простое число, α — любое целое положительное число, либо 2) $n = 2^{\alpha}$, где $0 \le \alpha \le 2$.

Теорема 11

$$\sum_{\forall d | m} \varphi(d) = m.$$

Теорема 6*

$$\sum_{\forall \delta | p-1} \psi(\delta) = p - 1.$$

Теорема 12

Если $a \equiv b \pmod{n_1}$, $a \equiv b \pmod{n_2}$,..., $a \equiv b \pmod{n_g}$, то $a \equiv b \pmod{N}$, где $N = \text{НОК}[n_1, n_2, \ldots, n_g]$.

Утверждение 13

Для произвольных натуральных чисел k и m из выполнимости сравнения $a \equiv b \pmod{m}$ следует сравнимость чисел ka и kb по модулю km, т. е. $ka \equiv kb \pmod{km}$.

Утверждение 14

Для произвольных натуральных чисел k и m из выполнимости сравнения $ka \equiv kb \pmod{km}$ следует сравнимость чисел a и b по модулю m, т. е. $a \equiv b \pmod{m}$.

Утверждение 15

Если обе части сравнения $f(x) \equiv g(x) \pmod{m}$ и модуль умножим на одно и то же число $k > 0$, то получим сравнение $kf(x) \equiv kg(x) \pmod{km}$, эквивалентное первоначальному.

Утверждение 16

Если НОД$(a, m)=d$ и $d \nmid b$, то сравнение $ax \equiv b \pmod{m}$ не имеет решений.

Утверждение 17

Если НОД$(a, m) = 1$, то сравнение $ax \equiv b \pmod{m}$ имеет единственное решение.

Утверждение 18

Числа класса $\overline{a}$ по модулю m образуют следующие k классов по модулю km: $\overline{a}, \overline{a+m}, \overline{a+2m}, \ldots, \overline{a+(k-1)m}$.

Утверждение 19

Если НОД$(a, m) = d$ и $d \mid b$, то сравнение $ax \equiv b \pmod m$ имеет d решений. Все эти решения принадлежат одному классу по модулю m/d.

Утверждение 20

Если НОД$(a, m) = 1$ и x пробегает значения, образующие приведенную систему вычетов, то ax также принимает значения, образующие приведенную систему вычетов по модулю m.

1.5. Теоремы о числе решений степенных сравнений

Теорема 13

1. При $p \nmid a$ сравнение $x^n \equiv a \pmod p$ по простому модулю $p > 2$ либо совсем не имеет решений, либо число решений равно наибольшему общему делителю n и $p-1$.

2. Сравнение (1) не имеет решений, если для $\delta =$ НОД$(n, p-1)$ $\delta \nmid \operatorname{ind} a$, и имеет δ решений, если $\delta \mid \operatorname{ind} a$.

Определение

1. Число a называется вычетом n-й степени по простому модулю p, если $p \nmid a$ и сравнение $x^n \equiv a \pmod p$ имеет решения.

2. Число a называется невычетом n-й степени по простому модулю p, если сравнение $x^n \equiv a \pmod p$ не имеет решений.

Теорема 14

По простому модулю $p > 2$ число классов вычетов n-й степени равно $(p-1)/\delta$, где $\delta = (n, p-1)$.

Теорема 15

Если $\delta = (n, p-1)$, то вычеты n-й степени по простому модулю $p > 2$ совпадают с вычетами степени d по этому модулю.

Теорема 13*

При $p \nmid a$ и $n \mid p-1$ сравнение $x^n \equiv a \pmod p$ по простому модулю $p > 2$ либо совсем не имеет решений, либо имеет n решений. По такому модулю a является вычетом n-й степени тогда и только тогда, когда $n \mid \operatorname{ind} a$.

Теорема 14*

По простому модулю $p>2$ и $n|p-1$ число классов вычетов n-й степени равно $(p-1)/n$.

Теорема 16

При $n|p-1$ число a является вычетом n-й степени по простому модулю $p>2$ тогда и только тогда, когда $a^{(p-1)/n} \equiv 1 \pmod{p}$.

Теорема 17

При $p \nmid a$ и $n|p-1$ все решения сравнения $x^n \equiv a \pmod{p}$ по простому модулю $p>2$ можно получить, умножая одно решение этого сравнения на различные решения сравнения $x^n \equiv 1 \pmod{p}$.

Другими словами, все корни n-й степени из $\bar{a}$ по модулю p можно получить, умножая один из этих корней на различные корни n-й степени из $\bar{1}$. Важным частным случаем степенных сравнений являются сравнения второй степени. Из доказанных выше теорем вытекают следующие следствия, относящиеся к случаю $n=2$.

Следствие 3

Необходимым и достаточным условием того, чтобы число a было квадратичным вычетом по простому модулю $p>2$ ($p \nmid a$), является выполнимость сравнения

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Следствие 4

Если a является квадратичным вычетом по простому модулю $p>2$ ($p \nmid a$), то сравнение $x^2 \equiv a \pmod{p}$ имеет два решения.

Следствие 5

По любому простому модулю $p>2$ ($p \nmid a$) число классов квадратичных вычетов и число классов квадратичных невычетов равно $\frac{p-1}{2}$.

Для сравнений $x^2 \equiv a \pmod{p}$ имеет место следующее утверждение.

Теорема 18

Необходимым и достаточным условием того, чтобы число a было квадратичным невычетом по простому модулю $p>2$ ($p \nmid a$), является выполнимость сравнения

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

ГЛАВА 2

Алгоритмический минимум

2.1. Вычисление наибольшего общего делителя и его линейного представления

Для нахождения наибольшего общего делителя двух целых чисел без разложения их на множители используется *алгоритм Евклида*. Пусть **MOD**(a, b) есть операция взятия остатка от деления a на b, а **QUO**(a, b) есть частное от деления a на b. В данном алгоритме используется следующее утверждение: если $a = bq + r$, где $b \neq 0$, и число d делит a и b, то оно делит и r, т. е. имеем $d|(a - bq)$. Это утверждение верно для любого делителя, включая наибольший общий делитель $d = \text{НОД}(a, b)$. Отсюда следует, что

$$\text{НОД}(a, b) = \text{НОД}(b, \textbf{MOD}(a, b)).$$

Алгоритм Евклида описывается следующим образом:

ВХОД: a и $b \neq 0$.

1. [Инициализация] $(a_0, a_1) := (a, b)$.
2. [Основной цикл] Пока $a_1 \neq 0$, выполнять

   $(a_0, a_1) := [a_1, \textbf{MOD}(a_0, a_1)]$.
3. Вернуть $d := a_0$.

ВЫХОД: $d = \text{НОД}(a, b)$.

Расширенный алгоритм Евклида

Для чисел, взаимно простых с модулем, операция деления по модулю определена как операция умножения на число, являющееся обратным по отношению к делителю. Для нахождения обратного элемента используется *расширенный алгоритм Евклида*, который позволяет вычислить линейное представление наибольшего общего делителя чисел a и b через значения этих чисел: $\text{НОД}(a, b) = ax + by$, где коэффициент при a есть обратный элемент

$x = a^{-1} \bmod b$ и коэффициент при b есть обратный элемент $y = b^{-1} \bmod a$. Расширенный алгоритм Евклида может быть представлен в виде:

ВХОД: a и $b \neq 0$.

1. [Инициализация] $(a_0, a_1) := (a, b)$; $(x_0, x_1) := (1, 0)$; $(y_0, y_1) := (0, 1)$.
2. [Основной цикл] Пока $a_1 \neq 0$, выполнять:

$$\{q := \mathbf{QUO}(a_0, a_1);$$
$$(a_0, a_1) := (a_1, a_0 - a_1 q);$$
$$(x_0, x_1) := (x_1, x_0 - x_1 q);$$
$$(y_0, y_1) := (y_1, y_0 - y_1 q)\}.$$

3. Вернуть $(d, x, y) := (a_0, x_0, y_0)$.

ВЫХОД: d, x, y, такие что $d = \text{НОД}(a, b) = ax + by$.

2.2. Китайская теорема об остатках

Эта теорема является одним из весьма полезных и часто используемых в криптографии результатов теории чисел. Она фактически утверждает, что любое значение из множества минимальных положительных представителей $(\mathbf{Z}/N)$ классов вычетов по модулю $N = n_1 n_2 \ldots n_g$, где $\forall\, i, j \in \{1, 2, \ldots, g\}$ $\text{НОД}(n_i, n_j) = 1$, может быть представлено в виде набора остатков от деления этого значения на каждый из сомножителей n_i, т. е. имеется взаимно однозначное соответствие $R \leftrightarrow (r_1, r_2, \ldots, r_g)$, где $R \in \mathbf{Z}/N$, $r_1 \in \mathbf{Z}/n_1$, $r_2 \in \mathbf{Z}/n_2$, …, $r_g \in \mathbf{Z}/n_g$.

Китайская теорема об остатках гласит следующее.

Теорема

Пусть $n_1, n_2, \ldots, n_g$ — набор попарно взаимно простых чисел, $N = n_1 n_2 \ldots n_g$; числа $c_1, c_2, \ldots, c_g$ удовлетворяют условиям $c_1 N/n_1 \equiv 1 \bmod n_1$, $c_2 N/n_2 \equiv 1 \bmod n_2$, …, $c_g N/n_g \equiv 1 \bmod n_g$. Тогда решение системы

$$\begin{cases} x \equiv r_1 \bmod n_1, \\ x \equiv r_2 \bmod n_2, \\ \quad \ldots \ldots \\ x \equiv r_g \bmod n_g \end{cases}$$

имеет вид $R' \equiv r_1 c_1 N/n_1 + r_2 c_2 N/n_2 + \ldots + r_g c_g N/n_g \pmod N$.

Доказательство

Поскольку $\forall i, j \in \{1, 2, \ldots, g\}$ и $i \neq j$ $n_i \left| \frac{N}{n_i} \right.$ (например $n_1 \left| \frac{N}{n_2} \right.$, $n_3 \left| \frac{N}{n_2} \right.$, …, $n_g \left| \frac{N}{n_2} \right.$), то $R' \bmod n_i = (r_1 c_1 N/n_1 + r_2 c_2 N/n_2 + \ldots + r_g c_g N/n_g) \bmod n_i = (r_i c_i N/n_i) \bmod n_i$.

То есть $R' \equiv r_i c_i N/n_i \equiv r_i \pmod{n_i}$ для $i = 1, 2, \ldots, g$.

Минимальное положительное число R из класса вычетов по модулю N, представляющего собой решение системы сравнений, и является тем элементом кольца $\mathbf{Z}/N$, который ставится в соответствие набору значений $r_1, r_2, \ldots, r_g$. Подобрать необходимые значения $c_i N/n_i \equiv 1 \bmod n_i$ достаточно просто. Их можно вычислить по формуле $c_i = N/n_i [(n_i/N) \bmod n_i]$. Если дано некоторое $R \in \mathbf{Z}/N$, то, выполнив деление R на каждое из чисел n_i, определим однозначно набор остатков, который ставится в соответствие заданному числу R. Фактически китайская теорема об остатках указывает способ решения сравнений указанного типа.

2.3. Алгоритм быстрого возведения в степень по модулю

Пусть требуется вычислить значение $S = a^W \bmod n$. Представим степень W в виде разложения по степеням числа 2:

$$W = w_{g-1} 2^{g-1} + w_{g-2} 2^{g-2} + \ldots + w_2 2^2 + w_1 2^1 + w_0,$$

где w_i есть цифра 0 или 1.

Преобразуем $S = a^W \bmod n$ следующим образом:

$$S = a^W \bmod n = a^{w_{g-1} 2^{g-1} + w_{g-2} 2^{g-2} + \ldots + w_2 2^2 + w_1 2^1 + w_0} \bmod n =$$

$$= (a^2)^{w_{g-1} 2^{g-2} + w_{g-2} 2^{g-3} + \ldots + w_2 2^1 + w_1 2^0} \cdot a^{w_0} \bmod n =$$

$$= ((a^2)^2)^{w_{g-1} 2^{g-3} + w_{g-2} 2^{g-4} + \ldots + w_2 2^0} \cdot (a^2)^{w_1} \cdot a^{w_0} \bmod n =$$

$$= (\ldots((a^2)^2 \ldots)^2)^{w_{g-1}} \cdot \ldots \cdot (a^8)^{w_3} \cdot (a^4)^{w_2} \cdot (a^2)^{w_1} \cdot a^{w_0} \bmod n.$$

Из последней формулы нетрудно вывести следующий псевдокод, описывающий алгоритм быстрого возведения в степень:

ВХОД:

1. $S := 1$ и $c := a$ {Присвоить начальные значения переменным S и c}
2. For $i := 0$ to $g - 1$ do {Основной цикл}

   2.1. If $w_i = 1$, then $S := Sc \bmod n$. Otherwise go to step 2.2.

   2.2. $c := c^2 \bmod n$.

ВЫХОД: $S = a^W \bmod n$.

В более понятном и удобном для программирования виде алгоритм быстрого возведения в степень записывается следующим образом.

ВХОД: Целочисленные значения n, $a > 0$ и $W \geq 0$.

1. Инициализируем переменные $S := 1$, $V := W$ и $c := a$.
2. Если $V = 0$, то СТОП.
3. Если $V \bmod 2 = 1$ (т. е. текущее значение V является нечетным), то присваиваем новые значения переменным $S := Sc \bmod n$ и $V := (V - 1)/2$ и переходим к шагу 5. В противном случае переходим к шагу 4.
4. Выполняем операцию присваивания $V := V/2$.
5. Выполняем операцию присваивания $c := c^2 \bmod n$.
6. Переходим к шагу 2.

ВЫХОД: Значение $S = a^W \bmod n$.

Нетрудно подсчитать, что средняя сложность данного алгоритма составляет $1.5g$ операций умножения двух g-битовых чисел плюс $1.5g$ операций деления $2g$-битовых чисел на g-битовое число. Для 1000-битовых и более длинных чисел данный алгоритм выполняется на ЭВМ достаточно быстро.

Если модуль может быть разложен на сравнительно небольшие простые делители, т. е. $n = p_1 p_2 \ldots p_g$, то возведение в степень по такому модулю может быть сильно упрощено, если использовать китайскую теорему об остатках. Сначала вычисляются вычеты $a^W \bmod p_i$ по каждому из простых делителей p_i, $i = 1, 2, \ldots, g$. Используя теорему Ферма, эти вычисления можно сделать достаточно быстрыми.

В результате получим следующую систему сравнений:

$$\begin{cases} a^{W'} \equiv r_1 \bmod p_1, & 0 \le r_1 < p_1, \\ a^{W'} \equiv r_2 \bmod p_2, & 0 \le r_1 < p_2, \\ \qquad\qquad \ldots\ldots \\ a^{W'} \equiv r_g \bmod p_g, & 0 \le r_1 < p_g. \end{cases}$$

Полагая $x = a^{W'}$ и решая по китайской теореме об остатках систему сравнений, приведенную выше, найдем значение $R \in \mathbf{Z}/n$, удовлетворяющее системе. Поскольку $a^{W'}$ также удовлетворяет рассматриваемой системе сравнений и все ее решения сравнимы между собой по модулю n, то $R \equiv a^{W'} \bmod n$, т. е. $S = R$.

2.4. Нахождение первообразных корней

Показателями могут быть только делители функции Эйлера от модуля m, т. е. делители обобщенной функции Эйлера $L(m)$, которая является наибольшим возможным показателем по модулю m. Для модулей вида p^s и $2p^s$, где $s \ge 1$, имеем $L(m) = \varphi(m)$ и существуют первообразные корни. Если модуль является простым числом p, то количество чисел, относящихся к показателю γ, равно функции Эйлера от числа γ, т. е. $\psi(\gamma) = \varphi(\gamma)$. Чем меньше показатель, тем меньше существует чисел, относящихся к нему. Наибольшее число чисел относится к показателю $p-1$, т. е. имеется достаточно большое число первообразных корней и при случайном выборе чисел мы с большой вероятностью попадаем на них. Нахождение первообразного корня осуществляется путем случайного выбора числа α и проверкой выполнимости условия $\alpha^{\frac{p-1}{d_i}} \ne 1 \bmod p$ для всех простых делителей d_i числа $p-1$. Этот способ основан на следующем утверждении:

Пусть имеем разложение $p-1 = d_1^{s_1} d_2^{s_2} \ldots d_h^{s_h}$. *Если для каждого простого делителя* d_i *числа* $p-1$ *выполняется условие* $\alpha^{\frac{p-1}{d_i}} \ne 1 \bmod p$, *то число* α *является первообразным корнем (примитивным элементом) по модулю* p.

Доказательство

Допустим, что α не является первообразным корнем и относится к показателю $\delta < p-1$. Поскольку $\delta \mid p-1$, то $k = (p-1)/\delta$ есть простой или состав-

ной делитель числа $p-1$, т. е., по крайней мере, для одного из делителей d_i имеем $d_i \mid k$. Следовательно, число $\frac{p-1}{d_i\delta}$ является целым. По предположению имеем: $\alpha^{\delta} = 1 \bmod p \Rightarrow (\alpha^{\delta})^{\frac{p-1}{d_i\delta}} = 1 \bmod p \Rightarrow \alpha^{\frac{p-1}{d_i}} = 1 \bmod p$, что противоречит исходному условию.

2.5. Нахождение чисел, относящихся к заданному показателю

Случай простого показателя

Если длина простого делителя γ существенно меньше длины простого модуля, то нахождение чисел, относящихся к γ как к показателю, путем случайного выбора чисел a и проверки соотношения $a^{\gamma} = 1 \bmod p$ является вычислительно неэффективным (на самом деле практически невыполнимым). Для нахождения числа α, относящегося к простому показателю γ, используется следующий вычислительно эффективный способ.

1. Выбирается число b, превосходящее 1 и меньшее числа p.
2. Вычисляется значение $\gamma' = (p-1)/\gamma$ и число $z = b^{\gamma'} \bmod p$.
3. Если $z \neq 1$, то в качестве числа α взять число z. В противном случае повторить шаги 1–3.

Действительно, для полученного числа $z \neq 1$ имеем $z = b^{(p-1)/\gamma} \bmod p$. Следовательно, согласно теореме Ферма, имеем $z^{\gamma} \equiv b^{p-1} \equiv 1 \bmod p$, т. е. число z относится к показателю γ. Известно, что при выполнении условия $z^{\gamma} \equiv 1 \bmod p$ показатель числа z делит γ. Так как γ есть простое число, то оно и является показателем.

Случай составного показателя

Если требуется найти число α, относящееся к составному показателю γ, каноническое разложение которого имеет вид $\gamma = q_1^{\omega_1} q_2^{\omega_2} \ldots q_z^{\omega_z}$, то можно воспользоваться следуюшим алгоритмом:

1. Выбирается случайное число b, превосходящее 1 и меньшее числа p.
2. Вычисляется значение $\gamma' = (p-1)/\gamma$ и число $z = b^{\gamma'} \bmod p$.

3. Если $z = 1$, то перейти к шагу 1.
4. Если для каждого простого делителя q_i числа γ выполняется условие $z^{\frac{\gamma}{q_i}} \neq 1 \bmod p$, то в качестве числа α взять число z. В противном случае повторить шаги 1–4.

Докажем, что этот алгоритм действительно находит число, относящееся к показателю γ. Для полученного числа $\alpha \neq 1$ имеем $\alpha = b^{(p-1)/\gamma} \bmod p$. Согласно теореме Ферма, имеем $\alpha^{\gamma} \equiv b^{p-1} \equiv 1 \bmod p$. Допустим, что α относится к показателю $\delta < \gamma$. Тогда $\delta \mid \gamma$ и $k = \gamma/\delta$ есть простой или составной делитель числа γ, т. е., по крайней мере, для одного из делителей q_i имеем $q_i \mid k$. Следовательно, число $\frac{\gamma}{q_i \delta}$ является целым. По предположению имеем: $\alpha^{\delta} = 1 \bmod p \Rightarrow (\alpha^{\delta})^{\frac{\gamma}{q_i \delta}} \equiv 1 \bmod p \Rightarrow \alpha^{\frac{\gamma}{q_i}} \equiv 1 \bmod p$, что противоречит условию, проверяемому на шаге 4 алгоритма поиска числа α.

2.6. Генерация простых чисел

Для генерации больших простых чисел могут быть использованы следующие два подхода:

- формируются случайные числа заданного размера и проверяется, являются ли они простыми, с помощью вероятностных тестов (псевдопростые числа);
- по определенной процедуре генерируются простые числа, проверка которых осуществляется с помощью детерминистических тестов на простоту.

В первом случае тесты строятся на основе определенных теорем из теории чисел, сформулированных и доказанных для простых чисел. Если число не удовлетворяет тесту, то оно не является простым и отбрасывается. Для проверки берется следующее случайное число требуемого размера. Если число проходит тест, то некоторый переменный параметр, используемый для тестирования, изменяется и тест повторяется снова. Число, прошедшее большое число опытов определенного типа, считается псевдопростым, поскольку вероятность, что составное число может пройти все тесты, пренебрежимо мала. Для того чтобы исключить некоторые возможные классы составных чисел, которые могут проходить тесты конкретного типа, используют несколько различных тестов, по каждому из которых выполняется большое

число опытов. Достоинством генерации псевдопростых чисел является сравнительная простота процедуры. Недостатком первого подхода является то, что после генерации большого псевдопростого числа p может оказаться достаточно сложным определение разложения числа $p-1$, которое необходимо знать, например, в случае ЭЦП на основе сложности задачи дискретного логарифмирования с сокращенной длиной подписи. Разложение числа $p-1$ представляет интерес также и для отсеивания некоторых классов слабых простых чисел. Следующие два вероятностных теста могут быть применены совместно. Пусть мы хотим проверить, является ли число p простым.

- *Тест Ферма* заключается в проверке соотношения $b^{p-1} = 1 \pmod p$ для большого числа различных значений b. Число различных использованных при тестировании значений b, для которых выполняется указанное соотношение, определяет число выполненных опытов по тесту Ферма. Однако известен класс составных чисел, которые проходят тест Ферма (числа Кармайкла; например $1105 = 5 \cdot 13 \cdot 17$ и $41\,041 = 7 \cdot 11 \cdot 13 \cdot 41$).
- *Тест Соловея–Штрассена* заключается в проверке равенств $\left(\frac{b}{p}\right) = 1$, где $\left(\frac{b}{p}\right)$ — символ Лежандра для значений b, являющихся квадратичными вычетами по модулю p, и $\left(\frac{b}{p}\right) = -1$ для значений b, являющихся квадратичными невычетами по модулю p (квадратичным вычетом называется число, являющееся квадратом некоторого числа x по модулю p; т. е. для квадратичного вычета существует квадратный корень: $b = x^2 \bmod p$).

Второй тест хорошо отсеивает числа Кармайкла. Вероятность того, что составное число пройдет один опыт по тесту Соловея–Штрассена, не превышает значения 0.5. Это позволяет получить оценку числа опытов, которые следует выполнить в соответствии с данным тестом, чтобы получить необходимо низкую вероятность принятия составного числа в качестве псевдопростого. Первый тест используется в качестве предварительной отбраковки чисел. Второму тесту подвергают только числа, прошедшие первый. (Второй тест на самом деле поглощает первый, поскольку проверка условия $b^{\frac{p-1}{2}} \bmod p = 1$ для значений b, являющихся квадратичными вычетами, фактически означает проверку по тесту Ферма.)

2.7. Детерминистическая генерация больших простых чисел

Способ на основе подбора разложения функции Эйлера

Формируется набор k простых чисел $\{q_1, q_2, \ldots, q_k\}$ сравнительно малой длины (например, имеющих 8–10 десятичных знаков). Причем числа $q_1, q_2, \ldots, q_k$ проверяются детерминистическим тестом на простоту, в качестве которого можно взять проверку на делимость на все натуральные числа от 2 до $\lceil \sqrt{q_i} \rceil$ (метод пробного деления; $\lceil g \rceil$ обозначает наименьшее целое число, не меньшее, чем число g). Из указанного набора случайным образом выбираются h простых чисел $m_1, m_2, \ldots, m_h$, вычисляется число p_1, имеющее следующую структуру:

$$p_1 = 1 + 2\prod_{i=1}^{i=h} m_i.$$

Затем выбирается некоторое число b и проверяется, выполняются ли для данного p_1 следующие два условия:

1. $b^{p_1-1} = 1 \pmod{p}$ и
2. $b^{\frac{p_1-1}{m_i}} \neq 1 \bmod p$ для всех $m_i \in \{m_1, m_2, \ldots, m_h\}$.

Если после нескольких попыток найдется некоторое b, которое удовлетворяет указанным выше двум соотношениям, то p является простым числом. Если такое число не найдено, то выбирается другой случайный набор простых чисел $m_1, m_2, \ldots, m_h$ из набора $q_1, q_2, \ldots, q_k$. Сформированное таким образом число p_1 имеет длину примерно в h раз больше средней длины чисел $q_1, q_2, \ldots, q_k$ (например, от $8h$ до $10h$ десятичных знаков). Можно аналогичным образом сформировать следующий набор простых чисел $\{p_1, p_2, \ldots, p_k\}$ и, используя их в качестве исходных, повторить рассматриваемую процедуру, формируя еще более длинные простые числа. Достоинством данного способа является то, что мы заведомо знаем разложение $p - 1$; кроме того, мы можем формировать это разложение таким образом, чтобы в нем содержались простые числа требуемой длины. Основным недостатком такого способа является то, что формируется только некоторый подкласс простых чисел заданной большой длины. Однако мощность этого подкласса может быть задана такой, что этим обстоятельством атакующий не сможет воспользоваться для раскрытия той или иной двухключевой криптосистемы, в которой будет использоваться данная процедура детерминистической генерации простых чисел.

Данный детерминистический тест основан на следующей ***теореме.***

Пусть p — целое нечетное число, превышающее 1. Если существует $b \le p-1$, такое что выполняются следующие условия: 1) $b^{p-1} = 1 \bmod p$ и 2) $b^{\frac{p-1}{m_i}} \neq 1 \bmod p$ для каждого простого делителя m_i числа $p-1$, то число p является простым.

Доказательство

Допустим, что p не является простым. Тогда функция Эйлера от p имеет значение меньшее чем $p-1$, т. е. $\varphi(p) < p-1$. Рассмотрим два случая: а) НОД$(b, p) = 1$ и б) НОД$(b, p) \neq 1$. В случае а) порядок числа b должен делить $\varphi(p) < p-1$, но по условию теоремы порядок b равен $p-1$. В случае б) не существует целых степеней n, для которых выполняется условие $b^n = 1 \bmod p$. В обоих случаях приходим к противоречию, которое доказывает утверждение теоремы. (Пояснение к случаю б): если НОД$(b, p) = \delta \neq 1$, то $\delta | b^n \bmod p$ для любого n, поскольку для остатка r от деления b^n на p имеем НОД$(b^n, r) = \delta$).

Способ по стандарту ГОСТ Р 34.10–94

Для генерации больших простых чисел в ГОСТ Р 34.10–94 используется детерминистический тест, основанный на следующей ***теореме.***

Пусть $p = qN + 1$, где q — нечетное простое число, N — четное число и $p < (2q+1)^2$. Число p является простым, если выполняются следующие два условия:

1) $2^{qN} = 1 \bmod p$ и

2) $2^N \neq 1 \bmod p$.

Доказательство

Пусть γ есть порядок числа 2 по модулю p и p имеет следующее каноническое разложение: $p = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_h^{\alpha_h}$. Ввиду условия 1) γ делит $p-1$, т. е. $\gamma | p-1$. В силу условия 2) γ не является делителем числа $\frac{p-1}{q}$. Отсюда следует, что $q | \gamma$. Согласно теореме Эйлера $2^{\varphi(p)} = 1 \bmod p$, следовательно, $\gamma | \varphi(p) \Rightarrow q | \varphi(p)$, где $\varphi(p) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_h^{\alpha_h - 1} (p_1 - 1)(p_2 - 1) \ldots (p_h - 1)$. Пусть q совпадает с простым множителем p_i. Из такого допущения следует, что $p = qn'$ для некоторого натурального числа n. Однако по условию теоремы

имеем $p = qN + 1$. Поскольку $q > 1$ не может делить число 1, то приходим к противоречию, из которого следует, что q должно делить число $p_i - 1$, по крайней мере, для некоторого одного из значений $i \in \{1, 2, \ldots, h\}$.

Таким образом, существует некоторое натуральное $n \geq 2$, такое что имеем $p_i - 1 = qn$ и $p_i = qn + 1$. Следовательно, при некотором натуральном m получим:

$$p = mp_i = m(qn + 1) = qN + 1 \Rightarrow m = q(N - mn) + 1.$$

При некотором натуральном $s \geq 0$ имеем $m = qs + 1$ и

$$p = (qn + 1)(qs + 1).$$

Пусть p есть составное число, тогда $s \geq 2$ (поскольку N и n — четные числа, а $s = N - mn$), из чего следует $p \geq (2q + 1)^2$. Это противоречит условию теоремы, следовательно, $s = 0$ и число p является простым.

Схема построения алгоритма описывается следующим образом. Пусть требуется сформировать простое число p длины $t \geq 17$ бит. С этой целью строится убывающий набор натуральных чисел $t_0, t_1, \ldots, t_s$, где $t_0 = t$ и $t_s < 17$ бит, для которых выполняется условие $t_i = [t_{i-1}/2]$. Последовательно вырабатываются простые числа $p_s, p_{s-1}, \ldots, p_0$, причем длина числа p_i равна значению t_i для всех $i = 1, \ldots, s$. Исходное простое значение p_s формируется путем случайного выбора числа размером менее 17 бит и проверки на простоту методом пробного деления.

Генерация простого числа p_{i-1} по простому числу p_i осуществляется с использованием формулы

$$p_{i-1} = p_i N + 1,$$

где N — случайное четное число, такое что длина числа $p_i N + 1$ равна значению t_i. Число p_{i-1} считается полученным, если одновременно выполнены следующие два условия:

1) $2^{p_i N} = 1 \bmod p_{i-1}$;

2) $2^N \neq 1 \bmod p_{i-1}$.

Если хотя бы одно из условий не выполнено, то значение N увеличивается на 2, вычисляется новое значение p_{i-1}, которое снова проверяется на простоту по указанным двум условиям. Такая процедура выполняется до тех пор, пока не будет получено простое число p_{i-1}.

2.8. Извлечение квадратных корней по модулю

Извлечение квадратного корня по модулю используется как базовый примитив в ряде криптосистем. При составном модуле эта операция выполняется следующим путем: 1) разложение модуля n на простые множители: $n = p_1^{\omega_1} p_2^{\omega_2} \ldots p_z^{\omega_z}$, 2) извлечение корня из заданного числа по каждому из простых модулей $p_1, p_2, \ldots, p_z$, и 3) последующее восстановление корня по составному модулю с помощью китайской теоремы об остатках. Вычисление корней по простому модулю сводится к одной или нескольким операциям возведения в степень по модулю. Сложность процедуры извлечения корня зависит от конкретного значения простого модуля. Наиболее простым является случай, когда модуль сравним с числом 3 по модулю 4: $p \equiv 3 \bmod 4$. Следующими по возрастанию сложности являются случаи $p \equiv 5 \bmod 8$ и $p \equiv 1 \bmod 8$ (случаи $p \equiv 3 \bmod 8$ и $p \equiv 7 \bmod 8$ относятся к случаю $p \equiv 3 \bmod 4$). При $p \equiv 1 \bmod 8$ используется общий алгоритм вычисления корней, который реализует операцию извлечения квадратного корня по произвольному простому модулю. Рассмотрим процедуру извлечения корней для указанных трех случаев.

Случай $p \equiv 3 \bmod 4$

Пусть a является квадратичным вычетом и требуется найти число x, такое что $x^2 \equiv a \bmod p$, где простое p удовлетворяет условию $p \equiv 3 \bmod 4$. Для квадратичных вычетов имеет место сравнение $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Умножая обе части этого сравнения на a, получаем: $a^{\frac{p+1}{2}} \equiv a \bmod p$. Поскольку $p \equiv 3 \bmod 4$, степень $\frac{p+1}{4}$ есть целое число, поэтому мы можем определить: $x = a^{\frac{p+1}{4}} \bmod p$. Возведением значения x в квадрат легко показать, что оно есть квадратный корень из числа a по модулю p. Таким образом, для рассматриваемого случая извлечение корня второй степени сводится к операции возведения в степень $\frac{p+1}{4}$ по модулю p:

$$\sqrt{a} \equiv a^{\frac{p+1}{4}} \bmod p.$$

Случай $p \equiv 5 \bmod 8$

Пусть a является квадратичным вычетом и требуется найти число x, такое что $x^2 \equiv a \bmod p$, где простое p удовлетворяет условию $p \equiv 5 \bmod 8$ (рис.1). Для квадратичных вычетов имеет место сравнение $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Поскольку $p \equiv 5 \bmod 8$, то при некотором натуральном k имеем: $p-1 = (8k+5)-1 = 4(2k+1)$. Поэтому $a^{\frac{p-1}{2}} = a^{2(2k+1)} \equiv 1 \bmod p$. Из последнего сравнения следует, что либо $a^{\frac{p-1}{4}} = a^{2k+1} \equiv 1 \bmod p$ (1), либо $a^{\frac{p-1}{4}} = a^{2k+1} \equiv -1 \bmod p$ (2). Если имеет место первый случай, то, умножая обе части сравнения (1) на a, имеем: $a^{\frac{p+3}{4}} = a^{2\frac{p+3}{8}} = (a^{\frac{p+3}{8}})^2 \equiv a \bmod p$, где $\frac{p+3}{8}$ есть целое число, откуда следует формула для вычисления квадратного корня

$$\sqrt{a} \equiv a^{\frac{p+3}{8}} \bmod p.$$

Если имеет место второй случай, то, умножая обе части сравнения (2) на -1, имеем: $a^{\frac{p-1}{4}} \cdot (-1) \equiv 1 \bmod p$. Теперь представим $-1 \bmod p$ как $b^{4k+2} \bmod p$, где b есть произвольный квадратичный невычет по модулю p. (Действительно, для невычета b имеем: $b^{\frac{p-1}{2}} = b^{\frac{8k+4}{2}} = b^{4k+2} \equiv -1 \bmod p$.) Таким образом, мы получили $a^{\frac{p-1}{4}} b^{4k+2} \equiv 1 \bmod p$ (3), где $\frac{p-1}{4} = 2k+1$ есть нечетное число. Умножая обе части сравнения (3) на a, получаем $a^{\frac{p+3}{4}} b^{4k+2} = a^{\frac{p+3}{4}} b^{\frac{p-1}{2}} \equiv a \bmod p$, где показатели степеней чисел a и b являются четными, поэтому мы можем определить $x = a^{\frac{p+3}{8}} b^{\frac{p-1}{4}} \bmod p$ (где показатели степеней чисел a и b являются натуральными числами).

Возведением значения x в квадрат легко показать, что оно есть квадратный корень из числа a по модулю p: $x^2 = a^{\frac{p+3}{4}} b^{\frac{p-1}{2}} \equiv a \bmod p$.

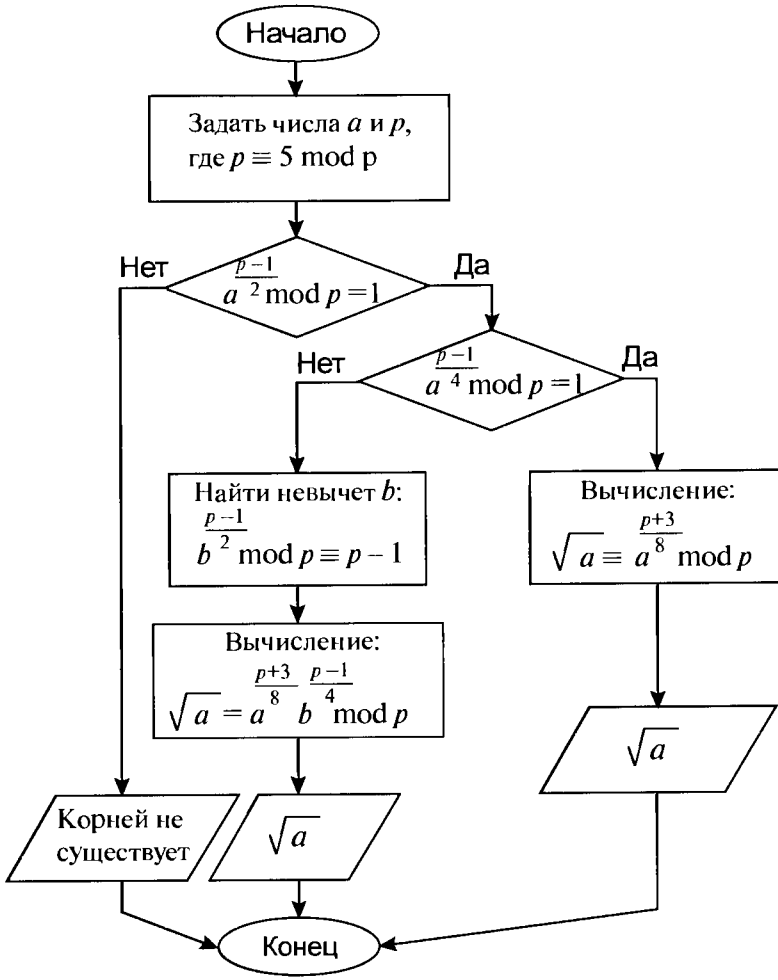

Рис. 1. Схема алгоритма вычисления квадратного корня по простому модулю p (случай $p \equiv 5 \bmod 8$)

Таким образом, для случая $a^{\frac{p-1}{4}} \equiv -1 \bmod p$ для вычисления квадратного корня может быть использована следующая формула:

$$\sqrt{a} = a^{\frac{p+3}{8}} b^{\frac{p-1}{4}} \bmod p .$$

При использовании этой формулы предварительно следует найти квадратичный невычет b, что осуществляется случайным выбором числа $b \le p-1$, за которым следует проверка выполнимости условия $b^{\frac{p-1}{2}} \bmod p = p-1$. Поскольку вероятность того, что случайное число является невычетом, равна 50%, то нахождение квадратичного невычета требует в среднем выполнения двух попыток.

Случай произвольного простого модуля

Пусть a является квадратичным вычетом и требуется найти число x, такое что $x^2 \equiv a \bmod p$, где p — произвольное простое число. В этом общем случае задача решается с использованием определенного расширения приемов, примененных в случае $p \equiv 5 \bmod 8$. Для произвольного p можно записать:

$$p-1 = 2^t r,$$

где $t \ge 1$ и r — нечетное число. Пусть для вычета a и любого невычета b справедливо сравнение

$$a^S b^Z \equiv 1 \bmod p, \qquad (4)$$

где S — нечетное число, а Z — четное число или ноль. Тогда, умножая обе части последнего сравнения на a, получаем $a^{S+1} b^Z \equiv a \bmod p$, следовательно, можно определить значение $x = a^{(S+1)/2} b^{Z/2} \bmod p$, которое является квадратным корнем из a (это доказывается простым возведением значения x в квадрат). Для того чтобы найти представление единицы в виде (4), воспользуемся сравнением $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, представив его в виде $a^{\frac{p-1}{2}} b^Z \equiv 1 \bmod p$, т. е. в виде, аналогичном (4), где в общем случае $S = (p-1)/2$ является четным и $Z = 0$. Рассмотрим сравнение (4) с начальными значениями $S = (p-1)/2$ и $Z = 0$, в котором осуществим ряд последовательных шагов одновременного деления обоих показателей степеней чисел a и b на два (на одном шаге выполняем две операции присваивания $S \leftarrow S/2$ и $Z \leftarrow Z/2$), пока не получим нечетное S. При этом перед некоторыми шагами деления к значению Z будем прибавлять число $(p-1)/2$, что соответствует умножению левой части (4) на $b^{\frac{p-1}{2}} \equiv -1 \bmod p$. Выполнение операции $Z \leftarrow Z + (p-1)/2$ будем осуществлять, если перед выполнением шага деления или при достижении условия прекращения цикла деления имеет место $a^S b^Z \equiv -1 \bmod p$. Заметим, что если

при исходных значениях $S = (p-1)/2$ и $Z = 0$ значение S является нечетным, то мы сразу имеем условие прекращения процесса деления показателей степеней на два, поэтому выполняется ноль шагов деления. В противном случае после первого шага деления имеем либо $a^S b^Z \equiv 1 \bmod p$, либо $a^S b^Z \equiv -1 \bmod$. Во втором случае мы дополнительно выполняем операцию $Z \leftarrow Z + (p-1)/2$ перед выполнением следующего шага деления или перед вычислением корня $\sqrt{a} = a^{\frac{S+1}{2}} b^{\frac{Z}{2}} \bmod p$ (если уже достигнуто нечетное значение S). Заметим, что на первом шаге деления осуществляется деление на два нулевого значения Z и только потом выполняется операция $Z \leftarrow Z + (p-1)/2$, поэтому если имеется ненулевое значение Z, то в его разложение двойка входит с показателем степени, превышающим показатель степени числа 2 в разложении S (после одного и того же шага деления показателей степени чисел S и Z). Следовательно, в момент достижения нечетного значения S число Z является четным.

Описанная выше процедура извлечения квадратных корней по простому модулю поясняется блок-схемой, приведенной на рис. 2.

Извлечение корней по составному модулю

Если составной модуль n представляется в виде произведения первых степеней простых чисел: $m = p_1, p_2, \ldots, p_s$, то нахождение квадратных корней сводится к нахождению квадратных корней по модулю, равному каждому из множителей $p_1, p_2, \ldots, p_s$. Легко видеть, что число $a \neq 0$, являющееся квадратичным вычетом по составному модулю, является квадратичным вычетом по всем модулям $p_1, p_2, \ldots, p_s$: $x^2 \equiv a \bmod m \Rightarrow x^2 \equiv a \bmod p_1$, $x^2 \equiv a \bmod p_2$, ..., $x^2 \equiv a \bmod p_s$. Каждое из последних s сравнений имеет два решения: x_1 и $p_1 - x_1$; x_2 и $p_2 - x_2$; ..., x_s и $p_s - x_s$ соответственно. Выбирая из каждой из этих пар по одному корню, можно составить 2^s различных систем сравнений вида

$$\begin{cases} x \equiv x_1' \bmod p_1, & x_1' \in \{x_1, p - x_1\}, \\ x \equiv x_2' \bmod p_2, & x_2' \in \{x_2, p - x_2\}, \\ \qquad\qquad \ldots\ldots \\ x \equiv x_s' \bmod p_s, & x_s' \in \{x_s, p - x_s\}. \end{cases}$$

Каждую из этих систем можно решить, используя китайскую теорему об остатках, в результате чего будет вычислено $2^{\backprime}$ различных корней $\sqrt{a} \bmod m$, значения которых не превышают m.

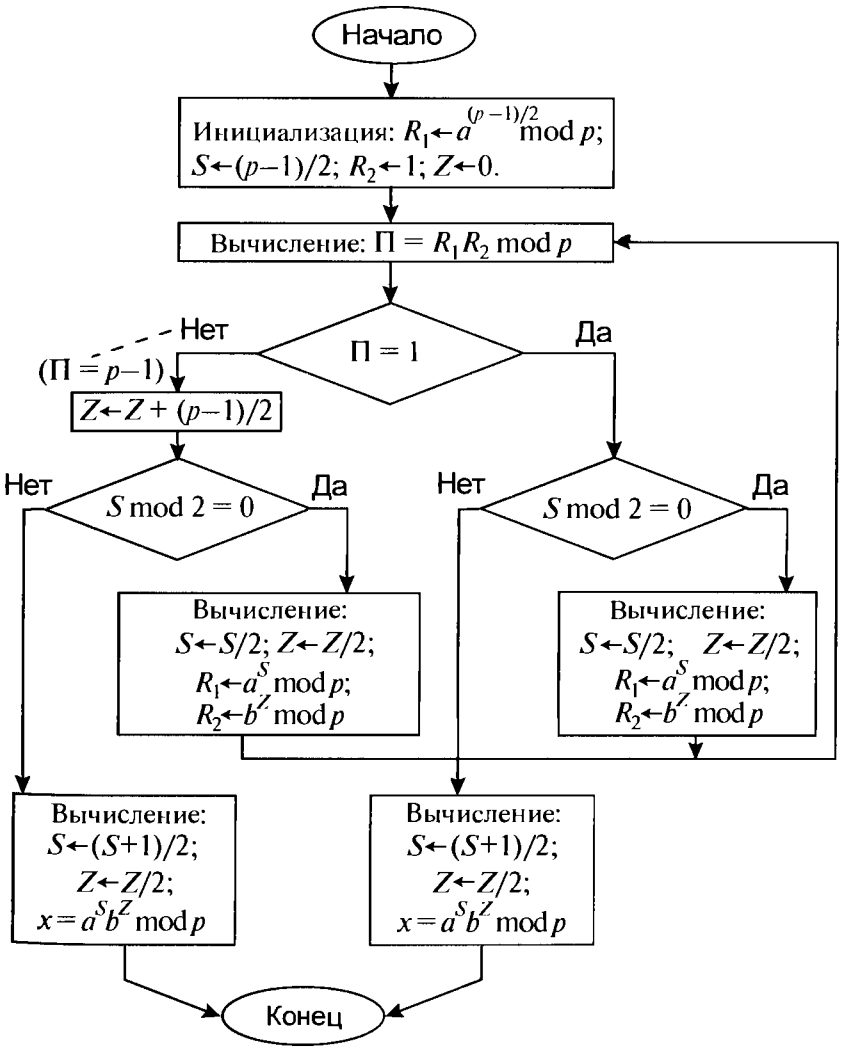

Рис. 2. Схема алгоритма вычисления квадратного корня из вычета a по простому модулю p (общий случай)

2.9. Извлечение корней степени $n > 2$ по простому модулю

Пусть число a является вычетом n-й степени по простому модулю p. Если НОД$(n, p-1) = 1$, то имеется единственный корень, где $z = r^{-1} \bmod p$. Если НОД$(n, p-1) = \delta$, то сравнение $x^n \equiv a \bmod p$ имеет δ решений. Если известно одно решение, например, x_0, то остальные решения сравнения $x^n \equiv a \bmod p$ (1) можно найти следующим путем:

1. Вычислить значения $a' = a^w \bmod p$, где $w = \delta / n \bmod p$, и перейти к рассмотрению сравнения $x^\delta \equiv a' \bmod p$ (2), которое равносильно (1). В частности, если x_0 есть решение (1), то x_0 является также и решением (2). (Решение x_0 удобнее искать как решение сравнения (2), поскольку $\delta \le n$.)
2. Поскольку $\delta \mid p-1$, то легко можно найти некоторое число g, относящееся к δ по модулю p как к показателю. Числа в множестве $\{g, g^2, ..., g^\delta\}$ являются попарно несравнимыми по модулю p и составляют δ решений сравнения $x^\delta \equiv 1 \bmod p$. Действительно, для всех $1 \le i \le \delta$ имеем $\left(g^i\right)^\delta \equiv \left(g^\delta\right)^i \equiv 1 \bmod p$.
3. Все решения сравнения (2) находим, умножая по модулю p решение x_0 на каждое из значений $g, g^2 \bmod p, ..., g^\delta \bmod p$. Действительно, для всех $1 \le i \le \delta$ имеем $\left(x_0 g^i\right)^\delta \equiv {x_0}^\delta \equiv a' \bmod p$. В силу равносильности сравнений (1) и (2) в качестве решения первого сравнения имеем следующие δ классов: $\overline{x_0 g}, \overline{x_0 g^2}, ..., \overline{x_0 g^\delta}$.

Таким образом, вопрос нахождения всех корней сводится к нахождению одного корня. Рассмотрим, как можно найти один корень третьей степени в случае $3 \mid p-1$. Пусть дано некоторое число $a \le p-1$. Выполним следующие шаги:

1. Проверяем условие $a^{\frac{p-1}{3}} \equiv 1 \bmod p$. Если это условие не выполняется, то корней не существует, т. е. число a является кубическим невычетом по модулю p.

2. Находим число $g \neq 1$, относящееся по модулю p к показателю 3. Для этого числа имеем: $g^2 \bmod p \neq 1$, $g^3 \bmod p = 1$.

3. Находим невычеты (b и c) третьей степени по модулю p, удовлетворяющие условиям $b^{\frac{p-1}{3}} \equiv g \bmod p$ и $c^{\frac{p-1}{3}} \equiv g^2 \bmod p$ (вычеты не могут удовлетворять ни одному из этих условий, а любой невычет удовлетворяет одному из этих условий). Нахождение указанных невычетов следует осуществить путем случайного выбора чисел и проверки выполнимости заданных условий.

4. Выполняем Алгоритм 1, представленный на рис. 3. В результате получим значение $x = \sqrt[3]{a} \bmod p$. Алгоритм 1 включает как составные части Алгоритмы 2 и 3, представленные в виде блок-схем на рис. 4 и рис. 5.

Работа Алгоритма 1 основана на поиске тройки чисел (s, t, u), таких что выполняется условие $a^s b^t c^u \equiv 1 \bmod p$ и при этом число s не делится на 3, а t и u делятся на 3. Если такая тройка чисел найдена, то мы имеем: либо $s \equiv 2 \bmod 3$, либо $s \equiv 1 \bmod 3$.

В первом случае мы можем вычислить число

$$x = a^{\frac{s+1}{3}} b^{\frac{t}{3}} c^{\frac{u}{3}} \bmod p,$$

которое и есть искомый корень третьей степени из числа a по модулю p. Действительно, возводя x в третью степень, получаем: $x^3 \equiv a^{s+1} b^t c^u \equiv a \bmod p$.

Во втором случае значение $s + 2$ делится на 3 и мы можем вычислить число

$$x' = a^{\frac{s+2}{3}} b^{\frac{t}{3}} c^{\frac{u}{3}} \bmod p,$$

которое представляет собой кубический корень из квадрата числа a:

$$x'^3 = a^{s+2} b^t c^u \bmod p \equiv a^2 \bmod p.$$

Воспользовавшись уже известным нам алгоритмом извлечения квадратного корня по простому модулю, мы можем вычислить число

$$x = \sqrt[2]{x'} \bmod p = \sqrt[2]{a^{\frac{s+2}{3}} b^{\frac{t}{3}} c^{\frac{u}{3}}} \bmod p,$$

которое представляет собой кубический корень из a или из $-a$. Покажем, что x' есть квадратичный вычет, а, значит, приведенная выше формула корректна.

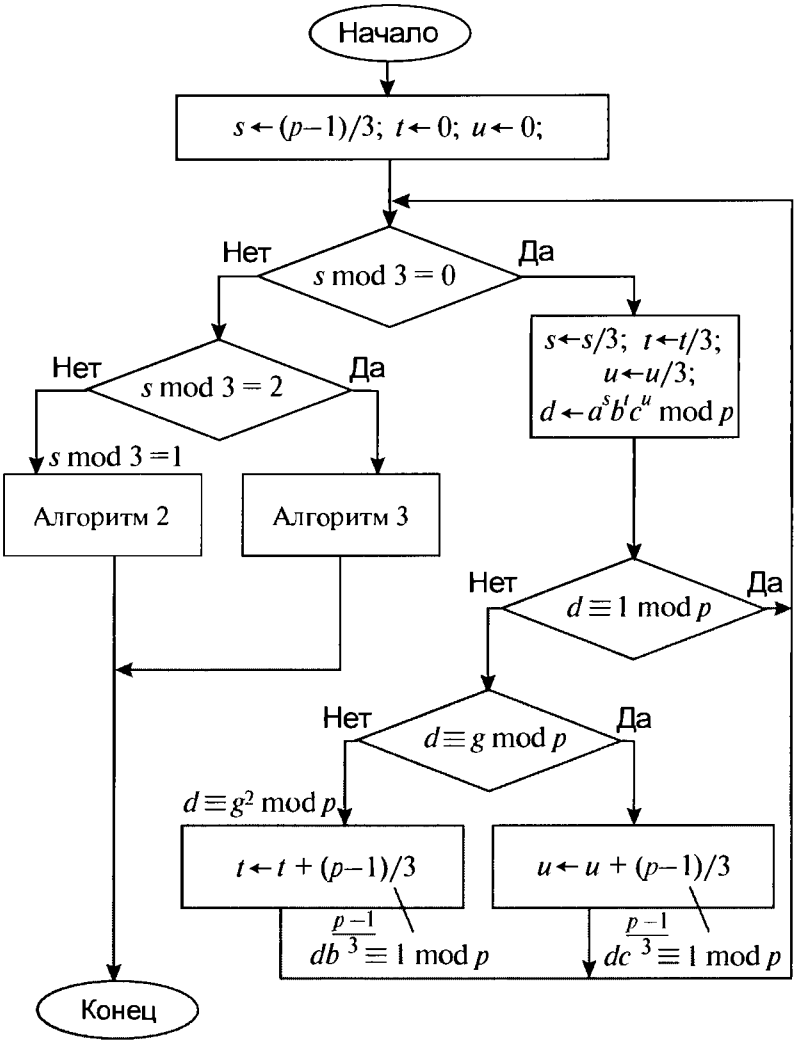

Рис. 3. Схема алгоритма вычисления кубического корня из вычета a по простому модулю p (общий случай)

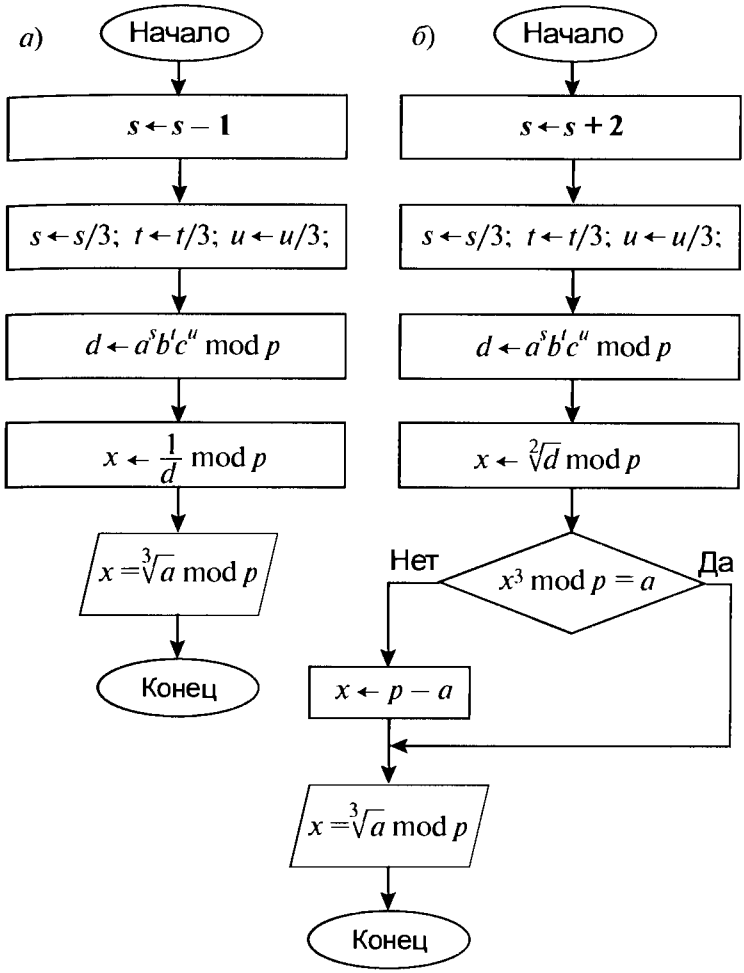

Рис. 4. Две версии Алгоритма 2: *а* — с вычислением обратных значений и *б* — с извлечением квадратного корня по модулю p

Очевидно, что значение x'^3 является квадратичным вычетом по модулю p, т.е. для него имеем $\left(x'^3\right)^{\frac{p-1}{2}} \equiv 1 \bmod p \Rightarrow (x'^{\frac{p-1}{2}})^3 \equiv 1 \bmod p$. Если предположить, что x' есть квадратичный невычет, то $x'^{\frac{p-1}{2}} \equiv -1 \bmod p \Rightarrow$

$\Rightarrow (x'^{\frac{p-1}{2}})^3 \equiv -1 \bmod p$. Полученное противоречие доказывает наше предположение. Очевидно, что $x^3 \equiv \sqrt[2]{a^{s+2}b^t c^u} \equiv \sqrt[2]{a^2} \equiv \pm a \bmod p$, поэтому вычисленное значение x следует возвести в третью степень. Если $x^3 \equiv a \bmod p$, то корень кубический найден. Если $x^3 \equiv -a \bmod p$, то корень кубический равен $\sqrt[3]{a} = p - x$.

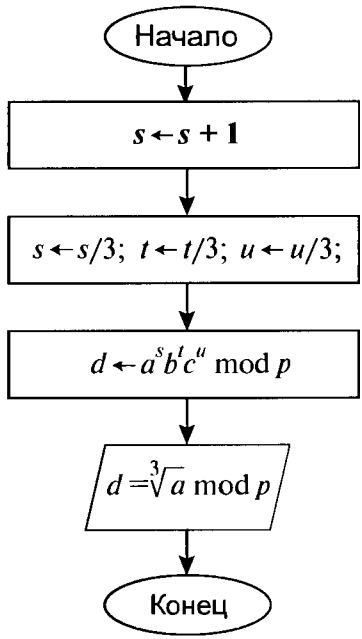

Рис. 5. Блок-схема Алгоритма 3

Для случая $s \equiv 1 \bmod 3$ может быть применен более эффективный альтернативный алгоритм вычисления искомого корня. Он основан на том, что значение $s-1$ делится на 3 и мы можем вычислить число

$$x' = a^{\frac{s-1}{3}} b^{\frac{t}{3}} c^{\frac{u}{3}} \bmod p,$$

которое представляет собой кубический корень из числа $a^{-1} \bmod p$:

$$x'^3 = a^{s-1} b^t c^u \bmod p \equiv a^{-1} \bmod p.$$

Искомый корень равен

$$\sqrt[3]{a} = x = x'^{-1} \bmod p = a^{\frac{1-s}{3}} b^{\frac{-t}{3}} c^{\frac{-u}{3}} \bmod p.$$

Действительно, имеем: $x^3 \equiv a^{1-s} b^{-t} c^{-u} \equiv \left(a^{s-1} b^t c^u\right)^{-1} \equiv a \bmod p$.

Работу Алгоритма 1 можно пояснить следующим образом. При инициализации устанавливаются значения $s = \frac{p-1}{3}$, $t = 0$ и $u = 0$, поэтому переменная $d = a^s b^t c^u \bmod p$ вначале имеет значение 1. Если s делится на три, то мы можем получить значение корня из d: $d \leftarrow \sqrt[3]{d} = \sqrt[3]{a^s b^t c^u} = a^{\frac{s}{3}} b^{\frac{t}{3}} c^{\frac{u}{3}} \bmod p$, которое может оказаться равным (в зависимости от случайно выбранных нами значений невычетов b и c): либо 1, либо g, либо $g^2 \bmod p \neq 1$. Рассмотрим эти три случая.

- Случай $d \equiv 1 \bmod p$. Снова выполняется проверка делимости s на число 3. Если $3 \mid s$, то еще раз извлекаем корень кубический из $d \equiv 1 \bmod p$ (это осуществляется тремя операциями присвоения $s \leftarrow s/3$, $t \leftarrow t/3$ и $u \leftarrow u/3$).
- Случай $d = g$. Осуществляется «виртуальное» умножение текущего значение d на $g^2 \bmod p = c^{\frac{p-1}{3}} \bmod p$ (это соответствует выполнению операции присвоения $u \leftarrow u + \frac{p-1}{3}$), а затем проверяется условие $3 \mid s$; если 3 не делит s, то осуществляется переход к выполнению Алгоритма 2 или Алгоритма 3.
- Случай $d = g^2 \bmod p \neq 1$. Осуществляется «виртуальное» умножение (по модулю p) текущего значение d на g (это соответствует выполнению операции присвоения $t \leftarrow t + \frac{p-1}{3}$), а затем проверяется условие $3 \mid s$; если 3 не делит s, то осуществляется переход к выполнению Алгоритма 2 или Алгоритма 3.

Нетрудно заметить, что в момент, когда будет получено значение s, которое не делится на 3, значения t и u будут кратными числу 3. Поэтому операции $t \leftarrow t/3$ и $u \leftarrow u/3$ в Алгоритмах 2 и 3 сохраняют целочисленные значения переменных t и u.

Алгоритм 1 даст на выходе одно значение кубического корня. Остальные два следует найти путем умножения полученного корня $\sqrt[3]{a} \bmod p$ на g и $g^2 \bmod p$. Какое из трех значений корня будет получено на выходе Алгоритма 1, зависит от выбора конкретных значений невычетов b и c.

Аналогичным образом для случая $5 \mid p-1$ можно составить алгоритм для вычисления корня 5-й степени по простому модулю, при этом в нем потребуется использовать алгоритмы извлечения корней 2-й и 3-й степеней. Затем перейти к составлению алгоритма для вычисления корня 7-й степени, в котором будет использован алгоритм вычисления корней 5-й степени и т. д. В общем случае для вычисления корня простой степени $q \mid p-1$ потребуется использование алгоритмов вычисления корней всех простых степеней, меньших степени q. Если степень корня составная, то достаточно использовать только алгоритмы вычисления корней степеней, не превышающих значение максимального простого множителя заданной составной степени.

2.10. Факторизация *B*-гладкого модуля RSA

Простое число p называется B-гладким, если все делители числа $p-1$ не превосходят некоторое сравнительно малое число B. Пусть имеем $d_i \le B$ $\forall d_i \mid p-1$, где d_i — простой делитель $p-1$. Модуль $n = pq$ в криптосистеме RSA называется B-гладким, если хотя бы один из его делителей является B-гладким. Рассмотрим B-гладкий модуль RSA, в котором для определенности B-гладкий множитель обозначим буквой p. Составим произведение

$$D = \prod_{r_i \le B} r_i^{s_i},$$

включающее в качестве множителей значения $r_i^{s_i}$, представляющие собой некоторые степени всех простых чисел r_i, не превосходящих B, причем показатели степени этих множителей таковы, что $r_i^{s_i} \ge n'$. Значение натурального числа n' следует выбрать из условия $n' \ge p$. Поскольку для достижения максимальной сложности задачи факторизации модуля RSA числа p и q выбираются такими, чтобы они имели примерно одинаковую длину и задавали большую разность $p-q$, то можно принять $n' \ge 2^{\frac{5 \cdot |n|}{9}}$, где $|n|$ — битовая длина числа n. Если учитывать произвольный выбор длин чисел p и q, то можно положить $n' = n$.

Поскольку число p является B-гладким, то все простые множители $d_i^{s_i'}$, входящие в $p-1$, и включены в произведение D. В силу условия $r_i^{s_i} \geq n' \geq p$ имеем также $s_i \geq s_i'$, поэтому $p-1 \mid D$. Учитывая малую теорему Ферма, записываем:

$$2^D = \left(2^{p-1}\right)^{\frac{D}{p-1}} \equiv 1 \bmod p \Rightarrow p \mid 2^D - 1.$$

Рассмотрим значение $Z = 2^D \bmod n$. Имеем:

$$Z \equiv 2^D \bmod n \Rightarrow Z \equiv 2^D \equiv 1 \bmod p \Rightarrow p \mid Z - 1.$$

Таким образом, число $2^D \bmod n - 1$ делится на p, поэтому нетривиальный делитель RSA-модуля может быть найден путем вычисления с помощью расширенного алгоритма Евклида наибольшего общего делителя чисел $2^D \bmod n - 1$ и n:

$$\text{НОД}(2^D \bmod n - 1, n) = p.$$

Обозначим произведение D как D_B, чтобы явно показать его зависимость от выбора значения B. Если нам надо разложить конкретный RSA-модуль, то мы не знаем заранее минимального значения B. Поэтому целесообразно начать разложение с малого значения B, постепенно увеличивая его, если $\text{НОД}(2^{D_B} \bmod n - 1, n) = 1$. При этом следует сохранять промежуточные значения $Z_B = 2^{D_B} \bmod n$, поскольку последующие значения $Z_{B'}$ получаются путем возведения Z_B в некоторую степень по модулю n.

2.11. Метод дискретного логарифмирования

Оптимизация переборного метода

Рассмотрим метод дискретного логарифмирования, впервые предложенный Д. Шенксом и известный под названием «шаг ребенка — шаг гиганта» (baby-step giant-step algorithm). Пусть нам требуется найти значение x $(0 \leq x < \gamma)$, удовлетворяющее условию $y = a^x \bmod p$, где значения y, α и p заданы, причем порядок числа α равен γ (т. е. α по модулю p относится к показателю γ). Вычислим $d = \left\lceil \sqrt{\gamma} \right\rceil$ (т. е. d является наименьшим из всех целых чи-

сел, превосходящих или равных значению $\sqrt{\gamma}$) и представим искомое значение x в виде $x = Qd + r$, где Q и r — целые числа, причем $0 \le r < d$ и $0 \le Q < d$. С учетом этого представления имеем:

$$y \equiv \alpha^x \equiv \alpha^{Qd+r} \equiv \alpha^{Qd}\alpha^r \bmod p;$$

$$y\left(\alpha^{-d}\right)^Q \equiv \alpha^r \bmod p.$$

Если найти пару значений $0 \le r < d$ и $0 \le Q < d$, удовлетворяющих последней формуле, то значение x вычисляется по формуле $x = Qd + r$. Непосредственный перебор требует выполнения не более γ испытаний различных пар значений (Q, r). Этот способ требует использования памяти малого объема, однако при $|\gamma| = 80$ бит и более прямой перебор в настоящее время практически неосуществим. Вычислительную сложность нахождения требуемой пары чисел (Q, r) можно существенно уменьшить, если выполнить определенные предвычисления и построить таблицу значений $\alpha^i \bmod p$ для $i = 0, 1, 2, \ldots, d-1$ (можно построить и использовать также и таблицу значений $y\left(\alpha^{-d}\right)^j \bmod p$, однако при изменении значения y эту таблицу надо будет вычислять повторно). Таблица $(i, \alpha^i \bmod p)$, отсортированная по значениям $\alpha^i \bmod p$, существенно упрощает задачу нахождения дискретных логарифмов для различных значений y. При наличии этой таблицы для значений $j = 0, 1, 2, \ldots, d-1$ требуется последовательно выполнить вычисление значения $y\left(\alpha^{-d}\right)^j \bmod p$ и проверку наличия полученного значения в таблице $(i, \alpha^i \bmod p)$. Для некоторого $j = j_0$ обязательно будет найдено значение $\alpha^{i_0} \bmod p$, такое что $\alpha^{i_0} \bmod p = y\left(\alpha^{-d}\right)^j \bmod p$, откуда получаем

$$x = j_0 d + i_0.$$

Таким образом, при наличии предварительно вычисленной таблицы $(i, \alpha^i \bmod p)$, содержащей d значений длиной $|p|$ (для ее хранения требуется память размером $d \cdot |p|$ бит), вычисление одного логарифма потребует выполнения не более d умножений по модулю p (поскольку $y\left(\alpha^{-d}\right)^{j+1} \bmod p = y\left(\alpha^{-d}\right)^j \alpha^{-d} \bmod p$, т. е. последующее значение получаем, умножая предыдущее на α^{-d}) и $d \log_2 d$ операций сравнения. Сложность

вычисления таблицы составляет d умножений по модулю p и $d \log_2 d$ операций сравнения (при выполнении сортировки по значениям $\alpha^l \bmod p$). В целом сложность метода «шаг ребенка — шаг гиганта» можно оценить используемой памятью $\sim\sqrt{\gamma}$ и временем $\sim\sqrt{\gamma}$.

Заметим, что размер модуля, по которому требуется выполнить логарифмирование, сам по себе не является определяющим в задании сложности дискретного логарифмирования. Наиболее существенным фактором является порядок числа α, задающего основание дискретного логарифма. При $|\gamma| = 80$ бит и менее вычисление дискретных логарифмов вполне реализуемо на практике для модулей размером 10^3 бит и более.

Метод вычисления индексов

Рассмотрим еще один метод вычисления значения x $(0 \le x < \gamma)$, удовлетворяющего условию $y = a^x \bmod p$. Используя идеи, лежащие в его основе, разработаны наиболее эффективные алгоритмы дискретного логарифмирования. В нем используется возможность построения подмножества простых чисел $(p_1, \ldots, p_s)$, таких что $\forall i \in \{1, \ldots, s\}$ имеем $p_i \le B$, где B — сравнительно небольшое число, и достаточно большая доля чисел из множества $\{1, 2, \ldots, \gamma\}$ может быть представлена в виде произведения некоторых степеней чисел $p_1, \ldots, p_s$, составляющих некоторую базу разложения (называемую B-гладкой). В дальнейшем будем полагать, что в качестве базы разложения выбраны все простые числа, не превосходящие B, а α есть первообразный корень по модулю p (т. е. будем рассматривать случай $\gamma = p - 1$). Метод может быть представлен в виде следующих трех шагов.

1-й шаг. Случайным образом выбираются различные значения k_j, для каждого из которых вычисляется значение $K_j = \alpha^{k_j} \bmod p$ и находится каноническое разложение числа K_j. Если в разложении K_j присутствуют простые множители, не входящие в базу разложения, то выбирается другое значение k_j. В противном случае формируется соотношение вида $K_j = \alpha^{k_j} \bmod p = \prod_{i=1}^{s} p_i^{z_{ji}}$, где $z_{ji} \ge 0$. Логарифмируя последнее равенство, получаем сравнение

$$\log_\alpha K_j = k_j \equiv \sum_{i=1}^{s} z_{ji} \log_\alpha p_i \bmod p - 1.$$

Действуя указанным способом, построим $t = s + \varepsilon$ (где число ε является сравнительно малым по сравнению с числом s) сравнений указанного типа и объединим их в следующую систему сравнений:

$$\begin{cases} k_1 \equiv \sum_{i=1}^{s} z_{1i} \log_\alpha p_i \bmod p-1, \\ k_2 \equiv \sum_{i=1}^{s} z_{2i} \log_\alpha p_i \bmod p-1, \\ \quad \cdots\cdots\cdots\cdots \\ k_t \equiv \sum_{i=1}^{s} z_{ti} \log_\alpha p_i \bmod p-1. \end{cases}$$

В этой системе имеется $s = t - \varepsilon$ неизвестных: $\log_\alpha p_1, \log_\alpha p_2, \ldots, \log_\alpha p_s$, которые являются индексами простых чисел, входящих в базу разложения.

2-й шаг. Используя методы линейной алгебры, решается приведенная выше система сравнений, в результате чего определяются значения индексов всех чисел, составляющих базу разложения, т. е. становятся известными значения

$$\log_\alpha p_1, \log_\alpha p_2, \ldots, \log_\alpha p_s.$$

Второй шаг является наиболее трудоемкой процедурой, поскольку в базах разложения, которые могут быть использованы, обычно присутствует большое число простых чисел, что задает большое число неизвестных в решаемой системе. После завершения второго шага сравнительно легко может быть вычислен индекс (дискретный логарифм) для произвольных значений y (при основании α; если последнее значение изменится, то потребуется повторить первый и второй шаги). Используется система, число сравнений в которой превышает число неизвестных, поскольку некоторые сравнения могут оказаться зависимыми (тогда при $t = s$ число решений было бы равно или больше $p-1$, т. е. было бы практически бесконечным для длин модуля, которые используются в системах ЭЦП).

3-й шаг соответствует процедурам непосредственного вычисления $x = \log_\alpha y \pmod p$. Выбирается случайное значение r, и вычисляется число $Y = y \cdot \alpha^r \bmod p$. Затем число Y разлагается на простые множители: $Y = \prod_{i=1}^{s} p_i^{z_i^{(y)}}$. Если значение Y не разлагается по нашей базе разложения, то вы-

бирается другое случайное число r. Если в разложении Y присутствуют только простые множители, входящие в базу разложения, то мы имеем:

$$y \cdot \alpha^r \bmod p = \prod_{i=1}^{s} p_i^{z_i^{(y)}} \Rightarrow r + \log_\alpha y \equiv \sum_{i=1}^{s} z_i^{(y)} \log_\alpha p_i \bmod p - 1.$$

В последнем сравнении неизвестной величиной является только $\log_\alpha y$, которая теперь легко вычисляется по формуле:

$$\log_\alpha y \equiv \left(\sum_{i=1}^{s} z_i^{(y)} \log_\alpha p_i \right) - r \bmod p - 1$$

или

$$\log_\alpha y = \left(-r + \sum_{i=1}^{s} z_i^{(y)} \log_\alpha p_i \right) \bmod p - 1.$$

Заметим, что если основание логарифма не является первообразным корнем, то задача дискретного логарифмирования будет относиться к некоторой подгруппе H_β, порядок которой равен показателю $\gamma < p - 1$, к которому относится основание логарифма по модулю p. Обычно в схемах ЭЦП с сокращенной длиной подписи используется простой показатель γ, длина которого в несколько раз (4–6 раз) меньше длины модуля числа p, поэтому приведенный выше метод вычисления индексов не может быть непосредственно применен для определения неизвестной величины x в уравнении $y = \beta^x \bmod p$, где y — элемент подгруппы H_β и β — число, относящееся по модулю p к показателю γ. Это связано с тем, что числа, входящие в подгруппу H_β, составляют очень малую долю из множества положительных целых чисел, не превышающих $p - 1$, и вероятность того, что простые числа некоторой выбираемой базы разложения будут входить в H_β, является пренебрежимо малой. Дискретное логарифмирование методом вычисления индексов может быть выполнено следующим путем.

Используя указанный метод, находим значение индекса u числа β при основании α, являющемся первообразным корнем, т. е. имеем $\beta = \alpha^u \bmod p$. Теперь исходное уравнение преобразуется в сравнение вида:

$$y \equiv \beta^x \equiv \alpha^{ux} \equiv \alpha^{x'} \bmod p.$$

С помощью метода вычисления индексов находим значение $x' \equiv ux \bmod p - 1$ (*), по которому можно легко вычислить x. Воспользуемся результатом задачи № 47 (*см. главу 6*): если β ($\beta \bmod p \neq 1$) относится по простому модулю p к простому показателю γ, то индекс u числа β (по модулю

p) удовлетворяет условию НОД$(u, p-1) = \frac{p-1}{\gamma} = d$. Таким образом, имеем целые числа $u' = \frac{u}{d}$ и $x'' = \frac{x'}{d}$, связанные сравнением $x'' \equiv u'x \bmod \gamma$ (**), которое вытекает из (*) путем деления модуля и обеих частей сравнения (*) на d. Из (**) получаем формулу для вычисления значения x:

$$x = \frac{x''}{u'} \bmod \gamma.$$

Для значений длины модуля $|p| \geq 1024$ и длины порядка подгруппы H_β $|\gamma| \leq 80$ метод логарифмирования «шаг ребенка — шаг гиганта» является более эффективным.

При оптимизации выбора значения ε описанный в этом разделе метод имеет трудоемкость, которая оценивается величиной

$$W \sim e^{c\sqrt{\log p (\log\log p)}},$$

где c — небольшая положительная константа. Дальнейшее развитие этого подхода позволило разработать методы дискретного логарифмирования, трудоемкость которых оценивается формулой

$$W \sim \exp\left(c'\sqrt[3]{\log p (\log\log p)^2}\right) = \exp\left(c'\sqrt[3]{|p| \log^2 |p|}\right),$$

которая в настоящее время и служит ориентиром при выборе длины модуля в криптосистемах, основанных на сложности задачи дискретного логарифмирования. Заметим, что лучшие методы разложения RSA-модуля n имеют трудоемкость, оцениваемую по аналогичной формуле:

$$W \sim \exp\left(c''\sqrt[3]{\log n (\log\log n)^2}\right) = \exp\left(c''\sqrt[3]{|n| \log^2 |n|}\right).$$

ГЛАВА 3

Краткий обзор классических криптосистем с открытым ключом

3.1. Открытое распределение ключей

Система Диффи–Хеллмана

В данной криптосистеме каждый абонент выбирает случайный секретный ключ x и вырабатывает открытый ключ y в соответствии с формулой

$$y = \alpha^x \pmod p.$$

Все абоненты размещают свои открытые ключи в общедоступном справочнике, который должен быть заверен специально созданным доверительным центром, чтобы исключить возможные нападения путем подмены открытых ключей или навязывания ложных открытых ключей. Если два абонента A и B хотят установить секретную связь, то они поступают следующим образом. Абонент A берет из справочника открытый ключ абонента B и, используя свой секретный ключ, вычисляет общий секретный ключ:

$$Z_{AB} = (y_B)^{x_A} = (\alpha^{x_B})^{x_A} = \alpha^{x_B x_A} \pmod p,$$

где y_A и y_B — открытые ключи абонентов A и B; x_A и x_B — соответствующие секретные ключи. Общий секретный ключ Z_{AB} нет необходимости передавать по сети связи, поскольку абонент B по известному из справочника открытому ключу абонента A аналогичным способом вычисляет значение

$$Z_{AB} = (y_A)^{x_B} = (\alpha^{x_A})^{x_B} = \alpha^{x_B x_A} \pmod p.$$

Предполагается, что оппоненту (потенциальному нарушителю) могут быть известны значения $y_B = \alpha^{x_B} \pmod p$ и $y_A = \alpha^{x_A} \pmod p$, передаваемые по открытому каналу, но, для того чтобы вычислить Z_{AB}, он должен решить трудную задачу дискретного логарифмирования. Общий секрет Z_{AB} может использоваться абонентами для шифрования сеансовых секретных ключей, а

последние — для шифрования сообщений с использованием симметричных методов шифрования.

Распределение ключей в системе RSA

В криптосистеме RSA сеансовые ключи шифруются по открытому ключу получателя и распределяются по открытому каналу. Процедура зашифрования выражается формулой:

$$C = K^{d} \bmod n.$$

Получатель расшифровывает сеансовый ключ с использованием своего секретного ключа:

$$K = C^{e} \bmod n.$$

Однако получатель должен получить гарантии того, что расшифрованный ключ был действительно отправлен подлинным отправителем. Аутентификация источника сообщения требует использования открытого ключа отправителя, поэтому отправитель должен подписать посланную криптограмму по своему секретному ключу d': $S = H^{d'} \bmod n'$, где H — хэш-функция от криптограммы C. Затем присоединить подпись S к отправляемому значению C. Если модуль отправителя n' больше модуля получателя, то он может отправить только значение $S = C^{d'} \bmod n'$, поскольку получатель, проверяя «подлинность» подписи в этом случае, может восстановить значение C, а затем по своему секретному ключу расшифровать C и получить значение ключа. Однако в последнем случае подлинность отправителя будет установлена окончательно только после того, как отправитель правильно зашифрует или расшифрует некоторое случайное пробное сообщение. Отправитель может подписать и хэш-функцию, полученную от значения ключа. (Подпись, полученная непосредственно по значению ключа, фактически раскрывает ключ, поэтому в открытом виде пересылаться по каналам связи не должна.)

3.2. Открытое шифрование

Способ Эль-Гамаля

Способ открытого шифрования Эль-Гамаля включает в себя составной частью систему открытого распределения ключей Диффи–Хеллмана. Каждый пользователь секретной сети выбирает секретный ключ x, вычисляет свой открытый ключ $y = \alpha^{x} \bmod p$ и помещает y в заверенный справочник. Шифро-

вание сообщения T, отправляемого пользователю i, осуществляется с помощью следующего алгоритма:

- выбрать случайное число R, которое по своей сути является разовым открытым ключом;
- вычислить $C' = \alpha^R \bmod p$ — разовый открытый ключ отправителя;
- используя открытый ключ i-го пользователя, вычислить $C'' = y^R T \bmod p$;
- отправить блок шифртекста (C', C'') пользователю i.

Расшифрование осуществляется пользователем i по следующему алгоритму:

- вычислить значение $(C')^x \equiv (\alpha^R)^x \equiv \alpha^{Rx} \bmod p$, которое по своей сути является разовым общим секретом (Z_{AB}) получателя и отправителя;
- вычислить значение $Z^{-1} = (\alpha^{Rx})^{-1} \bmod p$;
- расшифровать криптограмму C'': $T = C''Z^{-1} \bmod p$.

Способ Рабина

В схеме открытого шифрования Рабина используется RSA-модуль $n = pq$, в котором числа p и q сравнимы с числом 3 по модулю 4: $p \equiv 3 \bmod 4$ и $q \equiv 3 \bmod 4$, что обеспечивает при знании разложения модуля (числа p и q являются секретным ключом) возможность выполнения операции извлечения квадратного корня из квадратичных вычетов по модулю n.

Открытым ключом является значение n, с помощью которого сообщение $M < n$ зашифровывается путем возведения числа M в квадрат по модулю n:

$$C = M^2 \bmod n.$$

Процедура расшифрования состоит в извлечении квадратного корня из криптограммы C (очевидно, что она является квадратичным вычетом) по модулю n. Предварительно вычисляют корни из C по модулям p и q:

$$m_{p_1} = C^{\frac{p+1}{4}} \bmod p, \quad m_{p_2} = p - m_{p_1} = p - C^{\frac{p+1}{4}} \bmod p;$$

$$m_{q_1} = C^{\frac{q+1}{4}} \bmod q, \quad m_{q_2} = q - m_{q_1} = q - C^{\frac{q+1}{4}} \bmod q.$$

Из этих четырех значений вычисляются четыре возможных корня из C по модулю n:

$$M_1 = \left(m_{p_1} a + m_{q_1} b \right) \bmod n,$$

$$M_2 = \left(m_{p_1} a + m_{q_2} b \right) \bmod n,$$

$$M_3 = \left(m_{p_2} a + m_{q_1} b \right) \bmod n,$$

$$M_4 = \left(m_{p_2} a + m_{q_2} b \right) \bmod n,$$

где $a = q(q^{-1} \bmod p)$ и $b = p(p^{-1} \bmod q)$. Расшифрование неоднозначно. Для задания однозначности перед зашифрованием к исходному открытому сообщению можно присоединить некоторую заранее оговоренную метку.

3.3. Системы электронной цифровой подписи

Схема Эль-Гамаля

Пусть для абонента А имеем секретный ключ x_A и открытый ключ $y_A = \alpha^{x_A} \bmod p$. Подписью абонента A под документом M, где $M < p$, служит пара чисел (R, S), где $0 \le R < p - 1$ и $0 \le S < p - 1$, которая удовлетворяет уравнению

$$\alpha^M \equiv y_A{}^R R^S \bmod p.$$

Это *уравнение проверки подлинности подписи абонента* А. Данная система ЭЦП основана на том, что только действительный владелец секретного ключа x_A может выработать пару чисел (R, S), удовлетворяющую уравнению проверки подписи, по следующему алгоритму:

1. Сгенерировать случайное число k, удовлетворяющее условию: $0 < k < p - 1$ и НОД$(k, p - 1) = 1$.
2. Вычислить $R = \alpha^k \bmod p$.
3. Вычислить S из уравнения $M \equiv x_A R + kS \bmod (p - 1)$.

Из теории чисел известно, что последнее уравнение имеет решение для s, если НОД$(k, p - 1) = 1$. Это уравнение легко получить путем подстановки в уравнение проверки подписи значения $R = \alpha^k \bmod p$:

$$\alpha^M \equiv \alpha^{x_A R} \alpha^{kS} \equiv y_A{}^R R^S \bmod p.$$

Следует отметить, что для данного сообщения может быть выработано большое число различных подписей, соответствующих различным k. Однако выработать правильную подпись может только владелец секретного ключа.

Особенностью данной ЭЦП является то, что не допускается использовать одно и то же значение k для формирования подписи для двух разных сообщений, поскольку это делает возможным вычисление секретного ключа. Использованные значения k должны храниться в секрете. Обычно после выработки подписи они уничтожаются.

Схема Эль-Гамаля с сокращенной длиной параметра S

Уравнение проверки подписи

$$\alpha^M \equiv y_A^R R^S \bmod p$$

может выполняться также в случае, когда в качестве α берется число, относящееся к простому показателю q, где $q \mid p-1$. Для этого S должно быть вычислено из следующего соотношения

$$M \equiv x_A R + kS \bmod q.$$

Можно выбрать простой модуль p таким, чтобы разложение $p-1$ содержало простой множитель q, размер которого существенно меньше размера p. Например, для 2048-битового модуля p длина q может составлять 160 бит. В этом случае вычисляемое значение S будет иметь размер, не превышающий 160 бит. Благодаря этому достигается сокращение длины подписи почти в два раза (длина параметра R остается равной размеру модуля).

Схема Эль-Гамаля с сокращенной длиной параметров S и R

Соотношение проверки подписи

$$\alpha^M \equiv y_A^R R^S \bmod p$$

в схеме с сокращенным параметром S ($S<q$) может быть преобразовано в уравнение следующего вида

$$R = \alpha^{M/S} y_A^{-R/S} \bmod p.$$

При этом вместо R в степени при y_A можно использовать значение некоторой хэш-функции от значения R, т. е. $H(R)$. В этом случае уравнение проверки подписи имеет вид $R = \alpha^{M/S} y_A^{-H(R)/S} \bmod p$. Чтобы проверка была корректной, владелец секретного ключа должен вычислить параметр S из следующего сравнения

$$M \equiv x_A H(R) + kS \bmod q.$$

Поскольку при проверке подписи не требуется выполнять никаких вычислений с использованием параметра R, то проверка подписи может быть осуществлена в соответствии с уравнением

$$H(r) = H(\alpha^{M/s} y_A^{-H(R)/S} \bmod p).$$

В этом случае нет необходимости представлять проверяющему значение R, имеющее сравнительно большую длину. Достаточно для проверки представить значение $H(R)$, где размер значения хэш-функции равен, например, 160 бит. Этим достигается существенное сокращение длины подписи. Если используется вариант с сокращенной длиной параметра S, то общая длина подписи составляет порядка 320 бит вместо исходной длины 2048 бит или 4096 бит при 1024-битовом или 2048-битовом модуле p соответственно. Сокращение длины подписи не уменьшает стойкость системы ЭЦП, поскольку сложность задачи дискретного логарифмирования не изменяется, так как вычисления ведутся по модулю исходного размера.

В качестве хэш-функции $H(R)$ можно взять следующую: $H(R) = R \bmod q$, где q — показатель, используемый при сокращении параметра S. Тогда приходим к следующему уравнению проверки подписи:

$$R' = (\alpha^{M/S} y_A^{-R'/S} \bmod p) \bmod q,$$

где (R', S) есть подпись к сообщению M, а параметр R' вычисляется после выбора случайного числа k в соответствии с формулой $R' = (\alpha^k \bmod p) \bmod q$. Сравнение, используемое для вычисления параметра S, имеет вид:

$$M = x_A R' + kS \bmod q.$$

Американский стандарт DSA

Американский стандарт DSA (Digital Signature Algorithm) относится к схемам ЭЦП, основанным на сложности задачи дискретного логарифмирования, с сокращенной длиной подписи. В этом стандарте используются следующие параметры: p — простое число, длина которого выбирается в пределах $512 \le p \le 1024$; α — число, относящееся к показателю q по модулю p; q — простой делитель числа $p - 1$, имеющий значение от $2^{159} \le q \le 2^{160}$; т. е. $|q| = 160$ бит.

Секретный ключ представляет собой число x, $1 < x < q$.

Вычисление подписи к сообщению M включает следующие шаги.

1. Генерируется случайное число k, $1 < k < q$.
2. Вычисляется значение $R = (\alpha^k \bmod p) \bmod q$, являющееся первой частью подписи.
3. Вычисляется вторая часть подписи в соответствии со следующей формулой:

$$S = \frac{H + xR}{k} \bmod q,$$

где H — значение хэш-функции от подписываемого документа (сообщения).

Значение $S = 0$ не допускается стандартом. В этом случае выполняется повторное формирование подписи при новых значениях k до тех пор, пока не будет получено $S \neq 0$.

Проверка подлинности подписи осуществляется следующим образом.

1. Проверяется выполнение условий $R < q$ и $S < q$. Если они выполнены, то переходят к шагу 2, в противном случае подпись признается недействительной.
2. Вычисляется значение $R' = (\alpha^{H/S} y^{R/S} \bmod p) \bmod q$.
3. Сравниваются значения R и R'. Если $R = R'$, то подпись признается действительной.

Российский стандарт ГОСТ Р 34.10–94

Российский стандарт ГОСТ Р 34.10–94 похож на схему DSA. В нем специфицированы следующие параметры: p — простое число, причем $510 \le |p| \le 512$ либо $1022 \le |p| \le 1024$; q — простой делитель числа $p - 1$. $2^{255} \le q \le 2^{256}$ либо $2^{511} \le q \le 2^{512}$ соответственно; α — число, относящееся к показателю q по модулю p.

В стандарте ГОСТ Р 34.10–94 специфицирована процедура генерации простых чисел p и q.

Процедура вычисления подписи:

1. Генерируется случайное число k, $1 < k < q$.
2. Вычисляется значение $R = (\alpha^k \bmod p) \bmod q$, являющееся первой частью подписи.
3. В соответствии со стандартом ГОСТ Р 34.10–94 вычисляется хэш-функция H от подписываемого сообщения.

4. Вычисляется вторая часть подписи в соответствии со следующей формулой:

$$S = kH + xR \bmod q.$$

Если $S = 0$, процедура генерации подписи повторяется.

Проверка подлинности подписи:

1. Проверяется выполнение условий $R < q$ и $S < q$. Если они не выполняются, то выдается сообщение «Подпись недействительна».
2. В соответствии с алгоритмом ГОСТ Р 34.11–94 вычисляется значение хэш-функции H от сообщения.
3. Вычисляется значение $R' = (\alpha^{SH} y^{-RH} \bmod p) \bmod q$.
4. Сравниваются значения R и R'. Если $R = R'$, то подпись признается действительной.

Схема Онга–Шнорра–Шамира

Данная схема основана на использовании составного модуля n, что обеспечивает сложность извлечения квадратных корней по модулю n. Открытый ключ состоит из двух частей: RSA-модуля n и числа h, которое генерируется следующим образом. Генерируется секретный ключ в виде случайного числа k, взаимно простого с модулем n. Затем по секретному ключу вычисляется h:

$$h = -(k^{-1})^2 \bmod n = -k^{-2} \bmod n.$$

Для вычисления подписи (S_1, S_2) к сообщению M выбирается случайное число r, такое что r и n являются взаимно простыми. Затем используются соотношения:

$$S_1 = \frac{1}{2}\left[\frac{M}{r} + r\right] \bmod n,$$

$$S_2 = \frac{k}{2}\left[\frac{M}{r} - r\right] \bmod n.$$

Уравнение проверки подписи имеет вид

$$M = (S_1^2 + hS_2^2) \bmod n.$$

Следует отметить, что для нахождения секретного ключа и формирования подписи нет необходимости знать разложение модуля на множители, однако оба множителя должны быть большого размера. Также следует заметить, что

данная схема подписи не обладает необходимой криптографической стойкостью.

ЭЦП Шнорра

Схема Шнорра относится к случаю ЭЦП с сокращенной длиной и аналогична рассмотренным выше схемам, основанным на сложности задачи дискретного логарифмирования. В качестве параметра α используется число, относящееся по модулю p к простому показателю γ сравнительно малого размера (160–256 бит). Проверочное уравнение имеет вид $R = \alpha^S y^E \bmod p$.

Вычисление подписи к сообщению M включает следующие шаги:

1. Генерируется случайное число k, $1 < k < \gamma$.
2. Вычисляется значение $R = \alpha^k \bmod p$.
3. К сообщению M присоединяется число R и вычисляется хэш-функция H от значения $M\|R$: $E = H(M\|R)$.
4. Вычисляется значение S:

$$S \equiv k - xE \bmod q,$$

где x — секретный ключ.

Подписью является пара чисел (E, S).

Процедура проверки подлинности подписи осуществляется следующим образом:

1. Вычисляется значение R': $R' = \alpha^S y^E \bmod p$, где y — открытый ключ.
2. К сообщению M присоединяется число R' и вычисляется значение хэш-функции $E' = H(M\|R')$.
3. Выполняется сравнение значений E и E'. Если $E = E'$, то подпись считается подлинной.

Достоинством схемы подписи Шнорра является защищенность от атак на основе предварительно найденных коллизий, поскольку перед хэшированием подписываемого сообщения к нему присоединяется случайное значение R (поэтому заранее подготовленные коллизии становятся практически бесполезными для нарушителя). Кроме того, она позволяет реализовать протокол слепой подписи (СП), тогда как другие схемы ЭЦП, основанные на сложности задачи дискретного логарифмирования, требуют существенного модифицирования для реализации СП.

3.4. Слепая подпись

Слепая подпись на основе ЭЦП Шнорра

Протокол слепой подписи на основе ЭЦП Шнорра реализуется следующим образом. Пусть некий пользователь желает получить подпись к сообщению M таким образом, чтобы подписывающий 1) не мог ознакомиться с сообщением в ходе формирования подписи и 2) не мог впоследствии при получении M и соответствующей подписи идентифицировать пользователя, инициировавшего протокол СП для данного конкретного сообщения. Протокол СП осуществляется следующим образом:

1. Пользователь инициирует взаимодействие с подписывающим.
2. Подписывающий отправляет пользователю значение $R = \alpha^k \bmod p$.
3. Пользователь вычисляет значения $R' = R\alpha^{-\varepsilon}y^{-\tau} \bmod p$ (τ и ε — случайные числа, не превосходящие γ), $E' = H(M\|R')$ и $E = E' + \tau \bmod \gamma$, после чего отправляет подписывающему значение E.
4. Подписывающий вычисляет значение S, такое что $R = \alpha^S y^E \bmod p$, и направляет S пользователю.
5. Пользователь вычисляет подпись (E', S'), где $E' = E - \tau \bmod \gamma$ и $S' = S - \varepsilon \bmod \gamma$, которая является подлинной по отношению к сообщению M.

Подлинность подписи доказывается следующим образом. Из $R = \alpha^S y^E \bmod p$ следует $R\alpha^{-\varepsilon}y^{-\tau} = \alpha^{S-\varepsilon}y^{E-\tau} \bmod p$ и $R' = \alpha^{S'}y^{E'} \bmod p$. При этом проблема анонимности решается, поскольку любая тройка (R, S, E) из множества таких троек, которые формировались подписывающим, может быть сопоставлена с подписью (E', S') к данному документу M. Действительно, имеем: $\{R = \alpha^S y^E \bmod p$ и $R' = \alpha^{S'}y^{E'} \bmod p\} \Rightarrow \{R'/R \equiv \alpha^{S'-S}y^{E'-E} \equiv \alpha^{-\varepsilon}y^{-\tau} \bmod p\}$, т. е. при равновероятном случайном выборе «ослепляющих» слагаемых τ и ε подпись (E', S') с равной вероятностью была порождена из любой тройки, входящей в множество троек, сформированных подписывающим. Отметим также, что подписывающий не имеет даже возможности доказать, что на момент формирования подписи данного документа M он не был ознакомлен с ним.

«Слепая» подпись Чаума

Слепая подпись Чаума основана на криптосистеме RSA. Пусть пользователь A желает подписать некоторое сообщение M у пользователя B таким образом, чтобы последний не мог прочесть подписываемое сообщение. Для этого необходимо осуществить следующие шаги:

Пользователь A генерирует случайное простое число k, такое что НОД$(k, n) = 1$, где n — часть открытого ключа пользователя B. Затем пользователь A вычисляет значение $M' = k^e M \bmod n$ и предъявляет его пользователю B, чтобы последний подписал M' в соответствии со стандартной процедурой подписывания в системе RSA. Подписывающий не может прочесть сообщение M, поскольку оно преобразовано путем наложения на него «разового» ключа k^e с использованием операции модульного умножения.

Пользователь B подписывает сообщение M': $S' = (k^e M)^d \bmod n = kM^d \bmod n$. Заметим, что по значению подписи S' к сообщению M' подписывающий не имеет возможности вычислить $M^d \bmod n$. Заметим также, что по значению $M^d \bmod n$ легко вычислить M: $(M^d)^e \bmod n = M$. Это означает, что после получения значения $S = M^d \bmod n$ пользователь A должен держать его в секрете от подписавшего.

После получения от пользователя B значения S', используя расширенный алгоритм Евклида, пользователь A вычисляет для числа k мультипликативно обратный элемент k^{-1} в кольце вычетов по модулю n и формирует подпись пользователя B к сообщению M: $S \equiv k^{-1}S' \equiv k^{-1}kM^d \equiv M^d \bmod n$.

3.5. Схемы ЭЦП с восстановлением сообщения

Из проверочного уравнения схемы RSA видно, что если имеется подпись, то из нее можно восстановить сообщение. Схемы ЭЦП, обладающие таким свойством, называются схемами с восстановлением сообщения. Для них характерна следующая проблема. Взяв произвольную подпись и подставив ее в проверочное соотношение, всегда получается некоторое сообщение. Поэтому возникает вопрос о подлинности восстановленного сообщения, т. е. требуется выполнение дополнительной процедуры. Во многих случаях в качестве этой процедуры может служить анализ структуры сообщения, поскольку из «нелегальной» подписи восстанавливаются случайные сообщения. Однако в некоторых случаях требуется подписывать случайные сообщения. Тогда указанная проблема может быть преодолена присоединением к подписываемому сообщению некоторого заранее оговоренного числа или контрольной суммы, вычисляемой от сообщения. Контрольная сумма может быть передана вместе с подписью как внешний элемент.

Схема RSA

Криптосистема RSA основана на теореме Эйлера, согласно которой для любых взаимно простых целых чисел M и n, где $M < n$, выполняется соотношение

$$M^{\varphi(n)} \equiv 1 \bmod n.$$

В криптосистеме RSA в качестве числа M используется сообщение, которое необходимо подписать или зашифровать. Будем полагать, что условие взаимной простоты чисел M и n выполняется. Например, это обеспечивается тем, что в данной криптосистеме выбирается число n, равное произведению двух больших простых множителей, поэтому вероятность того, что случайное сообщение не будет взаимно простым с модулем, является пренебрежимо малой.

Формирование ключей. Каждый пользователь выбирает два больших не равных между собой простых числа p и q, находит их произведение $n = pq$ и вычисляет значение функции Эйлера от n:

$$\varphi(n) = (p-1)(q-1).$$

Значение n является частью открытого ключа. Числа p и q являются частью закрытого ключа. Числа p и q должны иметь специальную структуру, в частности, по крайней мере, одно из чисел $p-1$ или $q-1$ должно иметь один большой простой множитель. Размер модуля n должен быть не менее 1024 бит. Затем выбирается целое число d, такое что $d < \varphi(n)$ и НОД$(d, \varphi(n)) = 1$, и вычисляется e, удовлетворяющее условию

$$ed \equiv 1 \bmod \varphi(n).$$

Секретным ключом является тройка чисел (p, q, d). *Открытым ключом* является пара чисел (n, e), которая сообщается всем пользователям.

Процедура подписывания:

$$S = M^d \bmod n.$$

Процедура проверки подписи:

$$M' = S^e \bmod n.$$

Если $M' = M$, то сообщение M признается подписанным.

Схемы на основе сложности дискретного логарифмирования

На основе ряда описанных выше схем, основанных на сложности дискретного логарифмирования, легко могут быть построены ЭЦП с восстановлением сообщения.

Рассмотрим модифицированное проверочное уравнение схемы Эль-Гамаля $R = \alpha^{M/S} y^{-R/S} \bmod p$ и представим его в виде

$$M = MR^{-1}\alpha^{M/S} y^{-R/S} \bmod p.$$

Легко заметить, что значение сообщения M может быть встроено в элемент подписи R, если его формировать по формуле $R = M^{-1}\alpha^k \bmod p$. При этом значение M из степени при α следует заменить единицей, поскольку мы полагаем, что сообщение до проверки не имеется в наличии у проверяющего. Уравнения проверки и генерации подписи, соответственно, приобретают вид

$$M = \frac{\alpha^{S^{-1}} y^{-RS^{-1}}}{R} \bmod p,$$

$$S = \frac{1 - xR}{k} \bmod (p-1).$$

ЭЦП с восстановлением сообщения может быть также реализована и на основе схем с сокращенным размером подписи. Исходное проверочное уравнение $R' = (\alpha^{M/S} y^{-R'/S} \bmod p) \bmod q$ представим в виде

$$M = \frac{\alpha^{M/S} y^{-R'/S} \bmod p}{R'M^{-1}} \bmod q.$$

Встраивая сообщение в параметр R', т. е. задавая его вычисление по формуле $R' = M^{-1}(\alpha^k \bmod p) \bmod q$, получаем следующие уравнения проверки и генерации подписи:

$$M = \frac{\alpha^{S^{-1}} y^{-R'S^{-1}} \bmod p}{R'} \bmod q,$$

$$S = \frac{1 - xR'}{k} \bmod q.$$

ЭЦП Рабина

Схема ЭЦП Рабина основана на сложности вычисления квадратных корней по модулю n, представляющему собой произведение двух больших простых чисел p и q. Особенностью модуля n в данной схеме является то, что числа p и q являются сравнимыми с числом 3 по модулю 4, т. е. $p \equiv 3 \bmod 4$ и $q \equiv 3 \bmod 4$. Это требование значительно снижает сложность процедуры формирования подписи, которая состоит в извлечении квадратного корня по модулю n. Секретным ключом является пара чисел p и q.

Формирование открытого ключа n осуществляется путем перемножения чисел p и q: $n = pq$.

Вычисление подписи S к сообщению $M = (m_0, m_1, \ldots, m_i, \ldots, m_{h-1})$, где $\forall i \in \{0, 1, \ldots, h-1\}\ m_i \in \{0, 1\}$, включает следующие шаги:

1. Генерируется случайное число $R = (r_0, r_1, \ldots, r_i, \ldots, r_{t-1})$, где $\forall i \in \in \{0, 1, \ldots, t-1\}$ $r_i \in \{0, 1\}$, которое объединяется с сообщением:

$$M||R = (m_0, m_1, \ldots, m_{h-1}, r_0, r_1, \ldots, r_{t-1}).$$

Двоичному вектору $M||R$ сопоставляется число $a < n$. Проверяется выполнение условий $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ и $a^{\frac{q-1}{2}} \equiv 1 \bmod q$. Если одно из соотношений не выполняется, то генерируется новое случайное число R и процедура повторяется до тех пор, пока не будет найдено такое значение a, для которого оба условия выполняются, т. е. получено a, являющееся квадратичным вычетом по mod n.

2. Вычисляются значения $z_{p_1} \equiv a^{(p+1)/4} \bmod p$, $z_{q_1} \equiv a^{(q+1)/4} \bmod q$.

3. По китайской теореме об остатках вычисляется квадратный корень $Z = a^{1/2} \bmod n$.

4. В качестве подписи к M берется пара чисел (R, Z).

Проверка подлинности подписи осуществляется следующим образом:

1. Вычисляется значение a':

$$a' = Z^2 \bmod n.$$

2. Сравниваются значения $a = M||R$ и a'.

3. Если $a = a'$, то подпись признается подлинной.

Для схемы Рабина доказано, что ее стойкость эквивалентна сложности задачи разложения модуля. Эта схема обладает свойством восстановления сообщения, причем при проверке подписи одновременно проверяется и подлинность сообщения за счет того, что к подписи присоединяется число R, добавленное к сообщению.

3.6. Экзистенциальная подделка подписи и потайные каналы в системах ЭЦП

Проверочное уравнение в схемах ЭЦП с восстановлением сообщения (например, в RSA) задает вычислительную процедуру верификации от подписи к сообщению, т. е. по заданной подписи вычисляется сообщение. Причем верификация произвольно взятой подписи приведет к восстановлению некоторого сообщения. Это сообщение будет представлять собой случайную строку битов, поскольку процедура проверки подписи обладает сильными перемешивающими свойствами. Этим может воспользоваться нарушитель,

чтобы получить некоторый текст и подпись к нему, удовлетворяющую проверочному уравнению. Поскольку текст является случайным, то нарушитель имеет достаточно ограниченные возможности для осуществления некоторой атаки, основанной на указанной возможности. Возможность формирования таких подписей называется *экзистенциальной* подделкой подписи. Причем экзистенциальная подделка не обязательно связана со свойством восстановления сообщения при выполнении процедуры верификации подписи. Экзистенциальная подделка подписи возможна в схеме ЭЦП Эль-Гамаля, в американском стандарте DSA и российском ГОСТ Р 34.10–94.

Для некоторых криптографических протоколов возможность экзистенциальной подделки может оказаться достаточно критическим моментом. Для устранения такой возможности в схемах ЭЦП следует предусмотреть некоторый механизм, позволяющий проверить подлинность сообщения, восстановленного из подписи. Примером того, как это можно сделать, служит схема Рабина, где проверка подлинности обеспечивается использованием достаточно большого числа R, которое присоединяется к сообщению перед формированием подписи и служит в качестве одного из элементов подписи. Другим способом является формирование подписи не непосредственно по сообщению, а по хэш-функции, вычисляемой от сообщения. Эту проблему можно решить на основе придания определенной структуры подписываемому сообщению, например, присоединять к сообщению идентификационный номер подписывающего или двоичный вектор, который специфицируется алгоритмом ЭЦП. В следующем разделе будут рассмотрены схемы ЭЦП, устраняющие возможность экзистенциальной подделки подписи за счет использования нового механизма вычисления подписи.

Рассмотрим еще одну особенность систем ЭЦП, связанную с наличием скрытых каналов передачи секретных сообщений. Нетрудно заметить, что вместе с подписью можно передать и некоторую информацию, причем таким образом, чтобы нельзя было выявить и доказать этот факт. Например, отправитель и получатель могут договориться, что первый бит подписи передает один бит криптограммы. Поскольку в криптограмме биты принимают случайные значения, то сторонний наблюдатель не имеет возможности обнаружить, а тем более доказать, что протокол цифровой подписи используется для скрытой передачи шифртекстов. На самом деле с одной подписью можно передать не один, а несколько битов шифртекста. Пусть требуется встроить в подпись b-битовый блок криптограммы, двоичное значение которого равно t. Для этого подписывающий многократно модифицирует подписываемое сообщение (сохраняя его смысловое содержание) и каждый раз формирует подпись, пока первые b битов подписи не будут иметь двоичное значение t.

Именно эту подпись и соответствующее ей сообщение подписывающий отправит получателю. Очевидно, что для передачи в одной подписи b-битового блока криптограммы в среднем потребуется выполнить 2^b процедур формирования подписи. При $b \approx 16$ и более сложность встраивания шифртекста в подпись становится достаточно трудоемким процессом. Описанный способ организации потайного канала передачи зашифрованных сообщений приводит к достаточно низкой пропускной способности канала или высокой вычислительной сложности формирования необходимых значений цифровой подписи. Однако этот способ является универсальным, т. е. применимым совместно с любой схемой ЭЦП, и не требует передачи получателю секретного ключа, по которому формируется подпись (естественно, что ключ, по которому шифруется передаваемая информация, должен быть передан получателю).

Некоторые системы ЭЦП могут быть использованы для организации потайных каналов со сравнительно высокой пропускной способностью. Например, схема ЭЦП Эль-Гамаля допускает встраивание в подпись блоков шифртекста длиной, равной половине длины подписи, а схема Рабина — длиной, примерно равной длине l элемента подписи R (например $l-5$ битов используются для встраивания блока криптограммы, а 5 битов подбираются так, чтобы значение $M\|R$ было квадратичным вычетом). При этом в случае схемы Рабина передача секретного ключа подписи не требуется, а в случае схемы Эль-Гамаля — требуется.

Рассмотрим, как используется схема Эль-Гамаля для организации потайного канала. Предварительно подписывающий (он же является и отправителем шифртекста) передает получателю ключ симметричного шифрования, с помощью которого будет осуществляться шифрование информации, и свой секретный ключ, по которому будет формироваться подпись. Затем шифртекст (или непосредственно открытый текст) передается блоками следующим путем. Текущий блок (или конкатенация из нескольких блоков в зависимости от размера блоков применяемого алгоритма блочного шифрования) используется в качестве случайного числа k, по которому формируется элемент подписи $R=\alpha^k \bmod p$, а затем вычисляется элемент подписи $S=$ $=\dfrac{M-xR}{k} \bmod p-1$. Таким образом, некоторый шифртекст (или открытый текст) оказывается встроенным в подпись (R, S). Получатель, которому известен секретный ключ x формирования подписи, восстанавливает значение k по формуле, вытекающей из уравнения формирования подписи:

$$k=\frac{M-xR}{S} \bmod p-1.$$

Заметим, что, модифицируя сообщение M, подписывающий может сформировать значение S, которое является взаимно простым с $p-1$. При длине модуля $|p| = 1024$ бит в одной подписи можно передать около 1000 бит зашифрованной информации. Возвращаясь к описанию алгоритмов формирования и проверки подписи в американском стандарте DSA, ГОСТ Р 34.10–94, схеме Эль-Гамаля с сокращенной подписью и схеме Шнорра, можно установить, что эти системы ЭЦП могут быть использованы для организации потайных каналов с высокой пропускной способностью. Это связано с тем, что эти системы ЭЦП относятся к вероятностному типу, когда при формировании подписи используются случайные значения и само значение подписи к данному сообщению не является однозначным.

Рассмотрим механизм устранения скрытого канала при использовании схемы Эль-Гамаля. Введем в протокол подписи нового участника — цензора, задачей которого является обеспечение выбора действительно случайного числа k при формировании подписи. При этом цензор не должен иметь возможности каким-либо образом вычислить k, поскольку это дало бы ему возможность сразу же вычислить и секретный ключ x. Это обеспечивается следующей процедурой, в которой подписывающий и цензор совместно генерируют случайное число, используемое для вычисления параметра R. При этом подписывающий не может вычислить это случайное число, однако может убедиться, что R сформировано с использованием действительно случайного числа. Эта процедура включает следующие четыре шага:

1. Подписывающий формирует значение $R = \alpha^k \bmod p$ и отправляет его цензору.
2. Цензор выбирает случайное число $k' < p$ и направляет его подписывающему.
3. Подписывающий формирует значение $R' = \alpha^{k \cdot k'} \bmod p$, отправляет его цензору, а значения R' и $k \cdot k'$ использует для вычисления подписи.
4. Возводя R в степень k', цензор проверяет выполнимость условия $R' = R^{k'} \bmod p$. Если условие выполнено, то он убеждается, что подписывающий действительно использовал случайное значение $k \cdot k'$.

В следующем разделе будут рассмотрены вероятностные схемы ЭЦП, которые не позволяют реализовать встраивание потайных каналов с большой пропускной способностью. Это обеспечивается тем, что оба элемента подписи (R, S) вычисляются по формулам $R = \alpha^k \bmod p$ и $S = \alpha^g \bmod p$, причем показатели степеней k и g вычисляются одновременно путем решения системы из двух сравнений.

ГЛАВА 4

Схемы ЭЦП с новым механизмом формирования подписи

4.1. Схемы с формированием подписи на основе решения системы сравнений

Генерация подписи (R, S) в схемах ЭЦП на основе сложности дискретного логарифмирования может быть осуществлена с использованием нового механизма, в котором оба элемента подписи R и S представляются в одинаковом виде $R=\alpha^k \bmod p$ и $S=\alpha^g \bmod p$, где значения k и g вычисляются одновременно как одно из решений системы из двух сравнений, записываемых в зависимости от вида проверочного соотношения. Идея этого механизма состоит в том, чтобы сделать вычислительно невозможным вычисление одного из параметров R или S при наперед заданном значении второго параметра. Параметры R и S используются как аргументы двух различных функций $F_1(R, S)$ и $F_2(R, S)$. При определенных ограничениях на значения аргументов их можно изменять таким образом, что значение функции $F_2(R, S)$ будет оставаться неизменным. При этом значение функции $F_1(R, S)$ должно изменяться таким образом, что можно подобрать пару значений R и S, при которых будет выполняться некоторое проверочное соотношение. Таким образом, в определенной области пар значений R и S мы имеем $F_2 = Z = \text{const}$, поэтому проверочное соотношение в принципе может быть упрощено, что при определенном его виде позволит вычислить подпись $(R(Z), S(Z))$, зависящую от Z. При составлении конкретных вариантов подписи могут быть использованы, например, следующие пары функций (F_1, F_2): $(R/S \bmod p, RS \bmod p)$, $(RS \bmod p, R/S \bmod p)$, $(RS^M \bmod p, RS \bmod p)$, $(RS \bmod p, RS^2 \bmod p)$, $(RS^Z \bmod p, RS \bmod p)$, $(RS^Z \bmod p, R/S \bmod p)$, где $Z = RS \bmod p$. При этом значения R и S предполагается выражать через k и g в виде: $R=\alpha^k \bmod p$ и $S=\alpha^g \bmod p$. Условие постоянства значения функции $F_2 = R/S \bmod p$ запишется в виде $k - g \equiv U \bmod \gamma$, где γ есть некоторый показатель, к которому

число α относится по модулю p, и U — случайно выбираемое число. В случаях $F_2 = RS \bmod p$ и $F_2 = RS^M \bmod p$ условие постоянства запишется в виде $k + g \equiv U \bmod \gamma$ и $k + gM \equiv U \bmod \gamma$ соответственно. Учитывая, что в уравнение проверки подписи входит значение сообщения M или хэш-функции H от него, можно предложить следующие варианты проверочных соотношений:

$$R / S = y^{(RS \bmod p)^H} \alpha^{(RS \bmod p)} \bmod p,$$

$$R = S y^{H(RS \bmod p)} \alpha^{(RS \bmod p) \bmod \delta} \bmod p,$$

$$(R / S)^{(RS \bmod p)} = y^{(RS \bmod p) \bmod \delta} \alpha^H \bmod p,$$

где δ есть произвольное простое число длины $|\delta| \approx 0.25\,|p|$. Операция $F_2 \bmod \delta$ определяет некоторую сжимающую функцию F_2', значение которой остается постоянным, если значение $F_2 = RS \bmod p$ не изменяется. Это позволяет получить и использовать в проверочном соотношении две функции, зависящие от параметров R и S, причем такие, что их значения фиксируются одновременно при условии, что параметры k и g удовлетворяют определенным условиям.

Необходимость использования пары одновременно фиксируемых функций F_2 и F_2' связана с тем, что в проверочном соотношении требуется задать показатели степеней элементов y и α, зависящие от R и S. Если это условие не выполнено, то подпись может быть легко подделана путем включения фиксированной степени y или α как дополнительного множителя в представление одного из параметров R и S. Например, если проверочное соотношение имеет вид $R = S y^{(RS \bmod p)} \alpha^H \bmod p$, то подпись можно сформировать без использования секретного ключа. Это осуществляется следующим образом. Представим элементы подписи в виде $R = \alpha^H y^k \bmod p$ (1) и $S = y^g \bmod p$ (2). При $k + g \equiv U \bmod \gamma$ (3) значение $Z = RS \bmod p = \alpha^H y^U \bmod p$ является фиксированным и мы можем обеспечить выполнимость сравнения $\alpha^H y^k \equiv y^g y^Z \alpha^H \bmod p$ (очевидно, что при этом будет выполняться проверочное уравнение, поскольку имеет место $R = S y^Z \alpha^H \bmod p$), задавая еще одно условие, которому должны удовлетворять значения k и g, а именно условие $k \equiv g + Z \bmod \gamma$ (4). Таким образом, следует решить систему сравнений (3) и (4) и подставить решение в качестве значений показателей степеней k и g в выражения (1) и (2), определяющие значения элементов подписи R и S.

Если каждый из элементов y и α входит в проверочное соотношение в степенях, зависящих от вычисляемых параметров, то подделать подпись при-

веденным выше способом практически невозможно, если эти степени будут представлять собой две различные нелинейно связанные функции F_2 и F_2' (однако могут оказаться реализуемыми другие способы, которые будут рассмотрены далее). Следует подчеркнуть важность нелинейности связи между рассматриваемыми функциями. Если они будут отличаться постоянным множителем, то подделка подписи также тривиальна. Рассмотрим схему ЭЦП с проверочным сравнением $R y^{(RS \bmod p)} \equiv S\alpha^{H(RS \bmod p)} \bmod p$. Перепишем это сравнение в виде $R \equiv S\left(\alpha^H y^{-1}\right)^{(RS \bmod p)} \bmod p$ и представим элементы подписи в виде $R = \left(\alpha^H y^{-1}\right)^k \bmod p$ (5) и $S = \left(\alpha^H y^{-1}\right)^g \bmod p$ (6). При $k + g \equiv U \bmod \gamma$ (7) значение $Z = RS \bmod p = \left(\alpha^H y^{-1}\right)^U \bmod p$ является фиксированным и условием выполнимости проверочного сравнения является $k \equiv g + Z \bmod \gamma$ (8).

Действительно, если (7) и (8) выполняются, то имеем:

$$\left(\alpha^H y^{-1}\right)^k \equiv \left(\alpha^H y^{-1}\right)^g \left(\alpha^H y^{-1}\right)^Z \bmod p \Rightarrow R y^{(RS \bmod p)} \equiv S\alpha^{H(RS \bmod p)} \bmod p.$$

Таким образом, подпись может быть сформирована без использования секретного ключа путем совместного решения сравнений (7) и (8) и последующего вычисления элементов подписи по формулам (5) и (6).

Еще один вариант ЭЦП задается сравнением проверки подписи вида

$$(R\alpha)^{(RS \bmod p)} \equiv S^{(RS \bmod p) \bmod \delta} y^H \bmod p,$$

в котором внесение постоянного множителя в выражение, представляющее R или S, не позволяет сформировать подпись без знания секретного ключа, поскольку каждый элемент подписи возводится в степень, которая не является заранее заданной. Процедура формирования подписи состоит в следующем. Предполагая, что элементы подписи будут вычисляться по формулам $R = \alpha^k \bmod p$ (9) и $S = \alpha^g \bmod p$ (10), записываем условие фиксирования показателей степеней проверочного соотношения: $k + g \equiv U \bmod \gamma$ (11) и выбираем случайное значение $U < \gamma$, которое задает конкретные значения $Z = RS \bmod p = \alpha^U \bmod p$ и $Z' = (RS \bmod p) \bmod \delta = Z \bmod \delta$. Затем записываем проверочное сравнение в виде

$$\left(\alpha^k \alpha\right)^Z \equiv \left(\alpha^g\right)^{Z'} \left(\alpha^x\right)^H \bmod p \Rightarrow \alpha^{Z(k+1)} \equiv \alpha^{gZ' + xH} \bmod p.$$

Поскольку по предположению α относится к показателю γ, то из последней формулы следует дополнительное сравнение $Z(k+1) \equiv gZ' + xH \bmod \gamma$ (12), которое вместе с (11) обеспечивает выполнимость проверочного сравнения. Решая совместно сравнения (11) и (12), получаем формулы

$$g = \frac{ZU + Z - xH}{Z + Z'} \bmod \gamma \quad \text{и} \quad k = \frac{UZ' - Z + xH}{Z + Z'} \bmod \gamma,$$

по которым вычисляем значения k и g, а затем по (9) и (10) — элементы подписи R и S.

Описанная выше идеология построения схем ЭЦП потенциально устраняет возможность реализации скрытых каналов со сравнительно большой пропускной способностью, поскольку по секретному ключу и подписи (R, S) вычислительно сложно найти значение U, которое выбирается произвольным и могло бы быть использовано для передачи блоков шифртекста. Для вычисления U требуется вычислить и k, и g, однако для этого требуется решить задачу дискретного логарифмирования. В рассмотренных выше схемах потенциально устраняется и возможность экзистенциальной подделки подписи, однако предстоит решить еще одну проблему, связанную с подделкой подписи на основе замены переменных.

Идея атаки на основе замены переменных состоит в том, чтобы выбрать такую пару переменных значений (вместо переменных R и S), чтобы показатели степеней в проверочном соотношении зависели только от одной переменной. Тогда эту переменную можно выбрать произвольно, а вторую переменную вычислить как неизвестную. При этом наиболее сложной операцией процедуры подделки подписи ожидается операция извлечения корней различной степени по простому модулю, которая в общем случае является достаточно легко осуществимой. Проиллюстрируем эту атаку на примере последней из рассмотренных схем. Введем новую переменную $Z = RS \bmod p$ и переменную S выразим через Z и R: $S = R^{-1}Z \bmod p$. Теперь уравнение проверки подписи имеет вид:

$$R^Z \alpha^Z \equiv R^{-Z'} Z^{Z'} y^H \bmod p \Rightarrow R^{Z+Z'} \equiv Z^{Z'} \alpha^{-Z} y^H \bmod p,$$

где $Z' = Z \bmod \delta$. Из последнего сравнения непосредственно следует формула для вычисления значения элемента подписи R:

$$R = \left(Z^{Z'} \alpha^{-Z} y^H \right)^{\frac{1}{Z+Z'}} \bmod p.$$

В случаях простого и составного показателя γ, к которому по модулю p относится число α, достаточно легко найти значение Z, для которого сумма $Z + Z'$ имеет значение взаимно простое с γ, а значит, существует обратное по

отношению к ней значение $(Z+Z')^{-1} \bmod \gamma$. Для таких значений Z легко вычисляется R, а затем и $S = R^{-1}Z \bmod p$.

Устранение такой атаки достигается следующими двумя способами:

- вместо значения R в качестве элемента подписи следует указывать значение k, т. е. подпись приобретает вид (k, S), при этом проверочное соотношение следует модифицировать, заменяя в нем R на $\alpha^k \bmod p$ (фактически предлагается сделать небольшой шаг назад, поскольку при генерации подписи в гипотетической исходной схеме предварительно определялось значение k, а потом по нему вычислялся элемент подписи R);
- вместо простого модуля p может быть использован составной RSA-модуль, в результате чего без решения сложной задачи разложения модуля на простые множители операция вычисления корней будет вычислительно невыполнимой.

Возможен также вариант, в котором указанные два способа комбинируются. Во всех этих случаях экзистенциальная подделка подписи и эффективные скрытые каналы предотвращаются. В следующих разделах эти способы рассматриваются более подробно и раскрываются некоторые дополнительные преимущества, которые они обеспечивают при синтезе конкретных схем ЭЦП.

4.2. Схемы с подписью вида (*k*, *S*)

Отказ от использования значения R в качестве элемента подписи в схемах ЭЦП, в которых процедура генерации подписи включает решение системы сравнений, ведущий к заданию цифровой подписи в виде (k, S), не только устраняет возможность подделки подписи на основе замены переменных, но дает и другие положительные эффекты:

1. Становится возможным отказаться от одной из двух фиксируемых функций F_2 или F_2', поскольку число α возводится непосредственно в степень k, которая естественно приобретает конкретное значение только после решения системы сравнений. Становится достаточным включения в проверочные соотношения только одного множителя $y^{(\alpha^k S \bmod p)} \bmod p$ с показателем степени, определяемым после решения системы сравнений. Это обеспечивает упрощение вида проверочных соотношений.

2. Размер подписи может быть существенно сокращен, если в качестве числа α использовать число, относящееся по модулю p к простому показателю γ, длина которого существенно меньше длины числа p, например, $|\gamma| = 160 - 256$ бит.
3. Появляется возможность реализации схем ЭЦП, в которых условие фиксирования задается сравнениями, включающими произведение или отношение значений k и g.

Возможные варианты конкретной реализации схем ЭЦП с подписью вида (k, S) представлены в следующей таблице.

Таблица 4.1. Схемы ЭЦП с простым модулем

№ п/п	Проверочное соотношение	Формулы для вычисления значений k, g и S	Система решаемых сравнений и формула для вычисления Z по U
1	$S = \equiv y^{H(S\alpha^k \bmod p)+k} \bmod p$	$k = \frac{U - xHZ}{x+1} \bmod \gamma;$ $g = \frac{Ux + xHZ}{x+1} \bmod \gamma;$ $S = a^g \bmod p$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ g \equiv xHZ + xk \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod p$
2*	$S = \equiv H\alpha^k y^{(S\alpha^k \bmod p)} \bmod p$	$k = \frac{U - xZ}{2} \bmod \gamma;$ $g = \frac{U + xZ}{2} \bmod \gamma;$ $S = H\alpha^g \bmod p$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ g \equiv k + xZ \bmod \gamma; \end{cases}$ $Z = H\alpha^U \bmod p$
3	$y^{Hk+(S\alpha^k \bmod p)} \equiv \equiv S \bmod p$	$k = \frac{U - xZ}{xH+1} \bmod \gamma;$ $g = \frac{xHU + xZ}{xH+1} \bmod \gamma;$ $S = \alpha^g \bmod p$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ xHk + xZ \equiv g \bmod \gamma; \end{cases}$ $Z \equiv \alpha^U \bmod p$

№ п/п	Проверочное соотношение	Формулы для вычисления значений k, g и S	Система решаемых сравнений и формула для вычисления Z по U
4*	$S = \equiv Hy^{k+(\alpha S^k \bmod p)} \bmod p$	$k = \frac{-xZ \pm \sqrt{x^2Z^2 + 4xU}}{2x} \bmod \gamma;$ $g = xk + xZ \bmod \gamma;$ $S = H\alpha^g \bmod p$	$\begin{cases} kg \equiv U \bmod \gamma, \\ g \equiv xk + xZ \bmod \gamma; \end{cases}$ $Z = H\alpha^{U+1} \bmod p$
5	$S^H \equiv \equiv Hy^{(S\alpha^k \bmod p)+k} \bmod p$	$k = \frac{HU - xZ}{x + H} \bmod \gamma;$ $g = \frac{xU + xZ}{x + H};$ $S = H^{H^{-1}}\alpha^g \bmod p$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ gH \equiv xZ + xk \bmod \gamma; \end{cases}$ $Z = H^{H^{-1}}\alpha^U \bmod p$
6	$S\alpha^k \equiv \equiv \alpha^{H(y^k / S \bmod p)} \bmod p$	$k = \frac{HZ - U}{x + 1} \bmod \gamma;$ $g = \frac{xU + HZ}{x + 1} \bmod \gamma;$ $S = y^g \bmod p$	$\begin{cases} k - g \equiv U \bmod \gamma, \\ xg + k \equiv HZ \bmod \gamma; \end{cases}$ $Z = y^U \bmod p$
7	$(S\alpha)^k \equiv \equiv y^{(S^k \bmod p)H} \bmod p$	$k = xZH - U \bmod \gamma;$ $g = \frac{U}{xZH - U} \bmod \gamma;$ $S = \alpha^g \bmod p$	$\begin{cases} kg \equiv U \bmod \gamma, \\ (g+1)k \equiv xZH \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod p$

* Возможна экзистенциальная подделка подписи.

Как правило, в формулах процедуры генерации подписи присутствуют дроби, т. е. возникает необходимость выполнения операции деления по модулю γ. Если этот модуль является простым или равен произведению двух больших простых чисел, то для выбранных значений секретного ключа и числа U условие НОД$(\gamma, X) \neq 1$, где X есть значение знаменателя дроби, вы-

полняется с пренебрежимо малой вероятностью. Однако если α является первообразным корнем, когда имеем $\gamma = p - 1$, то требуется обеспечить выполнение условия НОД$(\gamma, X) = 1$. В различных случаях это можно сделать, выбирая соответствующее значение секретного ключа или значение U.

В некоторых схемах решение системы сравнений дает формулы с квадратными корнями. Для таких схем ЭЦП следует выбрать простое значение $\gamma \equiv 3 \bmod 4$, что обеспечит наиболее низкую сложность операции извлечения квадратного корня, которая в этом случае сводится к операции возведения в степень $(\gamma + 1)/4$ по модулю γ. Чтобы такое значение γ можно было бы подобрать, следует иметь это в виду заблаговременно при генерации модуля p.

4.3. Схемы с RSA-модулем

Отказ от использования простого модуля и переход к использованию вместо него составного модуля, равного произведению двух больших простых чисел, обеспечивающих достаточно высокую сложность задачи его факторизации, позволяет достаточно легко построить схемы ЭЦП с подписью вида (R, S), в которых возможность подделки подписи на основе замены переменных устраняется благодаря высокой сложности извлечения корней второй и более высоких степеней по составному модулю. При этом возникает еще и следующий дополнительный положительный момент. Становится возможным использовать в качестве открытого ключа значение модуля, за счет чего в проверочном соотношении устраняется присутствие параметра y и становится достаточно использования только одной из двух фиксируемых функций F_2 или F_2'.

Однако возникают некоторые новые обстоятельства, которые следует учитывать при разработке схем ЭЦП и генерации открытого ключа. Поскольку число α является зависимым от модуля, то его следует приводить как второй элемент открытого ключа, причем размер числа α примерно равен размеру модуля n. Таким образом, в схемах с RSA-модулем имеем открытый ключ (n, α), длина которого вдвое больше длины открытого ключа схем с простым модулем p. Более существенным является то, что возникают особые требования к генерации числа α. Они обусловлены тем, что наличие числа α для общего доступа создает дополнительные предпосылки к нахождению новых способов факторизации модуля. В частности, если показателем по модулю n является простое число, то может оказаться возможным нахождение делителя n путем вычисления НОД$(n, \alpha - 1) \neq 1$ [62, 71].

Рассмотрим типовую процедуру генерации числа α, относящегося по модулю n к простому показателю γ. Выбирается случайное число β, такое что

НОД$(\beta, n) = 1$, вычисляется значение $t = \varphi(n)/\gamma = (r-1)(q-1)/\gamma$, затем число $z = \beta^t \bmod n$. Если $z \neq 1$, то z берется в качестве числа α. Согласно теореме Эйлера имеем $\beta^{\varphi(n)} \equiv 1 \bmod n$, где $\varphi(n) = (r-1)(q-1)$. Рассмотрим наиболее вероятный случай, когда в каноническом разложении чисел $r-1$ и $q-1$ нет одинаковых больших множителей, т. е. γ делит либо $r-1$, либо $q-1$. Пусть для определенности γ делит $r-1$, но не делит $q-1$, тогда имеем:

$$\alpha = \beta^{\varphi(n)/\gamma} \bmod n \equiv \left(\beta^{(q-1)}\right)^{(r-1)/\gamma} \bmod n \Rightarrow$$

$$\Rightarrow \alpha \equiv \left(\beta^{(q-1)}\right)^{(r-1)/\gamma} \equiv 1^{(r-1)/\gamma} \equiv 1 \bmod q \Rightarrow$$

$$\Rightarrow \alpha - 1 \equiv 0 \bmod q \Rightarrow q \mid \alpha - 1 \Rightarrow \text{НОД}(\alpha - 1, n) = q.$$

Следовательно, в случае простого значения γ разложение модуля сводится к нахождению наибольшего общего делителя двух чисел $\alpha - 1$ и n. Для обеспечения высокого уровня стойкости схем с открытым ключом вида (n, α) требуется использовать составные значения γ, например, в качестве γ можно использовать значение функции Эйлера от модуля, т. е. $\gamma = \varphi(n) = (r-1)(q-1)$. Однако в этом случае высока вероятность того, что достаточно часто значения знаменателей дробей в формулах для вычисления параметров k и g будут оказываться не взаимно простыми с γ, что приводит к необходимости повторять процедуру генерации подписи. Наиболее приемлемым решением рассматриваемой проблемы является выбор в качестве γ числа, равного произведению двух достаточно больших простых делителей $\gamma' \mid (r-1)$ и $\gamma'' \mid (q-1)$, т. е. использовать такое α, что имеют место соотношения $\alpha^{\gamma'\gamma''} \equiv 1 \bmod n$, $\alpha^{\gamma'} \bmod n \neq 1$ и $\alpha^{\gamma''} \bmod n \neq 1$ [64].

При генерации α можно использовать формулу $\alpha = \beta^{\frac{(r-1)(q-1)}{\gamma'\gamma''}} \bmod n \neq 1$, где β — случайно выбираемое число в сочетании с проверкой выполнимости условия НОД$(n, \alpha - 1) = 1$. Если в качестве β выбирать случайное число, являющееся одновременно первообразным корнем по модулю r и по модулю q, то указанную проверку можно не выполнять [62], поскольку в этом случае условие НОД$(n, \alpha - 1) = 1$ выполняется всегда. Очевидно, что $\alpha^{\gamma'} \equiv \left(\beta^{\frac{(q-1)}{\gamma''}}\right)^{(r-1)} \equiv 1 \bmod r$ и $\alpha^{\gamma''} \equiv \left(\beta^{\frac{(r-1)}{\gamma'}}\right)^{(q-1)} \equiv 1 \bmod q$, поэтому имеют место соотношения НОД$(\alpha^{\gamma'} - 1, n) = r$ и НОД$(\alpha^{\gamma''} - 1, n) = q$.

Следовательно, если одно из чисел γ' или γ'' сравнительно мало, то разложение модуля можно осуществить подбором значения t, для которого имеет место НОД$(\alpha^t - 1, n) \neq 1$.

Имеется еще один вариант генерации «стойкого» значения α, который основан на использовании таких простых чисел r и q, что каждое из значений $r-1$ и $q-1$ делится на простой делитель γ, но не делится на γ^2. В этом случае для генерации α требуется использовать формулу $\alpha = \beta^{L(n)/\gamma} \bmod n \neq 1$, где $L(n) = $ НОК $[r-1, q-1]$ есть обобщенная функция Эйлера от модуля. Сформированное таким образом число α представимо в виде $\alpha = \beta^{uv} \bmod n \neq 1$, где $u = (r-1)/\gamma$ и $v = (q-1)/\gamma$. Если при генерации α мы будем использовать число β, являющееся одновременно первообразным корнем по модулю r и по модулю q, тогда выполняются следующие два условия: $\alpha \not\equiv 1 \bmod q$ и $\alpha \not\equiv 1 \bmod r$. Однако использование «двукратного» первообразного корня для генерации α не является необходимым. Можно использовать случайные значения β, но, после того как будет сформировано значение α, потребуется проверить выполнимость соотношений $\alpha \not\equiv 1 \bmod q$ и $\alpha \not\equiv 1 \bmod r$. Если хотя бы одно из них не выполняется, то следует взять новое значение β и повторить процедуру генерации α (вероятность того, что понадобится повторная процедура генерации α, является достаточно низкой [62]). Последний вариант формирования α мог бы обеспечить использование простых значений показателя γ длины $|\gamma| \approx 128 - 256$ бит. Однако в рассмотренных выше схемах ЭЦП, основанных на сложности факторизации модуля, он не может быть применен по следующей причине. В этих схемах число γ является секретным, а наличие общего делителя у чисел $(r-1)$ и $(q-1)$ приводит к тому, что он может быть легко вычислен по значению модуля [71]. Действительно, мы имеем:

$$n - 1 = (u\gamma + 1)(v\gamma + 1) - 1 = uv\gamma^2 + u\gamma + v\gamma = (uv\gamma + u + v)\gamma,$$

поэтому, раскладывая число $n-1$ на множители, достаточно легко найти секретное число γ.

Следует заметить, что возможны схемы ЭЦП рассматриваемого типа, в которых открытый ключ представлен только значением модуля, т. е. в них вместо (n, α) в качестве открытого ключа задается только значение n. В этих схемах α используется только в процедуре формирования подписи. В проверочное соотношение это значение не входит. Однако и в этих схемах при генерации подписи следует использовать число α, удовлетворяющее указанным выше условиям. Действительно, параметры R и S генерируются по фор-

мулам $R = \alpha^k \bmod n$ и $S = \alpha^\kappa \bmod n$, поэтому имеем: $R \equiv \alpha^k \bmod r$, $R \equiv \alpha^k \bmod q$, $S \equiv \alpha^\kappa \bmod r$ и $S \equiv \alpha^\kappa \bmod q$. Следовательно, если имеет место $\alpha \equiv 1 \bmod r$ или $\alpha = 1 \bmod q$, то выполняются и сравнения $R \equiv \alpha^k \equiv S \equiv \alpha^\kappa \equiv 1 \bmod r$ или $R \equiv \alpha^k \equiv S \equiv \alpha^\kappa \equiv 1 \bmod q$ соответственно. Таким образом, при нарушении ограничительных требований при генерации параметров α и γ факторизация модуля может быть выполнена достаточно легко, используя формулу НОД$(n, S-1) = w$ или НОД$(n, R-1) = w$, где $w = r$ или $w = q$, т. е. по любому из элементов подписи (R, S) можно будет выполнить разложение модуля.

В приводимых ниже вариантах схем ЭЦП (табл. 4.2) мы полагаем, что отмеченные ограничительные условия выполняются и значение $\gamma = \gamma'\gamma''$ является секретным элементом, а длины чисел γ, γ' и γ'' равны: $|\gamma| \approx 256 \div 512$, $|\gamma'| \approx 128 \div 256$ и $|\gamma''| \approx 128 \div 256$ бит. При этом числа γ' и γ'' желательно выбирать с учетом условия $|\gamma'| \approx |\gamma''|$.

Таблица 4.2. Схемы ЭЦП с составным модулем, использующие в качестве подписи пару чисел (R, S) или (k, S), где $S = \alpha^\kappa \bmod n$

№ п/п	Проверочное соотношение	Формулы для вычисления значений k и g и выражения для R и S	Система решаемых сравнений и выражение для Z
1	$R = S^{H(RS \bmod n)} \bmod n$	$k = \dfrac{UHZ}{HZ+1} \bmod \gamma;$ $g = \dfrac{U}{HZ+1} \bmod \gamma;$ $R = \alpha^k \bmod n$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ k \equiv gHZ \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod n$
2	$R^H \equiv S^{(RS \bmod n)} \bmod n$	$k = \dfrac{UZ}{H+Z} \bmod \gamma;$ $g = \dfrac{UH}{H+Z} \bmod \gamma;$ $R = \alpha^k \bmod n$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ kH \equiv gZ \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod n$
3*	$R = HS^{(RS \bmod n)} \bmod n$	$k = \dfrac{UZ}{Z+1} \bmod \gamma;$ $g = \dfrac{U}{Z+1} \bmod \gamma;$ $R = H\alpha^k \bmod n$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ k \equiv gZ \bmod \gamma; \end{cases}$ $Z = H\alpha^U \bmod n$

№ п/п	Проверочное соотношение	Формулы для вычисления значений k и g и выражения для R и S	Система решаемых сравнений и выражение для Z
4	$R = S^{(R^H S \bmod n)} \bmod n$	$k = \frac{UZ}{HZ+1} \bmod \gamma;$ $g = \frac{U}{HZ+1} \bmod \gamma;$ $R = \alpha^k \bmod n$	$\begin{cases} Hk + g \equiv U \bmod \gamma, \\ k \equiv gZ \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod n$
5	$R = S^H \alpha^{(RS \bmod n)} \bmod n$	$k = \frac{UH+Z}{H+1} \bmod \gamma;$ $g = \frac{U-Z}{H+1} \bmod \gamma;$ $R = \alpha^k \bmod n$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ k \equiv gH + Z \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod n$
6	$\alpha = R^H S^{(R^{-1} S \bmod n)} \bmod n$	$k = \frac{1-UZ}{H+Z} \bmod \gamma;$ $g = \frac{UH+1}{H+Z} \bmod \gamma:$ $R = \alpha^k \bmod n$	$\begin{cases} g - k \equiv U \bmod \gamma, \\ kH + gZ \equiv 1 \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod n$
7	$S = \alpha^{(HS\alpha^k \bmod n)+k} \bmod n$	$k = \frac{U-Z}{2} \bmod \gamma;$ $g = \frac{U+Z}{2} \bmod \gamma$	$\begin{cases} g + k \equiv U \bmod \gamma, \\ g \equiv Z + k \bmod \gamma; \end{cases}$ $Z = H\alpha^U \bmod n$
8	$S = \alpha^{(S^{kH} \bmod n)} \bmod n$	$k = \frac{U}{ZH} \bmod \gamma;$ $g = Z \bmod \gamma$	$\begin{cases} gkH \equiv U \bmod \gamma, \\ g \equiv Z \bmod \gamma; \end{cases}$ $Z = H\alpha^U \bmod n$
9	$S^k = \alpha^{(S^k H \bmod n)+k} \bmod n$	$k = U - Z \bmod \gamma;$ $g = \frac{U}{U-Z} \bmod \gamma$	$\begin{cases} gk \equiv U \bmod \gamma, \\ gk \equiv Z + k \bmod \gamma; \end{cases}$ $Z = H\alpha^U \bmod n$

* Возможна экзистенциальная подделка подписи.

Использование модуля RSA в схемах ЭЦП с подписью вида (R, S) автоматически не предотвращает возможность подделки подписи методом замены переменных, хотя создает предпосылки к этому. В каждом конкретном варианте следует рассмотреть эту атаку. Например, в схеме с проверочным уравнением $\alpha = R^H S^{(RS \bmod n)} \bmod n$, которое очень похоже на поверочное уравнение схемы 6 из табл. 4.2, подделка подписи возможна следующим путем. Введем новую переменную $Z = RS \bmod n$ и переменную R выразим через Z и S: $R = S^{-1}Z \bmod n$. В результате приводим уравнение проверки подписи к виду:

$$\alpha = S^{-H} Z^H S^Z \equiv S^{Z-H} Z^H \bmod n \Rightarrow S = \left(Z^H\right)^{(Z-H)^{-1}} \bmod n.$$

Подставляя в последнюю формулу значение $Z = H + 1$ (переменной Z можно придавать произвольные значения), легко вычислить $S = (H+1)^H \bmod n$ и $R = S^{-1}(H+1) \bmod n$, т. е. получена подпись (R, S), которая удовлетворяет исходному проверочному уравнению.

4.4. Применение простого модуля в схемах, основанных на сложности факторизации

В работе [63] рассматривается схема ЭЦП, основанная на сложности факторизации большого числа, хотя вычисления ведутся по простому модулю, имеющему структуру $p = 2n + 1$, где $n = qr$, q и r — большие простые числа. Это определяет ее отличие от других схем ЭЦП, основанных на сложности задачи факторизации, в которых при генерации и проверке подписи вычисления осуществляются по составному модулю. При этом одно из простых чисел q или r является секретным ключом и служит показателем, к которому относится число α. Пусть этим числом будет q. Открытым ключом является тройка чисел (p, α, λ), где λ есть параметр, связанный с размером секретного ключа: $|q| \le \lambda$, а α генерируется следующим образом. Выбирается случайное число β, такое что НОД$(\beta, n) = 1$, вычисляется значение $t = (p-1)/q = 2r$, затем — число $z = \beta^{2r} \bmod p$. Если $z \neq 1$, то z берется в качестве элемента α открытого ключа. Число n формируется путем генерации случайных простых чисел q и r длины 500 бит и более и последующего перемножения их значений. Затем на основе q и r формируется число $p = 2n + 1$, которое проверяется на простоту. Если p оказывается составным, то выбирается новая пара чисел q и r и вычисляется новое число p. Благодаря использованию простого модуля возможность использования значения α для решения задачи факторизации числа n (*см. разд. 4.3*) устраняется.

Генерация подписи к сообщению M осуществляется в соответствии со следующей процедурой:

1. Вычисляется значение хэш-функции от M: $H = H(M)$, причем $H \neq 0$ и $H \neq 1$ (если $H = 0$ или $H = 1$, то M модифицируется).
2. Генерируется случайное число k ($k < q$), и вычисляется параметр $R = \alpha^k \bmod p$.
3. Вычисляется значение $S = HR/k \bmod q$.
4. В качестве подписи берется значение (R, S).

Проверка подлинности подписи (R, S) осуществляется следующим образом.

1. Вычисляется значение хэш-функции от сообщения M: $H = H(M)$.
2. Вычисляется значение $\alpha^{HR} \bmod p$.
3. Вычисляется значение $R^S \bmod p$.
4. Если $|S| \leq \lambda$ и $R^S \bmod p = \alpha^{IIR} \bmod p$, то подпись признается подлинной.

В соответствии с приведенными выше алгоритмами генерации и проверки подписи имеем следующее уравнение проверки подлинности подписи:

$$R^S \bmod p = \alpha^{HR} \bmod p, \text{ где } |S| \leq \lambda.$$

В последнем соотношении важным условием является требование того, чтобы размер подписи не превышал размера секретного ключа $|q| \leq \lambda$. Этот момент является принципиальным, поскольку на основе открытого ключа легко сформировать подпись, в которой для параметра S выполняется соотношение $|S| \leq |n|$. Это может быть осуществлено по формуле $S = HR/k \bmod (p - 1)$. Однако формирование числа S длины $|S| \leq \lambda$ является вычислительно сложной задачей, требующей решения проблемы факторизации целого числа на два простых множителя специального вида.

Для практического использования систем ЭЦП представляется важным вопрос сокращения длины подписи. В рассматриваемой схеме ЭЦП длина подписи примерно равна $|R| + |S|$, где $|R| \approx |p| \approx 1000$ бит, $|S| \approx |q| \approx 500$ бит. С целью уменьшения размера подписи можно воспользоваться уравнением проверки подписи, представленным в таком виде:

$$R = \alpha^{HSR} \bmod p, \text{ где } |S| \leq \lambda.$$

Из последнего соотношения получаем формулу

$$F(R) = F(\alpha^{HSF(R)} \bmod p), \text{ где } |S| \leq \lambda,$$

которая может быть использована как уравнение проверки подписи при применении любой сжимающей однонаправленной функции F. Подписью в модифицированной схеме является пара чисел $F(R)$ и S. В частности, в качестве функции F может быть использована функция хэширования, используемая для вычисления значения $H = H(M)$. Уравнение генерации параметра S в случае произвольной функции F имеет вид:

$$S = k\,(HF(R))^{-1} \bmod q.$$

При использовании сжимающей функции F со 160-битовым выходом размер цифровой подписи составляет $|F| + |q| \approx 160 + 500 \approx 660$ бит. В качестве функции $F(x)$ может быть взят остаток от деления аргумента x на некоторое простое число p' длины 160 бит или более. В результате приходим к следующему уравнению проверки подписи:

$$R' = (\alpha^{HSR'} \bmod p) \bmod p',$$

где $|S| \le \lambda$ и $R' = (\alpha^{k} \bmod p) \bmod p'$. В схеме ЭЦП, соответствующей последнему уравнению проверки подлинности подписи, вычисление значения S осуществляется по следующей формуле:

$$S = k\,(HR')^{-1} \bmod q.$$

Этот механизм сокращения длины подписи обеспечивает уменьшение ее размера примерно вдвое при $|p| \approx 1000$ бит. При $|p| \approx 2000$ бит длина подписи уменьшается примерно в три раза по сравнению с исходной версией схемы ЭЦП.

Специфической для рассмотренных вариантов схем ЭЦП атакой [63] является попытка формирования «правильной» подписи большой длины и выделения «правильной подписи», удовлетворяющей условию $|S| \le \lambda$. С этой целью представляет интерес рассмотреть атаку, направленную на вычисление секретного ключа на основе возможности формирования значений R и S', удовлетворяющих уравнению $R = \alpha^{HRS' \bmod 2n} \bmod p$. Вычисляя по случайно выбранному значению k параметр $R = \alpha^{k} \bmod p$, атакующий легко может вычислить S' из сравнения $k \equiv HRS' \bmod 2n$. Легко заметить, что выполняется сравнение $HRS - k \equiv 0 \bmod q$, т. е. $q \mid (HRS - k)$. Вопрос состоит в следующем: можно ли, формируя различные пары значений R и S', соответствующие различным значениям H, получить такие значения $HRS - k$, которые можно легко разложить на множители, а затем, испытывая каждый множитель, найти секретный ключ q? Покажем, что такая атака имеет достаточно большую вычислительную сложность. Действительно, из условия $(HRS - k) \equiv 0 \bmod n$ следует $n \mid (HRS - k)$. Таким образом, значение $HRS - k$ содержит в качестве делителя

число n, поэтому разложение числа $HRS - k$ на простые множители не проще, чем факторизация n.

Рассмотренный выше подход к построению схем ЭЦП, основанных на сложности задачи факторизации, может быть применен и при построении схем ЭЦП, в которых параметры подписи вычисляются на основе решения системы сравнений. Основное достоинство использования простого модуля состоит в устранении проблем, связанных с выбором параметра α, являющегося элементом открытого ключа и применяемого для генерации элемента подписи S.

В приводимых ниже вариантах схем ЭЦП (см. табл. 4.3) мы полагаем, что используется простой модуль p, имеющий структуру $p = 2rq + 1$, где простые числа r и q являются сильными простыми числами, а показатель числа α по модулю p является простым и равен $\gamma = q$.

Таблица 4.3. Схемы ЭЦП с простым модулем $p = 2rq + 1$ и подписью вида (k, S)

№ п/п	Проверочные соотношения	Формулы для вычисления значений k, g и S	Система решаемых сравнений и формула для вычисления Z по U
1	$\alpha^k \equiv S^{H(\alpha^k S \bmod p)} \bmod p;$ $\lvert k\rvert \le \lambda$	$k = \dfrac{UHZ}{HZ+1} \bmod \gamma;$ $g = \dfrac{U}{HZ+1} \bmod \gamma;$ $S = \alpha^g \bmod p$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ k \equiv gHZ \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod p$
2	$\alpha^{kH} \equiv S^{(\alpha^k S \bmod p)} \bmod p;$ $\lvert k\rvert \le \lambda$	$k = \dfrac{UZ}{H+Z} \bmod \gamma;$ $g = \dfrac{UH}{H+Z} \bmod \gamma;$ $S = \alpha^g \bmod p$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ kH \equiv gZ \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod p$
3	$S \equiv \alpha^{(\alpha^k S \bmod p)+kH} \bmod p;$ $\lvert k\rvert \le \lambda$	$k = \dfrac{U-Z}{H+1} \bmod \gamma;$ $g = \dfrac{UH+Z}{H+1} \bmod \gamma;$ $S = \alpha^g \bmod p$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ g \equiv Z + kH \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod p$

№ п/п	Проверочные соотношения	Формулы для вычисления значений k, g и S	Система решаемых сравнений и формула для вычисления Z по U
4*	$S \equiv H\alpha^{(\alpha^k S \bmod p)+k} \bmod p$; $\lvert k \rvert \le \lambda$	$k = \frac{U - Z}{2} \bmod \gamma$; $g = \frac{U + Z}{2} \bmod \gamma$; $S = H\alpha^g \bmod p$	$\begin{cases} k + g \equiv U \bmod \gamma, \\ g \equiv Z + k \bmod \gamma; \end{cases}$ $Z = H\alpha^U \bmod p$
5	$\alpha = S^{(S^k \bmod p)+kH} \bmod p$; $\lvert k \rvert \le \lambda$	$k = \frac{UZ}{1 - UH} \bmod \gamma$; $g = \frac{1 - UH}{Z} \bmod \gamma$; $S = \alpha^g \bmod p$	$\begin{cases} kg \equiv U \bmod \gamma, \\ gZ + kgH \equiv 1 \bmod \gamma; \end{cases}$ $Z = \alpha^U \bmod p$
6*	$S = H\alpha^{(\alpha^k S^k \bmod p)-1} \bmod p$; $\lvert k \rvert \le \lambda$	$k = \frac{U}{Z} \bmod \gamma$; $g = Z - 1 \bmod \gamma$; $S = H\alpha^g \bmod p$	$\begin{cases} k + kg \equiv U \bmod \gamma, \\ g \equiv Z - 1 \bmod \gamma; \end{cases}$ $Z = H\alpha^U \bmod p$

* Возможна экзистенциальная подделка подписи.

4.5. Схемы с восстановлением сообщения

В схемах ЭЦП с восстановлением сообщения проверочное соотношение имеет вид уравнения, одна из частей (обычно левая) которого равна значению сообщения. Поэтому проверка подписи аналогична процедуре расшифрования: по полученной подписи (которую можно интерпретировать как шифртекст) в результате выполнения процедуры проверки подписи восстанавливается (расшифровывается) сообщение. Другими словами, вычисление идет от подписи к сообщению. В таких схемах произвольное случайное значение подписи также приведет к восстановлению некоторого случайного сообщения. Очевидно, что оно «корректно» соответствует использованной случайной подписи. Однако не менее очевидно, что оно не является подлинным, поскольку владелец секретного ключа не имел отношения к случайной подписи. Выход из этой противоречивой ситуации схем ЭЦП с восстановле-

нием сообщения состоит в том, что используется (явно или неявно) некоторая дополнительная информация, которая служит для подтверждения подлинности восстанавливаемого сообщения.

Неявное использование дополнительной информации состоит в том, что подлинное сообщение обладает в большинстве случаев определенной структурой (это осмысленный текст или данные в определенном формате). Если должны быть подписаны случайные данные, то следует задать явное использование дополнительной информации. Это можно сделать, например, следующими способами.

- Перед выполнением процедуры генерации подписи к сообщению присоединяется контрольная сумма, вычисленная по некоторому специфицированному алгоритму, и такое модифицированное сообщение подписывается. При проверке подписи модифицированное сообщение восстанавливается, контрольная сумма отделяется, от оставшегося сообщения вычисляется контрольная сумма и полученное значение сравнивается с полученной контрольной суммой. Если значения совпадают, то сообщение признается подлинным и подписанным (или можно сказать, что подпись признается подлинной, а значит, и сообщение, восстанавливаемое из нее, также подлинно).
- Контрольная сумма, например, значение хэш-функции, пересылается вне подписи, т. е. как отдельный элемент. При этом в уравнении проверки подписи этот элемент присутствует в явном виде как один из параметров.
- К сообщению присоединяется заранее специфицированный двоичный вектор, после чего модифицированное сообщение подписывается.

Рассмотрим последний вариант на примере криптосистемы RSA. Придание сообщению структурности можно осуществить по следующей схеме:

1. К сообщению M, которое необходимо подписать и передать по открытому каналу, присоединяется заранее условленный двоичный вектор V, например, имеющий длину $|V| = v = 64$ бит:
$$M' \rightarrow M||V.$$
2. Вырабатывается подпись для сообщения M':
$$S = M'^{d} \bmod n.$$
3. Значение S направляется принимающей стороне.
4. Принимающая сторона по значению S вычисляет значения
$$M^* = S^e \bmod n, \quad V' = M^* \bmod 2^v \text{ и } M = M^* \operatorname{div} 2^v.$$

5. Если V' равно условленному заранее значению V, т. е. если выполняется условие $V' = V$, то принимается решение, что сообщение M является подлинным. Вероятность ошибочного решения равна 2^{-v}.

Схемы цифровой подписи RSA и Рабина по определению являются схемами с восстановлением сообщения. Схема ЭЦП Эль-Гамаля, многие другие схемы, основанные на сложности задачи дискретного логарифмирования или сложности факторизации, могут быть преобразованы в схемы с восстановлением сообщения. Рассмотрим механизм такого преобразования на примере схемы ЭЦП из работы [63], которая была рассмотрена в разд. 4.4 и характеризуется проверочным уравнением

$$R = \alpha^{HRS} \bmod p, \text{ где } |S| \le \lambda.$$

Без существенных изменений исходную схему можно представить в виде

$$R^{-1} \alpha^{HRS} \equiv 1 \bmod p, \text{ где } |S| \le \lambda.$$

Зададим в этом соотношении процедуру вычисления параметра R в соответствии с формулой $R = M^{-1} \alpha^k \bmod p$, где M — сообщение $(M < p)$, т. е. «встроим» информацию, содержащуюся в сообщении, в элемент подписи R. С учетом этого имеем следующее изменение проверочного соотношения:

$$M = R^{-1} \alpha^{HRS} \bmod p, \text{ где } |S| \le \lambda.$$

При этом формула для вычисления элемента подписи S будет совпадать с выражением для генерации подписи в исходной схеме:

$$S = \frac{k}{HR} \bmod q.$$

Аналогичным образом можно преобразовать и схему ЭЦП с сокращенным размером подписи из [63] в схему с восстановлением сообщения. В этой схеме имеем элемент подписи R', который получен действием некоторой сжимающей функции на элемент $R = \alpha^k \bmod p$, например, $R' = \bmod p'$, и проверочное уравнение $R' = (\alpha^{HR'S} \bmod p) \bmod p'$. В случае, когда сжатие осуществляется операцией $\bmod p'$, информация о сообщении $M < p' << p$ может быть обратимо встроена в R' путем вычисления этого элемента по формуле:

$$R' = M^{-1} (\alpha^k \bmod p) \bmod p'.$$

Видно, что деление значения $\alpha^k \bmod p$ на R' по $\bmod p'$ восстанавливает сообщение M. Поскольку в исходном сообщении $\alpha^k \bmod p = \alpha^{HR'S} \bmod p$, то имеем:

$$M = \frac{\alpha^{HR'S} \bmod p}{R'} \bmod p', \text{ где } |S| \le \lambda.$$

Отметим, что в частном случае можно положить $p' = q$. Последнее уравнение и является проверочным соотношением для построенной нами схемы ЭЦП, сочетающей возможность сокращения размера подписи со свойством восстановления сообщения. Уравнение генерации подписи сохранилось в исходном виде:

$$S = \frac{k}{HR'} \bmod q.$$

Наличие параметра H в проверочных уравнениях полученных схем ЭЦП с восстановлением сообщения требует передачи значения хэш-функции проверяющему, чтобы он имел все параметры, входящие в проверочное соотношение. Это обеспечивает возможность подтверждения подлинности восстановленного сообщения путем вычисления значения хэш-функции от него и сравнения этого значения с полученным значением хэш-функции. В последних двух схемах ЭЦП с восстановлением сообщения можно положить $H = 1$, т. е. исключить значение хэш-функции из формул проверки и генерации подписи. При таком модифицировании этих схем ЭЦП при практическом использовании потребуется решать проблему подтверждения подлинности восстановленного сообщения, например, с использованием механизмов, рассмотренных несколько выше.

Рассмотрим преобразование схем ЭЦП, задаваемых стандартом ГОСТ Р 34.10–94 и американским стандартом DSS (*см. разд. 3.3*), в схемы с восстановлением сообщения. Проверочное уравнение стандарта DSS может быть преобразовано в следующее соотношение:

$$R = (\alpha^{1/S} y^{F(R,M)/S} \bmod p) \bmod q,$$

где F — произвольная сжимающая функция (например, это может быть хэширующая функция); M — подписываемое сообщение. Выбирая функцию $F(R, M) = M^{-1} R \bmod q$, получаем

$$R = (\alpha^{1/S} y^{M^{-1}R/S} \bmod p) \bmod q \Rightarrow M = \frac{(\alpha^{1/S} y^{M^{-1}R/S} \bmod p)}{RM^{-1}} \bmod q.$$

Из последнего соотношения видно, что если в качестве первого элемента подписи принять значение $R'' = M^{-1} (\alpha^k \bmod p) \bmod q$, то мы получим схему ЭЦП с восстановлением сообщения:

$$M = \frac{(\alpha^{1/S} y^{R''/S} \bmod p) \bmod q}{R''} \bmod q,$$

где подписью является пара чисел (R'', S), а генерация подписи осуществляется в соответствии с формулой $S = \frac{1 + xR''}{k} \bmod q$.

Аналогичные преобразования российского стандарта ГОСТ Р 34.10–94 приведут к схеме ЭЦП с восстановлением сообщения, основанной на проверочном уравнении

$$M = \frac{(\alpha^{S/H} y^{-R''/H} \bmod p) \bmod q}{R''} \bmod q.$$

где при генерации подписи используется формула $S = kH + xR'' \bmod q$. Последние две построенные схемы ЭЦП обладают следующими свойствами:

- восстановление сообщения при проверке подлинности подписи;
- компактный размер подписи;
- стойкость определяется сложностью задачи дискретного логарифмирования.

Однако несмотря на выгодные отличия от схем ЭЦП с восстановлением сообщения, основанных на сложности задачи факторизации, остается следующая проблема. Если размер сообщения превышает значение $|q|$, то требуется перейти к вариантам ЭЦП с увеличенным размером числа q. Соответственно этому будет увеличиваться длина подписи, всегда оставаясь вдвое больше, чем размер сообщения, так как оба параметра подписи имеют размер, примерно равный $|q|$. Учитывая, что информация «содержится» только в элементе подписи R, можно предложить следующий способ оптимизации размера подписи на случай различных размеров сообщения, который основан на использовании сжимающей функции $F(R, M) = M^{-1} R \bmod \delta$, где в качестве модуля δ берутся простые числа с длиной, превышающей $|q|$. Это позволяет сохранить неизменным значение $|q|$, и, соответственно, размер элемента подписи S будет оставаться неизменным при увеличении размера сообщения и длины «информационного» элемента подписи R. За счет увеличения размера элемента R можно внутри подписи передавать более длинные сообщения, причем размер второго элемента подписи будет сохраняться неизменным. В результате получим, что при увеличении размера передаваемых сообщений отношение длины подписи к длине сообщения будет уменьшаться, приближаясь к значению, близкому к 1. Таким образом, для некоторых приложений перспективной представляется схема ЭЦП с уравнениями проверки

$$M = \frac{(\alpha^{U/S} y^{R''/S} \bmod p) \bmod \delta}{R''} \bmod \delta,$$

$$M = \frac{(\alpha^{S/H} y^{-R''/H} \bmod p) \bmod \delta}{R''} \bmod \delta,$$

где $R'' = M^{-1} (\alpha^k \bmod p) \bmod \delta$.

Для того чтобы эта схема не требовала дополнительного указания на выбор значения модуля δ и обеспечивала корректность проверки подписи в случае плавающего размера сообщения, еще требуется решить следующую проблему, которая состоит в корректности выбора модуля δ при проверке подписи. Здесь мы предполагаем, что набор значений модуля δ специфицирован и при проверке подписи выбирается правильное значение δ, т. е. до того как сообщение восстановлено (для подписывающего задача проста — он выбирает минимальное значение δ, удовлетворяющее условию $\delta > M$). Очевидно, что для проверяющего решение о выборе правильного значения δ должно быть связано с размером элемента подписи R. Однако даже для больших значений сообщения (когда формирующий подпись выбирает большие значения δ) могут формироваться значения R, имеющие сравнительно малый размер. Если учесть, что вероятность получить значения R длиной на z бит меньше длины δ равна $\Pr = 2^{-z}$, то можно предложить следующий способ. Пусть специфицировано множество значений $\{\delta_1, \delta_1, \ldots, \delta_n\}$, последовательно увеличивающихся по длине на 8 бит. Тогда проверяющий может выбирать значение $\delta = \min\{\delta_i : \delta_i > R\}$ с вероятностью ошибки 2^{-256}. Если все-таки некоторое значение δ_j выбрано ошибочно (это будет видно из отрицательного результата выполнения процедуры проверки подписи), то следует перейти к значению $\delta = \min\{\delta_i : \delta_i > R, \delta_i \neq \delta_j\}$ и т. д. Таким образом, в этой простой схеме выбора значения модуля δ вычислительные издержки невысоки — одна дополнительная процедура проверки подписи примерно на 250 принятых сообщений. Проблема распознавания значения модуля δ, использованного при формировании подписи, снимается, если в протоколе передачи-приема сообщений оговорить передачу вместе с подписью z дополнительных битов, указывающих на номер использованного модуля δ_i.

Схемы ЭЦП, в которых процедура генерации подписи включает решение системы сравнений (*см. разд. 4.1–4.4*), легко могут быть преобразованы в схемы ЭЦП с восстановлением сообщения, если в проверочном соотношении один из элементов подписи (R, S) или элемент S подписи (k, S) возводится в заранее определенную степень. Обобщенный механизм такого преобразования состоит во встраивании сообщения в указанный элемент подписи, например, в элемент S, который входит в проверочное соотношение в виде S^c.

Это делается путем задания формулы для вычисления значения S в виде $S = M^{c^{-1}}\alpha^{g} \bmod p$, где значение c однозначно задается проверочным соотношением. При этом следует учитывать, что формула для вычисления значения Z по случайно выбираемому числу U должна быть соответствующим образом модифицирована, т. е. с учетом вида фиксируемой функции $F_2(R, S)$ или $F_2(\alpha^k, S)$. Например, если имеем $F_2(R, S) = RS \bmod p$ или $F_2(\alpha^k, S) = \alpha^k / S \bmod p$, то вычисление значения Z, как правило, следует выполнять по формулам $Z = M^{c^{-1}}\alpha^{U} \bmod p$ и $Z = M^{-c^{-1}}\alpha^{U} \bmod p$ соответственно. Рассматривая схемы, приведенные в табл. 4.1–4.2, можно установить, что все, кроме седьмой (девятой), могут быть легко преобразованы в схему с восстановлением сообщения. Этому преобразованию подвергаются также схемы 3, 4 и 6 из табл. 4.3.

Разберем конкретный вариант рассматриваемого преобразования на примере схемы с уравнением проверки подписи $R = y^{H(R\alpha^{g} \bmod p)}\alpha^{g} \bmod p$, где подписью является пара чисел (g, R). Зададим следующую формулу для вычисления параметра $R = M\alpha^{k} \bmod p$. Тогда будем иметь $M\alpha^{k} \equiv$ $\equiv M\, y^{H(M\alpha^{k}\alpha^{g} \bmod p)}\alpha^{g} \bmod p$. Из последнего сравнения видно, что значение M можно представить в виде

$$M = \frac{M\alpha^{k}}{y^{H(M\alpha^{k}\alpha^{g} \bmod p)}\alpha^{g}} \bmod p = \frac{R}{y^{H(R\alpha^{g} \bmod p)}\alpha^{g}} \bmod p.$$

Из последней формулы видно, что условием фиксирования значения функции $F_2(R, g) = M\alpha^{k}\alpha^{g} \bmod p$ является выполнимость сравнения $k + g \equiv$ $\equiv U \bmod \gamma$ (1), а равенство

$$M = \frac{R}{y^{H(R\alpha^{g} \bmod p)}\alpha^{g}} \bmod p \qquad (2)$$

выполняется, если между значениями k и g имеется связь, задаваемая сравнением $k \equiv xHZ + g \bmod \gamma$ (3), где значение Z вычисляется по формуле $Z = M\alpha^{U} \bmod p$. Таким образом, равенство (2) может быть использовано в качестве проверочного соотношения некоторой схемы ЭЦП со следующей процедурой генерации подписи:

1. Выбирается случайное число $U < \gamma$.

2. Вычисляется параметр $Z = M\alpha^{U} \bmod p$.
3. Решается система из сравнений (1) и (3), в результате чего получаем следующие расчетные формулы $k = \frac{U + xHZ}{2} \bmod \gamma$ и $g = \frac{U - xHZ}{2} \bmod \gamma$.
4. По полученным на предыдущем шаге формулам вычисляются значения k и g.
5. Вычисляется второй элемент цифровой подписи: $R = M\alpha^{k} \bmod p$.

Еще несколько вариантов схем ЭЦП с восстановлением сообщения приведено в таблице 4.4.

Таблица 4.4. Схемы ЭЦП с восстановлением сообщения

Проверочное уравнение и формула для вычисления значения R	**Формулы для вычисления значений k и g**	
$M = R\alpha^{-g} y^{(R\alpha^{g} \bmod p)} \bmod p$, $R = M\alpha^{k} \bmod p$	$k = \frac{U - xZ}{2} \bmod \gamma$	$g = \frac{U + xZ}{2} \bmod \gamma$, где $Z = M\alpha^{U} \bmod p$
$M = R^{H} y^{(R\alpha^{g} \bmod p)} \alpha^{g} \bmod p$, $R = M^{1/H}\alpha^{k} \bmod p$	$k = \frac{U + xZ}{1 - H} \bmod \gamma$	$g = \frac{HU + xZ}{H - 1} \bmod \gamma$, где $Z = M^{1/H}\alpha^{U} \bmod p$
$M = R^{-1} y^{(R\alpha^{g} \bmod p)} \alpha^{g} \bmod p$, $R = M^{-1}\alpha^{k} \bmod p$	$k = \frac{U + xZ}{2} \bmod \gamma$	$g = \frac{U - xZ}{2} \bmod \gamma$, где $Z = M^{-1}\alpha^{U} \bmod p$

4.6. Новые схемы ЭЦП с сокращенной длиной подписи

Стандарты DSS и ГОСТ Р 34.10–94, а также схема ЭЦП Шнорра обеспечивают достаточно малый размер цифровой подписи, что является их существенным достоинством для практического использования. Представляет интерес разработка схем с сокращенным размером подписи на основе механиз-

ма генерации подписи с решением системы сравнений. В разд. 4.1 была показана необходимость перехода от подписи вида (R, S) к подписи вида (k, S). При этом было достигнуто существенное сокращение размера подписи (при соответствующем выборе размера показателя γ, к которому относится число α по модулю p). Такой переход выглядит достаточно естественным, поскольку из решения системы сравнений мы предварительно определяем значения k и g, которые имеют размер, примерно равный $|\gamma|$, а затем вычисляем элементы R и S, которые имеют размер $|p|$ (или $|n|$ в зависимости от конкретного типа схемы ЭЦП).

Возникает идея об одновременном переходе от элементов R и S к значениям k и g, что сразу решает проблему сокращения размера подписи (пусть даже с возвращением к возможности экзистенциальной подделки подписи и возможности использования в качестве случайного числа U блока шифртекста, передаваемого вместе с подписью, — эти возможности при необходимости можно нейтрализовать некоторыми дополнительными механизмами протокола ЭЦП). Однако такой переход создает непосредственные предпосылки к вычислению секретных параметров рассматриваемых схем ЭЦП, которые состоят в том, что в известных системах из двух сравнений остаются только два неизвестных значения — x и U в схемах, основанных на сложности дискретного логарифмирования, или γ и U в схемах, основанных на сложности факторизации модуля.

Например, в схеме 4 из табл. 4.2 имеет место сравнение $k \equiv gZ \bmod \gamma$, из которого вытекает $gZ - k \equiv 0 \bmod \gamma \Rightarrow \gamma \mid gZ - k$, т. е., разлагая на множители значение $gZ - k$ и испытывая различные множители в качестве секретного ключа, легко найти истинное его значение. Этот способ вычисления значения γ по известным числам k и g применим ко всем схемам, представленным в табл. 4.2 и 4.3. Даже в случае, когда секретное число γ является достаточно большим (случай схем из табл. 4.3), выполняя эту атаку при использовании многих различных подписей (k, g), с большой вероятностью будет найдена подпись, для которой трудоемкость вычисления секрета γ окажется сравнительно низкой.

В случае схем, основанных на сложности дискретного логарифмирования (см. табл. 4.1), в системе из двух сравнений, определяющих значения k и g, второе сравнение (которое является сравнением первой степени относительно неизвестной величины x) позволяет легко выразить значение секретного ключа x через значения H, Z, k и g.

Эти замечания показывают, что такой прямолинейный подход к построению схем с сокращенным размером подписи не приводит к поставленной цели. Продолжая анализ систем сравнений, по которым вычисляются значения

k и g, можно заметить, что при перестановке в них переменных U и Z образуются системы сравнений, для которых для некоторой гипотетической схемы ЭЦП в процессе формирования подписи по заданным значениям H, Z, U и x однозначно вычисляются (по модулю γ) неизвестные k и g. При этом в предполагаемой атаке по заданным значениям элементов подписи (k, g) неизвестные U и x не могут быть определены однозначно: для произвольно выбранного значения $U < \gamma$ вычисляется единственное значение x. Это обстоятельство объясняется тем, что сравнения вида $f(k, g, Z) \equiv 0$ (А) не имеют прямого отношения к неизвестным U и x (значение U может быть определено по значению Z, но для этого требуется решить сложную задачу дискретного логарифмирования), т. е. переменные U и x входят только в одно из сравнений решаемой системы из двух сравнений, а именно в сравнение вида $f(k, g, H, U, x) \equiv 0$ (Б). Следовательно, поиск схем ЭЦП с сокращенным размером подписи следует проводить в направлении изменения механизма формирования подписи [68], а значит и изменения вида проверочного соотношения.

Рассмотрим конкретный вариант сравнения вида (А), а именно $k + g \equiv Z \bmod \gamma$ (1), где $Z = (\alpha^U \bmod p) \bmod \gamma$. Достаточно очевидно, что значение U, которое определяет величину Z, может быть выражено из сравнения типа (Б), поэтому достаточно естественным конкретным вариантом последнего является следующий: $xk + Hg \equiv U \bmod \gamma$ (2). Теперь попытаемся синтезировать сравнение проверки, задающее схему ЭЦП, в которой процедура генерации подписи основана на решении системы сравнений (1) и (2). Имеем:

$$Z = (\alpha^U \bmod p) \bmod \gamma = (\alpha^{xk+Hg} \bmod p) \bmod \gamma = (\alpha^{xk} \alpha^{Hg} \bmod p) \bmod \gamma. \quad (3)$$

Из (1) и (3) непосредственно следует искомое проверочное сравнение:

$$k + g \equiv (y^k \alpha^{Hg} \bmod p) \bmod \gamma. \quad (4)$$

Для синтеза других схем полезно выяснить особенности механизмов, лежащих в основе функционирования процедур схемы ЭЦП, основанной на проверочном сравнении (4). При знании секрета x мы можем представить выражение в скобках в виде степени основания α, показатель которой равен $U \equiv xk + Hg \bmod \gamma$. Выбирая произвольное значение $U < \gamma$, мы полагаем, что переходим к рассмотрению только таких пар (k, g), где $k < \gamma$ и $g < \gamma$, для которых выполняется сравнение (2) — условие фиксирования показателя степени. Далее мы можем вычислить значение Z, определяемое предварительно выбранной величиной U, т. е. получить конкретное значение правой части сравнения (1) и перейти к решению системы сравнений (1) и (2). Выбирая различные U, мы будем получать различные значения переменной Z и различные значения вычисляемой подписи (как это и должно быть в схеме ЭЦП вероятностного типа).

Уяснив физический смысл сравнения (4) как проверочного соотношения, мы можем перейти к синтезу схем ЭЦП «от идеи», а не от формально записанной системы из двух сравнений. При таком переходе весьма существенно сокращается число неудачных построений. Различные варианты схем ЭЦП с подобным механизмом формирования подписи представлены в табл. 4.5. Применяя метод синтеза «от идеи» для конструирования различных схем ЭЦП и осуществляя их анализ, можно установить следующие качественные моменты [68].

- Сравнение типа (А) можно задать в виде $f(k, g) \equiv Z \bmod \gamma$, где $f(k, g)$ — произвольная функция от аргументов k и g, однако такая, что совместное решение сравнений (А) и (Б) при известном секретном ключе будет достаточно простым. Например, можно использовать схемы с проверочными сравнениями вида $kg \equiv (y^k \alpha^{Hg} \bmod p) \bmod \gamma$ или $k \equiv g(y^k \alpha^{Hg} \bmod p) \bmod \gamma$. При этом вычисление элементов подписи потребует выполнения операции извлечения квадратных корней. Для значительного упрощения процедуры вычисления подписи следует выбрать параметры p и α, для которых можно взять значение $\gamma \equiv 3 \bmod 4$.
- Процедура генерации подписи обладает достаточно низкой трудоемкостью, если в схеме ЭЦП сравнение типа (Б) представляется в виде $f(k, g, H, x) \equiv U \bmod \gamma$, где $f(k, g, H, x)$ — произвольная функция не выше второй степени относительно аргументов k и g. Поэтому правая часть проверочного уравнения может иметь, например, вид $(y^{kg} \alpha^{Hg+k} \bmod p) \bmod \gamma$, $\left((y^k \alpha^H)^g \bmod p\right) \bmod \gamma$ или $(Hy^{g^2} \alpha^{g+k^2} \bmod p) \bmod \gamma$. Каждое из значений y и α должно возводиться в степень, зависящую, по крайней мере, от одного из элементов подписи, причем показатели степени чисел y и α не должны быть в линейной зависимости, в противном случае легко может быть осуществлена подделка подписи (т. е. формирование подписи без использования секретного ключа).
- В качестве левой части проверочного сравнения можно взять единственный элемент k и g. Это позволяет несколько упростить вид проверочного соотношения и формулы, используемые при вычислении подписи.
- Вместо простого модуля в скобках в правой части проверочного сравнения можно использовать модуль RSA. В этом случае в качестве открытого ключа будет использоваться пара значений (n, α), а секрет-

ным будет значение γ. Соответственно, правая часть сравнения проверки может быть записана в виде $(\alpha^{k+Hg} \bmod n) \bmod \delta$, $(\alpha^{k^2+Hg} \bmod n) \bmod \delta$, $(\alpha^{kgH} \bmod n) \bmod \delta$, где $\delta \neq \gamma$, и т. п. (соответствующие условия фиксирования имеют вид $k + Hg \equiv U \bmod \gamma$, $k^2 + Hg \equiv U \bmod \gamma$, $kHg \equiv U \bmod \gamma$ и т. п.).

- При использовании модуля RSA в качестве открытого ключа можно использовать тройку чисел (n, α, y), где $y = \alpha^x \bmod n$. Тогда при формировании подписи используются два секретных значения — γ и x. При этом все проверочные соотношения, задающие стойкие и корректные схемы ЭЦП по простому модулю, могут быть применены и с составным модулем.
- В правой части проверочного соотношения вместо выражения, включающего операцию $Z \bmod \gamma$, например, $(y^k \alpha^{Hg} \bmod p) \bmod \gamma$, можно использовать произвольную сжимающую функцию $F_c(Z)$, например, $F_c(y^k \alpha^{Hg} \bmod p)$, заменяя при этом знак сравнения на знак равенства. В этом случае значения элементов подписи будут вычисляться как результат совместного решения одного уравнения и одного сравнения. В частности, можно использовать следующую сжимающую функцию $F_c(Z) = Z \bmod \delta$, где $\delta \neq \gamma$, или $F_c(Z) = H(Z)$. Отметим, что при использовании произвольной сжимающей функции в качестве левой части проверочного уравнения следует выбрать некоторую линейную комбинацию элементов подписи.

Таблица 4.5. Схемы ЭЦП с сокращенной длиной подписи [68]

№ п/п	Проверочные соотношения	Формулы для вычисления значений k и g	Система решаемых сравнений и выражение для Z
1	$k = (y^k \alpha^{Hg} \bmod p) \bmod \gamma$	$k = Z$; $g = \dfrac{U - xZ}{H} \bmod \gamma$	$\begin{cases} xk + gH \equiv U \bmod \gamma, \\ k = Z; \end{cases}$ $Z = (\alpha^U \bmod p) \bmod \gamma$
2	$kg \equiv \equiv (Hy^k \alpha^{kg} \bmod p) \bmod \gamma$	$k = \dfrac{U - Z}{x} \bmod \gamma$; $g = \dfrac{Zx}{U - Z} \bmod \gamma$	$\begin{cases} xk + kg \equiv U \bmod \gamma, \\ kg \equiv Z \bmod \gamma; \end{cases}$ $Z = (H\alpha^U \bmod p) \bmod \gamma$

№ п/п	Проверочные соотношения	Формулы для вычисления значений k и g	Система решаемых сравнений и выражение для Z
3	$k = gH(y^k\alpha^g \bmod p) \bmod \gamma$	$k = \frac{UHZ}{xHZ+1} \bmod \gamma;$ $g = \frac{U}{xHZ+1} \bmod \gamma$	$\begin{cases} xk + g \equiv U \bmod \gamma, \\ k \equiv gHZ \bmod \gamma; \end{cases}$ $Z = (\alpha^U \bmod p) \bmod \gamma$
4*	$M = k(y^k\alpha^{gH} \bmod p) \bmod \gamma$	$k = \frac{M}{Z} \bmod \gamma;$ $g = \frac{UZ - xM}{HZ} \bmod \gamma$	$\begin{cases} xk + gH \equiv U \bmod \gamma, \\ M \equiv kZ \bmod \gamma; \end{cases}$ $Z = (\alpha^U \bmod p) \bmod \gamma$
5*	$M = \frac{g(y^k\alpha^g \bmod p)}{k} \bmod \gamma$	$k = \frac{UZ}{xZ+M} \bmod \gamma;$ $g = \frac{UM}{xZ+M} \bmod \gamma$	$\begin{cases} xk + g \equiv U \bmod \gamma, \\ M \equiv k^{-1}gZ \bmod \gamma; \end{cases}$ $Z = (\alpha^U \bmod p) \bmod \gamma$
6*	$M = g(\alpha^{gk^2} \bmod n) \bmod \delta,$ где $\delta \neq \gamma$	$g = \frac{M}{Z} \bmod \delta;$ $k = \pm\sqrt{\frac{U}{g}} \bmod \gamma$	$\begin{cases} gk^2 \equiv U \bmod \gamma, \\ M \equiv gZ \bmod \delta; \end{cases}$ $Z = (\alpha^U \bmod p) \bmod \delta$
7	$k = (H\alpha^{g^2+k^2} \bmod n) \bmod \delta,$ где $\delta \neq \gamma$	$k = Z;$ $g = \pm\sqrt{U - Z^2} \bmod \gamma$	$\begin{cases} g^2 + k^2 \equiv U \bmod \gamma, \\ k = Z; \end{cases}$ $Z = (H\alpha^U \bmod p) \bmod \delta$
8*	$M = \frac{Hy^k\alpha^g \bmod p}{k} \bmod \gamma$	$k = \frac{Z}{M} \bmod \gamma;$ $g = \frac{UM - xZ}{M} \bmod \gamma$	$\begin{cases} xk + g = U \bmod \gamma, \\ M \equiv k^{-1}Z \bmod \gamma; \end{cases}$ $Z = (H\alpha^U \bmod p) \bmod \gamma$
9	$k = H(\alpha^{kgH} \bmod n) \bmod \delta,$ где $\delta \neq \gamma$	$k = (HZ) \bmod \delta;$ $g = \frac{U}{kH} \bmod \gamma$	$\begin{cases} kgH \equiv U \bmod \gamma, \\ k \equiv HZ \bmod \delta; \end{cases}$ $Z = \alpha^U \bmod n$

* Схемы ЭЦП с восстановлением сообщения.

Полезно отметить другой способ генерации подписи в рассматриваемых схемах ЭЦП, применимый в случае, когда в проверочном соотношении в левой части присутствует только один элемент подписи, например g. Он аналогичен механизму формирования подписи в схеме Эль-Гамаля. Рассмотрим для примера схему 1 из табл. 4.5. Для генерации подписи можно поступить следующим образом. Вычислим значение k, используя случайно выбранное число t и формулу $k = (\alpha^t \bmod p) \bmod \gamma$. При таком представлении этого элемента подписи имеем: $(\alpha^t \bmod p) \bmod \gamma = (y^k \alpha^{lg} \bmod p) \bmod \gamma$, следовательно, имеем следующую формулу для вычисления второго элемента подписи: $g = \dfrac{t - xk}{H} \bmod \gamma$. Этот подход к формированию подписи применим также к схемам 6, 7 и 8 из табл. 4.5. В случае схемы 8 значение k следует представить в виде $k = M^{-1}(H\alpha^t \bmod p) \bmod \gamma$, после чего уравнение генерации подписи может быть легко получено в виде: $g = t - xk \bmod \gamma$. Однако универсальным для рассмотренного класса схем ЭЦП является способ генерации подписи, основанный на решении системы сравнений.

4.7. Новый подход к уменьшению размера подписи до 160 бит

Для практического использования представляют интерес схемы с минимальным размером подписи при обеспечении требуемого уровня стойкости. В предыдущем разделе были рассмотрены новые схемы ЭЦП, обеспечивающие достаточно малый размер подписи. При заданном уровне безопасности длина подписи в новых схемах примерно такая же, как и в ЭЦП Шнорра, стандартах DSS и ГОСТ Р 34.10–94. При уровне стойкости ЭЦП соответствующей сложности подделки подписи, равной $\approx 2^{80}$ операций возведения в степень по модулю, размер подписи равен 320 бит. Вопрос дальнейшего уменьшения размера подписи связан с применением новых механизмов построения схем ЭЦП, позволяющих устранить атаки, использующие парадокс дней рождения или возможность оптимизации полного перебора (как это делается, например, при вычислении дискретного логарифма методом больших и малых шагов). В связи с этим представляют интерес схемы ЭЦП с сокращенной подписью, основанные на сложности факторизации числа $n = rq$, равного произведению двух больших неизвестных простых чисел. Такими примерами являются схемы с открытым ключом вида (α, n) из *разд. 4.6*. Они являются стойкими в предположении о том, что задача разложения числа n при правильно выбранном значении α является трудной.

В этих схемах секретный ключ γ, представляющий собой порядок группы, генерируемой числом α, должен быть увеличен вдвое по сравнению с размером, достаточным для предотвращения атак на основе угадывания значения γ или на основе полного перебора. Это связано с тем, что число γ должно быть составным и содержать в качестве своих сомножителей, по крайней мере, по одному большому множителю из разложений чисел $r-1$ и $q-1$, т. е. $\gamma=\gamma'\gamma''$, где $\gamma'|r-1$ и $\gamma''|q-1$. Для разложения числа n с использованием известного значения α может быть применено вычисление наибольшего общего делителя чисел n и $(\alpha^{l} \bmod n)-1$. В этом способе факторизации методом последовательного перебора требуется найти такое значение i_0, при котором выполняется соотношение НОД$(\alpha^{i_0} \bmod n-1, n)\neq 1$ (в этом случае НОД равен либо r, либо q). Если задается уровень стойкости $\approx 2^{80}$ операций, то длина каждого из чисел γ' и γ'' должна быть равна 80 бит, т. е. имеем $|\gamma|\approx 160$ бит. Таким образом, элементы подписи (k, g) вычисляются по 160-битовому модулю, что определяет размер подписи, равный 320 бит. Особенностью схем с открытым ключом типа (α, n) является то, что удвоение размера элементов подписи связано не с атаками, использующими парадокс дней рождения, а с атаками, использующими параметр α для факторизации модуля n. Другой способ устранения возможности разложения модуля n связан с использованием простого значения γ, такого что $\gamma|r-1$ и $\gamma|q-1$, однако в этом случае секретное значение γ может быть найдено как делитель числа $n-1$. Если бы удалось найти некоторые конструктивные механизмы, обеспечивающие секретность простого порядка числа α, то можно было бы надеяться, что удастся разработать схемы ЭЦП с 80-битовыми элементами подписи, обеспечивающие указанный уровень безопасности.

Эту возможность можно попытаться реализовать с использованием трехуровневых проверочных соотношений. Идея состоит в следующем. Элементы подписи вычисляются по модулю третьего (верхнего) уровня, который является простым числом γ длины $|\gamma|\approx 80$ бит (мы рассматриваем принятый выше уровень безопасности; если его увеличить до значения $\approx 2^{96}$ или $\approx 2^{128}$ операций, то следует перейти к $|\gamma|\approx 96$ или 128 бит соответственно). При этом γ является показателем по секретному модулю q (модуль второго уровня) некоторого числа β. Чтобы обеспечить проверяющему возможность выполнения вычислений на втором уровне, ему предоставляется модуль $n=rq$, где $|r|\approx 512$ бит и $|q|\approx 512$ бит (при таких размерах делителей n сложность разложения n соответствует принятому уровню стойкости ЭЦП). Разложение n является секретным, однако тот факт, что число β является известным, не может быть использован для разложения этого модуля, поскольку β является генератором группы простого порядка по секретному модулю q. Отметим, что полезно выбрать такое β, которое относится по модулю n к большому,

например 384-битовому или 512-битовому, составному показателю. Предполагается, что при генерации подписи вычисления на втором уровне осуществляются по модулю q, а при проверке подписи — по модулю n. Чтобы вычисления по модулю n дали возможность проверить соответствие их результатов результатам вычислений по модулю q, вычисления первого типа надо взять по модулю q. Так как q является элементом секретного ключа, то указанное приведение делается «скрытно» (косвенно) путем выполнения вычислений на первом (нижнем) уровне по простому модулю, которые представляют собой возведение в степень числа α по простому модулю $p = 2rq + 1$, где α представляет собой число, относящееся по модулю p к показателю q (именно благодаря этому вычисления по модулю n приводятся скрытно к вычислениям по модулю q). Таким образом, открытым ключом является тройка чисел (α, β, p), а секретным — пара чисел (γ, q), где имеют место следующие соотношения: $\gamma | q - 1$, $q | (p-1)/2$, $\alpha^q \bmod p = 1$, $\beta^\gamma \bmod q = 1$, $\beta^\gamma \bmod n \neq 1$.

Уяснив эту конструктивную идею, легко составить конкретные варианты реализации схем с 80-битовыми элементами подписи (k, g).

Вариант 1 описывается следующим проверочным соотношением:

$$k - g = (\alpha^{\beta^{kgH} \bmod n} \bmod p) \bmod \delta,$$

где операция $\bmod \delta$ играет роль сжимающей функции. Вычисление подписи осуществляется на основе решения следующей системы соотношений:

$$\begin{cases} k - g = Z, \\ kgH \equiv U \bmod \gamma, \end{cases}$$

в которой значение $U < \gamma$ выбирается случайно, а значение Z вычисляется по формуле $Z = (\alpha^{\beta^{U} \bmod q} \bmod p) \bmod \delta$. Решение системы дает следующие формулы для вычисления элементов подписи: $g = -Z/2 \pm$ $\pm\sqrt{Z^2/4 + U/H} \bmod \gamma$ и $k = Z + g$.

Вариант 2 описывается следующим проверочным соотношением:

$$k = (\alpha^{\beta^{kgH} \bmod n} \bmod p) \bmod \delta,$$

где операция $\bmod \delta$ играет роль сжимающей функции. Вычисление подписи осуществляется на основе решения следующей системы соотношений:

$$\begin{cases} k = Z, \\ kgH \equiv U \bmod \gamma, \end{cases}$$

в которой значение $U < \gamma$ выбирается случайно, а значение Z вычисляется по формуле $Z = (\alpha^{\beta^{U} \bmod q} \bmod p) \bmod \delta$. Первый элемент подписи получаем непосредственно: $k = Z$, а второй находим по формуле $g = (kH)^{-1} U \bmod \gamma$. Во втором варианте сложность процедуры вычисления подписи в среднем примерно в 3 раза ниже по сравнению с первым вариантом. Это связано с тем, что во втором варианте не требуется выполнения операций извлечения квадратного корня (если $\gamma \equiv 3 \bmod 4$, то операция извлечения корня в первом варианте сводится к операции модульного возведения в степень; кроме того, с вероятностью 50% подкоренное выражение будет квадратичным невычетом). В обоих вариантах возможна следующая теоретическая атака. По известной подписи атакующий вычисляет значение $Y = \beta^{kgH} \bmod n$, вычисляет $X = \log_{\beta} Y \pmod n$ и находит значение γ как делитель числа $kgH - X$. Если бы порядок числа β по модулю n был бы сравнительно малым, то такая атака могла бы быть реализована практически (найти дискретный логарифм без знания порядка числа β можно, например, используя несколько модифицированный метод больших и малых шагов). В связи с этим требуется выбирать такое значение параметра β, чтобы он относился по модулю n к показателю достаточно большого размера.

Вариант 3 описывается следующим проверочным соотношением:

$$k = \left(\alpha^{\beta^{kg} \bmod n} \bmod p \right)^{H} \bmod \delta,$$

где операция $\bmod \delta$ играет роль сжимающей функции. Вычисление подписи осуществляется на основе решения следующей системы соотношений:

$$\begin{cases} k = Z, \\ kg \equiv U \bmod \gamma, \end{cases}$$

в которой значение $U < \gamma$ выбирается случайно, а значение Z вычисляется по формуле $Z = \left(\alpha^{\beta^{U} \bmod q} \bmod p \right)^{H} \bmod \delta$.

Вариант 4 отличается использованием двух проверочных соотношений при осуществлении проверки подлинности подписи:

$$R = \alpha^{\beta^{kgH} \bmod n} \bmod p,$$

где $k = H(HR \bmod p) \bmod \delta$.

В этом примере предполагается, что проверяющий по подписи (k, g) вычисляет значение R, а затем по значению R вычисляет значение k', которое должно быть равно значению k. Генерация подписи осуществляется следующим образом. Выбирается случайное значение $U < \gamma$, вычисляется $R = \alpha^{\beta^U \bmod q} \bmod p$ и $k = H(HR \bmod p) \bmod \delta$, после чего определяется второй элемент подписи: $g = \dfrac{U}{kH} \bmod \gamma$.

Вариант 5 представляет собой комбинирование варианта 4 с вычислением подписи на основе решения системы из двух сравнений. Проверочное уравнение имеет вид:

$$R = \alpha^{\beta^{kg} \bmod n} \bmod p,$$

где $k = \left(R^{(H\beta^g \bmod n)} \bmod p \right) \bmod \delta$.

При проверке подписи (k, g) вычисляется значение R, а затем по значению R вычисляется значение k'. Если подпись подлинная, то должно выполняться равенство $k' = k$. Генерация подписи осуществляется следующим образом. Выбирается случайное значение $T < \gamma$ и вычисляется значение $k = \left(\alpha^{(H\beta^T \bmod q)} \bmod p \right) \bmod \delta$. Вычисление подписи осуществляется на основе решения следующей системы соотношений:

$$\begin{cases} U + g \equiv T \bmod \gamma, \\ kg \equiv U \bmod \gamma, \end{cases}$$

где неизвестными являются значения U и g. Последнее значение вычисляется по формуле: $g = \dfrac{T}{k+1} \bmod \gamma$.

Представляет интерес вопрос о способах вычисления секретного значения γ, которые позволили бы избежать решения задачи факторизации модуля n. Покажем, что такие атаки в определенном смысле имеют сложность не ниже сложности факторизации n при известном открытом ключе (α, β, p). Допустим, что в результате такой атаки удалось вычислить значение γ. Тогда разложение n находится очень легко путем вычисления НОД$(\beta^\gamma \bmod n - 1, n) = q$. Это означает, что трудоемкость разложения n на простые множители не выше трудоемкости нахождения секретного элемента γ.

Если в структуру открытого ключа внести еще один элемент — $y = \beta^x \bmod p$, то возможно составление схем ЭЦП другого типа, в которых элементы подписи также имеют длину 80 бит. Рассмотрим несколько примеров.

Вариант 6 представлен проверочным уравнением вида:

$$k - g = \left(\alpha^{(\beta^{gH} y^k \bmod n)} \bmod p \right) \bmod \delta.$$

Процедура формирования подписи включает выбор случайного значения $U < \gamma$, вычисление значения $Z = \left(\alpha^{\beta^U \bmod q} \bmod p \right) \bmod \delta$ и решение следующей системы соотношений:

$$\begin{cases} k - g = Z, \\ gH + xk \equiv U \bmod \gamma, \end{cases}$$

Решение системы дает следующие формулы для вычисления элементов подписи: $g = \dfrac{U - xZ}{H + x} \bmod \gamma$ и $k = g + Z$.

Вариант 7 представлен проверочным уравнением вида:

$$k = \left(\alpha^{(\beta^{gH} y^k \bmod n)} \bmod p \right) \bmod \delta.$$

Этот вариант является упрощением варианта 6, благодаря чему процедура подписи может быть реализована двумя способами. Первый способ аналогичен процедуре генерации подписи предыдущей схемы ЭЦП и включает выбор случайного значения $U < \gamma$, вычисление значения первого элемента подписи $k = \left(\alpha^{\beta^U \bmod q} \bmod p \right) \bmod \delta$. Второй элемент подписи вычисляется из условия: $g = \dfrac{U - xk}{H} \bmod \gamma$. Второй способ реализации процедуры вычисления подписи основан на представлении первого элемента подписи в виде $k = \left(\alpha^{\beta^W \bmod q} \bmod p \right) \bmod \delta$, где значение $W < \gamma$ выбирается случайным образом. Значение второго элемента подписи определяется из соотношения $gH + xk \equiv W \bmod \gamma$: $g = \dfrac{W - xk}{H} \bmod \gamma$. Оба способа привели к одинаковым формулам для вычисления g. Отметим, что в варианте 6 второй способ генерации подписи неприменим.

Вариант 8 представлен следующими двумя проверочными уравнениями:

$$R = \alpha^{(\beta^g y^{kH} \bmod n)} \bmod p \text{ и } k = \left(R^{(\beta^g \bmod n)} \bmod p \right) \bmod \delta.$$

В этом примере предполагается, что проверка подписи (k, g) включает вычисление значения R, которое затем используется для вычисления числа k', которое в случае подлинной подписи должно быть равно значению k. Генерация подписи осуществляется следующим образом. Выбирается случайное число $T < \gamma$ и вычисляется значение первого элемента подписи $k = \left(R^{\beta^T \bmod q} \bmod p \right) \bmod \delta$. Второй элемент подписи вычисляется в результате решения следующей системы сравнений:

$$\begin{cases} U + g \equiv T \bmod \gamma, \\ g + kxH \equiv U \bmod \gamma, \end{cases}$$

где неизвестными являются значения U и g. Решая систему, получаем: $g = \dfrac{T - kxH}{2} \bmod \gamma$.

В схемах ЭЦП с сокращенным размером подписи обычно формируется двухэлементная подпись с элементами примерно одинакового размера. Однако в общем случае для заданного уровня стойкости элементы подписи могут иметь различный размер. Например, для уровня безопасности 2^z операций в схеме стандарта DSS можно выбрать следующие длины компонентов подписи: $|R'| \approx z$ бит и $|S| \approx 2z$ бит. В самом стандарте такая возможность не специфицирована, поэтому ее реализация требует использования следующего немного модифицированного проверочного уравнения:

$$R = (\alpha^{H/S} y^{R/S} \bmod p) \bmod \delta,$$

где δ — простое число размера $|\delta| \approx z$ бит (в стандарте специфицировано значение $\delta = q$, где q — показатель, к которому относится по модулю p число α).

Варианты 1 – 8 (и аналогичные им), представляющие попытки построения схем ЭЦП с сокращением обоих элементов подписи до размера z бит, могут служить основой для заданий для курсового или дипломного проектирования по исследованию их стойкости (разработке методов и алгоритмов вычисления секретного значения γ). В частности, можно показать, что варианты 1 – 8 позволяют сократить до значения z бит длину только одного из элементов подписи, поскольку имеются способы нахождения γ с трудоемкостью $\approx |\gamma| \sqrt{2^{|\gamma|}}$ операций сравнения при используемой памяти $\approx |p| \sqrt{2^{|\gamma|}}$ бит.

ГЛАВА 5

Варианты заданий для курсового проектирования

Выполнение работ по курсовому проектированию является важным этапом инженерной подготовки. Представляется целесообразным выдавать задания по таким темам, которые развивают умение пользоваться математическим аппаратом и одновременно углубляют понимание идей, на основе которых функционируют криптосистемы. Темы заданий для курсового проектирования могут быть выбраны из основных разделов криптографии, включенных в программу вузовской подготовки специалистов. Например, темы могут быть сформулированы в соответствии со следующими разделами:

1. Разработка и программная реализация (n, k)-пороговых схем разделения секрета на основе многочленов над конечными полями.
2. Разработка и программная реализация (n, k)-пороговых схем разделения секрета на основе китайской теоремы об остатках.
3. Разработка и/или анализ схем электронной цифровой подписи на основе сложности задачи дискретного логарифмирования.
4. Разработка и/или анализ схем электронной цифровой подписи, основанных на сложности задачи факторизации больших чисел специального вида.
5. Разработка и/или анализ симметричных шифров блочного типа на основе заданного перечня примитивов и характеристик.
6. Разработка и/или анализ симметричных шифров поточного типа на основе заданного перечня примитивов и требуемых характеристик.
7. Разработка и/или анализ хэш-функций.
8. Разработка алгоритмов факторизации. дискретного логарифмирования, извлечения корней по модулю, относящихся к заданным частным случаям параметров задачи.
9. Оптимизация вычислительных алгоритмов для реализации операций над большими числами.

Из данного списка мы уделим детальное внимание вариантам курсовых заданий, относящихся к тематике электронной цифровой подписи. Ниже предлагаются конкретные задания по этому разделу криптографии. Задачей курсового проектирования является проработка схемы ЭЦП, заданной проверочным уравнением.

Ниже в таблицах приведены схемы различного типа, сгруппированные по следующим признакам: 1) тип сложной задачи, положенной в основу схемы; 2) размер подписи; 3) наличие свойства восстановления сообщения при верификации подписи.

Задание для курсового проектирования включает:

- общую характеристику и обоснование схемы ЭЦП, построенной на основе заданного проверочного уравнения;
- описание процедуры генерации подписи и формулирование требований к ней;
- оценку стойкости и безопасных размеров параметров криптосхемы;
- вывод формул для вычисления параметров k и g;
- анализ схемы на наличие слабостей и поиск вариантов усиления с минимальным модифицированием;
- рассмотрение возможности экзистенциальной подделки подписи;
- рассмотрение возможности сокращения размера подписи;
- рассмотрение необходимости дополнительных требований к выбору параметров схемы ЭЦП;
- рассмотрение необходимости дополнительных требований к генерации ключей;
- рассмотрение возможности преобразования в схему ЭЦП с восстановлением сообщения;
- критический анализ на 1) наличие избыточных операций в процедурах генерации и проверки подписи, 2) несоответствие длины открытого ключа и подписи достигаемому уровню стойкости;
- программную реализацию схемы и генерацию примера работы схемы с искусственно уменьшенным размером значений ее параметров (с учетом программной реализации дополнительные варианты могут быть сформированы путем задания 1) разных размеров для основных параметров схемы, 2) различных способов их генерации, 3) различной структуры чисел, используемых как модули и т. д.).

5.1. Схемы ЭЦП на основе сложности дискретного логарифмирования

В заданных ниже вариантах схем цифровой подписи используются следующие параметры: $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся к некоторому простому показателю γ по модулю p; (k, S) — подпись. Общая схема генерации ключа: выбирается случайное число U, по которому вычисляется значение Z (обычно $Z = \alpha^U \bmod p$, однако в некоторых вариантах используется другая формула, которая указана в примечании), по значениям U и Z вычисляются значения k и g, последнее из которых определяет элемент подписи S (обычно $S = \alpha^g \bmod p$, хотя может быть реализована процедура формирования подписи, в которой $S = y^g \bmod p$).

1	Проверочное сравнение	$\alpha^k y^{H(Sa^k \bmod p)} \equiv S \bmod p$
	Значения параметров k и g	$k = \frac{U - xHZ}{2} \bmod \gamma;\ g = \frac{U + xHZ}{2} \bmod \gamma$
2	Проверочное сравнение	$\alpha^k y^{H(Sa^k \bmod q)} \equiv S \bmod p$
	Значения параметров k и g	$k = \frac{U - xHZ}{2} \bmod \gamma;\ g = \frac{U + xHZ}{2} \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ S \equiv \alpha^g \bmod (pq)$
3	Проверочное сравнение	$y^{Hk+(Sa^k \bmod q)} \equiv S \bmod p$
	Значения параметров k и g	$k = \frac{U - xZ}{xH + 1} \bmod \gamma;\ g = \frac{xHU + xZ}{xH + 1} \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ S \equiv \alpha^g \bmod (pq)$
4	Проверочное сравнение	$y^{Hk+(\alpha S^k \bmod p)} \equiv S \bmod p$
	Значения параметров k и g	$k = \frac{-xZ \pm \sqrt{x^2Z^2 + 4xHU}}{2xH} \bmod \gamma;$ $g = xHk + xZ \bmod \gamma$
	Примечание	$Z = \alpha^{U+1} \bmod p$

5	Проверочное сравнение	$S^{Hk} \equiv y^{(S\alpha^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{HU \pm \sqrt{H^2U^2 - 4HxZ}}{2H} \bmod \gamma;$ $g = U - k \bmod \gamma$
6	Проверочное сравнение	$S^{Hk} \equiv \alpha^{(Sy^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{UH \pm \sqrt{U^2H^2 - 4xHZ}}{2xH} \bmod \gamma;$ $g = U - xk \bmod \gamma$
7	Проверочное сравнение	$S^{Hk} \equiv \alpha^{(Sy^k \bmod q)} \bmod p$
	Значения параметров k и g	$k = \dfrac{UH \pm \sqrt{U^2H^2 - 4xHZ}}{2xH} \bmod \gamma;$ $g = U - xk \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ S \equiv \alpha^g \bmod (pq)$
8	Проверочное сравнение	$S^{Hk} \equiv y^{(S\alpha^k \bmod q)} \bmod p$
	Значения параметров k и g	$k = \dfrac{HU \pm \sqrt{H^2U^2 - 4HxZ}}{2H} \bmod \gamma;$ $g = U - k \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ S \equiv \alpha^g \bmod (pq)$
9	Проверочное сравнение	$S\alpha^k \equiv \alpha^{H(y^k / S \bmod q)} \bmod p$
	Значения параметров k и g	$k = \dfrac{HZ + U}{x + 1} \bmod \gamma;\ g = \dfrac{xHZ - U}{x + 1} \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ S \equiv \alpha^g \bmod (pq)$
10	Проверочное сравнение	$S\alpha^k \equiv \alpha^{H(y^k / S \bmod p)} \bmod p$

	Значения параметров k и g	$k = \frac{HZ+U}{x+1} \bmod \gamma;\ \ g = \frac{xHZ-U}{x+1} \bmod \gamma$
11	Проверочное уравнение	$S = \alpha^{(y^k S \bmod p)+kH} \bmod p$
	Значения параметров k и g	$k = \frac{U-Z}{x+H} \bmod \gamma;\ \ g = \frac{xZ+UH}{x+H} \bmod \gamma$
12	Проверочное уравнение	$y = S^{(\alpha^k S \bmod p)+kH} \bmod p$
	Значения параметров k и g	$k = \frac{HU-Z \pm \sqrt{(HU-Z)^2 - 4H(x-ZU)}}{2H} \bmod \gamma;$ $g = U - k \bmod \gamma$
13	Проверочное уравнение	$y = S^{(\alpha^k S \bmod q)+kH} \bmod p$
	Значения параметров k и g	$k = \frac{HU-Z \pm \sqrt{(HU-Z)^2 - 4H(x-ZU)}}{2H} \bmod \gamma;$ $g = U - k \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ \ S \equiv \alpha^g \bmod (pq)$
14	Проверочное уравнение	$y = S^{(\alpha^k S \bmod q)k+H} \bmod p$
	Значения параметров k и g	$k = \frac{UZ-H \pm \sqrt{(UZ-H)^2 + 4Z(UH-x)}}{2Z} \bmod \gamma;$ $g = U - k \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ \ S \equiv \alpha^g \bmod (pq)$
15	Проверочное уравнение	$y = (S^{(\alpha^k S \bmod p)k+H} \bmod p) \bmod q$
	Значения параметров k и g	$k = \frac{UZ-H \pm \sqrt{(UZ-H)^2 + 4Z(HU-x)}}{2Z} \bmod \gamma;$ $g = U - k \bmod \gamma$
	Примечание	$y = (\alpha^x \bmod p) \bmod q$

16	Проверочное сравнение	$Sy^k \equiv \alpha^{(S^k \bmod q)} \bmod p$
	Значения параметров k и g	$k = \dfrac{Z \pm \sqrt{Z^2 - 4xU}}{2x} \bmod \gamma;\ \ g = Z - xk \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ S \equiv \alpha^g \bmod (pq);\ Z = \alpha^U \bmod q$
17	Проверочное сравнение	$(Sy)^k \equiv \alpha^{(S\alpha^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{U+x}{2} \pm \sqrt{\dfrac{(U+x)^2}{4} - Z} \bmod \gamma;$ $g = U - k \bmod \gamma$
	Примечание	Возможна подделка подписи с использованием представления параметра S в виде $S = y^{-1}\alpha^g \bmod p$
18	Проверочное сравнение	$(Sy)^k \equiv \alpha^{(S^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{Z-U}{x} \bmod \gamma;\ \ g = \dfrac{Ux}{Z-U} \bmod \gamma$
19	Проверочное уравнение	$y = (S^{(\alpha^k / S \bmod p)+k+H} \bmod p) \bmod q$
	Значения параметров k и g	$k = \dfrac{U-Z-H}{2} \pm \sqrt{\dfrac{(U-Z-H)^2}{4} + (UZ + UH + x)}$ $\bmod \gamma;\ \ g = k - U \bmod \gamma$
	Примечание	Схема с открытым ключом малого размера: $y = (\alpha^x \bmod p) \bmod q$
20	Проверочное уравнение	$y = (S^{(\alpha^{-k} S \bmod p)kH} \bmod p) \bmod q$
	Значения параметров k и g	$k = \dfrac{-UZH \pm \sqrt{(UZH)^2 + 4xZH}}{2ZH} \bmod \gamma;$ $g = U + k \bmod \gamma$

	Примечание	Схема с открытым ключом малого размера: $y = (\alpha^x \bmod p) \bmod q$
21	Проверочное уравнение	$y = (S^{(\alpha^k S \bmod p)H} \bmod p) \bmod q$
	Значения параметров k и g	$k = U - \frac{x}{ZH} \bmod \gamma;\ g = \frac{x}{ZH} \bmod \gamma$
	Примечание	$y = (\alpha^x \bmod p) \bmod q$
22	Проверочное уравнение	$y = (S^{(H\alpha^k S \bmod p)} \bmod p) \bmod q$
	Значения параметров k и g	$k = U - \frac{x}{Z} \bmod \gamma;\ g = \frac{x}{Z} \bmod \gamma$
	Примечание	$Z = H\alpha^{U} \bmod p;\ y = (\alpha^x \bmod p) \bmod q$
23	Проверочное уравнение	$y = (S^{kH}\alpha^{(\alpha^k S \bmod p)} \bmod p) \bmod q$
	Значения параметров k и g	$k = \frac{UH \pm \sqrt{U^2H^2 + 4H(Z-x)}}{2H} \bmod \gamma;$ $g = U - k \bmod \gamma$
	Примечание	Схема с открытым ключом малого размера: $y = (\alpha^x \bmod p) \bmod q$
24	Проверочное уравнение	$y = (\alpha S^{(S^k H \bmod p)} \bmod p) \bmod q$
	Значения параметров k и g	$k = \frac{UZ}{x-1} \bmod \gamma;\ g = \frac{x-1}{Z} \bmod \gamma$
	Примечание	$Z = H\alpha^{U} \bmod p;\ y = (\alpha^x \bmod p) \bmod q$
25	Проверочное уравнение	$y = (\alpha S^{k(S^H{}^k \bmod p)} \bmod p) \bmod q$
	Значения параметров k и g	$k = \pm\sqrt{\frac{(x-1)H}{UZ}} \bmod \gamma;\ g = \frac{x-1}{kZ} \bmod \gamma$
	Примечание	$y = (\alpha^x \bmod p) \bmod q$

26	Проверочное уравнение	$y = (\alpha^{H(S\alpha^k \bmod q)} S^k \bmod p) \bmod \delta$
	Значения параметров k и g	$k = \frac{U}{2} \pm \sqrt{\frac{U^2}{4} + (HZ - x)} \bmod \gamma;$ $g = U - k \bmod \gamma$
	Примечание	$y = (\alpha^x \bmod p) \bmod \delta;\ S = \alpha^g \bmod (pq)$
27	Проверочное уравнение	$y = ((\alpha S)^{(HS^k \bmod p)} \bmod p) \bmod q$
	Значения параметров k и g	$k = \frac{UZ}{x - Z} \bmod \gamma;\ g = \frac{x - Z}{Z} \bmod \gamma$
	Примечание	$y = (\alpha^x \bmod p) \bmod q;\ Z = H\alpha^U \bmod p$
28	Проверочное сравнение	$y^H \equiv (\alpha S)^{(S^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \frac{UZ}{Hx - Z} \bmod \gamma;\ g = \frac{Hx - Z}{Z} \bmod \gamma$
29	Проверочное сравнение	$\alpha^H \equiv Sy^{(S^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \frac{U}{H - xZ} \bmod \gamma;\ g = H - xZ \bmod \gamma$
30	Проверочное уравнение	$y = (\alpha S)^{(HS^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \frac{UZ}{x - Z} \bmod \gamma;\ g = \frac{x - Z}{Z} \bmod \gamma$
	Примечание	$Z = H\alpha^U \bmod p$
31	Проверочное сравнение	$y^H \equiv (\alpha S)^{(\alpha^k S \bmod p)} \bmod p$
	Значения параметров k и g	$k = \frac{UZ - xH + Z}{Z} \bmod \gamma;\ g = \frac{Hx - Z}{Z} \bmod \gamma$
32	Проверочное сравнение	$y^k \equiv S\alpha^{(H\alpha^k S \bmod p)} \bmod p$

	Значения параметров k и g	$k = \frac{U+Z}{x+1} \bmod \gamma;\ \ g = \frac{Ux-Z}{x+1} \bmod \gamma$
	Примечание	$Z = H\alpha^{U} \bmod p$
33	Проверочное сравнение	$S^{H} \equiv y^{(\alpha^{k} S \bmod p)} \bmod p$
	Значения параметров k и g	$k = \frac{UH-xZ}{H} \bmod \gamma;\ \ g = \frac{xZ}{H} \bmod \gamma$
34	Проверочное сравнение	$Sy \equiv \alpha^{(Hy^{k} S \bmod q)} \bmod p$, где $y = \alpha^{x} \bmod (pq)$
	Значения параметров k и g	$k = U + 1 - \frac{Z}{x} \bmod \gamma;\ \ g = \frac{Z-x}{x} \bmod \gamma$
	Примечание	$\alpha^{\gamma} \equiv 1 \bmod q;\ S = y^{g} \bmod (pq);\ Z = Hy^{U} \bmod q$
35	Проверочное сравнение	$S^{(H\alpha^{k} S \bmod p)} \equiv y^{(\alpha^{k} S \bmod p)} \bmod p$
	Значения параметров k и g	$k = U - xZ / Z' \bmod \gamma;\ \ g = xZ / Z' \bmod \gamma$
	Примечание	$Z' = H\alpha^{U} \bmod p$
36	Проверочное сравнение	$S^{(\alpha^{-k} S \bmod p)} \equiv y^{(H\alpha^{k} S^{-1} \bmod p)} \bmod p$
	Значения параметров k и g	$k = -U + xZ' / Z \bmod \gamma;\ \ g = xZ' / Z \bmod \gamma$
	Примечание	$Z' = HZ^{-1} \bmod p$
37	Проверочное сравнение	$S^{(y^{k} S^{H} \bmod p)} \equiv \alpha^{(y^{-k} S^{-H} \bmod p)} \bmod p$
	Значения параметров k и g	$k = \frac{UZ - HZ'}{Zx} \bmod \gamma;\ \ g = Z' / Z \bmod \gamma$
	Примечание	$Z' = Z^{-1} \bmod p$
38	Проверочное сравнение	$S^{(H\alpha^{k} S \bmod q)} \equiv y^{(\alpha^{k} S \bmod p)} \bmod p$
	Значения параметров k и g	$k = U - xZ / Z' \bmod \gamma;\ \ g = xZ / Z' \bmod \gamma$

	Примечание	$\alpha^{\gamma} \equiv 1 \bmod q$; $S \equiv \alpha^{g} \bmod (pq)$; $Z' = H\alpha^{U} \bmod q$
39	Проверочное сравнение	$S^{(y^k S \bmod p)H} \equiv \alpha^{k(y^{-k}S^{-1} \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{UxHZ}{xHZ + Z'} \bmod \gamma$; $g = \dfrac{UZ'}{xHZ + Z'} \bmod \gamma$
	Примечание	$Z = y^{U} \bmod p$; $Z' = Z^{-1} \bmod p$
40	Проверочное сравнение	$S^{[(y^k S)^H \bmod p]} \equiv \alpha^{k+(y^k S \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{UxZ' - Z}{1 + xZ'} \bmod \gamma$; $g = \dfrac{U + Z}{1 + xZ'} \bmod \gamma$
	Примечание	$Z = y^{U} \bmod p$; $Z' = Z^{H} \bmod p$

5.2. Схемы ЭЦП на основе сложности факторизации RSA-модуля

В схемах на основе сложности факторизации составного модуля n, представляющего собой произведение двух больших сильных простых чисел ($n = pq$), используются следующие типовые параметры: (n, α) — открытый ключ, где $n = rq$ и α — число, относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$, где γ' и γ'' есть простые делители: $\gamma' | r - 1$ и $\gamma'' | q - 1$ (причем γ' не делит $q - 1$ и γ'' не делит $r - 1$); γ — секретный ключ; (g, R), (k, S) или (R, S) — подпись; H — хэш-функция от подписываемого документа.

Общая схема генерации ключа: выбирается случайное число U, по которому вычисляется значение Z (обычно $Z = \alpha^{U} \bmod n$, однако в некоторых вариантах используется другая формула, которая указана в примечании), по значениям U и Z определяются значения k и g, из которых вычисляются элементы подписи R и S (обычно $R = \alpha^{k} \bmod n$ и $S = \alpha^{g} \bmod n$, хотя эти параметры могут представляться и в другом виде при выполнении процедуры генерации подписи). Параметры p, q и r представляют собой достаточно большие простые числа, $|x|$ — обозначение длины числа x.

1	Проверочное уравнение	$H = R^{Q}S^{Q'} \bmod n$, где $Q = RS \bmod n$ и $\lvert R\rvert \approx \lvert S\rvert > 100$ бит

	Значения параметров k и g	$k = \dfrac{UZ^t}{Z^t - Z} \bmod \gamma;\ \ g = \dfrac{UZ}{Z - Z^t} \bmod \gamma$ Какие значения разумно выбрать для t?
	Примечание	$S \equiv H\alpha^g \bmod n;\ \ Z \equiv H\alpha^{t'} \bmod n$
2	Проверочное сравнение	$\alpha^{k+H(S\alpha^k \bmod n)} \equiv S \bmod n$
	Значения параметров k и g	$k = \dfrac{U - HZ}{2} \bmod \gamma;\ \ g = \dfrac{U + HZ}{2} \bmod \gamma$
	Примечание	$S \equiv \alpha^g \bmod n$
3	Проверочное сравнение	$S^{H+(S\alpha^k \bmod n)} \equiv \alpha^k \bmod n$
	Значения параметров k и g	$k = \dfrac{U(H + Z)}{H + Z + 1} \bmod \gamma;\ \ g = \dfrac{U}{H + Z + 1} \bmod \gamma$
	Примечание	$S \equiv \alpha^g \bmod n$
4	Проверочное сравнение	$\alpha^{Hk+(S^k \bmod n)} \equiv S \bmod n$
	Значения параметров k и g	$k = \dfrac{-Z \pm \sqrt{Z^2 + 4HU}}{2H} \bmod \gamma;$ $g = \dfrac{Z \pm \sqrt{Z^2 + 4HU}}{2} \bmod \gamma$
5	Проверочное сравнение	$S^{Hk} \equiv \alpha^{(S\alpha^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{HU \pm \sqrt{H^2U^2 - 4HZ}}{2H} \bmod \gamma;$ $g = U - k \bmod \gamma$
6	Проверочное уравнение	$\alpha = (RS)^{(S/R \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{1 - ZU}{2Z} \bmod \gamma;\ \ g = \dfrac{1 + ZU}{2Z} \bmod \gamma$
7	Проверочное сравнение	$S^{Hk} \equiv \alpha^{(S\alpha^k \bmod n')} \bmod n,$ где (α, n', n) — открытый ключ

	Значения параметров k и g	$k = \dfrac{UH \pm \sqrt{U^2H^2 - 4HZ}}{2H} \bmod \gamma;$ $g = U - k \bmod \gamma$
	Примечание	$\alpha^{\gamma} \equiv 1 \bmod n';\ S \equiv \alpha^{g} \bmod (n'n);\ n' = p'q'$
8	Проверочное сравнение	$R^{g} \equiv \alpha^{H(R\alpha^{g} \bmod p)} \bmod n$ и $R^{g} \equiv \alpha^{H(R\alpha^{g} \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{U}{2} \pm \sqrt{U^2/4 - HZ} \bmod \gamma;$ $g = \dfrac{U}{2} \mp \sqrt{U^2/4 - HZ} \bmod \gamma$
	Примечание	$\alpha^{\gamma} \equiv 1 \bmod p;\ R \equiv \alpha^{k} \bmod (pn)$
9	Проверочное сравнение	$S^{(S^k \bmod n)} \equiv \alpha^{H} \bmod n$
	Значения параметров k и g	$k = \dfrac{UZ}{H} \bmod \gamma;\ g = \dfrac{H}{Z} \bmod \gamma$
10	Проверочное сравнение	$\alpha S^{H(S^k \bmod n)} \equiv 1 \bmod n$
	Значения параметров k и g	$k = -HUZ \bmod \gamma;\ g = \dfrac{-1}{HZ} \bmod \gamma$
11	Проверочное сравнение	$S^{(S\alpha^k \bmod n)}\alpha^{Hk} \equiv 1 \bmod n$
	Значения параметров k и g	$k = \dfrac{UZ}{Z - H} \bmod \gamma;\ g = \dfrac{-HU}{Z - H} \bmod \gamma$
12	Проверочное уравнение	$\alpha = (HS)^{(S\alpha^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{UZ - 1}{Z} \bmod \gamma;\ g = \dfrac{1}{Z} \bmod \gamma$
	Примечание	$S = H^{-1}\alpha^{g} \bmod n;\ Z = H^{-1}\alpha^{U} \bmod n$
13	Проверочное сравнение	$\alpha^{Hk} \equiv S^{(S^k \bmod n)} \bmod n$

	Значения параметров k и g	$k = \pm\sqrt{UZ / H} \bmod \gamma;\ \ g = \pm\sqrt{UH / Z} \bmod \gamma$
14	Проверочное сравнение	$(\alpha S)^{Hk} \equiv \alpha^{(S^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{Z - UH}{H} \bmod \gamma;\ \ g = \dfrac{UH}{Z - UH} \bmod \gamma$
15	Проверочное сравнение	$(HS)^k \equiv \alpha^{H(S\alpha^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{U}{2} \pm \sqrt{U^2 / 4 - HZ} \bmod \gamma;$ $g = \dfrac{U}{2} \mp \sqrt{U^2 / 4 - HZ} \bmod \gamma$
	Примечание	$S = H^{-1}\alpha^g \bmod n;\ \ Z = H^{-1}\alpha^U \bmod n$
16	Проверочное сравнение	$S^{H+k} \equiv \alpha^{(S^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{UH}{Z - H} \bmod \gamma;\ \ g = \dfrac{Z - U}{H} \bmod \gamma$
17	Проверочное сравнение	$\alpha^{H+k} \equiv S^{(S^k \bmod n')} \bmod n$
	Значения параметров k и g	$k = \dfrac{H}{2} \pm \sqrt{H^2 / 4 + UZ} \bmod \gamma;$ $g = \dfrac{U}{k} \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod n';\ n' = r'q';$ $S = \alpha^g \bmod (n'n);$ $Z = \alpha^U \bmod (n'n)$
18	Проверочное сравнение	$S^{1+k} \equiv \alpha^{(HS^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{U}{Z - U} \bmod \gamma;\ \ g = Z - U \bmod \gamma$
	Примечание	$Z = H\alpha^U \bmod n$

19	Проверочное уравнение	$S = \alpha^{(HS^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \frac{U}{Z} \bmod \gamma;\ \ g = Z \bmod \gamma$
	Примечание	$Z = H\alpha^U \bmod n$
20	Проверочное сравнение	$S\alpha^k \equiv \alpha^{(HS^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \frac{Z}{2} \pm \sqrt{Z^2/4 - U} \bmod \gamma;$ $g = \frac{Z}{2} \mp \sqrt{Z^2/4 - U} \bmod \gamma$
	Примечание	$Z = H\alpha^U \bmod n$
21	Проверочное сравнение	$\alpha^H \equiv R^{(R^g \bmod p)} \bmod p$ и $\lvert g\rvert < 520$ бит, где $p = 2n + 1$ и $n = rq$
	Значения параметров k и g	$k = \frac{H}{Z} \bmod q;\ \ g = \frac{ZU}{H} \bmod q$
	Примечание	$\alpha^q \equiv 1 \bmod p$, q — секретный ключ
22	Проверочное сравнение	$\alpha^{Hg} \equiv R^{(R^g \bmod p)} \bmod p$ и $\lvert g\rvert < 520$ бит, где $p = 2n + 1$ и $n = rq$
	Значения параметров k и g	$k = \pm\sqrt{UH/Z} \bmod q;\ \ g = \pm\sqrt{UZ/H} \bmod q$
	Примечание	$\alpha^q \equiv 1 \bmod p$, q — секретный ключ
23	Проверочное сравнение	$\alpha^H \equiv R^{g+(R\alpha^g \bmod p)} \bmod p$ и $\lvert g\rvert < 520$ бит, где $p = 2n + 1$ и $n = rq$
	Значения параметров k и g	$k = \frac{U+Z}{2} \pm \sqrt{\frac{(U+Z)^2}{4} - H} \bmod \gamma;$ $g = \frac{U-Z}{2} \mp \sqrt{\frac{(U+Z)^2}{4} - H} \bmod \gamma$
	Примечание	$\alpha^q \equiv 1 \bmod p$, q — секретный ключ

24	Проверочное сравнение	$R^H \equiv y^{(R\alpha^g \bmod p)} \bmod p$ и $\lvert g\rvert < 520$ бит, где $p = 2n + 1$ и $n = rq$
	Значения параметров k и g	$k = \frac{xZ}{H} \bmod q;\ \ g = \frac{UH - xZ}{H} \bmod q$
	Примечание	$\alpha^q \equiv 1 \bmod p;\ \ y = \alpha^x \bmod p$ — элемент открытого ключа; (x, q) — секрет
25	Проверочное сравнение	$y^{Hg} \equiv R^{(R\alpha^g \bmod p)} \bmod p$ и $\lvert g\rvert < 520$ бит, где $p = 2n + 1$ и $n = rq$
	Значения параметров k и g	$k = \frac{xHU}{Z + xH} \bmod q;\ \ g = \frac{UZ}{Z + xH} \bmod q$
	Примечание	$\alpha^q \equiv 1 \bmod p;\ \ y = \alpha^x \bmod p$ — элемент открытого ключа; (x, q) — секрет
26	Проверочное сравнение	$\alpha^g \equiv R^{(HRy^g \bmod p)} \bmod p$ и $\lvert g\rvert < 520$ бит, где $p = 2n + 1$ и $n = rq$
	Значения параметров k и g	$k = \frac{U}{Zx + 1} \bmod q;\ \ g = \frac{UZx}{Zx + 1} \bmod q$
	Примечание	$\alpha^q \equiv 1 \bmod p;\ \ y = \alpha^x \bmod p;\ \ Z = Hy^U \bmod p$
27	Проверочное сравнение	$R^{H+g} \equiv \alpha^{(R^g \bmod p)} \bmod p$ и $\lvert g\rvert < 520$ бит, где $p = 2n + 1$ и $n = rq$
	Значения параметров k и g	$k = \frac{Z - U}{H} \bmod q;\ \ g = \frac{UH}{Z - U} \bmod q$
	Примечание	$\alpha^q \equiv 1 \bmod p,\ q$ — секрет
28	Проверочное сравнение	$R\alpha^{(RS \bmod n)} \equiv S^{(HRS \bmod n)} \bmod n$
	Значения параметров k и g	$k = \frac{UZ' - Z}{1 + Z'} \bmod \gamma;\ \ g = \frac{U + Z}{1 + Z'} \bmod \gamma$
	Примечание	$Z' = H\alpha^U \bmod n$

29	Проверочное сравнение	$R^{H+g} \equiv \alpha^{1+(R^{Hg} \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{Z+1-U/H}{H} \bmod \gamma;\ \ g = \dfrac{UH}{HZ+H-U} \bmod \gamma$
30	Проверочное сравнение	$R^{gH+\alpha} \equiv \alpha^{(HR^{g} \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{Z-UH}{\alpha} \bmod \gamma;\ \ g = \dfrac{U\alpha}{Z-UH} \bmod \gamma$
	Примечание	$Z = H\alpha^{U} \bmod n$
31	Проверочное уравнение	$k + v = (\alpha^{kgvH} \bmod n)^{(k-v \bmod \delta)} \bmod \delta$ (g, k, v) — подпись; (n, α) — открытый ключ
	Значения параметров k, v и g	$k = \dfrac{U_2 + Z^{U_2}}{2} \bmod \delta;\ \ v = \dfrac{Z^{U_2} - U_2}{2} \bmod \delta;$ $g = \dfrac{U_1}{Hkv} \bmod \gamma$
	Примечание	$U_1 < \gamma$ и $U_2 < \delta$ — случайные числа; $Z \equiv (\alpha^{U_1} \bmod n) \bmod \delta$
32	Проверочное уравнение	$k = H(\alpha^{kgH} \bmod n) \bmod \delta$
	Значения параметров k и g	$k = HZ \bmod \delta;\ \ g = \dfrac{U}{kH} \bmod \gamma$
	Примечание	$Z = (\alpha^{U} \bmod n) \bmod \delta$
33	Проверочное уравнение	$k = (H\alpha^{kg^2} \bmod n) \bmod \delta$
	Значения параметров k и g	$k = Z \bmod \delta;\ \ g = \pm\sqrt{\dfrac{U}{Z}} \bmod \gamma$
	Примечание	$Z = (H\alpha^{U} \bmod n) \bmod \delta$

34	Проверочное сравнение	$k^2 \equiv (H\alpha^{kg^2} \bmod n) \bmod \delta$
	Значения параметров k и g	$k = \pm\sqrt{Z} \bmod \delta;\ \ g = \pm\sqrt{\frac{U}{k}} \bmod \gamma$
	Примечание	$Z = (H\alpha^{U} \bmod n) \bmod \delta$
35	Проверочное уравнение	$k = (\alpha^{k-Hg} \bmod n) \bmod \delta$
	Значения параметров k и g	$k = Z;\ g = (Z-U)H^{-1} \bmod \gamma$
	Примечание	$Z = (\alpha^{U} \bmod n) \bmod \delta$
36	Проверочное сравнение	$k / g = (H\alpha^{k+g} \bmod n) \bmod \delta$
	Значения параметров k и g	$k = Zg;\ \ g = \frac{U}{Z+1} \bmod \gamma$
	Примечание	$Z = (H\alpha^{U} \bmod n) \bmod \delta$

5.3. Схемы ЭЦП с восстановлением сообщения

В приводимых ниже схемах ЭЦП, обладающих свойством восстановления сообщения M, используется такая же спецификация типовых параметров, как и в случаях предыдущих схем, основанных на 1) сложности задачи дискретного логарифмирования и 2) трудности факторизации RSA-модуля. Наличие особенностей поясняется в примечаниях (p, q и r — простые числа, $|q|$ — длина числа q).

1	Проверочное уравнение	$M = Sy^{rHk+(S\alpha^{k} \bmod p)} \bmod p$
	Значения параметров k и g	$k = \frac{U+xZ}{1-xH} \bmod \gamma;\ \ g = \frac{xHU+xZ}{xH-1} \bmod \gamma$
	Примечание	$S = M\alpha^{g} \bmod p;\ \ Z = M\alpha^{U} \bmod p$

2	Проверочное уравнение	$M = Sy^k \alpha^{(S\alpha^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{U+Z}{1-x} \bmod \gamma;\ \ g = \dfrac{xU+Z}{x-1} \bmod \gamma$
	Примечание	$S = M\alpha^g \bmod p;\ \ Z = M\alpha^U \bmod p$
3	Проверочное уравнение	$M = S\alpha^{k(Sy^k \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{Ux}{x-Z} \bmod \gamma;\ \ g = \dfrac{UZ}{Z-x} \bmod \gamma$
	Примечание	$S = My^g \bmod p;\ \ Z = My^U \bmod p$
4	Проверочное уравнение	$M = Sy^{(\alpha^k S \bmod q)} \bmod p$
	Значения параметров k и g	$k = U + xZ \bmod \gamma;\ \ g = -xZ \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ \ S \equiv M\alpha^g \bmod (pq);$ $Z = M\alpha^U \bmod q$
5	Проверочное уравнение	$M = Sy^{(\alpha^k S^H \bmod q)} \bmod p$
	Значения параметров k и g	$k = U + xZH \bmod \gamma;\ \ g = -xZ \bmod \gamma$
	Примечание	$\alpha^\gamma \equiv 1 \bmod q;\ \ S \equiv M\alpha^g \bmod (pq);$ $Z = M^H\alpha^U \bmod q$
6	Проверочное уравнение	$M = S\alpha^{(y^k S \bmod p)k} \bmod p$
	Значения параметров k и g	$k = \dfrac{U}{x-Z} \bmod \gamma;\ \ g = \dfrac{ZU}{Z-x} \bmod \gamma$
	Примечание	$S = M\alpha^g \bmod p;\ \ Z = M\alpha^U \bmod p$
7	Проверочное уравнение	$M = S^H y^{Q^2} \alpha^{kQ} \bmod p$, где $Q = \alpha^k S \bmod p$

	Значения параметров k и g	$k = \dfrac{HU + xZ^2}{H - Z} \bmod \gamma;\ g = \dfrac{-UZ - xZ^2}{H - Z} \bmod \gamma$
	Примечание	$S \equiv M'\alpha^g \bmod p;\ Z \equiv M'\alpha^U \bmod p;$ $M' = M^{1/H \bmod \varphi(p)} \bmod p$
8	Проверочное уравнение	$M = S^{-1}R^{(RS \bmod n)} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит
	Значения параметров k и g	$k = \dfrac{U}{1 + Z} \bmod \gamma;\ g = \dfrac{UZ}{Z + 1} \bmod \gamma$
	Примечание	$S = M^{-1}\alpha^g \bmod n;\ Z = M^{-1}\alpha^U \bmod n$
9	Проверочное уравнение	$M = R^Q S\alpha^{Qt} \bmod n$, где $Q = RS \bmod n$ и $\lvert R\rvert \approx \lvert S\rvert > 100$ бит
	Значения параметров k и g	$k = \dfrac{Z^t + U}{1 - Z} \bmod \gamma;\ g = \dfrac{-UZ - Z^t}{1 - Z} \bmod \gamma$ Какие значения разумно выбрать для t?
	Примечание	$S = M\alpha^g \bmod n;\ Z = M\alpha^U \bmod n$
10	Проверочное уравнение	$M = R^{-1}S^{(RS \bmod n)} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит
	Значения параметров k и g	$k = \dfrac{UZ}{1 + Z} \bmod \gamma;\ g = \dfrac{U}{1 + Z} \bmod \gamma$
	Примечание	$R = M^{-1}\alpha^k \bmod n;\ Z = M^{-1}\alpha^U \bmod n$
11	Проверочное уравнение	$M = R^H S^{-(RS \bmod n)} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит
	Значения параметров k и g	$k = \dfrac{UZ}{H + Z} \bmod \gamma;\ g = \dfrac{UH}{H + Z} \bmod \gamma$
	Примечание	$R = M^{1/H}\alpha^k \bmod n;\ Z = M^{1/H}\alpha^U \bmod n$ $M' = M^{1/H \bmod \varphi(n)} \bmod n$

12	Проверочное уравнение	$M = RS^{-(RS \bmod n')} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит и $\alpha^{\gamma} \equiv 1 \bmod n'$
	Значения параметров k и g	$k = \dfrac{UZ}{1+Z} \bmod \gamma$; $g = \dfrac{U}{1+Z} \bmod \gamma$
	Примечание	$S = \alpha^{g} \bmod (n'n)$; $R = M\alpha^{k} \bmod (n'n)$; $Z = M\alpha^{U} \bmod n'$
13	Проверочное уравнение	$M = SR^{(RS^{-1} \bmod n)} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит
	Значения параметров k и g	$k = \dfrac{U}{1+Z} \bmod \gamma$; $g = \dfrac{-UZ}{1+Z} \bmod \gamma$
	Примечание	$S = M\alpha^{g} \bmod n$; $Z = M\alpha^{U} \bmod n$
14	Проверочное уравнение	$M = SR^{(RS^{H} \bmod n)} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит
	Значения параметров k и g	$k = \dfrac{U}{1-ZH} \bmod \gamma$; $g = \dfrac{UZ}{ZH-1} \bmod \gamma$
	Примечание	$S = M\alpha^{g} \bmod n$; $Z = M^{H}\alpha^{U} \bmod n$
15	Проверочное уравнение	$M = S\alpha^{k-(Sy^{-k} \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{Z-Ux}{x+1} \bmod \gamma$; $g = \dfrac{U+Z}{x+1} \bmod \gamma$
	Примечание	$S = My^{g} \bmod p$; $Z = My^{U} \bmod p$
16	Проверочное уравнение	$M = S^{H'}(\alpha R)^{(RS \bmod n)} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит
	Значения параметров k и g	$k = \dfrac{UH'+Z}{H'-Z} \bmod \gamma$; $g = \dfrac{UZ+Z}{Z-H'} \bmod \gamma$
	Примечание	$S = M^{H'^{-1}}\alpha^{g} \bmod n$; $Z = M^{H'^{-1}}\alpha^{U} \bmod n$

17	Проверочное уравнение	$M = R^{-1}\alpha^{g(\alpha^g R \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{UZ}{1+Z} \bmod \gamma;\ \ g = \dfrac{U}{1+Z} \bmod \gamma$
	Примечание	$R = M^{-1}\alpha^k \bmod n;\ \ Z \equiv M^{-1}\alpha^U \bmod n$
18	Проверочное уравнение	$M = R^H \alpha^{g-(\alpha^g / R \bmod n)} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит
	Значения параметров k и g	$k = \dfrac{Z-U}{H+1} \bmod \gamma;\ \ g = \dfrac{UH+Z}{H+1} \bmod \gamma$
	Примечание	$R = M'\alpha^k \bmod n;\ \ Z = M'^{-1}\alpha^U \bmod n;$ $M' = M^{1/H \bmod \varphi(n)} \bmod n$
19	Проверочное уравнение	$M = RS^{-(RS \bmod n')} \bmod n$, где $\lvert R\rvert \approx \lvert S\rvert > 100$ бит и $\alpha^\gamma \equiv 1 \bmod n'$
	Значения параметров k и g	$k = \dfrac{UZ}{1+Z} \bmod \gamma;\ \ g = \dfrac{U}{1+Z} \bmod \gamma$
	Примечание	$S \equiv \alpha^g \bmod (n'n);\ \ R = M\alpha^k \bmod (n'n);$ $Z = M\alpha^U \bmod n'$
20	Проверочное уравнение	$M = R\alpha^{HF(R)} y^{(F(R)S \bmod p)} \bmod p$, где $F(R)$ — сжимающая функция, например, $F(R) = R \bmod \gamma$
	Значение параметра S	$S = \dfrac{[(-k - HF(R))/x \bmod \gamma]}{F(R)} \bmod p$
	Примечание	$R = M\alpha^k \bmod p$
21	Проверочное уравнение	$M = R\alpha^{HQ} y^{RQ} \bmod p$, где $Q = F(R)S \bmod p$ и $F(R)$ — сжимающая функция,

		например $F(R) = R \bmod \gamma$
	Значение параметра S	$S = \dfrac{[-k(H + xR)^{-1} \bmod \gamma]}{F(R)} \bmod p$
	Примечание	$R = M\alpha^k \bmod p$
22	Проверочное уравнение	$M = Sy^{k+(\alpha^k / S \bmod p)} \bmod p$
	Значения параметров k и g	$k = \dfrac{U - xZ}{x + 1} \bmod \gamma;\ \ g = \dfrac{-xZ - xU}{x + 1} \bmod \gamma$
	Примечание	$S = M\alpha^g \bmod p;\ \ Z = M^{-1}\alpha^U \bmod p$
23	Проверочное уравнение	$M = S\alpha^{k(S\alpha^k \bmod n)} \bmod n$
	Значения параметров k и g	$k = \dfrac{U}{1 - Z} \bmod \gamma;\ \ g = \dfrac{ZU}{Z - 1} \bmod \gamma$
	Примечание	$S = M\alpha^g \bmod n;\ \ Z = M\alpha^U \bmod n$
24	Проверочное уравнение	$M = R\alpha^{HRS} \bmod p;\ \ \lvert S\rvert < \dfrac{2\lvert q\rvert}{3}$, q — секретный ключ
	Значения параметров k и S	$S = \dfrac{-k}{RH} \bmod q$, где k — случайно выбираемое число
	Примечание	$p = 2qr + 1;\ \ R = M\alpha^k \bmod p$
25	Проверочное уравнение	$M = \dfrac{R^3}{\alpha^{(RS \bmod n)}} \bmod n$
	Значения параметров k и S	$S = \dfrac{3k \bmod \gamma}{R} \bmod n$, где k — случайно выбираемое число
	Примечание	$R = \sqrt[3]{M}\alpha^k \bmod n;\ \ \sqrt[3]{M} = M^{3^{-1} \bmod \varphi(n)} \bmod n$
26	Проверочное уравнение	$M = R^H \alpha^{(RS \bmod n)} \bmod n$

	Значения параметров k и S	k — случайно выбираемое число; $S = \dfrac{-kH \bmod \gamma}{R} \bmod n.$

5.4. Схемы ЭЦП с сокращенным размером подписи

К данному типу относятся схемы ЭЦП, в которых битовая длина подписи в несколько раз меньше, чем длина модуля, по которому осуществляется операция возведения в степень при формировании элементов подписи и ее проверке. Благодаря этому сложность подделки подписи или вычисления секретного ключа определяется сложностью дискретного логарифмирования по модулю большого простого числа (причем это число выбирается таким, что в разложении функции Эйлера от него содержится, по крайней мере, один большой множитель). В приводимых ниже схемах ЭЦП используется такая же спецификация типовых параметров, как и в предыдущих случаях: 1) схемах, основанных на сложности задачи дискретного логарифмирования, 2) схемах, основанных на сложности задачи факторизации, и 3) схемах, обладающих свойством восстановления сообщения M. Подпись представляет собой пару чисел (k, g) или тройку чисел (v, k, g). Значение M соответствует условию $M < \gamma$.

Схемы с сокращенным размером подписи, приводимые ниже, «выводятся» из некоторых типов схем, описанных выше. Это обстоятельство полезно принять во внимание для понимания, почему такой вид схем с сокращенной подписью «работает» и почему при генерации подписи используются данные конкретные формулы. Отметим также, что используемое число α относится по модулю p к числу γ как к показателю, причем γ играет также и роль «сжимающего» модуля. Однако в общем случае показатель числа α может не совпадать со «сжимающим» модулем. В этом случае процедура генерации подписи осуществляется по другим формулам. Указанные ниже варианты проверочных уравнений могут быть распространены и на последний случай, что удваивает число различных заданий.

1	Проверочное уравнение	$g = (\alpha^{kH} y^{g} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{U - xZ}{H} \bmod \gamma;\ \ g = Z \bmod \gamma$

2	Проверочное уравнение	$k = [(\alpha^{gH} y^k)^k \bmod p] \bmod \gamma$
	Значения параметров k и g	$k = Z \bmod \gamma;$ $g = \dfrac{U - xZ^2}{HZ} \bmod \gamma$
3	Проверочное уравнение	$k = (\alpha^g y^{k+H} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = Z \bmod \gamma;$ $g = U - xH - xZ \bmod \gamma$
4	Проверочное сравнение	$kg \equiv (\alpha^{k+g} y^{kH} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{U \pm \sqrt{U^2 - 4Z(1+xH)}}{2(1+xH)} \bmod \gamma;$ $g = \dfrac{2Z(1+xH)}{U \pm \sqrt{U^2 - 4Z(1+xH)}} \bmod \gamma$
5	Проверочное уравнение	$M = (k+g)(\alpha^k y^g \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{xM - UZ}{Z(x-1)} \bmod \gamma;\ g = \dfrac{UZ - M}{Z(x-1)} \bmod \gamma$
6	Проверочное уравнение	$g = (\alpha^{kH} y^{gk} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{U}{H + xZ} \bmod \gamma;\ g = Z \bmod \gamma$
7	Проверочное уравнение	$g = (\alpha^{k+H} y^{g+k} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{U - xZ - H}{1+x} \bmod \gamma;\ g = Z \bmod \gamma$
8	Проверочное уравнение	$M = \dfrac{k+g}{\alpha^k y^{gH} \bmod p} \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{xMZH - U}{xH - 1} \bmod \gamma;\ g = \dfrac{U - MZ}{xH - 1} \bmod \gamma$

9	Проверочное уравнение	$g = (\alpha^{kg} y^{kH} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{U}{Z + xH} \bmod \gamma;\ \ g = Z \bmod \gamma$
10	Проверочное уравнение	$H = g(\alpha^{k} y^{g} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{UZ - xH}{Z} \bmod \gamma;\ \ g = H / Z \bmod \gamma$
11	Проверочное уравнение	$M = \dfrac{(Hk - g)}{\alpha^{k} y^{g} \bmod p} \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{U + xMZ}{xH + 1} \bmod \gamma;\ \ g = \dfrac{HU - MZ}{xH + 1} \bmod \gamma$
12	Проверочное сравнение	$Hk \equiv (H\alpha^{k} y^{g} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = Z / H \bmod \gamma;\ \ g = \dfrac{HU - Z}{xH} \bmod \gamma,$ где $Z = (H\alpha^{U} \bmod p) \bmod \gamma$
13	Проверочное сравнение	$k / g \equiv H(H\alpha^{k} y^{g} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{UHZ}{ZH + x} \bmod \gamma;\ \ g = \dfrac{U}{ZH + x} \bmod \gamma,$ где $Z = (H\alpha^{U} \bmod n) \bmod \gamma$
14	Проверочное уравнение	$M = g(\alpha^{Hk} y^{g} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{UZ - xM}{ZH} \bmod \gamma;\ \ g = M / Z \bmod \gamma$
15	Проверочное уравнение	$M = k(\alpha^{k} y^{g} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = M / Z \bmod \gamma;\ \ g = \dfrac{UZ - M}{xZ} \bmod \gamma$

16	Проверочное уравнение	$M = k(\alpha^g y^k \bmod p)^H \bmod \gamma$
	Значения параметров k и g	$k = M Z^{-H} \bmod \gamma;\ g = \dfrac{Z^H U - x M}{Z^H} \bmod \gamma$
17	Проверочное уравнение	$M = kg(\alpha^k y^g \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{2xMZ^{-1}}{U \pm \sqrt{U^2 - 4xMZ^{-1}}} \bmod \gamma;$ $g = \dfrac{U \pm \sqrt{U^2 - 4xMZ^{-1}}}{2x} \bmod \gamma$
18	Проверочное уравнение	$M = k^{-1} g(\alpha^k y^g \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{UZ}{Z + xM} \bmod \gamma;\ g = \dfrac{UM}{Z + xM} \bmod \gamma$
19	Проверочное уравнение	$M = (k + g)(\alpha^k y^g \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{UZ - xM}{Z - xZ} \bmod \gamma;\ g = \dfrac{M - UZ}{Z - xZ} \bmod \gamma$
20	Проверочное уравнение	$M = kg^{-1}(\alpha^g y^{-k} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{UM}{Z - xM} \bmod \gamma;\ g = \dfrac{UZ}{Z - xM} \bmod \gamma$
21	Проверочное уравнение	$g = (\alpha^{H+k} y^{H-g} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = U + xZ - xH - H \bmod \gamma;\ g = Z \bmod \gamma$
22	Проверочное уравнение	$M = k^H (\alpha^g y^{-k} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{M^{1/H}}{Z^{1/H}} \bmod \gamma;\ g = \dfrac{UZ^{1/H} + xM^{1/H}}{Z^{1/H}} \bmod \gamma$

23	Проверочное уравнение	$k = (\alpha^{Hkg} y^{k+g} \bmod p) \bmod \delta$, где $\delta = \gamma$ или $\delta \neq \gamma$
	Значения параметров k и g	$k = Z \bmod \delta$; $g = \dfrac{U - xZ}{HZ + x} \bmod \gamma$
24	Проверочное уравнение	$k = H(\alpha^{k\ g} y^{k+g} \bmod p) \bmod \delta$, где $\delta = \gamma$ или $\delta \neq \gamma$
	Значения параметров k и g	$k = HZ \bmod \delta$; $g = \dfrac{U - k - xk}{x - 1} \bmod \gamma$
25	Проверочное уравнение	$g = (\alpha^{k^2} y^{Hg} \bmod p) \bmod \delta$, где $\delta = \gamma$ или $\delta \neq \gamma$
	Значения параметров k и g	$k = \pm\sqrt{U - xHg} \bmod \gamma$; $g = Z \bmod \delta$
26	Проверочное уравнение	$g = (\alpha^{kH} y^{k/g} \bmod p) \bmod \delta$, где $\delta = \gamma$ или $\delta \neq \gamma$
	Значения параметров k и g	$k = \dfrac{Ug}{Hg + x} \bmod \gamma$; $g = Z \bmod \delta$
27	Проверочное уравнение	$k = (\alpha^{kg} y^{Hk/g} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = Z \bmod \gamma$; $g = \dfrac{U \pm \sqrt{U^2 - 4xHMZ^2}}{2Z} \bmod \gamma$
28	Проверочное уравнение	$M = k(\alpha^{H/g} y^{kg} \bmod p) \bmod \delta$, где $\delta = \gamma$ или $\delta \neq \gamma$
	Значения параметров k и g	$k = MZ^{-1} \bmod \delta$; $g = \dfrac{U \pm \sqrt{U^2 - 2Hxk}}{2xk} \bmod \gamma$
29	Проверочное уравнение	$k = (\alpha^{1/g} y^{H/k} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = Z \bmod \gamma$; $g = \dfrac{Z}{UZ - xH} \bmod \gamma$

30	Проверочное сравнение	$gk \equiv M(\alpha^g y^k \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{U \pm \sqrt{U^2 - 4xMZ}}{2x} \bmod \gamma;$ $g = \dfrac{2xMZ}{U \pm \sqrt{U^2 - 4xMZ}} \bmod \gamma$
31	Проверочное уравнение	$g = [(\alpha^g y)^{kH} \bmod p] \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{U}{HZ + xH} \bmod \gamma;\ g = Z \bmod \gamma$
32	Проверочное сравнение	$g^H \equiv [(\alpha^k y^{1/g} \bmod p] \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{UZ^{1/H} - x}{Z^{1/H}} \bmod \gamma;\ g = Z^{1/H} \bmod \gamma$
33	Проверочное уравнение	$k = gH(\alpha^k y^{kg} \bmod p) \bmod \gamma$
	Значения параметров k и g	$k = \dfrac{-1 \pm \sqrt{1 + \dfrac{4xU}{HZ}}}{2xH^{-1}Z^{-1}} \bmod \gamma;$ $g = \dfrac{-1 \pm \sqrt{1 + \dfrac{4xU}{HZ}}}{2x} \bmod \gamma$
34	Проверочное уравнение	$v = (\alpha^k y^{vg} \bmod p)(\alpha^k y^{vH} \bmod p') \bmod \gamma,$ где $y = \alpha^x \bmod (pp'),\ \alpha^\gamma \equiv 1 \bmod p'$ и $\alpha^\gamma \equiv 1 \bmod p$
	Значения параметров v, k и g	$v = ZZ' \bmod \gamma,\ k = U' - xZZ'H \bmod \gamma,$ где $Z = \alpha^U \bmod p$ и $Z' = \alpha^{U'} \bmod p'$ $g = \dfrac{U + xZZ'H - U'}{xZZ'} \bmod \gamma,$ (v, k, g) — подпись

35	Проверочное уравнение	$M = v(Q + Q') \bmod \gamma$, где
		$Q = \alpha^k y^g \bmod p$, $Q' = \alpha^v y^{k+g} \bmod p$,
		(v, k, g) — подпись
	Значения параметров v, k и g	$v = M(Z + Z')^{-1} \bmod \gamma$; $k = \dfrac{U' - U - v}{x - 1} \bmod \gamma$,
		где $Z = \alpha^U \bmod p$ и $Z' = \alpha^{U'} \bmod p$
		$g = \dfrac{Ux - U' + v}{x(x-1)} \bmod \gamma$, $U' < \gamma$ и $U < \gamma$
		выбираются случайно, $U' \neq U$
36	Проверочное уравнение	$g = (\alpha^{kH} y^g \bmod n) \bmod \delta$,
		где $\delta \neq \gamma$, $y = \alpha^x \bmod n$
	Значения параметров k и g	$g = Z \bmod \delta$; $k = \dfrac{U - xg}{H} \bmod \gamma$,
		x — секретный элемент
37	Проверочное уравнение	$k = (\alpha^g y^{k+H} \bmod n) \bmod \delta$,
		где $\delta \neq \gamma$, $y = \alpha^x \bmod n$
	Значения параметров k и g	$k = Z \bmod \delta$; $g = U - xH - xk \bmod \gamma$,
		x — секретный элемент
38	Проверочное уравнение	$g = (\alpha^{kH} y^{gk} \bmod n) \bmod \delta$,
		где $\delta \neq \gamma$, $y = \alpha^x \bmod n$
	Значения параметров k и g	$g = Z \bmod \delta$; $k = \dfrac{U}{H + xg} \bmod \gamma$,
		x — секретный элемент
39	Проверочное уравнение	$g = (\alpha^{k+H} y^{g+k} \bmod n) \bmod \delta$,
		где $\delta \neq \gamma$, $y = \alpha^x \bmod n$

	Значения параметров k и g	$g = Z \bmod \delta;\ k = \dfrac{U - H - xg}{1 + x} \bmod \gamma,$ x — секретный элемент
40	Проверочное уравнение	$M = g(\alpha^{Hk} y^{g} \bmod n) \bmod \delta,$ где $\delta \neq \gamma,\ y = \alpha^{x} \bmod n$
	Значения параметров k и g	$g = M / Z \bmod \delta,$ где $M \leq \delta - 1;$ $k = \dfrac{U - xg}{H} \bmod \gamma,$ x — секретный элемент
41	Проверочное уравнение	$k = (\alpha^{kgH} \bmod n) \bmod \delta,$ где $\delta \neq \gamma$
	Значения параметров k и g	$k = Z \bmod \delta,$ где $Z = \alpha^{UH} \bmod n$ $g = \dfrac{U}{k} \bmod \gamma,$ γ — секретный элемент
42	Проверочное уравнение	$k = (\alpha^{kg} \bmod n)^{H} \bmod \delta,$ где $\delta \neq \gamma$
	Значения параметров k и g	$k = Z^{H} \bmod \delta,$ где $Z = \alpha^{U} \bmod p$ $g = \dfrac{U}{k} \bmod \gamma,$ γ — секретный элемент
43	Проверочное уравнение	$k = (\alpha^{k \pm gH} \bmod n) \bmod \delta,$ где $\delta \neq \gamma$
	Значения параметров k и g	$k = Z \bmod \delta,$ где $Z = \alpha^{U} \bmod p$ $g = \pm \dfrac{U - k}{H} \bmod \gamma,$ γ — секретный элемент
44	Проверочное уравнение	$k = (\alpha^{kg \pm H} \bmod n) \bmod \delta,$ где $\delta \neq \gamma$
	Значения параметров k и g	$k = Z \bmod \delta,$ где $Z = \alpha^{U} \bmod p$ $g = \dfrac{U \mp H}{k} \bmod \gamma,$ γ — секретный элемент

45	Проверочное уравнение	$M = k^H (\alpha^{k \pm gH} \bmod n) \bmod \delta$, где $\delta \neq \gamma$
	Значения параметров k и g	$k = Z^{-1/H} M^{1/H} \bmod \delta$, где $Z = \alpha^U \bmod p$
		$g = \pm \dfrac{U - k}{H} \bmod \gamma$, γ — секретный элемент
46	Проверочное уравнение	$M = k(\alpha^{k \pm g^3} \bmod n) \bmod \delta$,, где $\delta > \gamma$
	Значения параметров k и g	$k = MZ^{-1} \bmod \delta$, $Z = \alpha^U \bmod p$
		$g = [\pm(U - k)]^{3^{-1}} \bmod \gamma$, γ — секрет. элемент
47	Проверочные уравнения	$R = y^{F(H, R\alpha^g)} \alpha^g \bmod p$, $f = F(H, R\alpha^g)$, где (f, g) — подпись
	Значения параметров k и g	$k = \dfrac{U + xf}{2} \bmod \gamma$, где $f = F(H, Z) \bmod \gamma$. $Z = \alpha^U \bmod p$
		$g = \dfrac{U - xf}{2} \bmod \gamma$; выбрать самостоятельно сжимающую функцию F
48	Проверочные уравнения	$R = y^f \alpha^g \bmod p$, $f = (HR\alpha^g \bmod p) \bmod \gamma$, где (f, g) — подпись
	Значения параметров k и g	$k = \dfrac{U + xf}{2} \bmod \gamma$;
		$g = \dfrac{U - xf}{2} \bmod \gamma$, где $f = (H\alpha^U \bmod p) \bmod \gamma$
49	Проверочные уравнения	$R = y^{f+g} \bmod p$, $f = (HR\alpha^g \bmod p) \bmod \gamma$, где (f, g) — подпись
	Значения параметров k и g	$k = \dfrac{x(U + f)}{1 + x} \bmod \gamma$;

		$g = \dfrac{U - xf}{x + 1} \bmod \gamma$, где $f = (H\alpha^{U} \bmod p) \bmod \gamma$
50	Проверочные уравнения	$R = \left(\alpha^{f}\right)^{S} \bmod n$, $f = F(H, R)$, где (f, S) — подпись
	Значения параметров k и S	Генерация подписи: 1) $R = \alpha^{k} \bmod n$; 2) $f = F(H, R)$; 3) $S = k / f \bmod \gamma$, где γ — секретный элемент. Выбрать вариант сжимающей функции: $F = HR \bmod \delta$; $F = R^{H} \bmod \delta$; $F = H^{2} / R \bmod \delta$
51	Проверочные уравнения	$R = \alpha^{f+S^{2}} \bmod n$, $f = F(R, H)$, где (f, S) — подпись
	Значения параметров k и S	Генерация подписи: 1) $R = \alpha^{k} \bmod n$; 2) $f = F(R, H)$; 3) $S = \pm\sqrt{k - f} \bmod \gamma$, где γ — секретный элемент. Выбрать вариант сжимающей функции: $F = (H + R)^{2} \bmod \delta$; $F = (R + H^{2}) \bmod \delta$; $F = (H^{2} + R^{2}) \bmod \delta$

5.5. Задания повышенной сложности

Наиболее подготовленным студентам целесообразно предложить задания, требующие более самостоятельной работы по анализу, обоснованию и реализации схем ЭЦП. В этом случае схема ЭЦП может быть задана проверочным соотношением без детальной спецификации. Обоснование корректности проверочного соотношения, составление процедуры генерации подписи, формулировка требований к выбору параметров схемы ЭЦП, оценка сложности генерации и верификации подписи, анализ возможных атак и сопоставление с другими схемами выполняются студентами самостоятельно. Возможные ва-

рианты таких заданий представлены в приведенных ниже таблицах, где используются обозначения, принятые в предыдущих разделах этой главы.

Схемы ЭЦП, основанные на сложности задачи дискретного логарифмирования

№ п/п	Проверочное соотношение
1	$k = \left(\left(y_1^k \alpha_1^{gH} \bmod p_1\right) + \left(y_2^k \alpha_2^{gH} \bmod p_2\right)\right) \bmod \gamma$, где $p_1 \neq p_2$
2	$k \pm g = \left(\left(y_1^k \alpha_1^{g+H} \bmod p_1\right) + \left(y_2^k \alpha_2^{g+H} \bmod p_2\right)\right) \bmod \gamma$, где $p_1 \neq p_2$
3	$k = \left(y^k \alpha^{gH} \bmod p\right) \bmod \delta$, где $p = 2rq + 1$, $\lvert g \rvert \approx \frac{\lvert p \rvert}{2}$ и (k, g) — подпись
4	$k \pm g = \left(\left(y_1^k \alpha_1^{gH} \bmod p\right) \pm \left(y_2^k \alpha_2^{gH} \bmod n\right)\right) \bmod \gamma$, где (y_1, y_2) — открытый ключ
5	$R = y^{H(R\alpha^g \bmod p) \bmod \gamma} \alpha^g \bmod p$ или $R = y^{HE} \alpha^g \bmod p$, где $E = (R\alpha^g \bmod p) \bmod \gamma$
6	$R = (y_1^E \alpha_1^{Hg} \bmod p_1 + y_2^E \alpha_2^{Hg} \bmod p_2) \bmod \gamma$, где (y_1, y_2) — открытый ключ, $E = F(R, H)$, F — сжимающая функция
7	$R = (y_1^E \alpha^{Hg} \bmod p_1 + y_2^E \alpha^{Hg} \bmod p_2) \bmod \gamma$, где (y_1, y_2) — открытый ключ. $E = F(R, H)$. F — сжимающая функция
8	$R = y^E \alpha^{Hg} \bmod p$, где $E = (R^g \bmod p) \bmod \gamma$ и (g, E) — подпись
9	$R = y^E \alpha^{H \pm g} \bmod p$, где $E = (R^g \bmod p) \bmod \gamma$ и (g, E) — подпись
10	$R = y^{g^{-1}E} \alpha^{gH} \bmod p$, где $E = (R^g \bmod p) \bmod \gamma$ и (g, E) — подпись
11	$R = y^g \alpha^{g^{-1}EH} \bmod p$, где $E = (R^g \bmod p) \bmod \gamma$ и (g, E) — подпись
12	$R = y^{HE} \alpha^g E^2 \bmod p$, где $E = R\alpha^g \bmod p$ и (g, E) — подпись

№ п/п	Проверочное соотношение
13	$R = y^E \alpha^g E^H \bmod p$, где $E = R\alpha^g \bmod p$ и (g, E) — подпись
14	$R = y^{EH} \alpha^g E^g \bmod p$, где $E = R\alpha^g \bmod p$ и (g, E) — подпись

Схемы ЭЦП, основанные на сложности задачи факторизации

№ п/п	Проверочное соотношение
1	$R = \alpha^{ES} \bmod n$, где $E = F(R, H)$, F — сжимающая функция, (E, S) — подпись
2	$R = \left(\alpha^{ES} + \beta^{ES}\right) \bmod n$, где $\alpha \neq \beta$, $E = F(R, H)$, F — сжимающая функция
3	$R = \left(\alpha^{ES} + \beta^{ES} + \omega^{ES}\right) \bmod n$, где $\alpha \neq \beta \neq \omega$, $E = F(R, H)$, F — сжимающая функция
4	$k \pm g = \left(\left(y_1^k \alpha_1^{gH} \bmod n_1\right) \pm \left(y_2^k \alpha_2^{gH} \bmod n_2\right)\right) \bmod \delta$, где (y_1, y_2) — открытый ключ
5	$g + k = (\alpha^{k \pm gH} \bmod n) \bmod \delta$, где $\delta \neq \gamma$
6	$g + k = (\alpha^{kg} \bmod n)^H \bmod \delta$, где $\delta \neq \gamma$
7	$gk^{-1} = \left(\left(\alpha^{gk} \bmod n\right) + \left(\alpha^{gkH} \bmod n\right)\right) \bmod \delta$, где $\delta \neq \gamma$
8	$g = k\left(\left(\alpha_1^{kgH} \bmod n_1\right) + \left(H\alpha_2^{kgH} \bmod n_2\right)\right) \bmod \delta$, где $n_1 \neq n_2$ и $(n_2, \alpha_2, n_1, \alpha_1)$ — открытый ключ
9	$k = \left[H\left(\alpha_1^{kg} \bmod n_1\right) + \left(\alpha_2^{kgH} \bmod n_2\right)\right] \bmod \delta$, где $n_1 \neq n_2$ и $(n_2, \alpha_2, n_1, \alpha_1)$ — открытый ключ
10	$R = \alpha^{EH} E^g \bmod n$, где $E = R\alpha^g \bmod n$ и (g, E) — подпись

№ п/п	Проверочное соотношение
11	$R = \alpha^{gEH} \bmod n$, где $E = (R\alpha^{g} \bmod n) \bmod \delta$ и (g, E) — подпись
12	$R = \alpha^{gEH} \bmod n$, где $E = (R^{g} \bmod n) \bmod \delta$ и (g, E) — подпись

Схемы ЭЦП с трехэлементной подписью (k, g, v)

№ п/п	Проверочное соотношение
1	$k = \left(\left(y^{k}\alpha^{gH} \bmod p\right) + \left(y^{g\pm H}\alpha^{v} \bmod p\right)\right) \bmod \gamma$
2	$g \pm k = \left(\left(y^{k}\alpha^{gH} \bmod p\right) + \left(y^{kg}\alpha^{v\pm H} \bmod p\right)\right) \bmod \gamma$
3	$g \pm k \pm v = \left(\left(y^{k}\alpha^{g\pm H} \bmod p\right) + \left(y^{g}\alpha^{k\pm v} \bmod p\right)\right) \bmod \gamma$
4	$k = \left(\left(\alpha^{gkH} \bmod n\right) + \left(\alpha^{vg^{2}} \bmod n\right)\right) \bmod \delta$
5	$g \pm k = \left(\left(\alpha^{k^{2}H\pm g} \bmod n\right) + \left(\alpha^{kgv} \bmod n\right)\right) \bmod \delta$
6	$gk^{-1} = \left(\left(\alpha^{gkH} \bmod n\right) + \left(\alpha^{kv\pm H} \bmod n\right)\right) \bmod \delta$

Схемы ЭЦП, взлом которых требует одновременного решения двух различных сложных задач — дискретного логарифмирования и факторизации

№ п/п	Проверочное соотношение
1	$\alpha^{H} = y^{R}R^{S^{2}} \bmod p$, где $p = 2rq + 1$, r и q — простые числа
2	$R = y^{E}\alpha^{S^{2}} \bmod p$, где $p = 2rq + 1$, (E, S) — подпись

№ п/п	Проверочное соотношение
3	$k = \left(y^{kH} \alpha^{S^2} \bmod p \right) \bmod \delta$, где $p = 2rq + 1$, (k, S) — подпись
4	$k = \left(y^{k} \alpha^{S^2 \pm H} \bmod p \right) \bmod \delta$, где $p = 2rq + 1$, (k, S) — подпись
5	$k^2 = \left(y^{k} \alpha^{g \pm H} \bmod p \right) \bmod n$, где $p = 2rq + 1$, $n = rq$ и (k, g) — подпись
6	$k = \left(\left(y^{k} \alpha^{gH} \bmod p \right) + \beta^{kgv+H} \bmod n \right) \bmod \delta$, где (y, n, β) — открытый ключ
7	$k = \left(\left(y^{k+H} \alpha^{g} \bmod p \right) + \beta^{kv+gH} \bmod n \right) \bmod \delta$, где (y, n, β) — открытый ключ

5.6. Генерация числовых примеров

В качестве иллюстраций в пояснительную записку к курсовому проекту (курсовой работе) могут быть включены числовые примеры, генерируемые с помощью программы, реализующей заданную схему ЭЦП. Желательно, чтобы эти примеры отражали все этапы функционирования схемы ЭЦП:

1. Формирование системных параметров, являющихся общими для всех предполагаемых пользователей.
2. Генерацию открытого и секретного ключей.
3. Процедуру генерации подписи.
4. Процедуру проверки подлинности подписи.

Такое задание может быть использовано при проведении практических занятий. Для этого обучаемым задаются конкретные варианты схем ЭЦП с краткими теоретическими пояснениями. Они должны сгенерировать числовые примеры, иллюстрирующие вычислительный процесс на одном или нескольких этапах, указанных выше. Для этого могут быть использованы программы, позволяющие выполнять над большими числами типовые операции модульной арифметики. Ниже приводятся некоторые частные примеры.

Пример 1. Схема ЭЦП задана проверочным сравнением

$$\alpha^k \equiv Sy^{\alpha^k S \bmod p}\alpha^{\left(H\left(\alpha^k S \bmod p\right)\right)\bmod \delta} \bmod p.$$

Сформируем системные параметры:

p = 11882429488026351022427721066379892803 57;

α = 68250220082135354422389774242962653489 5;

γ = 18726613052735935810340979053 3;

δ = 1000000000000000003.

Выберем секретный ключ x = 12345678900987654321, тогда открытый ключ $y = \alpha^x \bmod p$ = 51519503062644985713521134707294411 5270.

Пусть значение хэш-функции от сообщения, которое надо подписать, равно H = 11223344556677889900.

Процедура генерации подписи:

1. Выберем случайное значение U ($U < p - 1$):

   U = 13894564231549754238457865456.

2. Вычислим значение

   $Z = \alpha^U \bmod p$ = 64701698466156431941656940816468800 2775.

3. Решая систему $\begin{cases} k + g = U \bmod \gamma, \\ k = g + xZ + \left(HZ \bmod \delta\right) \bmod \gamma, \end{cases}$ получаем:

   $$k = \frac{U - xZ - \left(HZ \bmod \delta\right)}{2} \bmod \gamma = 68742013608792151040356901280;$$

   $$g = \frac{U + xZ + \left(HZ \bmod \delta\right)}{2} \bmod \gamma = 13241868115011696130151075 4709.$$

4. Вычисляем $S = \alpha^g \bmod p$ = 25127402077641808427192285642803083 15.

Подписью является пара чисел (k, S) = (68742013608792151040356901280, 25127402077641808427192285642803083 15).

Проверка подписи:

$$Sy^{\alpha^k S \bmod p}\alpha^{\left(H\left(\alpha^k S \bmod p\right)\right)\bmod \delta} \bmod p = 55896938576706922941565114662228 1013229,$$

α^k = 55896938576706922941565114662228 1013229.

Пример 2. Схема ЭЦП задана проверочным сравнением

$$\alpha^{k+H(S\alpha^k \bmod n)} \equiv S \bmod n.$$

Генерация секретного ключа:

r = 383362910191212665347748З;

q = 453734664575509506525229;

γ' = 200734627 ($\gamma' | r-1$);

γ'' = 96948517 ($\gamma'' | q-1$);

$\gamma = \gamma'\gamma''$ = 19460924З98198159.

Генерация открытого ключа:

$n = rq$ = 173945041466301053728325502589117579353272291860З;

α = 144283268386114390834001298036541333835767938141З.

Пусть H = 786453156704564531567560.

Процедура генерации подписи:

1. Выбираем случайное значение $U < \gamma$:
   U = 344476610.
2. Вычисляем значение $Z = \alpha^U \bmod n$:
   Z = 172155816056124122192424959631233728556701770812З.
3. Решая систему сравнений $\begin{cases} k + g = U \bmod \gamma, \\ k + HZ = g \bmod \gamma, \end{cases}$ получаем:

   $$k = \frac{U - HZ}{2} \bmod \gamma = 3147453087865669;$$

   $$g = \frac{U + HZ}{2} \bmod \gamma = 16313471654809100.$$

4. Вычисляем $S = \alpha^g \bmod p$:
   S = 125230090658607125842512070317007281419514841706З.

Подписью является пара чисел (k, S):

k = 3147453087865669;

S = 125230090658607125842512070317007281419514841706З.

Проверка подписи:

$$\alpha^{k+H(S\alpha^k \bmod n)} = 125230090658607125842512070317007281419514841706 6,$$

$$S \bmod n = 125230090658607125842512070317007281419514841706 6.$$

Пример 3. Схема ЭЦП описывается проверочным сравнением

$$S^{(S^k \bmod n)} \equiv \alpha^H \bmod n.$$

Генерация секретного ключа:

$r = 863151485261213534633759$;

$q = 86247561966378373427412 43$;

$\gamma' = 498957821$ ($\gamma' \mid r - 1$);

$\gamma'' = 495912449$ ($\gamma'' \mid q - 1$);

$\gamma = \gamma'\gamma'' = 247439394959813629$.

Генерация открытого ключа:

$n = rq = 744447112114380436105374313903546348808 1109422437$;

$\alpha = 168754170955043342893915075479733762663466305991 8$.

Пусть $H = 102304506708901203564879 4$.

Процедура генерации подписи:

1. Выбираем случайное число $U < p - 1$:
   $U = 94802439$.
2. Вычисляем $Z = \alpha^U \bmod p$:
   $Z = 472845994950097711450157095105196104923471978662 4$.
3. Решая систему сравнений $\begin{cases} kg = U \bmod \gamma, \\ gZ = H \bmod \gamma, \end{cases}$ получаем

   $$k = \frac{UZ}{H} \bmod \gamma = 112067023254131784;$$

   $$g = \frac{H}{Z} \bmod \gamma = 69513503932762868.$$

4. Вычисляем $S = \alpha^g \bmod n$:
   $S = 975879197401968446233797752454854932871552031322$.

Получена подпись (k, S), где

k = 112067023254131784;

S = 97587919740196844623379775245485493287155203 1322.

Проверка подписи:

$$S^{(S^k \bmod n)} = 57405068519815122984307768133345626933414296013 24,$$

$$\alpha^H \bmod n = 57405068519815122984307768133345626933414296013 24.$$

ГЛАВА 6

Задачник

6.1. Элементы теории чисел

1. Показать существование чисел, относящихся по модулю n к простому делителю γ функции Эйлера $\varphi(n)$ как к показателю, где $n = p$, $n = p^k$ или $n = 2p^k$ (p — простое нечетное число, k — натуральное число).
2. Доказать, что квадратичный вычет по простому модулю не является первообразным корнем по этому же модулю.
3. Пусть все отличные от 1 квадратичные вычеты по простому модулю p относятся по $\bmod p$ к одному и тому же простому показателю q. Доказать, что $p = 2q + 1$.
4. Найти число, относящееся по простому модулю p к показателю γ и одновременно являющееся квадратичным невычетом по этому же модулю, для случаев а) $\gamma = 2$, $p = 23$; б) $\gamma = 7$, $p = 23$; в) $\gamma = 11$, $p = 23$; г) $\gamma = 4$, $p = 29$; д) $\gamma = 11$, $p = 67$.
5. Доказать, что биномиальный коэффициент C_p^k, где p — простое число, при $1 \le k < p$ делится на p.
6. Используя метод математической индукции, доказать, что для любого m и простого p, таких что $m < p$, справедливо равенство $m^p \bmod p = m$.
7. Доказать, что для любых целых чисел a и b справедливо равенство $(a + b)^p \bmod p = (a^p + b^p) \bmod p$, где p — простое число.
8. Пусть a — квадратичный вычет по простому модулю p, причем $p \equiv 3 \bmod 4$. Доказать, что квадратный корень из a может быть вычислен по формуле $\sqrt{a} = a^{\frac{p+1}{4}} \bmod p$.
9. Пусть a — квадратичный вычет по простому модулю p, причем $p \equiv 7 \bmod 8$. Доказать, что квадратный корень из a может быть вычислен по формуле $\sqrt{a} = a^{\frac{p+1}{4}} \bmod p$.

10. Найти число, относящееся к показателю γ одновременно по простому модулю q и по простому модулю p (рассмотреть случай выполнения условий $\gamma | q-1$ и $\gamma | p-1$, причем γ^2 не делит ни одно из чисел $q-1$ и $p-1$).

11. Найти число, относящееся к показателю γ одновременно по простому модулю q и по простому модулю p (рассмотреть случай выполнения условий $\gamma^s | p-1$ и $\gamma^s | q-1$, где s есть значение степени числа γ в разложении обоих чисел $p-1$ и $q-1$).

12. Найти число, относящееся по простому модулю p к показателю γ и одновременно относящееся по простому модулю q к показателю δ, в случае выполнения следующих условий НОД$(\gamma, q-1)=1$ и НОД$(\delta, p-1)=1$.

13. Показать способ нахождения числа, относящегося к числу γ как к показателю по модулю p ($\gamma | p-1$) и к числу δ как к показателю по модулю q ($\delta | q-1$). Рассмотреть следующий случай: p и q — числа, для которых НОД$(p, q)=1$, НОД$(\delta, \gamma)=1$, НОД$(\gamma, q-1)=1$ и НОД$(\delta, p-1)=1$.

14. Пусть известно разложение числа $p-1$, где p есть большое простое число размера 1024 бит, причем в разложении имеется простой множитель γ размера 160 бит. Указать вычислительно эффективный способ нахождения числа α, относящегося к показателю γ.

15. Пусть известно разложение числа $p-1$, где p есть большое простое число. Указать вычислительно эффективный способ нахождения числа α, относящегося к показателю $\gamma = d_1 d_2 d_3$ (произведение трех простых делителей числа $p-1$).

16. Доказать, что первообразные корни по простому модулю являются квадратичными невычетами по этому же модулю.

17. Известно, что первообразные корни по простому модулю являются квадратичными невычетами по этому же модулю. Верно ли обратное утверждение?

18. Доказать, что первообразный корень по простому модулю $p \geq 3$ является квадратичным невычетом степени $n | p-1$.

19. Пусть известно разложение числа $p-1$, где p есть простое число. Как проверить то, что число α является первообразным корнем?

20. Для числа α, относящегося к простому показателю γ по простому модулю p, имеется γ различных чисел $\{\alpha^1, \alpha^2 \bmod p, \alpha^3 \bmod p, \ldots, \alpha^\gamma \bmod p = 1\}$. Доказать, что все эти числа относятся по модулю p к показателю γ.

21. Пусть число α есть первообразный корень по простому модулю p. Доказать, что число $\alpha^{-1} \bmod p$ также является первообразным корнем по модулю p.

22. Числа α и β относятся по модулю n к простым показателям γ и δ соответственно. Доказать, что для всех $i \in \{1, 2, \ldots, \gamma - 1\}$ и $j \in \{1, 2, \ldots, \delta - 1\}$ числа $\alpha^i \beta^j$ относятся по mod n к показателю $\varepsilon = \gamma\delta$.

23. Пусть некоторое число δ есть показатель по модулю n. Доказать, что любой простой делитель γ числа δ является показателем по модулю n.

24. Пусть некоторое число δ есть показатель по модулю n и некоторый делитель γ числа δ представим в виде произведения двух простых чисел: $\gamma = \pi\sigma$. Доказать, что γ является показателем по модулю n.

25. Пусть некоторое число δ есть показатель по модулю n и некоторый делитель γ числа δ представим в виде произведения нескольких простых чисел: $\gamma = \pi\sigma \ldots \tau$. Доказать, что γ является показателем по модулю n.

26. Пусть некоторое число δ есть показатель по модулю n и некоторый делитель γ числа δ представим в виде $\gamma = \pi^k$, где π — простое число, k — натуральное число. Доказать, что γ является показателем по модулю n.

27. Пусть некоторое число δ есть показатель по модулю n и γ есть некоторый делитель числа δ. Доказать, что γ является показателем по модулю n.

28. Показать, что если число $a = b^{L(m)/\gamma} \bmod m \neq 1$, где γ есть некоторый делитель обобщенной функции Эйлера $L(m)$, относится к показателю γ по модулю $m = pq$, причем γ входит в каноническое разложение чисел $\varphi(p)$ и $\varphi(q)$ в степени s и $t < s$ соответственно, то $a \equiv 1 \bmod q$.

29. Доказать следующее утверждение: если существует двукратный первообразный корень по mod p^α и по mod q^β, то обобщенная функция Эйлера числа $p^\alpha q^\beta$ есть показатель по mod $(p^\alpha q^\beta)$.

30. Найти число, являющееся одновременно первообразным корнем по mod p^α и по mod q^β.

31. Для любых ли значений чисел m, n, $\delta \mid \varphi(m)$ и $\gamma \mid \varphi(n)$ можно найти число x, относящееся к числам δ и γ как к показателям по модулю m и модулю n соответственно?

32. Предложить вычислительно эффективный способ нахождения числа x, относящегося к числам δ и γ как к показателям по mod p и по mod q, где p и q — простые числа, $\delta \mid p - 1$ и $\gamma \mid q - 1$.

33. Оценить верхнюю границу мощности множества чисел $\{x: 1 < x < pq\}$, относящихся к числам δ и γ как к показателям по $\bmod p$ и по $\bmod q$, где p и q — простые числа, $\delta \mid p-1$ и $\gamma \mid q-1$.

34. Пусть требуется найти число α, относящееся по модулю p к показателю γ, длина которого существенно меньше длины p, и одновременно являющееся первообразным корнем по простому модулю q. Предложите вычислительно эффективный способ решения этой задачи.

35. Пусть требуется найти число α, относящееся по модулю p к показателю γ, длина которого существенно меньше длины p, и одновременно являющееся квадратичным вычетом по модулю q. Предложите вычислительно эффективный способ решения этой задачи.

36. Пусть p и q — простые числа и α есть число, относящееся к простому показателю γ по модулю pq. Тогда имеем $\alpha^{\gamma} \equiv 1 \bmod (pq) \Rightarrow \alpha^{\gamma} \equiv 1 \bmod p$ и $\alpha^{\gamma} \equiv 1 \bmod q$. Очевидно, что может иметь место случай, когда γ делит только одно из чисел $p-1$ и $q-1$. Объясните, почему в этом случае γ не может быть показателем одного из чисел.

37. Пусть требуется найти число α, относящееся по простому модулю p к показателю γ, длина которого существенно меньше длины p, и одновременно являющееся квадратичным невычетом по RSA-модулю $n = pq$. Предложите вычислительно эффективный способ решения этой задачи.

38. Найти натуральное число α, относящееся к простому показателю γ по модулю p и по модулю q, где p и q — простые числа, причем γ входит в каноническое разложение чисел $p-1$ и $q-1$ в одинаковой степени $s \geq 1$ и $\text{НОД}\left(\frac{p-1}{2\gamma^s}, \frac{q-1}{2\gamma^s}\right) = 1$.

39. Показать, что не существует числа α, относящегося к простому показателю γ по модулю p и по модулю q, где p и q — простые числа, если γ входит в каноническое разложение чисел $p-1$ и $q-1$ в различной степени.

40. Для числа $\alpha < p$, относящегося к показателю γ по простому модулю p, имеется γ различных чисел $\{\alpha^1, \alpha^2 \bmod p, \alpha^3 \bmod p, \ldots, \alpha^{\gamma} \bmod p = 1\}$, для которых при любом $i < \gamma$ имеем $(\alpha^i)^{\gamma} = (\alpha^{\gamma})^i \equiv 1 \bmod p$. Относятся ли все эти числа к показателю γ? Содержатся ли среди этих чисел все числа, относящиеся к показателю γ? Содержатся ли среди них числа, не относящиеся к показателю γ?

41. Доказать, что индексы первообразных корней по простому модулю есть числа, взаимно простые с числом $p-1$.

42. Доказать следующее утверждение. Если НОД$(z, p-1) \neq 1$, где p — простое число ($p > 2$) и z — индекс некоторого числа $a < p-1$ (т. е. $z = \text{ind}\, a$), то a не является первообразным корнем.

43. Доказать, что при любом основании g индекс i (по простому модулю p) числа a удовлетворяет соотношению НОД$(i, p-1) = d$, где число d не зависит от g.

44. Найти количество классов по простому модулю p, индекс которых удовлетворяет условию НОД$(i, p-1) = d$, где d есть некоторый делитель числа $p-1$.

45. Сколько имеется различных первообразных корней по простому модулю p?

46. Доказать, что любое число i, такое что НОД$(i, p-1) = 1$, является индексом первообразного корня.

47. Число a ($a \bmod p \neq 1$) относится по простому модулю p к простому показателю δ. Доказать, что индекс i числа a (по модулю p) удовлетворяет условию $\text{НОД}(i, p-1) = \dfrac{p-1}{\delta}$.

48. Число a ($a \bmod p \neq 1$) относится по простому модулю p к показателю δ. Доказать, что индекс i числа a (по модулю p) удовлетворяет условию $\text{НОД}(i, p-1) = \dfrac{p-1}{\delta}$.

49. Индекс i (по простому модулю p) числа a ($a \bmod p \neq 1$) удовлетворяет условию $\text{НОД}(i, p-1) = \dfrac{p-1}{\delta}$. Показать, что число a относится к показателю δ.

50. Индекс некоторого числа g является взаимно простым с $p-1$, где p есть простое число. Доказать, что g есть первообразный корень по модулю p.

51. Пусть число a относится по простому модулю p к показателю γ. Доказать, что a представимо в виде $a \equiv b^{\frac{p-1}{\gamma}} \bmod p$.

52. Тест на простоту числа p состоит в проверке выполнимости соотношения $a^{\varphi(n)} = 1 \bmod n$, где $n = pq$ и q — заведомо простое число. Показать, что этот тест является эквивалентным тесту Ферма по отношению к числам Кармайкла.

53. Дано значение модуля. Как найти число, относящееся к заданному составному показателю по этому модулю?

54. Вычислить число первообразных корней по модулям 67; 47; 97; 131.

55. Определить количество чисел, относящихся к показателю 2 по модулям 67; 47; 97; 131.

56. Определить количество чисел, относящихся к показателю 11 по модулям 23; 67; 133.

57. Оценить вероятность того, что случайно выбранное число $a < p$ окажется первообразным корнем по модулю p.

58. Указать все показатели по модулям 17, 196 и 625.

59. Указать все показатели по модулю $n = 3 \cdot 5 \cdot 129 \cdot 257$.

60. Оценить вероятность случайного выбора числа $a < p$, где p — простое число, относящегося к делителю $\delta | p - 1$ как к показателю.

61. Оценить вероятность того, что для случайного числа $\beta (1 < \beta < p)$ будет выполняться сравнение $\beta^{(p-1)/\delta} \bmod p \neq 1$ (это вероятность генерации числа, относящегося к показателю δ), где $p = 2\delta rq + 1$, причем δ, r и q — простые числа.

62. Пусть g — первообразный корень по простому модулю p. Показать, что для любого числа $a < p - 1$, взаимно простого с $p - 1$, и любого делителя δ числа $p - 1$ выполняется условие $(g^a)^{\frac{p-1}{\delta}} \bmod p \neq 1$.

63. Пусть простой модуль p представим в виде $p = 4k + 1$. Показать, что если число a является квадратичным вычетом (невычетом), то число $p - a$ является квадратичным вычетом (невычетом).

64. Пусть простой модуль p представим в виде $p = 4k + 3$. Показать, что если число a является квадратичным вычетом (невычетом), то число $p - a$ является квадратичным невычетом (вычетом).

65. Чему равен наибольший общий делитель двух последовательных натуральных чисел n и $n + 1$? Объясните почему.

66. Показать, что при любом простом p число p делит число $2^p - 2$.

67. Показать, что для любого натурального $n > 2$ функция Эйлера $\varphi(n)$ принимает четные значения.

68. Чему равна вероятность случайного выбора двух целых чисел, которые делятся на заданное число d?

69. Пусть вероятность случайного выбора двух взаимно простых натуральных чисел a и b равна $P = \Pr[\text{НОД}(a,b) = 1]$. Определите вероятность

P_d = Pr[НОД(a,b) = d] случайного выбора двух чисел, наибольший общий делитель которых равен d.

70. Используя равенство $\sum_{i=1}^{\infty} \frac{1}{i^2} = \frac{\pi^2}{6}$, вычислите вероятность случайного выбора двух чисел a и b, таких что НОД (a, b) = 1.

71. Доказать, что для простых чисел вида $p = 2^k \gamma + 1$, где γ — простое число, вероятность случайного выбора числа α ($\alpha < p$), относящегося по модулю p к показателю δ ($\delta < p - 1$), не содержащему делитель γ, равна $1/\gamma$.

72. Доказать, что для простых чисел вида $p = 2a^k \gamma + 1$, где a и γ — простые числа, вероятность случайного выбора числа α ($\alpha < p$), относящегося по модулю p к показателю δ ($\delta < p - 1$), не содержащему делитель γ, равна $1/\gamma$.

73. Доказать, что для простых чисел вида $p = 2u\gamma + 1$, где u и γ — простые числа, вероятность случайного выбора числа α ($\alpha < p$), относящегося по модулю p к показателю δ ($\delta < p - 1$), не содержащему делитель γ, равна $1/\gamma$.

74. Доказать, что для простых чисел вида $p = 2^k \gamma r + 1$, где r и γ — простые числа, вероятность случайного выбора числа α ($\alpha < p$), относящегося по модулю p к показателю δ ($\delta < p - 1$), не содержащему делитель γ, равна $1/\gamma$.

75. Доказать, что для простых чисел вида $p = 2^k \gamma rz + 1$, где r, z и γ — простые числа, вероятность случайного выбора числа α ($\alpha < p$), относящегося по модулю p к показателю δ ($\delta < p - 1$), не содержащему делитель γ, равна $1/\gamma$.

76. Доказать, что нечетное число a является первообразным корнем по модулю $2p$ тогда и только тогда, когда a является первообразным корнем по модулю p.

77. Сколько существует различных первообразных корней по модулю $2p$?

78. Доказать, что нечетное число a является первообразным корнем по модулю $2p^{\alpha}$ тогда и только тогда, когда a является первообразным корнем по модулю p^{α}.

79. Доказать, что нечетное число a относится по модулю $2p^{\alpha}$, где $\alpha \geq 1$, к показателю $\gamma | p^{\alpha-1}(p-1)$ тогда и только тогда, когда a относится по модулю p^{α} к показателю γ.

80. Показать, что число классов, относящихся по модулю $2p^{\alpha}$ к показателю $\gamma | p^{\alpha}(p-1)$, равно числу классов, относящихся к γ как к показателю по модулю p^{α}.

81. Сколько существует различных чисел, относящихся по модулю $2p$ к показателю $\gamma | (p-1)$?

82. Числа a и b относятся по модулю n к показателям γ и δ соответственно. Показать, как можно найти число x, относяшееся к показателю $\varepsilon = \text{НОД}(\gamma, \delta)$.

83. Числа a и b относятся по модулю n к показателям γ и δ соответственно. Показать, как можно найти число x, относящееся к показателю $\eta = \text{НОК}[\gamma, \delta]$.

84. Показать, что для значения b, являющегося взаимно простым с n, выполняется соотношение $a/b \equiv ab^{\varphi(n)-1} \bmod n$, где $\varphi(n)$ — функция Эйлера.

85. Вывести формулу $\varphi(p^{\alpha}) = p^{\alpha-1}(p-1)$ для значения функции Эйлера от числа p^{α}, где p — простое число.

86. Сколько в множестве последовательных натуральных чисел $\{1, 2, \ldots, 5000\}$ имеется таких чисел, которые являются взаимно простыми с числом 50?

87. Сколько в множестве последовательных натуральных чисел $\{1, 2, \ldots, 30000\}$ имеется таких чисел, которые не являются взаимно простыми с числом 50?

88. Предложить способ генерации простого числа p длины $\approx |p|$, такого что $p-1$ содержит заданный простой множитель γ длины $|\gamma| \approx \frac{1}{4}|p|$.

89. Доказать, что число a, относящееся по модулю p^{α}, где $\alpha > 1$, к простому показателю $\gamma \neq p$, относится к этому же показателю и по модулю p.

90. Доказать, что первообразный корень по простому модулю p относится по модулю p^{α}, где $\alpha > 1$, к показателю $p^{\alpha-1}(p-1)$, где $i \in \{1, 2, \ldots, \alpha\}$.

91. Показать, что число a, относящееся по модулю p к простому показателю γ, не всегда относится к этому же показателю и по модулю p^{α}, где $\alpha > 1$. Указать число a, такое что $a^{\gamma} \equiv 1 \bmod p$ и $a^{\gamma} \bmod p^{\alpha} \neq 1$.

92. Показать, что для числа a, относящегося по модулю p^{α} к показателю $\delta = p^{i}$, где $i = 1, 2, \ldots, \alpha - 1$, выполняется сравнение $a \equiv 1 \bmod p$.

93. Показать, что для числа a, относящегося по модулю p^{α} к показателю $\delta = p^{i}\gamma$, где γ — простой делитель числа $p - 1$ и $i = 1, 2, \ldots, \alpha - 1$, выполняется сравнение $a^{\gamma} \equiv 1 \bmod p$, т. е. a относится по модулю p к показателю γ.

94. Доказать, что при простом p число $p - 1$ относится по модулю p к показателю 2. Существуют ли числа другого вида, относящиеся по простому модулю к показателю 2?

95. По какому из модулей 13, 79 и 89 существует больше чисел, относящихся к показателю 3?

96. Доказать следующее утверждение. Если существует квадратный корень из a по модулю $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$, то a — квадратичный вычет по каждому из простых модулей $p_1, p_2, \ldots, p_s$.

97. Найти все числа, относящиеся к показателю 2 одновременно по модулю 13 и по модулю 43.

98. Найти все числа, относящиеся к показателю 2 одновременно по модулю 77 и по модулю 119.

99. Показать, что для простых чисел p и q задача дискретного логарифмирования по RSA-модулю $n = pq$ эквивалентна по сложности задаче дискретного логарифмирования по модулям p и q.

100. Решить систему сравнений $x \equiv a \bmod m_1$ (1) и $x \equiv b \bmod m_2$ (2) для случая НОД$(m_1, m_2) = 1$.

101. Вычислить значение $\left(3^{57^{127}}\right) \bmod 19$.

102. Решить систему сравнений $\begin{cases} x \equiv 17 \bmod 39, \\ x^2 \equiv 19 \bmod 79. \end{cases}$

103. Решить систему сравнений $\begin{cases} x \equiv 11 \bmod 51, \\ x^3 \equiv 11 \bmod 47. \end{cases}$

104. Решить систему сравнений $\begin{cases} x \equiv 11 \bmod 51, \\ x^2 \equiv 11 \bmod 47. \end{cases}$

105. Решить систему сравнений $\begin{cases} x \equiv 37 \bmod 137, \\ x^{10} \equiv 37 \bmod 127. \end{cases}$

106. Сколько решений имеют сравнения $x^4 \equiv 37 \bmod 79$ (1); $x^4 \equiv 76 \bmod 79$ (2) и $x^4 \equiv 9 \bmod 79$ (3)?

107. Определить, какие из чисел 1034, 1234, 1959, 2477, 3074 и 4179 являются квадратичными вычетами по RSA-модулю $n = 5963$.

108. Вычислить значение функции Эйлера и обобщенной функции Эйлера для чисел 2301; 900 и 10965.

109. Вычислить значение функции Эйлера и обобщенной функции Эйлера для чисел $2(2^{16}+1)$; 254; 2^k, где k — натуральное число.

110. Найти линейное представление с целыми коэффициентами для наибольшего общего делителя чисел $a = 13$; $b = 87$.

111. Найти линейное представление для наибольшего общего делителя чисел $a = 11$; $b = 97$.

112. Найти линейное представление для наибольшего общего делителя чисел $a = 23$; $b = 121$.

113. Найти линейное представление для наибольшего общего делителя чисел $a = 35$; $b = 169$.

114. Найти все целочисленные решения уравнения $34x + 289y = 187$.

115. Извлечь кубический корень из чисел 5, 21, 31, 32, 36, 37 и 39 по модулю 41.

116. Извлечь квадратный корень из чисел 11, 17, 51, 99, 105, 121 и 132 по модулю 139.

117. Извлечь корень четвертой степени по модулю 137 из числа 81.

118. Решить сравнение $x^3 \equiv 8 \bmod 19$.

119. Решить сравнение $x^5 \equiv 32 \bmod 101$.

120. Пусть x_0 есть корень сравнения $\sqrt[n]{x} \equiv a \bmod p$, где $a \neq 1$, и $n \mid p-1$. Описать процедуру нахождения всех остальных корней.

121. Сколько решений имеют сравнения $x^3 \equiv 89 \bmod 139$ (1), $x^3 \equiv 33 \bmod 139$ (2) и $x^3 \equiv 89 \bmod 137$ (3)?

122. При каких значениях a система сравнений $\begin{cases} x \equiv a \bmod 139, \\ x^3 \equiv 45 \bmod 139 \end{cases}$ имеет решения?

123. По каким простым модулям число 1521 является квадратичным вычетом?

124. По каким простым модулям число $N = p_1^{2s_1} \cdot p_2^{2s_2} \cdot \ldots \cdot p_k^{2s_k}$, где $p_1, p_2, \ldots, p_k$ — простые числа, является квадратичным вычетом?

125. Корни каких степеней n ($n \le 66$) из числа 58 существуют по модулю 67?

126. Доказать, что первообразный корень по простому модулю является невычетом по любой степени.

6.2. Схемы ЭЦП

6.2.1. ЭЦП на основе сложности факторизации

1. Вычислить закрытый ключ d криптосистемы RSA, соответствующий открытому ключу $e = 97$, для значений модуля $n_1 = 299$ и $n_2 = 527$.

2. Вычислить открытый ключ e криптосистемы RSA, соответствующий закрытому ключу $d = 101$, для значений модуля $n_1 = 187$ и $n_2 = 319$.

3. Вычислить закрытый ключ d криптосистемы RSA, соответствующий открытому ключу $e = 151$, для значений модуля $n_1 = 299$ и $n_2 = 551$.

4. В криптосистеме RSA при значении модуля $n = 187$ и открытом ключе $e = 141$ ($e = 101$) зашифрование сообщений $M = 67$ и $M = 69$ не приводит к преобразованию последних. Объясните почему.

5. Какому условию должен удовлетворять открытый ключ e и модуль n в криптосистеме RSA, чтобы 7 последовательных шифрований возвращали исходное значение сообщения?

6. Чему равно минимальное значение веса Хемминга у шифрующей экспоненты e в криптосистеме RSA?

7. Показать, что для модуля n системы RSA выполняется условие $\varphi(n^2) = n\varphi(n)$.

8. В криптосистеме RSA с модулем $n = 5963$ и закрытым $d = 37$ и открытым $e = 157$ ключами пятикратное шифрование сообщения $M = 57$ дает криптограмму, совпадающую с исходным сообщением. При этом для других исходных сообщений M пятикратное шифрование не возвращает начальное значение. Объясните почему.

9. Может ли в системе RSA с модулем $n = 190847$ шестикратное зашифрование произвольного сообщения m быть эквивалентным процедуре подписывания? А в случае следующих значений модуля n: а) 280081, б) 50629, в) 170171, г) 5448187?

10. Показать, как можно разложить RSA-модуль n по известному значению функции Эйлера $\varphi(n) = 2^s t$, где t — нечетное число.

11. Предложить схему слепой подписи с уравнением проверки подписи $S^3 \bmod n = H$, где S — подпись, H — хэш-функция от подписываемого документа.

12. Записать процедуру генерации подписи (S, R) в схеме ЭЦП с уравнением проверки подписи $H \| R \equiv S^2 \bmod n$, где n — RSA-модуль. С какой целью используется параметр R? Из каких соображений может выбираться размер этого числа? Какие дополнительные требования накладываются на модуль n по сравнению со схемой RSA?

13. Является ли стойкой схема ЭЦП с уравнением проверки подписи $H = S^2 + SR \bmod n$, где n — RSA-модуль, (R, S) — подпись?

14. Является ли стойкой схема ЭЦП с уравнением проверки подписи $H = S^3 + S^2 R \bmod n$, где n — RSA-модуль, (R, S) — подпись?

15. Является ли стойкой схема ЭЦП с уравнением проверки подписи $H = R^2 + RS^2 \bmod n$, где n — RSA-модуль? С какой целью используется параметр R? Какие могут быть даны рекомендации по выбору модуля?

16. Составить уравнение генерации подписи в схеме ЭЦП с уравнением проверки $\alpha = (S + H)^H \bmod n$, где n — RSA-модуль. Является ли целесообразным переход от исходного уравнения проверки подписи вида $S^H \bmod n = \alpha$ к указанному выше соотношению?

17. Составить уравнение генерации подписи в схеме ЭЦП с уравнением проверки $\alpha = (SH)^H \bmod n$, где n — RSA-модуль. Обосновать переход от исходного уравнения проверки подписи $S^H \bmod n = \alpha$ к указанному выше. Сравнить со схемой ЭЦП из предыдущей задачи. Какая из них предпочтительна?

18. Рассмотреть систему ЭЦП с уравнением проверки $S^{H^2+H} \bmod n = \alpha$, где (n, α) — открытый ключ, n — RSA-модуль. Вывести формулу для расчета подписи. С какой целью в качестве показателя в этом уравнении используется сумма значения хэш-функции и его квадрата? Как изменится время генерации и время проверки подписи?

19. Рассмотреть систему ЭЦП с проверочным сравнением следующего вида $\alpha^{H \operatorname{div} 2^{64}} + (H \bmod 2^{64}) \cdot 2^{64} \equiv S^H \bmod n$, где (n, α) — открытый ключ, n — RSA-модуль, H — 128-битовое значение хэш-функции. Записать формулу для вычисления подписи. С какой целью осуществлено усложнение исходного уравнения проверки подписи $\alpha = S^H \bmod n$? Как изменится время генерации и время проверки подписи?

20. В схеме ЭЦП с RSA-модулем $n = pq$ и открытым ключом (n, α) подписью является пара чисел (R, S). Уравнение проверки подписи имеет вид

$R^H \equiv \alpha^{SR} \bmod n$. Оценить длину подписи. Модифицировать уравнение проверки с целью сокращения размера подписи.

21. В схеме ЭЦП с уравнением проверки подписи $\alpha = S^H \bmod n$, где $n =$ $= 18165893$, выбрать закрытый ключ γ и вычислить открытый ключ α.

22. В схеме ЭЦП с уравнением проверки подписи $\alpha = S^H \bmod n$, где $n =$ $= 2267509013701$, выбрать закрытый ключ γ и вычислить открытый ключ α.

23. В схеме ЭЦП с уравнением проверки подписи $\alpha = S^H \bmod n$, где $n =$ $= 288949277$, выбрать закрытый ключ γ и вычислить открытый ключ α.

24. Является ли стойкой схема ЭЦП с проверочным сравнением $S\alpha^{H(S\alpha^k \bmod n)} \equiv 1 \bmod n$, где (k, S) — подпись? Предложите вариант ее усиления путем введения дополнительного неравенства.

25. Сравните схемы ЭЦП, заданные проверочными уравнениями $k =$ $= (\alpha'^{kgH} \bmod p') \bmod \delta \quad (|g| < \frac{2}{3}|p'|)$ и $k = (\alpha^{kgH} \bmod n) \bmod \delta$, где n — RSA-модуль ($n = pq$ и $|n| \approx |p'|$); $p' = 2n' + 1$ — простое число; $n' =$ $= r'q'$ — произведение двух больших простых чисел r' и q', таких что $|r'| \approx |q'| \approx 0.5|p'|$; α' — число, относящееся по модулю p' к показателю q'; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$; δ — некоторое простое число ($0.2|n| < |\delta| < 0.5|n|$). В первой схеме секретным ключом является значение q', а открытым ключом — пара чисел (p', α'). Во второй схеме секретным ключом является значение γ, а открытым ключом — пара чисел (n, α). Подписью является пара чисел (k, g). Опишите отличительные особенности этих двух схем и процедуру генерации подписи.

26. В некоторой схеме ЭЦП, заданной проверочным уравнением $k =$ $= (\alpha_1^{k+g} \alpha_2^{(v+g)H} \bmod n) \bmod \delta$, где n — RSA-модуль ($n = pq$); (n, α_1, α_2) — открытый ключ; α_1 — число, относящееся по модулю n к показателю $\gamma_1 | \varphi(n)$; α_2 — число, относящееся по модулю n к показателю $\gamma_2 | \varphi(n)$; γ_1 и $\gamma_2 \neq \gamma_1$ — секретные числа; δ — некоторое простое число ($|\gamma_1| < |\delta| < |\gamma_2|$), подписью является тройка чисел (k, g, v). Опишите процедуру генерации подписи. Каким специфическим требованиям должны удовлетворять числа γ_1 и γ_2?

27. Схема ЭЦП представлена проверочным уравнением следующего вида $M = S\alpha^{(S\alpha^k \bmod n)} \bmod n$, где n — RSA-модуль ($n = pq$); (n, α) — откры-

тый ключ; M — подписываемое сообщение; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$. Подписью является пара чисел (k, S). Опишите процедуру генерации подписи. Каким специфическим требованиям должны удовлетворять числа α и γ?

28. Схема ЭЦП представлена проверочным уравнением $k = (\alpha^{k+g} \bmod n) \cdot (\alpha^{(v+g)M} \bmod n) \bmod \delta$, где n — RSA-модуль $(n = pq)$; (n, α) — открытый ключ; M — подписываемое сообщение; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$; γ — секретное число, не связанное с простым модулем δ. Подписью является тройка чисел (g, k, v). Опишите процедуру генерации подписи.

29. Схема ЭЦП представлена проверочным уравнением $k = (\alpha^{k+g-v} \bmod n) \cdot (\alpha^{(v+g)M} \bmod n) \bmod \delta$, где n — RSA-модуль $(n = pq)$; (n, α) — открытый ключ; M — подписываемое сообщение; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$; γ — секретное число, не связанное с простым модулем δ. Подписью является тройка чисел (g, k, v). Опишите процедуру генерации подписи.

30. Схема ЭЦП представлена проверочным уравнением вида $k + v = (\alpha^{kgvH} \bmod n)^{(k - v \bmod \delta)} \bmod \delta$, где n — RSA-модуль $(n = pq)$; (n, α) — открытый ключ; M — подписываемое сообщение; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$; γ — секретное число, не связанное с простым модулем δ. Подписью является тройка чисел (g, k, v). Опишите процедуру генерации подписи.

31. Схема ЭЦП представлена проверочным уравнением вида $k = (\alpha^{kg} \bmod n)^H \bmod \delta$, где n — RSA-модуль $(n = pq)$; (k, g) — подпись; α — число, относящееся по модулю n к показателю $\gamma = \gamma' \gamma''$ (γ' и γ'' есть простые делители: $\gamma' | p - 1$ и $\gamma'' | q - 1$, причем γ' не делит $q - 1$ и γ'' не делит $p - 1$); γ — секретный ключ; H — хэш-функция от подписываемого документа. Показать, как формируются значения γ и α. Описать процедуру генерации подписи.

32. Схема ЭЦП представлена проверочным уравнением вида $M = k(\alpha^{k+g} \bmod n) \bmod \delta$, где n — RSA-модуль $(n = pq)$; (k, g) — подпись; α — число, относящееся по модулю n к показателю $\gamma = \gamma' \gamma''$ (γ' и γ'' есть простые делители: $\gamma' | p - 1$ и $\gamma'' | q - 1$); γ — секретный ключ; H — хэш-функция от подписываемого документа. Как формируются значения γ и α? Описать процедуру генерации подписи.

33. В схеме ЭЦП с RSA-модулем $n = pq$ подписью является пара неравных между собой чисел (R, S), где длина каждого из чисел больше 100 бит. Сравнение проверки подписи имеет вид $R^H \equiv S^{RS \bmod n} \bmod n$. Показать, как генерируется подпись.

34. В схеме ЭЦП с RSA-модулем $n = pq$ подписью является пара неравных между собой чисел (R, S), где длина каждого из чисел больше 100 бит. Сравнение проверки подписи имеет вид $R^H \equiv S^{(RS \bmod n)} \bmod n$. Обосновать требования к выбору секретного ключа $\gamma = \gamma'\gamma''$ (см. задачу 32).

35. Пусть простое число γ делит $\varphi(m)$ и не делит $\varphi(\delta)$, где φ — функция Эйлера. Доказать, что число α, относящееся к показателю γ по модулю $m\delta$, сравнимо с 1 по модулю δ. Верно ли доказываемое утверждение для произвольного числа γ?

36. В схеме ЭЦП с RSA-модулем $n = pq$ и открытым ключом (n, α) подписью является пара неравных между собой чисел (R, S), где длина каждого из чисел больше 100 бит. Сравнение проверки подписи имеет вид $RS^{(RS \bmod n)} \equiv \alpha^H \bmod n$. Описать процедуру генерации подписи. Можно ли в этой схеме осуществить подделку подписи, т. е. сформировать подпись без знания секретного ключа?

37. В схеме ЭЦП с RSA-модулем $n = pq$ и открытым ключом (n, α) подписью является пара неравных между собой чисел (R, S), где длина каждого из чисел больше 100 бит. Сравнение проверки подписи имеет вид $RS^{(R:S \bmod n)} \equiv \alpha^{H(R:S \bmod n)} \bmod n$. Описать процедуру генерации подписи. Можно ли в этой схеме осуществить подделку подписи, т. е. сформировать подпись без знания секретного ключа?

38. В схеме ЭЦП с RSA-модулем $n = pq$ и открытым ключом (n, α) подписью является пара неравных между собой чисел (R, S), где длина каждого из чисел больше 100 бит. Сравнение проверки подписи имеет вид $RS^H \equiv \alpha^{(RS^2 \bmod n)} \bmod n$. Описать процедуру генерации подписи. Можно ли в этой схеме осуществить подделку подписи?

39. В схеме ЭЦП с RSA-модулем $n = pq$ уравнение проверки подписи (R, S) имеет вид $R = S^{H(RS \bmod n)} \bmod n$, где $R \neq 1$ и $S \neq 1$. Записать формулы, по которым генерируется подпись. Можно ли подделать подпись с использованием новой переменной $Z = RS \bmod n$?

40. В схеме ЭЦП с RSA-модулем $n = pq$ уравнение проверки подписи (R, S), где длина каждого из чисел больше 100 бит, имеет вид $R = S^{(RS)^H \bmod n} \bmod n$. Записать формулы, по которым генерируется подпись.

41. Может ли практически использоваться схема ЭЦП с RSA-модулем $n = pq$, в которой уравнение проверки подписи (R, S) имеет вид

$R = S^{(RS \bmod n)^H} \bmod n$? Записать формулы, по которым генерируется подпись. Почему требуется, чтобы длина чисел R и S была больше некоторого достаточно большого значения, например, превышала 100–200 бит?

42. В схеме ЭЦП с RSA-модулем $n = pq$ и открытым ключом (n, α) подписью является пара неравных между собой чисел (R, S), где длина каждого из чисел больше 100 бит. Сравнение проверки подписи имеет вид $RS \equiv \alpha^{(RS^H \bmod n)} \bmod n$. Описать процедуру генерации подписи. В связи с чем в процедуру проверки подписи включено требование, чтобы размер чисел R и S был достаточно большим?

43. В схеме ЭЦП с RSA-модулем $n = pq$ уравнение проверки подписи (R, S), где длина каждого из чисел больше 100 бит, имеет вид $R = S^{(SR^H \bmod n)} \bmod n$. Записать формулы, по которым генерируется подпись.

44. В схеме ЭЦП с RSA-модулем $n = pq$ уравнение проверки подписи (R, S), где длина каждого из чисел больше 100 бит, имеет вид $R = S^{(S^{1/H} R^H \bmod n)} \bmod n$. Записать формулы, по которым генерируется подпись. Может ли данная система ЭЦП использоваться на практике?

45. В схеме ЭЦП с RSA-модулем $n = pq$ сравнение проверки подписи (R, S), где длина каждого из чисел R и S больше 100 бит, имеет вид $R^H \equiv S^{(RS^H \bmod n)} \bmod n$. Записать формулы, по которым генерируется подпись.

46. Показать, как генерируется подпись (R, S, V), где длина каждого из чисел R, S и V больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $R^{(VS \bmod n)} \equiv S^H V^{(RS \bmod n)} \bmod n$, где n есть открытый ключ и секретным ключом является разложение модуля n. Записать формулы, по которым генерируется подпись. Является ли стойкой данная схема ЭЦП?

47. Показать, как генерируется подпись (R, S, V), где длина каждого из чисел R, S и V больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $V^H R^{(VRS \bmod n)} \equiv S^{(VS/R \bmod n)} \bmod n$, где n есть открытый ключ и секретным ключом является разложение модуля n. Записать формулы, по которым генерируется подпись. Рассмотреть возможность подделки подписи путем замены переменных.

48. Корректна ли схема ЭЦП со сравнением проверки подписи вида $R^{(VS \bmod n)} \equiv S^{(VR \bmod n)} V^{H(RS \bmod n)} \bmod n$, где n есть открытый ключ, секретным ключом является разложение модуля n и подписью является тройка «нетривиальных» чисел (R, S, V), т. е. достаточно больших чисел, например, больше 100 бит?

49. Корректна ли схема ЭЦП со сравнением проверки подписи вида $R^{(IS \bmod n)} \equiv S^{(IR \bmod n)} V^H \bmod n$, где n есть открытый ключ, секретным ключом является разложение модуля n и подписью является тройка «нетривиальных» чисел (R, S, V), т. е. достаточно больших чисел, например, больше 100 бит? Рассмотрите возможность подделки подписи.

50. Дана схема ЭЦП со сравнением проверки подписи S следующего вида: $\alpha^H \equiv y^S \bmod n$, в котором $n = pq$ и $y = \alpha^{\gamma} \bmod n$, где α — число, относящееся по модулю n к достаточно большому показателю γ, (p, q, γ, x) — секретный ключ. Записать уравнение генерации подписи по секретному ключу и показать, что эта схема ЭЦП не является безопасной. Предложить вариант ее усиления.

51. В схеме ЭЦП с уравнением проверки подписи S вида $R = \alpha^{IIRS} \bmod n$ и открытым ключом n, где $n = pq$, число α является общим для всех пользователей. Записать уравнение генерации подписи и сформулировать требования к выбору α.

52. Дана исходная схема ЭЦП с уравнением проверки подписи (R, S) следующего вида: $R = (S^{HR} \bmod n) \bmod z$, где $n = pq$ есть открытый ключ, представляющий собой RSA-модуль, и z — простое число сравнительно малой длины. Преобразовать эту схему в ЭЦП с сокрашенной длиной подписи.

53. Схема ЭЦП задана проверочными соотношениями $|g| < 610$ бит и $R \equiv \equiv \alpha^{H(R^g \bmod p)} \bmod p$, где $p = 2n + 1$; n представляет собой произведение двух больших простых чисел r и q: $n = rq$; α — число, относящееся по модулю p к показателю q; (α, p) — открытый ключ; q — секретный ключ длиной $|q| \approx 600$ бит; (g, R) — подпись. Запишите процедуру генерации подписи. Почему контролируется разрядность подписи при проверке ее подлинности?

54. Проанализируйте схему ЭЦП, заданную проверочными соотношениями $|g| < 770$ бит и $\alpha^g \equiv R^{H(R^g \bmod p)} \bmod p$, где $p = 2n + 1$; n представляет собой произведение двух больших простых чисел r и q: $n = rq$; α — число, относящееся по модулю p к показателю q; (α, p) — открытый ключ; q — секретный ключ длиной $|q| \approx 768$ бит; (g, R) — подпись. Запишите процедуру генерации подписи. Почему контролируется разрядность подписи при проверке ее подлинности?

55. Схема ЭЦП задана проверочным соотношением $R^{H g^2} \equiv \alpha^{(R^g \bmod n)} \bmod n$, где $n = pq$ — открытый ключ, представляющий собой RSA-модуль; α — число, относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$, где γ' и γ'' есть простые делители: $\gamma' | p - 1$ и $\gamma'' | q - 1$; γ — секретный ключ; (g, R) — подпись. Запишите процедуру генерации подписи.

56. Проанализируйте схему ЭЦП, заданную проверочными соотношениями $|g| < 520$ бит и $\alpha^H \equiv R^{(R^g \bmod p)} \bmod p$, где $p = 2n + 1$; n представляет собой произведение двух больших простых чисел r и q: $n = rq$; α — число, относящееся по модулю p к показателю q; (α, p) — открытый ключ; q — секретный ключ длиной около 512 бит; (g, R) — подпись. Запишите процедуру генерации подписи. Объясните, почему разрядность подлинной подписи не должна превышать 520 бит.

57. Показать, каким образом можно сократить размер подписи в схеме ЭЦП, заданной проверочным неравенством $|g| < 520$ бит и проверочным уравнением $R = \alpha^{HRg} \bmod p$, где $p = 2n + 1$; n представляет собой произведение двух больших простых чисел r и q: $n = rq$; α — число, относящееся по модулю p к показателю q; (α, p) — открытый ключ; q — секретный ключ длиной $|q| \approx 512$ бит; (g, R) — подпись. Запишите процедуру генерации подписи. Почему контролируется разрядность подписи при проверке ее подлинности?

58. Каким образом следует выбрать простой модуль p в схеме ЭЦП со сравнением проверки $\alpha^H \equiv y^R R^{S^2} \bmod p$, где $y = \alpha^x \bmod p$ — секретный ключ, α — первообразный корень по модулю p и (R, S) — подпись, чтобы взлом схемы требовал решения двух трудных задач: дискретного логарифмирования и факторизации числа, представляющего собой произведение двух больших простых множителей?

59. Схема ЭЦП представлена проверочным сравнением вида $k + Hg \equiv \equiv (\alpha^{k-Hg} \bmod n) \bmod \delta$, где n — RSA-модуль $(n = pq)$; (n, α) — открытый ключ; H — значение хэш-функции, соответствующей подписанному сообщению; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$; γ — секретное число, не связанное с простым модулем δ (γ является составным и содержит в качестве своих сомножителей, по крайней мере, по одному большому делителю чисел $p - 1$ и $q - 1$). Подписью является пара чисел (g, k). Опишите процедуру генерации подписи.

60. Укажите два различных механизма формирования подписи в схеме ЭЦП с проверочным уравнением $k = (\alpha^{Hgk} \bmod n) \bmod \delta$, где n — RSA-модуль $(n = pq)$; (n, α) — открытый ключ; H — значение хэш-функции, соответствующей подписанному сообщению; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$; γ — секретное число, не связанное с простым модулем δ (γ является составным и содержит в качестве своих сомножителей, по крайней мере, по одному большому делителю чисел $p - 1$ и $q - 1$). Подписью является пара чисел (g, k). Какой из механизмов является более общим?

61. Дана исходная схема ЭЦП с уравнением проверки подписи $\alpha = S^H \bmod n$, где (n, α) — открытый ключ, n — RSA-модуль, S — подпись. С целью сокращения размера открытого ключа параметр α определен соотношением $\alpha = F(n)$, где F — некоторая специфицированная хэш-функция, благодаря чему открытый ключ полностью задается параметром n. Записать уравнение генерации подписи и оценить ее длину и стойкость.

62. Схема ЭЦП представлена проверочным сравнением вида $Hk + g \equiv (\alpha^{Hk \cdot g} \bmod n) \bmod \delta$, где n — RSA-модуль $(n = pq)$: (n, α) — открытый g ключ; H — значение хэш-функции, соответствующей подписанному сообщению; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$; γ — секретное число, не связанное с простым модулем δ (γ является составным и содержит в качестве своих сомножителей, по крайней мере, по одному большому делителю чисел $p - 1$ и $q - 1$). Подписью является пара чисел (g, k). Опишите процедуру генерации подписи.

63. Схема ЭЦП представлена проверочным сравнением вида $k / g \equiv H(\alpha^{k-g} \bmod n) \bmod \delta$, где n — RSA-модуль $(n = pq)$; (n, α) — открытый ключ; H — значение хэш-функции, соответствующей подписанному сообщению; α — число, относящееся по модулю n к показателю $\gamma | \varphi(n)$; γ — секретное число, не связанное с простым модулем δ (γ является составным и содержит в качестве своих сомножителей, по крайней мере, по одному большому делителю чисел $p - 1$ и $q - 1$). Подписью является пара чисел (g, k). Опишите процедуру генерации подписи (укажите два способа).

6.2.2. ЭЦП на основе сложности дискретного логарифмирования

64. Схема ЭЦП задана сравнением проверки подписи вида $y^H S \equiv R\alpha^{(RS \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Показать, как с использованием секретного ключа генерируется подпись (R, S), в которой длина каждого из чисел R и S больше 100 бит. Записать формулы, по которым генерируется подпись. Какие требования можно рекомендовать к выбору параметра α? Можно ли подделать подпись, т. е. вычислить «правильное» значение подписи без знания секретного ключа?

65. Показать, как используется секретный ключ при генерации подписи (R, S), где длина каждого из чисел R и S больше 100 бит, в схеме ЭЦП

с проверочным сравнением вида $y^H S \equiv R^y \alpha^{(RS \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Записать формулы, по которым генерируется подпись. Какие требования можно рекомендовать к выбору параметра α? Возможна ли в этой схеме подделка подписи?

66. Показать, как генерируется подпись (R, S), где длина каждого из чисел R и S больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $y^{(RS \bmod p)} S \equiv R^H \alpha \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Записать формулы, по которым генерируется подпись. Какие требования можно рекомендовать к выбору параметра α? Предложить способы подделки подписи.

67. Показать, как генерируется подпись (R, S, V), где длина каждого из чисел R, S и V больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $VR^{(VRS \bmod p)} \equiv S^{(SRV \bmod p)} y^H \alpha \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Записать формулы, по которым генерируется подпись. Можно ли подделать подпись? Какое число можно выбрать в качестве параметра α?

68. По какой схеме генерируется подпись (R, S, V), где длина каждого из чисел R, S и V больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $R^{(SR^H V \bmod p)} \equiv S^{(SRV^{-H} \bmod p)} y \alpha^H \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера? Дать предварительную оценку безопасности данной схемы ЭЦП. Какое число можно выбрать в качестве параметра α?

69. Показать, как генерируется подпись (R, S), где длина каждого из чисел R и S больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $\alpha^H S \equiv y R^{(RS^y \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Записать формулы, по которым генерируется подпись. Какие требования можно рекомендовать к выбору параметра α? Является ли безопасной данная схема ЭЦП?

70. Показать, как генерируется подпись (R, S), где длина каждого из чисел R и S больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $\alpha^H S \equiv (R^y)^{(RS \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Записать формулы, по которым генерируется подпись. Какие требования можно рекомендовать к выбору параметра α? Является ли данная схема ЭЦП стойкой?

71. Показать, как генерируется подпись (R, S), где длина каждого из чисел R и S больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $\alpha^H S \equiv (Ry)^{(RS \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Записать формулы, по которым генерируется подпись. Какие требования можно рекомендовать к выбору параметра α? Оценить безопасность этой схемы ЭЦП.

72. Показать, как генерируется подпись (R, S), где длина каждого из чисел R и S больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $\alpha^H S \equiv Ry^{(RS \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Записать формулы, по которым генерируется подпись. Оценить безопасность этой схемы ЭЦП.

73. Показать, как генерируется подпись (R, S), где длина каждого из чисел R и S больше 100 бит, в схеме ЭЦП со сравнением проверки подписи вида $RS \equiv \alpha^H y^{(R^y S \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера. Записать формулы, по которым генерируется подпись. Какие требования можно рекомендовать к выбору параметра α? Является ли данная схема ЭЦП безопасной?

74. Показать, как можно подделать подпись (R, S), где длина каждого из чисел R и S больше 100 бит, в схеме ЭЦП с уравнением проверки подписи вида $R = S\alpha^{H(RS \bmod p)} y^{(RS \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера, α — число, относящееся по модулю p к простому делителю $\gamma | p - 1$.

75. Объясните, почему схема ЭЦП с проверочным уравнением вида $R = \alpha^{(y^H R^S \bmod p)} \bmod p$ не является удовлетворительной ($y = \alpha^x \bmod p$ — открытый ключ, α — первообразный корень, x — секретный ключ, (R, S) — подпись).

76. Какое из следующих двух проверочных уравнений задает предпочтительную схему ЭЦП: $R = y^{1\alpha^H y^S R \bmod p)} \bmod p$ и $R = y^{1\alpha^{S y^H R \bmod p)}} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому простому показателю γ, (R, S) — подпись? Для выбранной схемы запишите процедуру генерации подписи.

77. Какое из следующих двух проверочных сравнений задает предпочтительную схему ЭЦП: $\alpha^H \equiv y^{(R^S \bmod p)} R \bmod p$ и $\alpha^H \equiv y^{(R^S \bmod \gamma)} R \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, отно-

сящееся к γ (γ — простое число) как к показателю по простому модулю p, (R, S) — подпись? Для выбранной схемы запишите процедуру генерации подписи.

78. Схема ЭЦП задана проверочным сравнением $R^{Hg^2} \equiv y\alpha^{(R^g \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p - 1$; (g, R) — подпись. Запишите процедуру генерации подписи.

79. Схема ЭЦП задана проверочным сравнением $R^{H-g} \equiv y^{(R\alpha^g \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p - 1$; (g, R) — подпись. Запишите процедуру генерации подписи и покажите, какие требования следует наложить на выбор простого числа γ с целью снижения сложности процедуры генерации подписи.

80. Какое из следующих двух проверочных уравнений задает предпочтительную схему ЭЦП: $R = y^{H(\alpha R^S \bmod p)} \bmod p$ и $R = \alpha y^{H(R^S \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому простому показателю γ, (R, S) — подпись? Объясните почему. Для выбранной схемы опишите процедуру формирования подписи.

81. Дана исходная схема ЭЦП с проверочным уравнением вида $R = \alpha^{H(Ry^g \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому показателю γ, (R, g) — подпись. Запишите процедуру формирования подписи в исходной схеме и преобразуйте ее в схему ЭЦП с восстановлением сообщения. Какие ограничения накладываются на выбор секретного ключа в этих схемах? Можно ли сформировать подпись без использования секретного ключа?

82. Дана исходная схема ЭЦП с проверочным сравнением вида $R^H \equiv y^{(R\alpha^g \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому показателю γ, (R, g) — подпись. Запишите процедуру формирования подписи в исходной схеме и преобразуйте ее в схему ЭЦП с восстановлением сообщения. Какие ограничения накладываются на выбор показателя γ в этих схемах?

83. Дана схема ЭЦП с восстановлением сообщения, заданная проверочным уравнением $M = HR(y\alpha)^{(Ry^g \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ ($x < \gamma$); α — число, относящееся по просто-

му модулю p к некоторому простому показателю γ; (R, g) — подпись. В этой схеме значение хэш-функции H от сообщения M ($H < \gamma$) направляется вместе с подписью для возможности одновременной проверки подлинности подписи и самого сообщения. Запишите процедуру формирования подписи в этой схеме ЭЦП. За счет чего обеспечивается контроль подлинности сообщения? Является ли стойкой схема ЭЦП с проверочным уравнением вида $M = HR y^{(R^{\gamma} g \bmod p)} \bmod p$ или вида $M = HR\alpha y^{(R^{\gamma} g \bmod p)} \bmod p$?

84. Дана схема ЭЦП, заданная проверочным уравнением вида $1 = R\alpha^{H + (R^{\gamma} y^{g} \bmod p)} \bmod p$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ ($x < \gamma$); α — число, относящееся по простому модулю p к некоторому простому показателю γ; (R, g) — подпись. Можно ли эту схему преобразовать в ЭЦП с восстановлением сообщения путем замены левой части на значение сообщения M? Объясните почему и опишите процедуру генерации подписи, соответствующей исходному проверочному уравнению.

85. Рассмотрите схему ЭЦП, предложенную для реализации протокола слепой подписи и заданную проверочным уравнением вида $R = H\alpha^{(R^{\gamma} y^{g} \bmod p)} \bmod p$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ ($x < \gamma$); α — число, относящееся по простому модулю p к некоторому простому показателю γ; (R, g) — подпись. Покажите, как предполагается осуществить процедуру формирования подписи к некоторому документу вслепую. Решает ли данная схема проблему обеспечения анонимности? Объясните почему.

86. Рассмотрите схему ЭЦП, основанную на сложности задачи извлечения квадратных корней по RSA-модулю $n = pq$, где p и q — большие простые числа, в которой в качестве проверочного уравнения используется соотношение $H = S^2 \bmod n$. Покажите, как осуществить процедуру формирования подписи S вслепую. Решает ли данная схема проблему обеспечения анонимности? Можно ли ее применять на практике? Объясните почему.

87. Можно ли использовать в протоколе слепой подписи схему ЭЦП, заданную проверочным уравнением $RH = \alpha^{(RH^{\gamma} g \bmod p)} \bmod p$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ ($x < \gamma$); α — число, относящееся по простому модулю p к некоторому простому показателю γ; (R, g) — подпись? Объясните почему.

88. Рассмотрите схему ЭЦП, предложенную для реализации протокола слепой подписи и заданную проверочным уравнением вида $RH =$

$= \alpha^{(R^2 H y^R \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ ($x < \gamma$); α — число, относящееся по простому модулю p к некоторому простому показателю γ; (R, g) — подпись. Покажите, как предполагается осуществить процедуру формирования подписи к некоторому документу вслепую. Решает ли данная схема проблему обеспечения анонимности? Объясните почему.

89. Для реализации протокола слепой подписи предложена схема ЭЦП, заданная проверочным уравнением $R = Hy^{(R\alpha^R \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ ($x < \gamma$); α — число, относящееся по простому модулю p к некоторому простому показателю γ; (R, g) — подпись. Опишите процедуру формирования подписи вслепую. Обеспечивает ли данная схема анонимность? Объясните почему.

90. Можно ли в протоколе слепой подписи использовать схему ЭЦП, заданную проверочным уравнением $R = H^2 \alpha^{(HRy^R \bmod p)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ ($x < \gamma$); α — число, относящееся по простому модулю p к некоторому простому показателю γ; (R, g) — подпись? Покажите, как предполагается осуществить процедуру формирования подписи к некоторому документу вслепую. Решает ли данная схема проблему обеспечения анонимности? Объясните почему.

91. Оцените возможность подделки подписи и вычисления секретного ключа по подписи в схемах ЭЦП, заданных следующими двумя проверочными уравнениями: $k = (\alpha^{k+g} \bmod p)(\alpha^v y^{kg} \bmod p) \bmod \gamma$ и $k = (\alpha^{k+g} \bmod p)^{(y^{vgk} \bmod p)} \bmod \gamma$, где (v, k, g) — подпись; $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся к простому показателю γ по модулю p. Опишите процедуру формирования подписи.

92. Показать, как генерируется подпись (R, S) в схеме ЭЦП с сокращенной длиной подписи (например, до 320 бит), в которой уравнение проверки подписи реализует восстановление подписанного сообщения m: $m = R(y^{HRS} \alpha^S \bmod p) \bmod q$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, p — простой модуль большого размера, q — простой модуль длины 160 бит и α — число, относящееся по модулю p к показателю γ, длины 160 бит.

93. Рассмотрите схему ЭЦП с уравнением проверки подписи вида $R = y^H \alpha^{SR} \bmod p$, где открытый ключ y формируется по секретному ключу

x ($x < p-1$) по формуле $y = x\alpha^x \bmod p$, α — первообразный корень по простому модулю p. Разовый открытый ключ R формируется в виде $R = x^{1/H}\alpha^k \bmod p$ (k — случайное число, $k < p-1$). Элемент S подписи (R, S) вычисляется из уравнения $S = R^{-1}(k - xH) \bmod p - 1$. Покажите, что стойкость этой схемы ЭЦП не выше сложности задачи дискретного логарифмирования.

94. Является ли стойкой схема ЭЦП с проверочным сравнением вида $R^H y^{H(SR \bmod q)} \equiv S\alpha^{(SR \bmod r)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся к некоторому простому показателю γ по каждому из простых модулей p, q и r; (R, S) — подпись? Как можно усилить эту схему?

95. Является ли стойкой схема ЭЦП с проверочным сравнением вида $\alpha^k y^{H(S\alpha^k \bmod q)} \equiv S\alpha^{(S\alpha^k \bmod r)} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся к некоторому простому показателю γ по каждому из простых модулей p, q и r; (k, S) —подпись? Опишите процедуру генерации подписи. Имеются ли специальные требования к выбору параметров α, p, q и r?

96. Какое из следующих двух проверочных сравнений задает предпочтительную схему ЭЦП: $R^S \equiv y^{\alpha^{HR}} \bmod p$ или $R^S \equiv y\alpha^{HR} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к простому показателю $\gamma = (p-1)/2$ и одновременно являющееся первообразным корнем по модулю γ; (R, S) — подпись? Для выбранной схемы запишите процедуру генерации подписи.

97. Дана схема ЭЦП с проверочным уравнением $R = \alpha^{(Ry^{g_H \bmod n})} \bmod n$, где (α, y, n) — открытый ключ, в котором модуль n представляет собой произведение двух больших простых чисел r и q: $n = rq$, α — число, относящееся по модулю n к показателю γ, $y = \alpha^x \bmod n$; разложение модуля, x и γ являются секретными элементами схемы; (g, R) — подпись. Запишите процедуру генерации подписи. Предложите на основе заданной схемы более экономичную конструкцию. Можно ли в этой схеме сократить размер подписи?

98. Дана схема ЭЦП со сравнением проверки подписи $\alpha^H \equiv yR^S \bmod p$, где открытый ключ y формируется по формуле $y = \alpha^x \bmod p$, α — первообразный корень по модулю p, x — секретный ключ, $x < \varphi(p)$. Разовый открытый ключ R формируется в виде $R = \alpha^k \bmod p$ (k — случайное число, $k < \varphi(p)$). Элемент S подписи (R, S) вычисляется из уравнения $S = k^{-1}(H - x) \bmod \varphi(p)$. Показать, что при простом модуле p данная

схема не является безопасной. При каком модуле данная схема является безопасной?

99. Рассмотрите схему ЭЦП со сравнением проверки подписи $\alpha^k S^H \equiv y^H \alpha^{(S\alpha^k R \bmod p)} \bmod p$, где открытый ключ y формируется по секретному ключу x ($x < \gamma$) по формуле $y = x\alpha^x \bmod p$, α — число, относящееся по простому модулю p к простому показателю γ достаточно большой длины. Показать, как формируется подпись (k, S). Доказать, что стойкость этой схемы ЭЦП имеет один порядок со сложностью задачи дискретного логарифмирования.

100. Дана схема ЭЦП с уравнением проверки подписи вида $R = y^H \alpha^{RS} \bmod p$. Показать, как можно осуществить подделку подписи без знания секретного ключа.

101. Дана схема ЭЦП со сравнением проверки подписи вида $\alpha^R \equiv y^{HS} R^S \bmod p$. Показать, как можно осуществить подделку подписи без знания секретного ключа.

102. Дана схема ЭЦП со сравнением проверки подписи вида $\alpha^{HS} \equiv y^R R^S \bmod p$. Показать, как можно осуществить формирование правильной подписи без знания секретного ключа.

103. Дана схема ЭЦП со сравнением проверки подписи вида $\alpha^{HS} \equiv y^{Rf(H)} R^S \bmod p$, где $f(H)$ есть произвольная функция от H. Показать, как можно осуществить формирование правильной подписи без знания секретного ключа.

104. Показать, как можно осуществить формирование правильной подписи без знания секретного ключа в случае схемы ЭЦП со сравнением проверки вида $R^{f(H)} \equiv \alpha^H y^{RS} \bmod p$, где $f(H)$ есть произвольная функция от H.

105. Показать, как можно осуществить формирование правильной подписи без знания секретного ключа в случае схемы ЭЦП со сравнением проверки вида $R^{F(R)} \equiv \alpha^{HS} y^{Sf(H)} \bmod p$, где $f(H)$ и $F(R)$ есть произвольные функции от H и R соответственно.

106. Показать, как можно получить случайное значение H и правильную подпись к нему для американского стандарта DSA.

107. Показать, как можно получить случайное значение H и правильную подпись к нему для стандарта ГОСТ Р 34.10–94.

108. Дана схема ЭЦП со сравнением проверки подписи вида $\alpha^H \equiv y^{RS} R \bmod p$. Показать, как можно осуществить формирование правильной подписи для произвольного значения хэш-функции.

109. Дана схема ЭЦП со сравнением проверки подписи вида $\alpha^{H} \equiv \equiv y^{R^H} R^S \bmod p$. Можно ли без знания секретного ключа вычислить тройку чисел R, S и H, таких что (R, S) является правильной подписью к документу, хэш-функция от которого равна H? Сравнить данную схему с ЭЦП Эль-Гамаля.

110. Схема ЭЦП с восстановлением сообщения M задана проверочным уравнением $M = k^{t}(\alpha^{k} y^{g} \bmod p) \bmod \gamma$, где $y = \alpha^{x} \bmod p$ — открытый ключ;

x — секретный ключ; α — число, относящееся по простому модулю p к простому показателю γ: $\gamma | p-1$; (k, g) — подпись. Запишите процедуру генерации подписи.

111. Схема ЭЦП с восстановлением сообщения M задана проверочным уравнением $M = (k + g)(\alpha^{k} y^{g} \bmod p) \bmod \gamma$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю γ; (k, g) — подпись. Запишите процедуру генерации подписи.

112. Схема ЭЦП с восстановлением сообщения M задана проверочным уравнением $M = \dfrac{k - g}{\alpha^{k} y^{g} \bmod p} \bmod \gamma$, где $y = \alpha^{x} \bmod p$ — открытый ключ;

x — секретный ключ; α — число, относящееся по простому модулю p к простому показателю γ; (k, g) — подпись. Запишите процедуру генерации подписи.

113. Схема ЭЦП с восстановлением сообщения M задана проверочным уравнением $M = \dfrac{(k + g)^{H}}{\alpha^{k} y^{g} \bmod p} \bmod \gamma$, где H — значение хэш-функции от сообщения; $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к простому показателю γ; (k, g) — подпись. Запишите процедуру генерации подписи. С какой целью в проверочное уравнение входит значение H?

114. Схема ЭЦП с восстановлением сообщения M задана проверочным уравнением $M = g(\alpha^{Hk} y^{g+H} \bmod p) \bmod \gamma$, где H — значение хэш-функции от сообщения, $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к простому показателю γ; (k, g) — подпись. Запишите процедуру генерации подписи. С какой целью в проверочное уравнение входит значение H?

115. Схема ЭЦП с восстановлением сообщения M задана проверочным уравнением $M = g + H(\alpha^{k} y^{g} \bmod p) \bmod \gamma$, значение хэш- ключ; α —

число, относящееся по простому модулю p к простому показателю γ; (k, g) — подпись. Запишите процедуру генерации подписи. С какой целью в проверочное уравнение входит значение H?

116. Какое из двух проверочных сравнений $g + k \equiv (\alpha^{kg} y^H \bmod p) \bmod \gamma$ и $gk \equiv M(\alpha^g y^k \bmod p) \bmod \gamma$, где M — сообщение; $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к простому показателю γ; (k, g) — подпись, определяет схему ЭЦП, допускающую подделку подписи? Запишите процедуру генерации подписи.

117. Какое из двух проверочных сравнений $g + M \equiv (\alpha^g y^k \bmod p) \bmod \gamma$ и $gk \equiv M(\alpha^{g/k} y^{k/g} \bmod p) \bmod \gamma$, где M — сообщение; $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к простому показателю γ; (k, g) — подпись, определяет схему ЭЦП, допускающую подделку подписи? Запишите процедуру генерации подписи.

118. Показать способ подделки подписи в системе ЭЦП с уравнением проверки подписи $m = \alpha^{RS} yR \bmod p$.

119. Показать способ подделки подписи в системе ЭЦП с уравнением проверки подписи $m = \alpha^{f(R)S} yR \bmod p$.

120. Показать способ подделки подписи в системе ЭЦП со сравнением проверки подписи $\alpha^{HS} \equiv y^R R^S \bmod p$.

121. Показать способ подделки подписи в системе ЭЦП со сравнением проверки подписи $\alpha^{HR} \equiv y^S R \bmod p$.

122. Показать способ подделки подписи в системе ЭЦП со сравнением проверки подписи $\alpha^{RS} \equiv y^H R \bmod p$.

123. Преобразовать ЭЦП со сравнением проверки подписи $\alpha^H \equiv y^R R^S \bmod p$, где $R = \alpha^k \bmod p$, в ЭЦП с сокращенной длиной подписи.

124. Преобразовать ЭЦП со сравнением проверки подписи $\alpha^S \equiv y^R R^H \bmod p$, где $R = \alpha^k \bmod p$, в ЭЦП с сокращенной длиной подписи.

125. Преобразовать схему ЭЦП со сравнением проверки подписи $\alpha^H \equiv y^R R^S \bmod p$, где $R = \alpha^k \bmod p$, в схему ЭЦП с сокращенной длиной подписи и восстановлением подписанного сообщения.

126. Проверочное сравнение $k^2 \equiv (\alpha^{Hk} y^g \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому простому показателю γ: $\gamma | p - 1$; (k, g) — подпись, задает схему ЭЦП с сокращенной длиной подписи. Подпись

вычисляется как решение системы сравнений $Hk + xg \equiv U \bmod \gamma$ (1) и $k^2 \equiv Z \bmod \gamma$ (2), где U — произвольное число ($U < \gamma$) и $Z = \alpha^{U} \bmod p$. Можно ли при формировании подписей к двум разным сообщениям использовать одно и то же значение U? Уточните процедуру генерации подписи. Какие требования целесообразно наложить на выбор числа γ?

127. Преобразовать схему ЭЦП, заданную проверочным сравнением $k^2 \equiv \equiv H(\alpha^k y^g \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому простому показателю γ, и (k, g) — подпись, в схему с восстановлением сообщения. Обеспечивается ли проверка подлинности сообщения непосредственно при проверке подлинности подписи в построенной схеме?

128. В схеме ЭЦП, заданной проверочным сравнением вида $k \equiv \equiv H(\alpha^k y^g \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому простому показателю γ, и (k, g) — подпись, произвольная пара значений k и g соответствует некоторому легко вычисляемому значению H как подлинная подпись. Приведите несколько вариантов, как можно устранить такую возможность, не повышая сложность процедуры проверки подписи. Опишите процедуру генерации подписи в модернизированных схемах.

129. Схема ЭЦП задана проверочным сравнением $y^{\alpha^{HR}} \equiv R^{y'^{S}} \bmod p$, где $y \equiv \equiv \alpha^{\alpha^x} \bmod p$ и $y' \equiv \alpha^x \bmod \gamma$ — элементы открытого ключа (y, y'); x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю γ, где $\gamma = (p - 1)/2$, и являющееся одновременно первообразным корнем по модулю γ; (R, S) — подпись. Опишите процедуру генерации подписи. Можно ли в этой схеме ЭЦП использовать простое число p с другой структурой, чтобы сократить размер подписи (за счет элемента S) путем выбора числа γ длиной 256 бит? Можно ли добиться сокращения размера параметра S?

130. Можно ли положить в основу схемы ЭЦП проверочное уравнение вида $v = (\alpha_1^{g+v} y^k \bmod p_1)(\alpha_2^{k+vH} y^g \bmod p_2) \bmod \gamma$, где $p_1 \neq p_2$; H — значение хэш-функции, соответствующее подписываемому сообщению; y — открытый ключ; α_i — число, относящееся по простому модулю p_i ($i = 1, 2$) к некоторому простому показателю γ_i; (k, g, v) — подпись? Как следует вычислять открытый ключ по секретному? Запишите процедуру генерации подписи.

131. Показать, как можно подделать подпись в схеме ЭЦП с проверочным уравнением $g = (\alpha^{gk} y^{(gkH \bmod \gamma) \bmod \delta} \bmod p) \bmod \delta$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к простому показателю γ; (k, g) — подпись, δ — простое число, такое что $|\delta| \approx |\gamma|$. Описать процедуру генерации подписи.

132. В схеме ЭЦП с проверочным сравнением $Mg \equiv k(\alpha^g y^{-k} \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому простому показателю γ, (k, g) — подпись, для вычисления элементов подписи используются следующие формулы: $k = \dfrac{UM}{Z - xM} \bmod \gamma$ (1) и $g = \dfrac{UZ}{Z - xM} \bmod \gamma$ (2), где число $U < \gamma$ выбирается случайно и $Z = \alpha^U \bmod p$. Объясните, почему атакующий не может реализовать вычислительно эффективную процедуру нахождения значения секретного ключа путем совместного решения двух линейных сравнений (1) и (2) с двумя неизвестными x и U.

133. Предложите ограничения, которые следует наложить на функцию $f(k, g)$, чтобы схема ЭЦП, задаваемая проверочным уравнением $k = (H\alpha^{f(k,g)} y^k \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому показателю γ, обладала достаточно эффективными процедурами генерации и проверки подписи, в качестве которой служит пара чисел (k, g).

134. Схема ЭЦП задается проверочным уравнением следующего вида $k = (\alpha^{Hg} y^{f(k,g)} \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому показателю γ. Предложите варианты функции $f(k, g)$, обеспечивающие безопасность цифровой подписи и эффективность ее вычисления.

135. Схема ЭЦП задается проверочным уравнением следующего вида $k = g^{-1}[(\alpha^{Hg/k} y)^{g/k} \bmod p] \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ, x — секретный ключ, α — число, относящееся по простому модулю p к некоторому показателю γ. Укажите способ подделки подписи.

136. Схема ЭЦП задается проверочным сравнением следующего вида $kg \equiv (\alpha^{g+k^{-1}} y^H \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому показателю γ, (k, g) — подпись к документу, хэш-функция от которого равна H. Укажите способ подделки подписи.

137. Две схемы ЭЦП задаются проверочными уравнениями $k = (\alpha^{gk} \bmod p)(\alpha^{g^{-v}} y^{kH} \bmod p) \bmod \gamma$ и $k = (\alpha^{gk} y \bmod p)^{(\alpha^{H} y^{kv} \bmod p)} \bmod \gamma$, где (k, g, v) — подпись к документу, хэш-функция от которого равна H; $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому показателю γ. Укажите способ формирования подписи в каждой из них. Какая из них не является безопасной?

138. Схема ЭЦП задана проверочными соотношениями следующего вида $k = (\alpha^{kgH} \bmod p) \bmod \delta$ и $|g| < \frac{2}{3}|p|$, где $p = 2n + 1$; $n = rq$ — произведение двух больших простых чисел r и q, таких что $|r| \approx |q| \approx 0.5|p|$; α — число, относящееся по модулю p к показателю q; δ — некоторое простое число $(0.2|p| < |\delta| < 0.5|p|)$. Секретным ключом является значение q, а открытым ключом — пара чисел (p, α). Подписью является пара чисел (k, g). Опишите процедуру генерации подписи. Какую нагрузку несет сравнение длин чисел p и g?

139. Укажите требования к параметру α и простым числам p и δ, при которых уравнение $k = \alpha^{k^{-1} g} (y^{v} \alpha^{kH} \bmod p) \bmod \delta$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p - 1$ и одновременно являющееся первообразным корнем по модулю δ; (k, g, v) — подпись, может служить в качестве проверочного соотношения некоторой схемы ЭЦП. Запишите процедуру генерации подписи.

140. Схема ЭЦП задана проверочным сравнением $k^2 \equiv (\alpha^{g} y^{kH} \bmod p) \bmod \gamma$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p - 1$; (k, g) — подпись. Запишите процедуру генерации подписи.

141. Схема ЭЦП задана проверочным сравнением $k^2 \equiv (\alpha^{g^2 H} y^{k} \bmod p) \bmod \gamma$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p - 1$; (k, g) — подпись. Запишите процедуру генерации подписи.

142. Схема ЭЦП задана проверочным сравнением следующего вида $k + g \equiv H(\alpha^{kg} y^{k+g} \bmod p) \bmod \gamma$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p - 1$; (k, g) — подпись. Опишите процедуру генерации подписи.

143. Схема ЭЦП задана проверочным сравнением следующего вида $k - H \equiv (H\alpha^{k} y^{g} \bmod p) \bmod \gamma$, где $y = \alpha^{x} \bmod p$ — открытый ключ; x —

секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (k, g) — подпись. Опишите процедуру генерации подписи.

144. Схема ЭЦП задана проверочным сравнением следующего вида $k + H \equiv (\alpha^{gH} y^k \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (k, g) — подпись. Опишите процедуру генерации подписи.

145. Схема ЭЦП задана проверочным сравнением следующего вида $k + g \equiv H(\alpha^k y^g \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (k, g) — подпись. Опишите процедуру генерации подписи.

146. Схема ЭЦП задана проверочным сравнением следующего вида $k + g \equiv (\alpha^{H(k-g)} y^k \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (k, g) — подпись. Опишите процедуру генерации подписи.

147. Укажите два различных механизма формирования подписи в схеме ЭЦП с проверочным уравнением $k = (\alpha^{Hg} y^k \bmod p) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (k, g) — подпись. Какой из механизмов является более общим?

148. Схема ЭЦП задана проверочными уравнениями $R = y^E \alpha^S \bmod p$ и $E = HR \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (E, S) — подпись. Опишите процедуру генерации подписи.

149. Схема ЭЦП задана проверочными уравнениями $R = y^E \alpha^g \bmod p$ и $E = (\alpha^g R^H \bmod n) \bmod \gamma$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (E, g) — подпись. Опишите процедуру генерации подписи.

150. Схема ЭЦП задана проверочными уравнениями $R = y^{(HRS \bmod p)} \bmod p$ и $S = \alpha^{(RS \bmod p)\, v} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (R, S, v) — подпись. Опишите процедуру генерации подписи.

151. Схема ЭЦП задана проверочным уравнением следующего вида $R = S\alpha^{H(RS \bmod p)} y^{(RS \bmod p)v} \bmod p$, где $y = \alpha^x \bmod p$ — открытый ключ; x — секретный ключ; α — число, относящееся по простому модулю p к некоторому простому показателю $\gamma | p-1$; (R, S, v) — подпись. Опишите процедуру генерации подписи.

6.2.3. Комбинированные схемы ЭЦП

152. Дана схема ЭЦП с проверочным соотношением $R = y^E \alpha^S \bmod p$, где $E = F(R, H)$, F — сжимающая функция, (v, p, α) — открытый ключ ($v = \alpha^x \bmod p$, x — секретный ключ), (E, S) — подпись. Каким требованиям должны удовлетворять параметры этой схемы ЭЦП, чтобы раскрытие этой криптосистемы требовало решения двух сложных задач: дискретного логарифмирования и факторизации числа, представляющего собой произведение двух больших простых чисел? Раскройте процедуры проверки и генерации подписи.

153. Дана схема ЭЦП с проверочным соотношением $R = y^E \alpha^{gH} \bmod p$, где $E = F(R\alpha^g \bmod p)$, F — сжимающая функция, (v, p, α) — открытый ключ ($y = \alpha^x \bmod p$, x — секретный ключ), (E, g) — подпись. Каким требованиям должны удовлетворять параметры этой схемы ЭЦП, чтобы раскрытие этой криптосистемы требовало решения двух сложных задач: дискретного логарифмирования и факторизации числа, представляющего собой произведение двух больших простых чисел? Раскройте процедуры проверки и генерации подписи.

154. Дана схема ЭЦП с проверочным соотношением $R = \alpha^{kgH} \bmod n$, где $E = F(R^g \bmod n)$, F — сжимающая функция, (n, α) — открытый ключ, (E, g) — подпись, α — число, относящееся к показателю γ (γ является элементом секретного ключа). Раскройте процедуры проверки и генерации подписи.

155. Дана схема ЭЦП с проверочным соотношением $R = \alpha^{Eg} \bmod n$, где $E = F(R^{gH} \bmod n)$, F — сжимающая функция, (n, α) — открытый ключ, (E, g) — подпись, α — число, относящееся к показателю γ (γ является элементом секретного ключа). Раскройте процедуры проверки и генерации подписи.

156. Дана схема ЭЦП с проверочным соотношением $R = \alpha^{EgH} \bmod n$, где $E = F(R^{g+H} \bmod n)$, F — сжимающая функция, (n, α) — открытый ключ, (E, g) — подпись, α — число, относящееся к показателю γ (γ является элементом секретного ключа). Раскройте процедуры проверки и генерации подписи.

157. Дана схема ЭЦП с проверочным соотношением $k = F(\alpha_1^{kgH} \bmod n_1 + \alpha_2^{kg+H} \bmod n_2)$, где F — сжимающая функция, $(n_1, \alpha_1, n_2, \alpha_2)$ — открытый ключ, (k, g) — подпись, α_1 и α_2 — числа, относящиеся по модулям n_1 и n_2, соответственно, к показателю γ. Описать процедуру генерации подписи.

158. Дана схема ЭЦП с проверочным соотношением $g - k = F(\alpha_1^{kgH} \bmod n_1 + \alpha_2^{kg+H} \bmod n_2)$, где F — сжимающая функция, $(n_1, \alpha_1, n_2, \alpha_2)$ — открытый ключ, (k, g) — подпись, α_1 и α_2 — числа, относящиеся по модулям n_1 и n_2, соответственно, к показателю γ. Описать процедуру генерации подписи.

159. Дана схема ЭЦП с проверочным соотношением $k = F(\alpha^{k+g+H} \bmod n)$, где F — сжимающая функция, (n, α) — открытый ключ, (k, g) — подпись, α — число, относящееся по модулю n к показателю γ. Показать возможность подделки подписи. Предложить простой вариант усиления этой схемы ЭЦП.

160. Дана схема ЭЦП с проверочным соотношением $k + g = F(\alpha^{kgH} \bmod n)$, где F — сжимающая функция, (n, α) — открытый ключ, (k, g) — подпись, α — число, относящееся по модулю n к показателю γ. Описать процедуру генерации подписи.

161. Дана схема ЭЦП с проверочным соотношением $R = \alpha^{kH+g} \bmod n$, где $E = F(R^g \bmod n)$, F — сжимающая функция, (n, α) — открытый ключ, (k, g) — подпись, α — число, относящееся по модулю n к показателю γ. Описать процедуру генерации подписи.

162. Дана схема ЭЦП с проверочным сравнением следующего вида $k + v \equiv \psi[k * R + (vH) * G] \bmod p$, где G и R — точки некоторой эллиптической кривой (ЭК), причем $R = s * G$, где G — генератор подгруппы (точек ЭК) простого порядка p, s — секретный ключ; ψ — функция, отображающая точку ЭК в значение, равное ее координате X; (k, v) — подпись; * — операция умножения точки на число. Описать обобщенную процедуру генерации подписи.

163. Дана схема ЭЦП с проверочным сравнением следующего вида $k \equiv v \cdot \psi[k * R + (vH) * G] \bmod p$, где G и R — точки некоторой эллиптической кривой (ЭК), причем $R = s * G$, где G — генератор подгруппы (точек ЭК) простого порядка p, s — секретный ключ; ψ — функция, отображающая точку ЭК в значение, равное ее координате X; (k, v) — подпись; * — операция умножения точки на число. Описать обобщенную процедуру генерации подписи.

164. Дана схема ЭЦП с проверочным уравнением следующего вида $k = (\alpha^{kgH} \bmod n) + \psi[k * R + (vH) * G]$, где G и R — точки некоторой эллиптической кривой (ЭК), причем $R = s * G$, где G — генератор подгруппы (точек ЭК) простого порядка p, s — секретный элемент; (α, n, R) — открытый ключ, где α — число, относяшееся по модулю n к показателю γ; (s, γ) — секретный ключ; ψ — функция, отображающая точку ЭК в значение, равное ее координате X; (k, g, v) — подпись; * — операция умножения точки на число. Описать обобщенную процедуру генерации подписи.

165. Дана схема ЭЦП с проверочным уравнением следующего вида $k = \psi_1[k * R_1 + (vH) * G_1] + \psi_2[k * R_2 + (w + H) * G_2]$, , где G_1, G_2, R_1 и R_2 — точки некоторых эллиптических кривых (ЭК), причем $R_1 = s_1 * G_1$ и $R_2 = s_2 * G_2$, где G_1 и G_2 — генераторы подгрупп (точек ЭК) простых порядков p_1 и p_2, соответственно; (s_1, s_2) — секретный ключ; (R_1, R_2) — открытый ключ, ψ_1 и ψ_2 — функции, отображающие точку ЭК в значение, равное ее координате X; (k, v, w) — подпись; * — операция умножения точки на число. Описать обобщенную процедуру генерации подписи.

166. Дана схема ЭЦП с проверочным уравнением следующего вида $k = \{(y^{kH} \alpha^{g} \bmod p') + \psi[k * R + (vH) * G]\} \bmod p$, , где G и R — точки некоторой эллиптической кривой (ЭК), причем $R = s * G$, где G — генератор подгруппы (точек ЭК) простого порядка p; s — секретный элемент; $y = \alpha^{x} \bmod p'$ — открытый ключ, где α — число, относящееся по модулю p' к показателю γ; (s, x) — секретный ключ; ψ — функция, отображающая точку ЭК в значение, равное ее координате X; (k, g, v) — подпись; * — операция умножения точки на число. Описать обобщенную процедуру генерации подписи.

167. Схема ЭЦП задана проверочными соотношениями вида: 1) $R = y^{S^2} \alpha^{kH} \bmod p$, 2) $E = (R\alpha^{S^2} \bmod p) \bmod \gamma$ и 3) $|S| < 610$ бит. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является тройка чисел (α, y, p), секретным — пара чисел (x, q), где $y = \alpha^{x} \bmod p$. Разрядность q составляет $|q| \approx 600$ бит; (E, S) — подпись. Запишите процедуру генерации подписи. Какие трудные задачи обеспечивают безопасность данной схемы ЭЦП?

168. Схема ЭЦП задана проверочными соотношениями: 1) $R = y^{S^2} \alpha^{E} \bmod p$, 2) $E = (R^{H} \bmod p) \bmod \gamma$ и 3) $|S| < 610$ бит. Модуль p имеет следующую

структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является тройка чисел (α, y, p), секретным — пара чисел (x, q), где $y = \alpha^x \bmod p$. Разрядность q составляет $|q| \approx 600$ бит; (E, S) — подпись. Запишите процедуру генерации подписи. Решение какой сложной задачи обеспечивает возможность вычислить секретные значения?

169. Схема ЭЦП задана проверочными соотношениями: 1) $R = y^E \alpha^{S^2} \bmod p$, 2) $E = R^H \bmod \gamma$, где γ — 128-битовое простое число, и 3) $|S| < 610$ бит. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является тройка чисел (α, y, p), секретным — пара чисел (x, q), где $y = \alpha^x \bmod p$. Разрядность q составляет $|q| \approx 600$ бит; (E, S) — подпись. Запишите процедуру генерации подписи. Решение какой сложной задачи обеспечивает возможность подделки подписи к произвольно выбранному сообщению? Можно ли использовать вместо $R = y^E \alpha^{S^2} \bmod p$ проверочное уравнение $R = y^E \alpha^Z \bmod p$, где подписью является пара чисел (E, Z)? К чему приводит такая замена?

170. Схема ЭЦП задана проверочными соотношениями: 1) $R = y^{EH} \alpha^{S^2} \bmod p$, 2) $E = (R \alpha^S \bmod p) \bmod \gamma$ и 3) $|S| < 610$ бит. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является тройка чисел (α, y, p), секретным — пара чисел (x, q), где $y = \alpha^x \bmod p$. Разрядность q составляет $|q| \approx 600$ бит; (E, S) — подпись. Запишите процедуру генерации подписи. Какие трудные задачи обеспечивают безопасность данной схемы ЭЦП?

171. Схема ЭЦП задана проверочным уравнением $k = (y^{kH} \alpha^g \bmod p) \bmod \delta$, где $|g| < 610$ бит. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является тройка чисел (α, y, p), секретным — пара чисел (x, q), где $y = \alpha^x \bmod p$. Разрядность q составляет $|q| \approx 600$ бит; (k, g) — подпись. Запишите процедуру генерации подписи. Можно ли сказать, что взлом этой схемы ЭЦП требует одновременного решения двух сложных задач — дискретного логарифмирования и факторизации большого числа специального вида?

172. В схеме ЭЦП с проверочным уравнением $\alpha = S^H \bmod n$, где S — подпись, n представляет собой произведение двух больших простых чисел r и q, пара чисел (α, n) — открытый ключ, размер подписи примерно равен размеру модуля n. Поэтому с целью уменьшения длины подписи предложена модифицированная схема ЭЦП с проверочным сравнением $B = \alpha^{S^H \bmod n} \bmod p$, где модуль p имеет следующую структуру: $p = 2qr + 1$, S — подпись, $|S| < 610$ бит. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является тройка чисел (B, α, p), секретным — тройка чисел (x, q, β), где $B = \alpha^H \bmod p$. Разрядность q составляет $|q| \approx 600$ бит. За счет чего обеспечивается сокращение размера подписи? Какому требованию должен удовлетворять элемент открытого ключа β в случае модифицированной схемы ЭЦП? Запишите процедуру генерации подписи. Покажите, что сформированная подпись удовлетворяет проверочному соотношению.

173. В схеме ЭЦП с проверочными уравнениями $R = \alpha^{H^1 y^S \bmod n} \bmod p$ и $E = R^H \bmod \delta$ модуль p имеет структуру $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, параметр α представляет собой число, относящееся по модулю p к показателю q, δ — простое число размера 128 бит. Подписью является пара чисел (E, S). Открытым ключом является четверка чисел (α, β, p, y), секретным — тройка чисел (x, q, γ), где $y = \beta^x \bmod q$ и γ — простой показатель, к которому относится по модулю q число β. Разрядность q составляет $|q| \approx 600$ бит. Запишите процедуру генерации подписи. Оцените, какие математические задачи требуется решить, чтобы вычислить элементы секретного ключа.

174. Легко видеть, что схема ЭЦП с проверочным сравнением вида $\beta^H \equiv y^S R \bmod p$, где $y = \beta^x \bmod p$ — открытый ключ, (R, S) — подпись, не является безопасной. Является ли безопасной схема ЭЦП с проверочным сравнением $\alpha^{H^H \bmod n} \equiv \alpha^{y^S R \bmod n} \bmod p$, в котором модуль p имеет структуру $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, параметр α представляет собой число, относящееся по модулю p к показателю q? Подписью является пара чисел (R, S), где $|R| < 610$ бит. Открытым ключом является четверка чисел (α, β, p, y), секретным — тройка чисел (x, q, γ), где $y = \beta^x \bmod q$ и γ — простой показатель, к которому относится (по модулю q) число β. Разрядность чисел r и q составляет $|r| \approx |q| \approx 600$ бит. Запишите процедуру генерации подписи. Оцените, какие математические задачи требуется решить, чтобы вычислить элементы секретного ключа.

175. Оцените размер подписи и безопасность схемы ЭЦП с проверочным сравнением $y^R = \alpha^{\beta^{HS} \bmod n} \bmod p$, где модуль p имеет структуру $p = 2n + 1$ (n представляет собой произведение двух больших простых чисел r и q), параметр α представляет собой число, относящееся по модулю p к показателю q. Подписью является пара чисел (R, S). Открытым ключом является четверка чисел (α, β, p, y), секретным — тройка чисел (x, q, γ), где $y = \alpha^{\beta^x} \bmod q$ и γ — простой показатель размером $|\gamma| \approx 128$ бит, к которому относится по модулю q число β. Разрядность чисел r и q составляет $|r| \approx |q| \approx 600$ бит. Запишите процедуру генерации подписи.

176. Оцените размер подписи и безопасность схемы ЭЦП с проверочным сравнением $y^{R^S \bmod n} \equiv \alpha^{\beta^H \bmod n} \bmod p$, где модуль p имеет структуру $p = 2n + 1$ (n представляет собой произведение двух больших простых чисел r и q), параметр α представляет собой число, относящееся по модулю p к показателю q. Подписью является пара чисел (R, S). Открытым ключом является четверка чисел (α, β, p, y), секретным — тройка чисел (x, q, γ), где $y = \alpha^{\beta^x} \bmod p$ и γ — простой показатель размером $|\gamma| \approx$ ≈ 128 бит, к которому относится по модулю q число β. Разрядность чисел r и q составляет $|r| \approx |q| \approx 600$ бит. Запишите процедуру генерации подписи.

177. Сравните две схемы ЭЦП, заданные следующими проверочными сравнениями: $R^{y^S \bmod n} \equiv \alpha^{\beta^H \bmod n} \bmod p$ и $y^{R^S \bmod n} \equiv \alpha^{\beta^H \bmod n} \bmod p$, где модуль p имеет структуру $p = 2rq + 1$ (r и q — большие простые числа, $|r| \approx |q| \approx 600$ бит), параметр α представляет собой число, относящееся по модулю p к показателю q. Подписью является пара чисел (R, S). Открытым ключом является четверка чисел (α, β, p, y), секретным — тройка чисел (x, q, γ), где $y = \beta^x \bmod q$ и γ — простой показатель размером $|\gamma| \approx 128$ бит, к которому относится по модулю q число β.

178. Схема ЭЦП задана проверочными соотношениями вида: 1) $R = \alpha^{\beta^{SH+E} \bmod n} \bmod p$ и 2) $E = R^H \bmod \delta$, где (E, S) — подпись. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел (q, γ), где γ — простой показатель размером $|\gamma| \approx 96$ бит, к которому относится по модулю q число β. Разрядность чисел r и q составляет $|r| \approx |q| \approx 600$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи. Решение каких сложных задач обеспечивает возможность вычислить секретный ключ?

179. Схема ЭЦП задана проверочными соотношениями вида: 1) $R = \alpha^{H(M)} \bmod n \bmod p$ и 2) $E = R \bmod \delta$, где (E, S) — подпись. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел (q, γ), где γ — простой показатель размером $|\gamma| \approx 96$ бит, к которому относится по модулю q число β. Разрядность чисел r и q составляет $|r| \approx |q| \approx 600$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи. Решение каких сложных задач обеспечивает возможность вычислить секретный ключ?

180. Схема ЭЦП задана проверочными уравнениями: 1) $R = \alpha^{H(M)} \bmod n \bmod p$ и 2) $E = (R^S \bmod n \bmod p) \bmod \delta$, где (E, S) — подпись. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел (q, γ), где γ — простой показатель размером $|\gamma| \approx 160$ бит, к которому относится по модулю q число β. Разрядность чисел r и q составляет $|r| \approx |q| \approx 512$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи.

181. Схема ЭЦП задана двумя проверочными уравнениями вида: 1) $R = \alpha^{S \cdot H(M)} \bmod n \bmod p$ и 2) $E = (R^S \bmod p) \bmod \delta$, где (E, S) — подпись. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел (q, γ), где γ — простой показатель размером $|\gamma| \approx 160$ бит, к которому относится по модулю q число β, используемое при генерации подписи. Разрядность чисел r и q составляет $|r| \approx |q| \geq 512$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи.

182. Схема ЭЦП задана проверочными уравнениями: 1) $R = \alpha^{H(S+1)^2} \bmod n \bmod p$ и 2) $E = (R^S \bmod n \bmod p) \bmod \delta$, где (E, S) — подпись. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел

(q, γ), где γ — простой показатель размером $|\gamma| \approx 160$ бит, к которому относится по модулю q число β. Разрядность чисел r и q составляет $|r| \approx |q| \approx 512$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи.

183. Схема ЭЦП задана проверочными уравнениями: 1) $R = \alpha^{H^{S_1} \bmod n} \bmod p$ и 2) $E = (R^{\beta^{HS} \bmod n} \bmod p) \bmod \delta$, где (E, S) — подпись. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел (q, γ), где γ — простой показатель размером $|\gamma| \approx 160$ бит, к которому относится по модулю q число β. Разрядность чисел r и q составляет $|r| \approx |q| \approx 512$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи.

184. Схема ЭЦП задана двумя проверочными уравнениями вида: 1) $R = \alpha^{H^{S_1} \bmod n} \bmod p$ и 2) $E = R^H \bmod \delta$, где (E, S) — подпись. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел (q, γ), где γ — простой показатель размером $|\gamma| \approx 160$ бит, к которому относится по модулю q число β, используемое при генерации подписи. Разрядность чисел r и q составляет $|r| \approx |q| \geq 512$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи.

185. Схема ЭЦП задана двумя проверочными уравнениями вида: 1) $R = \alpha^{(S\beta^{E_1} \bmod n)} \bmod p$ и 2) $E = R^H \bmod \delta$, где (E, S) — подпись. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел (q, γ), где γ — простой показатель размером $|\gamma| \approx 96$ бит, к которому относится по модулю q число β, используемое при генерации подписи. Разрядность чисел r и q составляет $|r| \approx |q| \geq 512$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи. Оцените размер подписи.

186. Схема ЭЦП задана двумя проверочными уравнениями вида: 1) $R = \alpha^{(S\beta^{E_1} \bmod n)} \bmod p$ и 2) $E = (R^S H \bmod p) \bmod \delta$, где (E, S) — подпись.

Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p), секретным — пара чисел (q, γ), где γ — простой показатель размером $|\gamma| \approx 96$ бит, к которому относится по модулю q число β, используемое при генерации подписи. Разрядность чисел r и q составляет $|r| \approx |q| \geq 512$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Запишите процедуру генерации подписи. Оцените размер подписи.

187. Сравните схемы ЭЦП, заданные проверочными уравнениями: 1) $R = \alpha^{H^{E \cdot S} \bmod n} \bmod p$ и 2) $R = b^{E \cdot S} \bmod n$, где (E, S) — подпись. В обеих схемах используется дополнительное проверочное соотношение $E = R^H \bmod \delta$. Модуль p имеет следующую структуру: $p = 2n + 1$, где n представляет собой произведение двух больших простых чисел r и q, т. е. $n = rq$. Параметр α представляет собой число, относящееся по модулю p к показателю q. Открытым ключом является пара чисел (α, p) в первой схеме и (b, n) — во второй. Секретным ключом является пара чисел (q, γ) в первой схеме и ε — во второй. Число γ представляет собой простой показатель размером $|\gamma| \approx 96$ бит, к которому относится по модулю q число β. Число ε представляет собой показатель, к которому относится по модулю n число b. Разрядность чисел r и q составляет $|r| \approx |q| \geq 512$ бит. Простое число $\delta \neq \gamma$ имеет размер $|\delta| \approx 96$ бит. Оцените размер подписи для обеих схем.

188. Каким образом следует выбрать простой модуль p в схеме ЭЦП с уравнением проверки вида $R = (\alpha^H y'^R)^{S^2} \bmod p$, где $y = \alpha^x \bmod p$ есть открытый ключ, x — секретный ключ, (R, S) — подпись, чтобы раскрытие криптосистемы требовало решения двух трудных задач: факторизации и дискретного логарифмирования? Какие рекомендации можно дать по выбору параметра α?

189. Нарушитель, получив подпись S' к подготовленному им значению хэш-функции H', сформировал «несанкционированную» подпись к значению хэш-функции H. Каким образом он сделал это, если уравнением проверки подписи является $\alpha = S^H \bmod n$, где (n, α) — открытый ключ, n — RSA-модуль?

190. Схема ЭЦП задана проверочным сравнением $R^{Hg^3} \equiv \alpha^{(R^g \bmod n)} \bmod n$, где $n = pq$ — открытый ключ, представляющий собой RSA-модуль; α — число, относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$, где γ' и γ'' есть простые делители: $\gamma' | p - 1$ и $\gamma'' | q - 1$; γ — секретный ключ; (g, R) —

подпись. Запишите процедуру генерации подписи и покажите, какие требования следует наложить на выбор модуля γ с целью снижения сложности процедуры генерации подписи.

191. Сравните сложность генерации подписи в схемах ЭЦП, заданных следующими двумя вариантами проверочного сравнения вида $R^{Hg^3} \equiv \alpha^{(R^{g^2} \bmod n)} \bmod n$ и $R^{Hg^3} \equiv \alpha^{(R^g \bmod n)} \bmod n$, где $n = pq$ — открытый ключ, представляющий собой RSA-модуль; α — число, относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$, где γ' и γ'' есть простые делители: $\gamma' | p-1$ и $\gamma'' | q-1$; γ — секретный ключ; (g, R) — подпись. Сравните сложность процедур генерации подписи в этих схемах.

192. Рассмотрите два варианта проверочных сравнений $R^H \equiv \alpha^S \bmod p$ и $R' \equiv (\alpha^{S^2 H} \bmod p) \bmod \delta$, где $p = 2n + 1$; n представляет собой произведение двух больших простых чисел r и q: $n = rq$; α — число, относящееся по модулю p к показателю q; (α, p) — открытый ключ; q — секретный ключ длиной 512 бит; (S, R) и (S, R') — подпись в первом и втором варианте соответственно. Какие недостатки можно указать для этих вариантов? Какой из них можно усовершенствовать, чтобы построить схему ЭЦП?

ГЛАВА 7

Ответы, решения и пояснения

7.1. Элементы теории чисел

1. По условию имеем $\gamma \mid \varphi(n)$, $t = \dfrac{\varphi(n)}{\gamma}$ — целое число. По теореме Эйлера $a^{\varphi(n)} = a^{\gamma t} = (a^t)^{\gamma} \equiv 1 \bmod n$, т. е. все числа $z = a^t \bmod n \neq 1$ относятся к показателю γ. Покажем существование таких чисел. Если существуют первообразные корни (случай модуля, имеющего вид $n = p$, $n = p^k$ или $n = 2p^k$, где p — простое нечетное число, k — натуральное число), то, взяв в качестве a первообразный корень, получаем $a^t = a^{\frac{\varphi(n)}{\gamma}} \bmod n \neq 1$.

2. Доказательство: по определению для квадратичного вычета α имеем $\alpha^{\frac{p-1}{2}} \bmod p = 1$, т. е. α не является первообразным корнем.

3. Количество всех квадратичных вычетов, не равных единице, равно $\psi_1 = \dfrac{p-1}{2} - 1$. Количество всех чисел, которые относятся по простому модулю к простому показателю q, равно $\psi_2 = \varphi(q) = q - 1$. Приравнивая $\psi_1 = \psi_2$, получаем $((p-1)/2) - 1 = q - 1 \Rightarrow p = 2q + 1$.

4. В случае а) существует единственное число, удовлетворяющее условию задачи — 2. Остальные 10 невычетов — это первообразные корни. Это справедливо для всех модулей p вида $p = 2q + 1$, где q — простое число. В случае б) решений нет, так как число 7 не может быть показателем по модулю 23. В случае в) имеем $\alpha^{11} \bmod 23 = 1$, т. е. $\alpha^{\gamma} \bmod p = \alpha^{\frac{p-1}{2}} \bmod p = 1$, следовательно, все числа, относящиеся по модулю 23 к показателю 11, являются квадратичными вычетами. Следовательно,

решений нет. В оставшихся двух случаях имеем решения, например: г) 12; д) 30.

5. Биномиальный коэффициент есть целое положительное число, определяемое по формуле $C_p^k = \frac{p(p-1)...(p-k+1)}{1 \cdot 2 \cdot ... \cdot k}$, где все числа в знаменателе являются взаимно простыми с p. Следовательно, множитель p в числителе не сокращается, а, значит, число C_p^k делится на p.

6. При $m = 1$ равенство с очевидностью выполняется. Пусть оно выполняется при $m = k$. Тогда, если $k < p$, имеем: $(k+1)^p \bmod p =$ $= \sum_{i=0}^{i=p} C_p^i k^{p-i} \bmod p = k^p + \sum_{i=1}^{i=p-1} C_p^i + 1 \bmod p = k + 1$.

7. Рассмотрим случай НОД$(a, p) = 1$ и НОД$(b, p) = 1$. Используя формулу бинома Ньютона, получаем: $(a+b)^p \bmod p = \sum_{i=0}^{i=p} C_p^i a^{p-i} b^i \bmod p =$ $= (a^p + \sum_{i=1}^{i=p-1} C_p^i + b^p) \bmod p = (a^p + b^p) \bmod p$ (известно, что биномиальный коэффициент C_p^i, где p — простое число, при $1 \le i < p$ делится на p). В случае НОД$(a, p) = p$ и НОД$(b, p) = p$ обе части заданного равенства равны нулю.

8. Для квадратичных вычетов справедливо соотношение $a^{\frac{p-1}{2}} \bmod p = 1$. Умножая обе части этого равенства на a, получаем: $a^{\frac{p+1}{2}} \bmod p = a$. Поскольку $p \equiv 3 \bmod 4$, то число $\frac{p+1}{2}$ является четным, поэтому можно определить $x = a^{\frac{p+1}{4}} \bmod p$. Так как $x^2 \equiv a^{\frac{p+1}{2}} \equiv a \bmod p$, то x — квадратный корень из a.

9. Так как $p \equiv 7 \bmod 8$, то $p \equiv 8k + 7 = 4(2k+1) + 3 \Rightarrow p \equiv 3 \bmod 4$. Для квадратичных вычетов справедливо соотношение $a^{\frac{p-1}{2}} \bmod p = 1 \Rightarrow$ $\Rightarrow a^{\frac{p+1}{2}} \bmod p = a$. Поскольку $p \equiv 3 \bmod 4$, то число $\frac{p+1}{2}$ является чет-

ным, поэтому можно определить $x = a^{\frac{p+1}{4}} \bmod p$. Так как $x^2 \equiv a^{\frac{p+1}{2}} \equiv$ $\equiv a \bmod p$, то $\sqrt{a} = x = a^{\frac{p+1}{4}} \bmod p$.

10. Найдем число α, относящееся по модулю pq к показателю γ. Такой показатель по модулю pq существует, поскольку γ делит $\varphi(pq)$. Число α и есть искомое число. Действительно, из условия $\alpha^{\gamma} \equiv 1 \bmod pq$ следует справедливость сравнений $\alpha^{\gamma} \equiv 1 \bmod p$ и $\alpha^{\gamma} \equiv 1 \bmod q$. Осталось показать, как найти такое число α, для которого выполняются условия $\alpha \bmod p \neq 1$ и $\alpha \bmod q \neq 1$. Значение α следует формировать в соответствии с формулой $\alpha = \beta^{\frac{(p-1)(q-1)}{\gamma^2}} \bmod pq \neq 1$. Причем в качестве числа β следует взять число, являющееся одновременно первообразным корнем по $\bmod p$ и по $\bmod q$. В этом случае имеем: $\alpha = \beta^{uv} \bmod pq \neq 1$, где $u = (p-1)/\gamma$ и $v = (q-1)/\gamma$. Из последней формулы видно, что выполняются неравенства $\alpha \bmod q \neq 1$ и $\alpha \bmod p \neq 1$. Действительно, сравнение $\alpha \equiv \beta^{uv} \equiv 1 \bmod q$ или $\alpha \equiv \beta^{uv} \equiv 1 \bmod p$ может выполняться только в случае, если $uv \equiv 0 \bmod (q-1)$ или $uv \equiv 0 \bmod (p-1)$ соответственно. Однако последние соотношения не выполняются, поскольку по построению чисел p и q значение uv не делится ни на $q-1$, ни на $p-1$.

11. Найдем число α, относящееся по модулю pq к показателю γ. Такой показатель по модулю pq существует, поскольку γ делит $\varphi(pq)$. Из условия $\alpha^{\gamma} \equiv 1 \bmod pq$ следует справедливость сравнений $\alpha^{\gamma} \equiv 1 \bmod p$ и $\alpha^{\gamma} \equiv 1 \bmod q$. Нужно показать, как найти такое число α, для которого выполняются условия $\alpha \bmod p \neq 1$ и $\alpha \bmod q \neq 1$. Значение α следует формировать в соответствии с формулой $\alpha = \beta^{\frac{(p-1)(q-1)}{\gamma^{s+1}}} \bmod pq \neq 1$, где в качестве числа β следует взять число, являющееся одновременно первообразным корнем по $\bmod p$ и по $\bmod q$. В этом случае выполняются неравенства $\alpha \bmod q \neq 1$ и $\alpha \bmod p \neq 1$, поскольку сравнение $\alpha \equiv \beta^{\frac{(p-1)(q-1)}{\gamma^{s+1}}} \equiv 1 \bmod p$ или $\alpha \equiv \beta^{\frac{(p-1)(q-1)}{\gamma^{s+1}}} \equiv 1 \bmod q$ может выполняться только в случае, если $\frac{(p-1)(q-1)}{\gamma^{s+1}} \equiv 0 \bmod p-1$ или $\frac{(p-1)(q-1)}{\gamma^{s+1}} \equiv$ $\equiv 0 \bmod q-1$ соответственно. Однако ни одно из последних соотноше-

ний не выполняется, поскольку число $\frac{(p-1)(q-1)}{\gamma^{s+1}}$ не делится нацело ни на $q-1$, ни на $p-1$.

12. Найдем число α, относящееся по модулю pq к показателю $\gamma\delta$. Такой показатель по модулю pq существует, поскольку $\gamma\delta$ делит $\varphi(pq)$ (из условия задачи следует, что γ делит $\varphi(p)$ и δ делит $\varphi(q)$). Число α и есть искомое число. Действительно из условия $\alpha^{\gamma\delta} \equiv 1 \bmod pq$ следует справедливость сравнений $\alpha^{\gamma\delta} \equiv 1 \bmod p$ и $\alpha^{\gamma\delta} \equiv 1 \bmod q$. Эти сравнения можно представить в виде $(\alpha^{\gamma})^{\delta} \equiv 1 \bmod p$ и $(\alpha^{\delta})^{\gamma} \equiv 1 \bmod q$. Поскольку НОД$(\delta, p-1) = 1$, то δ не может быть показателем по модулю p, поэтому $\alpha^{\gamma} \equiv 1 \bmod p$ (в противном случае мы имели бы число $\alpha^{\gamma} \bmod p \neq 1$, которое относится к показателю δ по модулю p). Поскольку НОД$(\gamma, q-1) = 1$, то γ не может быть показателем по модулю q, поэтому $\alpha^{\delta} \equiv 1 \bmod q$ (в противном случае справедливость сравнения $(\alpha^{\delta})^{\gamma} \equiv 1 \bmod q$ означала бы, что число $\alpha^{\delta} \bmod q \neq 1$ относится к показателю γ по модулю q).

13. Находим число α, относящееся по модулю pq к показателю $\gamma\delta$. Это и есть искомое число. *Доказательство*: $\alpha^{\gamma\delta} \equiv 1 \bmod pq$ и $\alpha^{\gamma\frac{\delta}{d_i}} \neq 1 \bmod pq$ для любых простых делителей $d_i | pq$. Следовательно, $\alpha^{\gamma\delta} \equiv (\alpha^{\gamma})^{\delta} \equiv$ $\equiv 1 \bmod p$. Поскольку НОД$(\delta, p-1) = 1$, то δ не может быть показателем $\Rightarrow \alpha^{\gamma} \equiv 1 \bmod p$. Аналогично можно показать, что $\alpha^{\delta} \equiv 1 \bmod q$. Покажем, что γ и δ есть минимальные значения, для которых выполняются два последних соотношения. Если для некоторого $\gamma' | \gamma$ имеем $\alpha^{\gamma'} \equiv 1 \bmod p$, то $\alpha^{\gamma'\delta} \equiv 1 \bmod p$ (1). Поскольку $\alpha^{\delta} \equiv 1 \bmod q$, то $\alpha^{\delta\gamma'} \equiv 1 \bmod q$ (2). Из (1) и (2) следует $\alpha^{\delta\gamma'} \equiv 1 \bmod pq$, что противоречит тому, что число α относится по модулю pq к показателю $\delta\gamma$. Противоречие доказывает, что γ есть минимальный показатель степени числа α, для которого выполняется $\alpha^{\gamma} \equiv 1 \bmod p$. Аналогично показывается, что δ есть минимальный показатель, для которого выполняется сравнение $\alpha^{\delta} \equiv 1 \bmod q$.

14. Выбрать случайное число x и вычислить значения $t = (p-1)/\gamma$ и $z = x^t \bmod p$. Если $z \neq 1$, то $\alpha = z$. Действительно, $\alpha^{\gamma} = x^{p-1} \equiv 1 \bmod p$.

15. Выбрать случайное число x и вычислить значения $t = (p-1)/\gamma$ и $z = x^t \bmod p$. Если $z \neq 1$, то проверить выполнимость для $i = 1, 2$ и 3 следующего условия: $z^{\frac{\gamma}{d_i}} \bmod p \neq 1$. Если во всех трех случаях условие

выполняется, то z есть искомое число α. В противном случае выбрать новое число x и повторить приведенные выше вычисления.

16. Доказательство: если α есть первообразный корень, то по определению имеем $p-1=\min\{\gamma:\ \alpha^{\gamma}\equiv 1 \bmod p\} \Rightarrow \alpha^{\frac{p-1}{2}} \bmod p \neq 1$, т. е. α — квадратичный невычет.

17. Нет. Например, число $p-1$ относится по простому модулю p к показателю 2, хотя является квадратичным невычетом по mod p. Число квадратичных невычетов по модулю p равно $\frac{p-1}{2} > \varphi(p-1)$ при $p \geq 7$.

18. Известно, что число a является вычетом n-й степени, где $n \mid p-1$, тогда и только тогда, когда $a^{\frac{p-1}{n}} \equiv 1 \bmod p$. Последнее соотношение означает, что a не является первообразным корнем по модулю p, т. е. вычет не является первообразным корнем.

19. Требуется проверить выполнимость условия $\alpha^{\frac{p-1}{d_i}} \neq 1 \bmod p$ для каждого простого делителя d_i числа $p-1$. Если это имеет место, то число α является первообразным корнем.

20. Для $i=1,2,\ldots,\gamma-1$ имеем $(\alpha^i)^{\gamma}=(\alpha^{\gamma})^i \equiv 1^i \bmod p$. Поскольку выполняется сравнение $(\alpha^i)^{\gamma} \equiv 1 \bmod n$, то показатель числа α^i делит γ, но γ по условию есть простое число, следовательно, показатель α^i есть γ.

21. Пусть для некоторого числа $\gamma \mid p-1$, где $\gamma < p-1$ выполняется соотношение $(\alpha^{-1})^{\gamma} \equiv 1 \bmod p$. Из последнего условия следует: $(\alpha^{\gamma})^{-1} \equiv$ $\equiv 1 \bmod p \Rightarrow \alpha^{\gamma} \equiv 1 \bmod p$, что противоречит условию задачи, согласно которому число α есть первообразный корень по модулю p.

22. Для $i=1,2,\ldots,\gamma-1$ и $j=1,2,\ldots,\delta-1$ имеем $(\alpha^i\beta^j)^{\gamma\delta}=(\alpha^{\gamma})^i(\beta^{\delta})^j \equiv$ $\equiv 1 \bmod n$. Поскольку выполняется сравнение $(\alpha^i\beta^j)^{\gamma\delta} \equiv 1 \bmod n$, то показатель числа $\alpha^i\beta^j$ делит число $\varepsilon=\gamma\delta$. Последнее означает, что показателем $\alpha^i\beta^j$ может быть только одно из следующих трех чисел: ε, γ и δ. Покажем, что γ и δ не являются показателями числа $\alpha^i\beta^j$. Действительно, $(\alpha^i\beta^j)^{\gamma}=(\alpha^{\gamma})^i\beta^{j\gamma} \equiv \beta^{j\gamma} \bmod n$. Поскольку δ не делит $j\gamma$, то $\beta^{j\gamma} \bmod n \neq 1$. Аналогично: $(\alpha^i\beta^j)^{\delta}=\alpha^{\delta i}(\beta^{\delta})^j \equiv \alpha^{\delta i} \bmod n \neq 1$, поскольку γ не делит δi. Таким образом, ε есть показатель (по модулю n) числа $\alpha^i\beta^j$.

23. По условию имеем $a^{\delta} = a^{\gamma t} = (a^t)^{\gamma} \equiv 1 \bmod n$, где t — натуральное число, причем $z = a^t \bmod n \neq 1$. Поскольку γ — простое число, то число z относятся к показателю γ.

24. По условию для некоторого числа a имеем $a^{\delta} = a^{\pi t} = (a^t)^{\pi} \equiv 1 \bmod n$, где t — натуральное число, причем $z_1 = a^t \bmod n \neq 1$. Поскольку π — простое число, то число z_1 относится к показателю π. Аналогично можно показать, что при некотором целом u число $z_2 = a^u \bmod n \neq 1$ относится к показателю σ. Далее легко показать, что число $z_3 = z_1 z_2$ относится по модулю n к показателю $\gamma = \pi\sigma$.

25. По условию для некоторого числа a имеем $a^{\delta} = a^{\pi t_1} = (a^{t_1})^{\pi} \equiv 1 \bmod n$, где t_1 — натуральное число, причем $z_1 = a^{t_1} \bmod n \neq 1$. Поскольку π — простое число, то число z_1 относится к показателю π. Аналогично можно показать, что при некотором целом t_2 число $z_2 = a^{t_2} \bmod n \neq 1$ относится к показателю σ. Число $z_1 z_2$ относится по модулю n к показателю $\gamma = \pi\sigma$. При некотором целом t_3 число $z_3 = a^{t_3} \bmod n \neq 1$ относится к показателю τ. Поскольку НОД$(\pi\sigma, \tau) = 1$, то по известной теореме число $z_1 z_2 z_3$ относится к показателю $\pi\sigma\tau$. Продолжая аналогичные рассуждения, утверждение задачи доказывается для произвольного числа простых сомножителей числа γ.

26. По условию для некоторого числа a имеем $a^{\delta} = a^{t\pi^k} = (a^t)^{\pi^k} \equiv 1 \bmod n$, где t — натуральное число, причем $z_0 = a^t \bmod n \neq 1$, $z_1 = a^{t\pi} \bmod n \neq 1$, ..., $z_{k-1} = a^{t\pi^{k-1}} \bmod n \neq 1$. Видим, что наименьшей натуральной степенью g, для которой имеет место $z_0^g \bmod n = 1$, является число π^k, т. е. число z_0 относится к показателю π^k. Утверждение доказано.

27. Представим γ в виде канонического разложения $\gamma = \pi_1^{k_1} \pi_2^{k_2} ... \pi_s^{k_s}$. Рассмотрим множитель $\pi_i^{k_i}$, где π_i — простое число, k_i — натуральное число. По условию для некоторого числа a имеем $a^{\delta} = a^{t\pi_i^{k_i}} = (a^t)^{\pi_i^{k_i}} \equiv 1 \bmod n$, где t — натуральное число, причем $w_i = z_0 = a^t \bmod n \neq 1$, $z_1 = a^{t\pi_i} \bmod n \neq 1$, ..., $z_{k_i - 1} = a^{t\pi_i^{k_i - 1}} \bmod n \neq 1$. Видим,

что наименьшей натуральной степенью g, для которой имеет место $z_0^g \bmod n = 1$, является число $\pi_i^{k_i}$. т. е. число w_i относится к показателю $\pi_i^{k_i}$. Таким образом, каждый из множителей $\pi_i^{k_i}$ есть показатель по модулю n. Далее применяем известную теорему о взаимно простых показателях: если числа w_i и w_j относятся к показателям $\pi_i^{k_i}$ и $\pi_j^{k_j}$ соответственно, и НОД$(\pi_i^{k_i}, \pi_j^{k_j}) = 1$, то число $w_i w_j$ относится к показателю $\gamma_{ij} = \pi_i^{k_i}\pi_j^{k_j}$. Применяя эту теорему несколько раз, доказываем утверждение задачи.

28. Из условия следует, что $\varphi(q) | L(m)/\gamma$. Поскольку $b^{\varphi(q)} \equiv 1 \bmod q$, то $a \equiv b^{L(m)/\gamma} \equiv (b^{\varphi(q)})^{\frac{L(m)\cdot\gamma}{\varphi(q)}} \equiv 1 \bmod q$.

29. Пусть a — двукратный первообразный корень по $\bmod p^\alpha$ и по $\bmod q^\beta$. Обобщенная функция Эйлера равна $L(p^\alpha q^\beta) = \text{НОК}(p^{\alpha-1}(p-1), q^{\beta-1}(q-1))$. Ее каноническое разложение включает набор простых множителей, возможно возводимых в некоторую степень. Если некоторый из этих множителей встречается только в каноническом разложении числа $p^{\alpha-1}(p-1)$ или числа $q^{\beta-1}(q-1)$, то будем его считать множителем числа P или числа Q соответственно. Если простой множитель встречается в разложении обоих чисел $p^{\alpha-1}(p-1)$ и $q^{\beta-1}(q-1)$, то будем считать его множителем числа P, если он входит с большей степенью в разложение числа $p^{\alpha-1}(p-1)$, или множителем числа Q, если он входит с большей степенью в разложение числа $q^{\beta-1}(q-1)$. Если рассматриваемый множитель $L(p^\alpha q^\beta)$ входит с одинаковой степенью в разложения чисел $p^{\alpha-1}(p-1)$ и $q^{\beta-1}(q-1)$, то будем считать его множителем числа C. Таким образом, можно записать $L(p^\alpha q^\beta) = PQC$. В соответствии с обобщенной теоремой Эйлера имеем: $a^{L(n)} \equiv 1 \bmod (p^\alpha q^\beta)$. Пусть d_i есть простой множитель, входящий с некоторой степенью в разложение числа P. Тогда справедливы следующие два соотношения: $a^{(P/d_i)QC} \equiv 1 \bmod q^\beta$, поскольку число $q^{\beta-1}(q-1)$ делит степень $(P/d_i)QC$, и $a^{(P/d_i)QC} \bmod p^\alpha \neq 1$, поскольку число $p^{\alpha-1}(p-1)$ не делит степень $(P/d_i)QC$. Из указанных двух соотношений следует, что $a^{L(p^\alpha q^\beta)/d_i} \bmod (p^\alpha q^\beta) = a^{(P/d_i)QC} \bmod (p^\alpha q^\beta) \neq 1$. Если d_i есть простой множитель, входящий с некоторой степенью в разложение числа

Q, то аналогично доказывается, что $a^{L(p^\alpha q^\beta)/d_i} \bmod\left(p^\alpha q^\beta\right) \neq 1$. Если d_i есть простой множитель, входящий с некоторой степенью в разложение числа C, то имеем: $a^{PQ(C/d_i)} \bmod q^\beta \neq 1$, поскольку число $q^{\beta-1}(q-1)$ не делит степень $PQ(C/d_i)$, и $a^{PQ(C/d_i)} \bmod p^\alpha \neq 1$, поскольку число $p^{\alpha-1}(p-1)$ не делит степень $(P/d_i)QC$, т. е. и в этом случае выполняется $a^{L(p^\alpha q^\beta)/d_i} \bmod (p^\alpha q^\beta) \neq 1$. Таким образом, $a^{L(p^\alpha q^\beta)} \bmod (p^\alpha q^\beta) = 1$ и ни при каком показателе $\delta < L(p^\alpha q^\beta)$ не выполняется соотношение $a^\delta \bmod (p^\alpha q^\beta) = 1$, т. е. $L(p^\alpha q^\beta)$ есть показатель, к которому относится число a по модулю $p^\alpha q^\beta$.

30. Пусть a_p — первообразный корень по $\bmod p^\alpha$ и a_q — первообразный корень по $\bmod q^\beta$. Все числа вида $a' = a_p + N_p p^\alpha$ относятся к классу $\overline{a_p}$ по $\bmod p^\alpha$. Все числа вида $a'' = a_q + N_q q^\beta$ относятся к классу $\overline{a_q}$ по $\bmod q^\beta$. Нам необходимо найти числа, входящие одновременно в оба указанных класса, т. е. найти такие значения N_p и N_q, при которых выполняется равенство $a_p + N_p p^\alpha = a_q + N_q q^\beta$, которое можно переписать в виде $N_p p^\alpha - N_q q^\beta = a_q - a_p$. Последнее соотношение представляет собой диофантово уравнение относительно неизвестных N_p и N_q, которое заведомо имеет решение, поскольку НОД $(p^\alpha, q^\beta) = 1$. Все решения этого уравнения могут быть найдены следующим путем. С помощью расширенного алгоритма Евклида находятся решения уравнения вида $N_p p^\alpha - N_q q^\beta = 1$, которые затем умножаются на число $a_q - a_p$. Любое найденное решение (N_p^*, N_q^*) задает некоторый искомый «двукратный» первообразный корень $a = a_p + N_p^* p^\alpha = a_q + N_q^* q^\beta$.

31. При случайном выборе указанных чисел с большой вероятностью искомое число x может быть найдено. Однако это можно сделать не во всех случаях. Например, известно, что нечетное число a относится по модулю $2p^\alpha$, где $\alpha \geq 1$, к показателю $\gamma | p^{\alpha-1}(p-1)$ тогда и только тогда, когда a относится по модулю p^α к показателю γ. Поэтому не существует чисел, относящихся одновременно к δ и $\gamma \neq \delta$ как к показателям по модулям $m = 2p^\alpha$ и $n = p^\alpha$.

32. Известен вычислительно эффективный алгоритм нахождения чисел, относящихся к любому допустимому показателю по любому модулю. Пусть a_p — число, относящееся к δ как к показателю по $\bmod p$, и a_q — число, относящееся к γ как к показателю по $\bmod q$. Все числа вида $a' = a_p + N_p p$ относятся к классу $\overline{a_p}$ по $\bmod p$. Все числа вида

$a'' = a_q + N_q q$ относятся к классу $\bar{a}_q$ по mod q. Нам необходимо найти числа, входящие одновременно в оба указанных класса, т. е. найти такие значения N_p и N_q, при которых выполняется равенство $a_p + N_p p = a_q + N_q q$, которое можно переписать в виде $N_p p - N_q q = a_q - a_p$. Последнее соотношение представляет собой диофантово уравнение относительно неизвестных N_p и N_q, которое имеет решение, поскольку НОД$(p, q) = 1$. Найдем с помощью расширенного алгоритма Евклида решение уравнения вида $N_p p - N_q q = 1$. Пусть этим решением является пара значений $N_p' = c_p$ и $N_q' = c_q$. Тогда пара значений $N_p = c_p(a_q - a_p)$ и $N_q = c_q(a_q - a_p)$ есть частное решение уравнения $N_p p - N_q q = a_q - a_p$. Все решения последнего уравнения можно найти, складывая полученное частное решение с общим решением соответствующего ему однородного уравнения $N_p p - N_q q = 0$. Общим решением последнего является множество пар значений $N_q'' = kp$ и $N_p'' = kq$, соответствующих всевозможным целым значениям $k = \pm 1, \pm 2, \pm 3, \ldots$ Таким образом, все решения уравнения $N_p p - N_q q = a_q - a_p$ описываются соотношениями: $N_p = c_p(a_q - a_p) + kq$ и $N_q = c_q(a_q - a_p) + kp$. Искомые значения выражаются следующей формулой: $x = a_p + c_p(a_q - a_p)p + kqp$ (или $x = a_q + c_q(a_q - a_p)q + kpq$).

33. Известно, что количество чисел, относящихся к числам δ и γ как к показателям по простым модулям p и q, равно, соответственно, $\psi(\delta) = \varphi(\delta)$ и $\psi(\gamma) = \varphi(\gamma)$. Обозначим множества этих чисел как $\{a_p\}$ и $\{a_q\}$ соответственно. В соответствии с решением предыдущей задачи каждая пара элементов из этих множеств задает множество чисел, относящихся к числам δ и γ как к показателям по mod p и по mod q соответственно: $x = a_p + c_p(a_q - a_p)p + kqp$. При некотором единственном значении k получаем одно из искомых значений множества $\{x: 1 < x < pq\}$. Поскольку некоторые из указанных пар могут задавать одно и то же значение $1 < x < pq$, то получаем $\#\{x: 1 < x < pq\} \le \varphi(\delta)\varphi(\gamma)$.

34. Поскольку вероятность того, что случайно выбранное число есть первообразный корень, является сравнительно высокой, а вероятность случайного выбора числа α, относящегося по модулю p к показателю γ, очень мала, то первоначально надо генерировать числа, удовлетворяющие второму условию, а затем проверять, является ли каждое из них первообразным корнем по модулю q. Таким образом, вычислительно эффективным является следующий способ. Выбирается случайное число x, и вычисляются значения $t = (p-1)/\gamma$ и $z = x^t \bmod p$. Если $z \ne 1$ и Z^{γ/d_i} для всех нетривиальных делителей d_i/γ, то $\alpha = z$. Проверить, является ли α первообразным корнем по модулю q. При неудаче попытку повторить.

35. Вероятность того, что случайно выбранное число есть квадратичный вычет по простому модулю, является сравнительно высокой (равна 0.5). Вероятность случайного выбора числа α, относящегося по модулю p к показателю γ, очень мала, поэтому первоначально надо сформировать число, удовлетворяющее второму условию. Затем следует проверить, является ли оно квадратичным вычетом по модулю q. Таким образом, вычислительно эффективным является следующий способ. Выбирается случайное число x и вычисляются значения $t = (p-1)/\gamma$ и $z = x^t \bmod p$. Если $z \neq 1$ и Z^{γ/d_i} для всех нетривиальных делителей d_i/γ, то $\alpha = z$. Проверяется выполнимость условия $\alpha^{\frac{q-1}{2}} \bmod q = 1$. При неудаче попытку повторить.

36. Если γ не делит одно из чисел $p-1$ и $q-1$, например, число $q-1$, то справедливость соотношения $\alpha^{\gamma} \equiv 1 \bmod q$ означает, что $\alpha \equiv 1 \bmod q$ (так как в этом случае γ не может быть показателем по модулю q).

37. Вероятность того, что случайно выбранное число есть квадратичный невычет по RSA-модулю, является сравнительно высокой (равна 3/4). Вероятность случайного выбора числа α, относящегося по модулю p к показателю γ, очень мала, поэтому первоначально надо сформировать число, удовлетворяющее второму условию. Затем следует проверить, является ли оно квадратичным невычетом по модулю n. Таким образом, вычислительно эффективным является следующий способ. Выбирается случайное число x и вычисляются значения $t = (p-1)/\gamma$ и $z = x^t \bmod p$. Если $z \neq 1$ и Z^{γ/d_i} для всех нетривиальных делителей d_i/γ, то $\alpha = z$. Проверяется выполнимость хотя бы одного из следующих двух условий $\alpha^{\frac{q-1}{2}} \bmod q = q-1$ и $\alpha^{\frac{q-1}{2}} \bmod p = p-1$. При неудаче попытку повторить.

38. Требуемое число можно найти следующим образом. Выбирается случайное число x, являющееся одновременно первообразным корнем по модулю p и по модулю q. Затем вычисляются значения $t = \frac{L(pq)}{\gamma}$, где $L(pq)$ — обобщенная функция Эйлера и $z = x^t \bmod (pq)$. Если $z \neq 1$, то $\alpha = z$. Действительно, с учетом условий $\gamma^s \mid p-1$, $\gamma^s \mid q-1$, $\text{НОД}\left(\frac{p-1}{2\gamma^s}, \frac{q-1}{2\gamma^s}\right) = 1$ и обобщенной теоремы Эйлера имеем:

$$\alpha^{\gamma} = \left(x^{\frac{L(pq)}{\gamma}} \right)^{\gamma} = x^{L(pq)} \equiv 1 \bmod (pq) \Rightarrow \alpha^{\gamma} \equiv 1 \bmod p \quad \text{и} \quad \alpha^{\gamma} \equiv 1 \bmod q.$$

При этом $\alpha \bmod p \neq 1$ и $\alpha \bmod q \neq 1$. Последние соотношения легко доказать следующим путем: $\alpha \equiv x^{\frac{t(pq)}{\gamma}} \equiv x^{\frac{(p-1)(q-1)}{\gamma \cdot t}} \equiv \left(x^{\frac{p-1}{\gamma}} \right)^{\frac{q-1}{\gamma'}} \bmod (pq)$,

следовательно, $\alpha \equiv \left(x^{\frac{p-1}{\gamma}} \right)^{\frac{q-1}{\gamma'}} \bmod p$. Поскольку целое число $\frac{q-1}{\gamma'}$ не делится ни на один нетривиальный делитель числа $p-1$, то ни один из его делителей не может быть показателем по модулю p. В силу того, что $x^{\frac{p-1}{\gamma}} \bmod p \neq 1$ (число x есть первообразный корень по модулю p), имеем $\alpha \bmod p \neq 1$. Аналогично показывается, что $\alpha \bmod q \neq 1$.

39. Отметим, что понятие показателя определено для чисел, которые не сравнимы с единицей по заданному модулю. Допустим существование числа α, относящегося к простому показателю γ по модулю p и по модулю q. Если $\alpha \bmod p \neq 1$ и $\alpha \bmod q \neq 1$, то $\alpha \bmod (pq) \neq 1$. Согласно допущению имеем $\alpha^{\gamma} \equiv 1 \bmod p$ и $\alpha^{\gamma} \equiv 1 \bmod q$, следовательно, $\alpha^{\gamma} \equiv 1 \bmod (pq)$, т. е. число α относится к показателю γ по модулю pq. Выберем некоторое число x и вычислим значения $t = \frac{L(pq)}{\gamma}$, где $L(pq)$ — обобщенная функция Эйлера, и $z = x^t \bmod (pq)$. Если $z \neq 1$, то z — число, относящееся к показателю γ по модулю pq. Тогда множество $\{z^1, z^2 \bmod (pq), z^3 \bmod (pq), \ldots, z^{\gamma} \bmod (pq) = 1\}$ содержит все числа, относящиеся к показателю γ по модулю pq. При некотором j будем иметь $z^j \bmod (pq) = \alpha$. Следовательно, α представляется в виде $z = x^{tj} \bmod (pq) = (x^j)^t \bmod (pq) = v^t \bmod (pq)$. Таким образом, мы представили число α в виде $\alpha \equiv b^{\frac{t(pq)}{\gamma}} \bmod (pq)$. В соответствии с утверждением задачи № 28 имеет место либо $\alpha \equiv 1 \bmod p$, либо $\alpha \equiv 1 \bmod q$. Получено противоречие, которое доказывает утверждение задачи № 39.

40. Известно, что количество чисел α, не превышающих $p-1$ и относящихся по простому модулю к показателю $P(\alpha)$, равно $\psi(P(\alpha)) = \varphi(P(\alpha))$. В случае простого показателя $P(\alpha) = \gamma$ имеем $\psi(\gamma) = \varphi(\gamma) = \gamma - 1$, т. е. заданное множество чисел включает $\gamma - 1$ отличных от 1 элементов, следовательно, оно исчерпывает все классы, относящиеся по модулю p к показателю γ. В случае составного показателя $P(\alpha) = \gamma$ имеем $\psi(\gamma) = \varphi(\gamma) < \gamma - 1$, т. е. заданное множество чисел включает также и числа, относящиеся к некоторым другим показателям, которые являются делителями $P(\alpha)$.

41. Пусть a и g есть первообразные корни по модулю p. Допустим, что i и j есть индексы чисел a и g при основании g и a соответственно. Можно записать: $g \equiv a^{i} \equiv (g^{i})^{j} \equiv g^{ij} \bmod q$, следовательно, $ij \equiv 1 \bmod p-1$ или $j \equiv i^{-1} \bmod p-1$, но обратный элемент существует, только если НОД$(i, p-1) = 1$.

42. Пусть a и g есть первообразные корни по модулю p. Допустим, что i и j есть индексы первообразных корней a и g при основании g и a соответственно. Можно записать: $a \equiv g^{i} \equiv (a^{j})^{i} \equiv a^{ij} \bmod q$, следовательно, $ij \equiv 1 \bmod p-1$, что может выполняться только в случае, если НОД$(i, p-1) = 1$. Следовательно, необходимым условием того, что некоторое число a есть первообразный корень по модулю p, является то, что индекс числа a является взаимно простым с $p-1$. Это доказывает утверждение задачи.

43. Пусть $i = \mathrm{ind}_{g} a$ и НОД$(i, p-1) = d$. Для индекса i' числа a при некотором другом основании g' имеем $i' = \mathrm{ind}_{g'} a$. Представляя a в виде степеней первообразных корней g и g', получим $a \equiv g'^{i'} \equiv (g^{j})^{i'} \equiv g^{ji'} \equiv g^{i} \bmod p$, где $j = \mathrm{ind}_{g} g'$, откуда следует $ji' \equiv i \bmod p-1$. Поскольку НОД$(j, p-1) = 1$ (известно, что индексы первообразных корней являются числами, взаимно простыми с $p-1$), то НОД$(i', p-1) =$ НОД$(ji', p-1) =$ НОД$(i, p-1) = d$.

44. Можно доказать, что индекс i (по простому модулю p) числа a удовлетворяет соотношению НОД$(i, p-1) = d$, где число d не зависит от выбора первообразного корня в качестве основания (см. предыдущую задачу). Поскольку любое число $j \le p-1$ является индексом некоторого класса по модулю p и различным индексам соответствуют различные классы, то задача сводится к нахождению количества чисел $j \le p-1$, таких что НОД$(j, p-1) = d$. Если выполняется последнее условие, то выполняется и соотношение НОД$\left(\frac{j}{d}, \frac{p-1}{d}\right) = 1$, и наоборот. Количество

различных классов $\bar{z}$, представители $z = j/d$ которых удовлетворяют условию НОД $\left(z, \frac{p-1}{d}\right) = 1$, равно $\varphi\left(\frac{p-1}{d}\right)$. Это и есть искомое количество классов.

45. В соответствии с решением предыдущей задачи число классов по простому модулю p, индекс которых удовлетворяет условию НОД$(i, p-1) = d$, равно $\varphi\left(\frac{p-1}{d}\right)$. При $d = 1$ получаем число ψ первообразных корней по простому модулю p: $\psi = \varphi(p-1)$.

46. Допустим противное, т. е. что число $z = g^t \bmod p$ $(1 < z < p)$ при некотором первообразном корне g само не является первообразным корнем. Тогда число z относится к некоторому делителю $\delta < p-1$ числа $p-1$ как к показателю по модулю p. Из нашего предположения получаем: $z^\delta \equiv (g^t)^\delta \equiv g^{t\delta} \equiv 1 \bmod p$. Поскольку g есть первообразный корень, то последнее соотношение имеет место, если и только если $p-1 \mid i\delta$. Так как $\delta < p-1$, то i содержит нетривиальный делитель числа $p-1$. Полученное противоречие доказывает утверждение задачи.

47. Пусть i есть индекс (по простому модулю p) числа a. Учитывая условие задачи, имеем: $a^\delta \equiv (g^t)^\delta \equiv g^{t\delta} \equiv 1 \bmod p$, где g есть некоторый первообразный корень и $g^{t\delta} \equiv 1 \bmod p \Leftrightarrow p-1 \mid i\delta \Rightarrow \frac{p-1}{\delta} \mid i$. Поскольку $a \bmod p \neq 1$, то $i < p-1$. Показатель δ есть простое число, поэтому НОД$(i, p-1) = \frac{p-1}{\delta}$.

48. Пусть $a^\delta \equiv (g^t)^\delta \equiv g^{t\delta} \equiv 1 \bmod p$, где g есть некоторый первообразный корень и i есть индекс числа a по модулю p при основании g. По условию задачи имеем: $g^{t\delta} \equiv 1 \bmod p \Leftrightarrow p-1 \mid i\delta \Rightarrow \frac{p-1}{\delta} \mid i$. Для любого нетривиального делителя d показателя δ имеем: $a^{\delta \cdot d} \equiv (g^t)^{\delta \cdot d} \equiv g^{t\delta/d} \bmod p \neq 1$, следовательно, $p-1$ не делит число $\frac{i\delta}{d}$, т. е. $\frac{p-1}{\delta/d}$ не делит число i. Следовательно, для любого нетривиального делителя d имеем соотношение НОД$(i, p-1) < \frac{p-1}{\delta/d}$, поэтому НОД$(i, p-1) = \frac{p-1}{\delta}$.

49. Пусть для некоторого первообразного корня g имеем: $a \equiv g^i \bmod p$. Заметим, что условие $\text{НОД}(i, p-1) = \dfrac{p-1}{\delta}$ будет выполняться для индекса при основании по любому первообразному корню, т. е. его реализация не зависит от выбора конкретного значения g. Так как $\text{НОД}(i, p-1) = \dfrac{p-1}{\delta} = \gamma$, то $\gamma | i$ и $p-1 | i\delta$. Следовательно, имеем $i\delta = k(p-1)$ и $a^\delta \equiv g^{i\delta} \equiv (g^{p-1})^k \equiv 1 \bmod p$, где k есть некоторое натуральное число. Если δ есть простое число, то из $a^\delta \equiv 1 \bmod p$ следует, что δ является показателем числа a. Путь δ есть составное число. Предположим, что δ не является показателем числа a. Тогда для некоторого нетривиального делителя d числа δ имеем: $a^{\delta/d} \equiv 1 \bmod p$, где $\delta' = \delta/d$ есть показатель числа a по модулю p. Известно (см. предыдущую задачу), что индекс и показатель числа a удовлетворяют соотношению $\text{НОД}(i, p-1) = \dfrac{p-1}{\delta'} = \dfrac{d(p-1)}{\delta}$, что противоречит условию задачи. Полученное противоречие показывает, что предположительно составное число δ является показателем по модулю p.

50. Известно, что индексы первообразных корней являются числами, взаимно простыми с $p-1$. Различным первообразным корням соответствуют различные индексы. Известно, что количество первообразных корней по простому модулю p равно $\varphi(p-1)$. Значение $\varphi(p-1)$ по определению равно количеству чисел, взаимно простых с $p-1$. Таким образом, мы показали взаимно однозначное соответствие между множеством первообразных корней и множеством чисел, взаимно простых с $p-1$, которое доказывает утверждение задачи.

51. Возьмем некоторый первообразный корень β. Существует индекс i, такой что $a = \beta^i \bmod p$. По условию задачи имеем: $a^\gamma \equiv \beta^{i\gamma} \equiv 1 \bmod p \Rightarrow$ $\Rightarrow p-1 | i\gamma \Rightarrow i = k(p-1)/\gamma$, где k есть натуральное число. Таким образом, имеем: $a \equiv \beta^i \equiv (\beta^k)^{\frac{p-1}{\gamma}} \equiv b^{\frac{p-1}{\gamma}} \bmod p$.

52. Пусть для предполагаемого простого p выполняется тест Ферма, т. е. выполняется соотношение $a^{p-1} = 1 \bmod p$ для всех проверяемых значений основания a. Поскольку q — заведомо простое число, то для тех же значений a имеем $a^{q-1} = 1 \bmod q$. По известной теореме из выполнимости указанных двух соотношений следует выполнимость и соотношения $a^{\varphi(n)} = 1 \bmod n$. Числа Кармайкла проходят проверку по соотноше-

нию $a^{p-1} = 1 \bmod p$, поэтому они пройдут и проверку по формуле $a^{\varphi(n)} = 1 \bmod n$.

53. Следует выбрать случайное число β ($1 < \beta < p$). Если $\beta^{(p-1)/\delta} \bmod p \neq 1$, где δ — заданный составной показатель, то число $\beta^{(p-1)/\delta} \bmod p$ может относиться только к показателям $\gamma | \delta$. Поэтому следует проверить выполнимость условия $\beta^{(p-1)/d_i} \neq 1 \bmod p$ для всех простых делителей d_i числа δ. Если это так, то $\beta^{(p-1)/\delta} \bmod p$ является искомым числом. Если хотя бы для одного делителя d_i это условие не выполняется, то следует сформировать другое случайное число β и повторить описанную процедуру.

54. Все перечисленные модули $p = 67$, 47, 97 и 131 являются простыми, поэтому искомое количество чисел равно $\varphi(\varphi(p)) = \varphi(p-1) = 20$, 22, 32 и 48 соответственно.

55. Все перечисленные модули являются простыми, поэтому искомое количество чисел равно $\varphi(2) = 1$.

56. Для простых чисел $p = 23$ и 67 число 11 является делителем $p - 1$, поэтому для этих модулей искомое количество чисел равно $\varphi(11) = 10$. Функция Эйлера от составного модуля 133 равна $\varphi(7 \cdot 19) = \varphi(7) \cdot \varphi(19) = 2^3 \cdot 3^2$. В разложении $\varphi(133)$ множителя 11 нет, поэтому оно не может быть показателем по модулю 133. В этом случае искомых чисел нет.

57. В качестве числа a могут быть выбраны $p - 2$ различных чисел ($a \neq 1$). По определению первообразный корень — это число, относящееся по модулю p к показателю $p - 1$. Количество чисел, относящихся к $p - 1$ как к показателю по модулю p, равно $\psi(p-1) = \varphi(p-1)$. Искомая вероятность равна $\varphi(\varphi(p))/(p-2) = \varphi(p-1)/(p-2)$.

58. Показателями могут быть только делители обобщенной функции Эйлера $L(n)$, где n — значение модуля. При $n = 17$ имеем $L(17) = \varphi(17) = 16$ и 4 различных показателя: 2, 4, 8 и 16. При $n = 196$ имеем $L(196) = L(2^2 \cdot 7^2) = 2^2 \cdot 3 \cdot 7$ и 11 различных показателей: 2, 4, 3, 7, 6, 12, 14, 28, 21, 42, и 84. При $n = 625$ имеем $L(625) = L(5^4) = 5^3 \cdot 2^2$ и 11 различных показателей: 2, 4, 5, 25, 125, 10, 50, 250, 20, 100 и 500.

59. Показателями могут быть только делители $L(n) = \text{НОК}[\varphi(3), \varphi(5), \varphi(129), \varphi(257)] = 256$. Следовательно, имеется по модулю $n = 3 \cdot 5 \cdot 129 \cdot 257$ восемь различных показателей: 2, 4, 8, 16, 32, 64, 128 и 256.

60. В качестве числа a могут быть выбраны $p - 2$ различных чисел ($a \neq 1$). Количество чисел, относящихся к $\delta | p - 1$ как к показателю по модулю p, равно $\psi(\delta) = \varphi(\delta)$. Искомая вероятность равна $\varphi(\delta)/(p-2)$.

61. Представим искомую вероятность в виде

$$Prob\left(\beta^{\frac{p-1}{\delta}} \neq 1 \bmod p\right) = 1 - Prob\left(\beta^{\frac{p-1}{\delta}} = 1 \bmod p\right).$$

Имеем $Prob\left(\beta^{\frac{p-1}{\delta}} = 1 \bmod p\right) = Prob\left(\beta^{2rq} = 1 \bmod p\right)$. Соотношение $\beta^{2rq} = 1 \bmod p$ выполняется, если число β относится к показателю 2, $2r$, $2q$ или $2qr$, поэтому $Prob\left(\beta^{2rq} = 1 \bmod p\right) =$

$= \dfrac{\psi(2) + \psi(r) + \psi(q) + \psi(rq) + \psi(2r) + \psi(2q) + \psi(2rq)}{p-2}$, где $\psi(x)$ — количество чисел, относящихся к x как к показателю по модулю p. Используя верную для простого модуля формулу $\psi(x) = \varphi(x)$, получаем $Prob\left(\beta^{\frac{p-1}{\delta}} \neq 1 \bmod p\right) = 1 - \dfrac{1 + 2(r-1) + 2(q-1) + 2(r-1)(q-1)}{p-2}$. При условии, что множители δ, r и q имеют большие значения, получаем следующую приближенную формулу: $Prob\left(\beta^{\frac{p-1}{\delta}} \neq 1 \bmod p\right) \approx 1 - \dfrac{1}{\delta}$.

62. Поскольку g — первообразный корень, то $g' = g^{\frac{p-1}{\delta}} \bmod p \neq 1$. Поскольку по условию число a не делит $p-1$, то это число не может быть показателем по модулю p, поэтому $(g')^a = (g^a)^{\frac{p-1}{\delta}} \bmod p \neq 1$.

63. Имеем $p - a \equiv -a \bmod p$. Возводя число $-a$ в степень $\dfrac{p-1}{2}$, получаем $(-a)^{\frac{p-1}{2}} \equiv (-a)^{2k} \equiv (-1)^{2k} a^{2k} \equiv a^{2k} \equiv a^{\frac{p-1}{2}} \bmod p$. Поскольку значения $(p-a)^{\frac{p-1}{2}} \bmod p$ и $a^{\frac{p-1}{2}} \bmod p$ равны, то числа a и $p-a$ являются одновременно либо квадратичными вычетами, либо квадратичными невычетами.

64. Имеем $p-a \equiv -a \bmod p$. Возводя число $-a$ в степень $\frac{p-1}{2}$, получаем $(-a)^{\frac{p-1}{2}} \equiv (-a)^{2k+1} \equiv (-1)^{2k+1} a^{2k+1} \equiv -a^{2k+1} \equiv -a^{\frac{p-1}{2}} \bmod p$. Таким образом, значения $(p-a)^{\frac{p-1}{2}} \bmod p$ и $a^{\frac{p-1}{2}} \bmod p$ имеют противоположные знаки, поэтому если число a является квадратичным вычетом (невычетом), то число $p-a$ является квадратичным невычетом (вычетом).

65. Для двух последовательных чисел всегда выполняется соотношение НОД$(n, n+1) = 1$. Это непосредственно следует из алгоритма Евклида, с помощью которого находится наибольший общий делитель двух чисел. Это также следует из того, что любой общий делитель числа $n+1$ и числа n одновременно является делителем числа n и остатка от деления $n+1$ на число n.

66. В соответствии с малой теоремой Ферма для любого простого p и любого числа a, такого что НОД$(p, a) = 1$, имеет место $a^p \equiv a \bmod p \Rightarrow$ $\Rightarrow p \mid (a^p - a)$. При $a = 2$ имеем $p \mid (2^p - 2)$.

67. В каноническом разложении любого из указанных натуральных чисел присутствует хотя бы один нечетный простой множитель p, возведенный в степень $\alpha \geq 1$. В соответствии с теоремой о мультипликативности функции Эйлера в каноническое разложение $\varphi(n)$ войдет множитель $p^{\alpha-1} \mid (p-1)$. Значение $p-1$ является четным, поэтому значение $\varphi(n)$ также является четным.

68. Все целые числа разбиваются на d классов вычетов по модулю d. Вероятность случайного выбора числа, относящегося к любому из этих классов, включая и класс $\bar{0}$, к которому относятся числа, делящиеся на d, равна $1/d$. Предполагая, что случайный выбор двух чисел представляет собой два независимых события, получаем, что искомая вероятность равна $(1/d)^2$.

69. Все целые числа разбиваются на d классов вычетов по модулю d. Вероятность случайного выбора числа, относящегося к любому из этих классов, равна $1/d$. Это есть вероятность выбора одного числа, делящегося на d. Вероятность случайного выбора двух чисел a и b, делящихся на d, равна $(1/d)^2$. Если при этом НОД$(a/d, b/d) = 1$, то НОД$(a, b) = d$. Поскольку числа a и b выбираются случайно, то значения a/d и b/d также являются случайными. По условию Pr[НОД$(a/d, b/d) = 1] = P$, поэтому $P_d = \Pr[\text{НОД}(a, b) = d] = P/d^2$.

70. Предположим, что вероятность случайного выбора двух взаимно простых натуральных чисел a и b равна $P = \Pr[\text{НОД}(a, b) = 1]$. Все целые числа разбиваются на d классов вычетов по модулю d. Вероятность случайного выбора числа, относящегося к любому из этих классов, равна $1/d$. Это есть вероятность выбора одного числа, делящегося на d. Вероятность случайного выбора двух чисел a и b, делящихся на d, равна $(1/d)^2$. Если при этом $\text{НОД}(a/d, b/d) = 1$, то $\text{НОД}(a, b) = d$. Поскольку числа a и b выбираются случайно, то значения a/d и b/d также являются случайными. По предположению $\Pr[\text{НОД}(a, b) = 1] = P$, поэтому $P_d = \Pr[\text{НОД}(a, b) = d] = P/d^2$. Сумма вероятностей P_d по всем возможным значениям d равна 1, поскольку это соответствует вероятности события случайного выбора произвольных двух чисел. Таким образом имеем:

$$\sum_{d=1}^{\infty} P_d = \sum_{d=1}^{\infty} P/d^2 = P\sum_{d=1}^{\infty} 1/d^2 = P\frac{\pi^2}{6} = 1, \text{ откуда получаем } P = \frac{6}{\pi^2} \approx 0.6.$$

71. Для решения задачи можно воспользоваться теоремой, согласно которой число чисел, относящихся к некоторому показателю δ, равно функции Эйлера от δ. Вероятность найдем как отношение количества чисел, относящихся ко всевозможным показателям, не содержащим в качестве делителя значения γ, к числу $p-1$. Количество чисел β, таких что $\beta^{2^k} \equiv 1 \bmod p$, равно $p-1-\sum_{i=0}^{k}\varphi\left(2^i\gamma\right) = p-1-\sum_{i=1}^{k}2^{i-1}(\gamma-1)-(\gamma-1) =$

$$= p-1-(\gamma-1)\left(\sum_{i=1}^{k}2^{i-1}+1\right) = p-1-(\gamma-1)2^k = 2^k.$$

Следовательно, $\text{Prob}\left(\beta^{2^k} \equiv 1 \bmod p\right) = \frac{2^k}{p-1} = \frac{2^k}{2^k\gamma} = \frac{1}{\gamma}$.

72. Вероятность равна отношению количества чисел, относящихся ко всевозможным показателям, не содержащим в качестве делителя значения γ, к числу $p-1$. Количество указанных чисел равно:

$$p-1-\sum_{i=0}^{k}\left(\varphi\left(2a^i\gamma\right)+\varphi\left(a^i\gamma\right)\right) = p-1-2\left(\sum_{i=1}^{k}a^{i-1}(\gamma-1)(a-1)+(\gamma-1)\right) =$$

$$= p-1-2(\gamma-1)\left(\sum_{i=1}^{k}a^{i-1}(a-1)+1\right) = p-1-2(\gamma-1)\left(\sum_{i=1}^{k}\left(a^i-a^{i-1}\right)+1\right) =$$

$$= p-1-2(\gamma-1)a^k = 2\gamma a^k - 2\gamma a^k + 2a^k = 2a^k.$$

$$\text{Prob}\left(\beta^{2a^k} \equiv 1 \bmod p\right) = \frac{2a^k}{p-1} = \frac{2a^k}{2a^k\gamma} = \frac{1}{\gamma}.$$

73. Вероятность равна отношению количества чисел, относящихся ко всевозможным показателям, не содержащим в качестве делителя значения γ, к числу $p-1$. Количество чисел β, таких что $\beta^{2u} \equiv 1 \bmod p$, равно
$p-1-\varphi(2\gamma u)-\varphi(2\gamma)-\varphi(\gamma u)-\varphi(\gamma)=p-1-2(\gamma-1)(u-1)-2(\gamma-1)=$
$=p-1-2(\gamma-1)u=2\gamma u-2\gamma u+2u=2u.$

$$\mathrm{Prob}\left(\beta^{2u} \equiv 1 \bmod p\right)=\frac{2u}{p-1}=\frac{2u}{2u\gamma}=\frac{1}{\gamma}.$$

74. Вероятность равна отношению количества чисел, относящихся ко всевозможным показателям, не содержащим в качестве делителя значения γ, к числу $p-1$. Количество чисел β, таких что $\beta^{2^k r} \equiv 1 \bmod p$, равно

$$p-1-\sum_{i=0}^{k}\left(\varphi\left(2^i\gamma r\right)+\varphi\left(2^i\gamma\right)\right)=$$

$$=p-1-\sum_{i=1}^{k}\left(2^{i-1}(\gamma-1)(r-1)+(\gamma-1)(r-1)+2^{i-1}(\gamma-1)+(\gamma-1)\right)=$$

$$=p-1-(\gamma-1)\sum_{i=1}^{k}\left(2^{i-1}(r-1)+(r-1)+2^{i-1}+1\right)=$$

$$=p-1-(\gamma-1)\left(2^k(r-1)+2^k\right)=p-1-(\gamma-1)2^k r=2^k r.$$

$$\mathrm{Prob}\left(\beta^{2^k r} \equiv 1 \bmod p\right)=\frac{2^k r}{p-1}=\frac{2^k r}{2^k r\gamma}=\frac{1}{\gamma}.$$

75. Вероятность равна отношению количества чисел, относящихся ко всевозможным показателям, не содержащим в качестве делителя значения γ, к числу $p-1$. Количество чисел β, таких что $\beta^{2^k rz} \equiv 1 \bmod p$, равно

$$p-1-\sum_{i=0}^{k}\left(\varphi\left(2^i\gamma rz\right)+\varphi\left(2^i\gamma r\right)+\varphi\left(2^i\gamma z\right)+\varphi\left(2^i\gamma\right)\right)=p-1-$$

$$-\sum_{i=1}^{k}\begin{pmatrix}2^{i-1}(\gamma-1)(r-1)(z-1)+(\gamma-1)(r-1)(z-1)+\\ 2^{i-1}(\gamma-1)(z-1)+(\gamma-1)(z-1)+2^{i-1}(\gamma-1)(r-1)+\\ (\gamma-1)(r-1)+2^{i-1}(\gamma-1)+(\gamma-1)\end{pmatrix}=$$

$$=p-1-2^k\left((\gamma-1)(r-1)(z-1)+(\gamma-1)(z-1)+(\gamma-1)(r-1)+(\gamma-1)\right)=$$

$$=p-1-2^k\left(z(\gamma-1)(r-1)+(\gamma-1)z\right)=$$

$$=p-1-2^k zr(\gamma-1)=2^k zr\gamma-2^k zr\gamma+2^k zr=2^k zr.$$

$$\mathrm{Prob}\left(\beta^{2^k r} \equiv 1 \bmod p\right) = \frac{2^k rz}{p-1} = \frac{2^k rz}{2^k r\gamma z} = \frac{1}{\gamma}.$$

76. Доказательство *достаточности*. Пусть некоторое нечетное число a является первообразным корнем по модулю p. Поскольку $\varphi(p) = \varphi(2p) = p-1$, то все делители чисел $\varphi(p)$ и $\varphi(2p)$ совпадают. Для любого нетривиального делителя $d \mid \varphi(p)$ имеем: $a^{\varphi(p)/d} \equiv a^{(p-1)/d} \bmod p \neq 1$, т. е. p не делит число $a^{(p-1)/d} - 1$. Следовательно, $2p$ также не делит число $a^{(p-1)/d} - 1$. Последнее означает, что для любого нетривиального делителя $d \mid \varphi(2p)$ имеем: $a^{\varphi(2p)/d} \equiv a^{(p-1)/d} \bmod 2p \neq 1$, т. е. число a является первообразным корнем по модулю $2p$ (сравнение $a^{\varphi(2p)} \equiv a^{(p-1)} \equiv 1 \bmod 2p$ выполняется согласно теореме Эйлера). Доказательство *необходимости*. Пусть a является первообразным корнем по модулю $2p$. Тогда для любого нетривиального делителя $d \mid \varphi(2p)$ имеем: $a^{\varphi(2p)/d} \equiv a^{(p-1)/d} \bmod 2p \neq 1$, т. е. $2p$ не делит число $a^{(p-1)/d} - 1$. Поскольку число a нечетное, то и число $a^{(p-1)/d}$ тоже является нечетным, поэтому $a^{(p-1)/d} - 1$ имеет четное значение, т. е. делится на 2. Следовательно, p не делит число $a^{(p-1)/d} - 1$. Последнее означает, что для любого нетривиального делителя $d \mid \varphi(p)$ имеем: $a^{\varphi(p)/d} \equiv a^{(p-1)/d} \bmod p \neq 1$, т. е. число a является первообразным корнем по модулю p (сравнение $a^{\varphi(p)} \equiv a^{(p-1)} \equiv 1 \bmod p$ выполняется согласно малой теореме Ферма).

77. Все различные нечетные первообразные корни по модулю p являются первообразными корнями по модулю $2p$ (см. решение предыдущей задачи). Эти числа являются минимальными положительными представителями некоторых классов по модулю p. Каждому из этих классов в множестве $\{1, 2, \ldots, 2p\}$ принадлежат 2 различных числа (четное и нечетное). Четные первообразные корни (из множества $\{1, 2, \ldots, p\}$) по модулю p образуют другие классы первообразных корней, которым принадлежат нечетные числа множества $\{p+1, p+2, \ldots, 2p\}$. Пусть четное число b есть первообразный корень по модулю p. Тогда нечетное число $b+p$ есть также первообразный корень по модулю p. В соответствии с результатом предыдущей задачи $b+p$ есть первообразный корень по модулю $2p$. Очевидно, что различным четным числам $b_1 < p$ и $b_2 < p$ соответствуют различные нечетные числа $b_1 + p < 2p$ и $b_2 + p < 2p$. Таким образом, получаем нижнюю оценку количества первообразных корней по модулю $2p$ среди чисел множества $\{1, 2, \ldots, 2p\}$: число классов первообразных корней по модулю $2p$ не меньше числа классов первообразных корней по модулю p, которое равно $\varphi(p-1)$. Покажем, что это есть точное значение числа классов первообразных корней по модулю $2p$. Действительно, как уже указывалось выше, любое нечетное чис-

ло b ($p < b < 2p$), являющееся первообразным корнем по модулю $2p$, является одновременно и первообразным корнем по модулю p, т. е. число первообразных корней по модулю $2p$ не превышает числа первообразных корней по модулю p. Таким образом, число классов первообразных корней по модулю $2p$ равно $\varphi(p-1)$.

78. Доказательство *достаточности*. Пусть некоторое нечетное число a является первообразным корнем по модулю p^α. Поскольку $\varphi(p^\alpha) = \varphi(2p^\alpha) = p^{\alpha-1}(p-1)$, то все делители чисел $\varphi(p^\alpha)$ и $\varphi(2p^\alpha)$ совпадают. Для любого нетривиального делителя $d \mid \varphi(p^\alpha)$ имеем: $a^{\varphi(p^\alpha)/d} \equiv a^{p^{\alpha-1}(p-1)/d} \bmod p^\alpha \neq 1$, т. е. p^α не делит число $a^{p^{\alpha-1}(p-1)/d} - 1$. Следовательно, $2p^\alpha$ также не делит число $a^{p^{\alpha-1}(p-1)/d} - 1$. Последнее означает, что для любого нетривиального делителя $d \mid \varphi(2p^\alpha)$ имеем: $a^{\varphi(2p^\alpha)/d} \equiv a^{p^{\alpha-1}(p-1)/d} \bmod 2p^\alpha \neq 1$, т. е. число a является первообразным корнем по модулю $2p^\alpha$ (сравнение $a^{\varphi(2p^\alpha)} \equiv a^{p^{\alpha-1}(p-1)} \equiv 1 \bmod 2p^\alpha$ выполняется согласно теореме Эйлера). Доказательство *необходимости*. Пусть a является первообразным корнем по модулю $2p^\alpha$. Тогда для любого нетривиального делителя $d \mid \varphi(2p^\alpha)$ имеем: $a^{\varphi(2p^\alpha)/d} \equiv a^{p^{\alpha-1}(p-1)/d} \bmod 2p^\alpha \neq 1$, т. е. $2p^\alpha$ не делит число $a^{p^{\alpha-1}(p-1)/d} - 1$. Поскольку число a нечетное, то и число $a^{p^{\alpha-1}(p-1)/d}$ тоже является нечетным, поэтому $a^{p^{\alpha-1}(p-1)/d} - 1$ имеет четное значение, т. е. делится на 2. Следовательно, p^α не делит число $a^{p^{\alpha-1}(p-1)/d} - 1$. Последнее означает, что для любого нетривиального делителя $d \mid \varphi(p^\alpha)$ имеем: $a^{\varphi(p^\alpha)/d} \equiv a^{p^{\alpha-1}(p-1)/d} \bmod p^\alpha \neq 1$, т. е. число a является первообразным корнем по модулю p (сравнение $a^{\varphi(p^\alpha)} \equiv a^{p^{\alpha-1}(p-1)} \equiv 1 \bmod p^\alpha$ выполняется согласно теореме Эйлера).

79. Доказательство *достаточности*. Пусть некоторое нечетное число a относится по модулю p^α к показателю γ. Поскольку $\varphi(p^\alpha) = \varphi(2p^\alpha) = p^{\alpha-1}(p-1)$, то все делители чисел $\varphi(p^\alpha)$ и $\varphi(2p^\alpha)$ совпадают. В соответствии с принятым условием для любого нетривиального делителя $d \mid \gamma$ имеем: $a^{\gamma/d} \equiv \bmod p^\alpha \neq 1$, т. е. p^α не делит число $a^{\gamma/d} - 1$. Следова-

тельно, $2p^\alpha$ также не делит число $a^\gamma - 1$. Последнее означает, что для любого нетривиального делителя $d|\gamma$ имеем: $a^{\gamma/d} \equiv \bmod 2p^\alpha \neq 1$. С учетом принятого условия также имеем: $a^\gamma \equiv 1 \bmod p^\alpha \Rightarrow p^\alpha | (a^\gamma - 1)$. Поскольку число a нечетное, то и число $a^{\gamma/d}$ тоже является нечетным, поэтому $a^{\gamma/d} - 1$ имеет четное значение, т. е. делится на 2. Поскольку значение p^α нечетное, то из $p^\alpha | (a^\gamma - 1)$ следует $2p^\alpha | (a^\gamma - 1)$, т. е. $a^\gamma \equiv 1 \bmod 2p^\alpha$. Достаточность доказана. Доказательство *необходимости*. Пусть число a относится по модулю $2p^\alpha$, где $\alpha \geq 1$, к показателю γ. Тогда для любого нетривиального делителя $d|\gamma$ имеем: $a^{\gamma/d} \bmod 2p^\alpha \neq 1$, т. е. $2p^\alpha$ не делит число $a^{\gamma/d} - 1$. Поскольку число a нечетное, то и число $a^{\gamma/d}$ тоже является нечетным, поэтому $a^{\gamma/d} - 1$ имеет четное значение, т. е. делится на 2. Следовательно, p^α не делит число $a^{\gamma/d} - 1$. Последнее означает, что для любого нетривиального делителя $d|\gamma$ имеем: $a^{\gamma/d} \bmod p^\alpha \neq 1$. Из принятого условия $a^\gamma \equiv 1 \bmod 2p^\alpha$ следует $2p^\alpha | (a^\gamma - 1) \Rightarrow p^\alpha | (a^\gamma - 1)$, т. е. число a относится по модулю p^α, где $\alpha \geq 1$, к показателю γ.

80. Все различные нечетные числа, относящиеся по модулю p^α к показателю $\gamma | p^\alpha (p-1)$, одновременно относятся по модулю $2p^\alpha$ к тому же показателю, и наоборот (см. решение предыдущей задачи). Эти числа являются минимальными положительными представителями некоторых классов чисел, относящихся по модулю p^α к показателю γ. Каждому из этих классов в множестве $\{1, 2, ..., 2p^\alpha\}$ принадлежат 2 различных числа (четное и нечетное). Четные из них образуют дополнительные классы чисел, относящихся по модулю p^α к показателю γ. Дополнительным классам принадлежат нечетные числа множества $\{p^\alpha + 1, p^\alpha + 2, ..., 2p^\alpha\}$. Пусть четное число b есть число, относящееся по модулю p^α к показателю γ. Тогда нечетное $b + p$ есть также число, относящееся по модулю p^α к показателю γ. В соответствии с результатом предыдущей задачи $b + p$ есть число, относящееся по модулю $2p^\alpha$ к показателю γ. Очевидно, что различным четным числам $b_1 < p^\alpha$ и $b_2 < p^\alpha$ соответствуют различные нечетные числа $b_1 + p^\alpha < 2p^\alpha$ и $b_2 + p^\alpha < 2p^\alpha$. Таким образом, получаем нижнюю оценку количества чисел, относящихся по модулю $2p^\alpha$ к показателю γ, среди чисел множества $\{1, 2, ..., 2p^\alpha\}$: их количество не меньше числа классов, относящихся по модулю p^α к показателю γ. Покажем, что это есть точное значение числа классов, относящихся по модулю $2p^\alpha$ к показателю γ. Действительно, как уже указывалось выше, любое нечетное число $b (p^\alpha < b < 2p^\alpha)$, относящееся по модулю $2p^\alpha$ к показателю γ, относится к γ как к показателю и по модулю p^α. Таким образом, число классов, относящихся к γ как к показате-

лю по модулю $2p^{\alpha}$, равно числу классов, относящихся по модулю p^{α} к показателю γ.

81. Все различные нечетные числа, относящиеся по модулю p к показателю $\gamma | (p-1)$, одновременно относятся по модулю $2p$ к тому же показателю, и наоборот (см. решение предыдущей задачи). Эти числа являются минимальными положительными представителями некоторых классов чисел, относящихся по модулю p к показателю γ. Каждому из этих классов в множестве $\{1, 2, \ldots, 2p\}$ принадлежат 2 различных числа (четное и нечетное). Четные из них образуют дополнительные классы чисел, относящихся по модулю p к показателю γ. Дополнительным классам принадлежат нечетные числа множества $\{p+1, p+2, \ldots, 2p\}$. Пусть четное число b есть число, относящееся по модулю p к показателю γ. Тогда нечетное $b+p$ есть также число, относящееся по модулю p к показателю γ. В соответствии с результатом предыдущей задачи $b+p$ есть число, относящееся по модулю $2p$ к показателю γ. Очевидно, что различным четным числам $b_1 < p$ и $b_2 < p$ соответствуют различные нечетные числа $b_1 + p < 2p$ и $b_2 + p < 2p$. Таким образом, получаем нижнюю оценку количества чисел ($\psi_{2p}(\gamma)$), относящихся по модулю $2p$ к показателю γ, среди чисел множества $\{1, 2, \ldots, 2p\}$: их количество не меньше числа классов, относящихся по модулю p к показателю γ, которое равно $\psi_p(\gamma) = \varphi(\gamma)$, т. е. $\psi_{2p}(\gamma) \geq \psi_p(\gamma)$. Покажем, что это есть точное значение числа классов, относящихся по модулю $2p$ к показателю γ. Действительно, как уже указывалось выше, любое нечетное число $b (p < b < 2p)$, относящееся по модулю $2p$ к показателю γ, относится к γ как к показателю и по модулю p, т. е. $\psi_p(\gamma) \geq \psi_{2p}(\gamma)$ Таким образом, число классов, относящихся по модулю $2p$ к показателю γ, равно $\varphi(\gamma)$.

82. Прямолинейным способом нахождения требуемого числа является использование формулы $x = \beta^{\frac{L(n)}{\varepsilon}} \bmod n \neq 1$, где β — случайно выбираемое число и $L(n)$ — обобщенная функция Эйлера от модуля. Однако этот способ может оказаться сложным для практического использования, если модуль представляет собой произведение двух больших простых чисел. В этом случае можно воспользоваться следующей формулой: $x = a^{\frac{\gamma}{\varepsilon}} \bmod n$ или $x' = b^{\frac{\delta}{\varepsilon}} \bmod n$. Действительно, имеем: $x^{\varepsilon} \equiv a^{\gamma} \equiv 1 \bmod n$ и $x'^{\varepsilon} \equiv b^{\delta} \equiv 1 \bmod n$. Если ε — простое число, то оно есть показатель чисел a и b по модулю n. Если ε — составное число, то для любого нетривиального делителя $d \mid \varepsilon$ имеем: $x^{\varepsilon/d} \equiv a^{\gamma/d} \bmod n \neq 1$ и $x'^{\varepsilon/d} \equiv b^{\delta/d} \bmod n \neq 1$, поскольку показателями чисел a и b по условию

являются γ и δ соответственно. Следовательно, ε — минимальное число, для которого выполняются условия $x^{\varepsilon} \equiv 1 \bmod n$ и $x'^{\varepsilon} \equiv 1 \bmod n$, т. е. оно является показателем.

83. Если разложение числа n легко получить, то тогда можно вычислить обобщенную функцию Эйлера $L(n)$ и воспользоваться формулой $x = \beta^{\frac{L(n)}{\eta}} \bmod n \neq 1$, где $\eta = \text{НОК}[\gamma, \delta]$ и β — произвольно выбираемое число, которая позволяет найти числа, относящиеся к любому нетривиальному делителю $L(n)$ как к показателю по модулю n. Если η — составное число, то дополнительно следует проверить выполнимость условия $x^{\eta/d} \bmod n \neq 1$ для всех нетривиальных делителей $d | \eta$. Если составное n трудно разложить на множители, то тогда можно воспользоваться следующим способом: 1) найти число a', относящееся к показателю $\mu = \gamma/\varepsilon$, где $\varepsilon = \text{НОД}(\gamma, \delta)$; 2) учитывая соотношение $\text{НОД}(\mu, \delta) = 1$, найти число x, относящееся к показателю $\mu\delta$, воспользовавшись для этого формулой $x \equiv a'b \bmod n$, где предварительно вычисляется $a' = a^{\varepsilon} \bmod n$ (имеем $a'^{\mu} \bmod n = 1$ и $a'^{\mu/d} \bmod n \neq 1$ для всех нетривиальных делителей $d | \mu$).

84. В соответствии с теоремой Эйлера для b, взаимно простого с n, имеем: $b^{\varphi(n)} = bb^{\varphi(n)-1} \equiv 1 \bmod n \Rightarrow b^{-1} \equiv b^{\varphi(n)-1} \bmod n$. По определению операции деления по модулю записываем: $a/b = ab^{-1} \equiv ab^{\varphi(n)-1} \bmod n$.

85. Среди множества чисел $\{1, 2, \ldots, p^{\alpha}\}$ только числа, кратные числу p, а именно числа $\{p, 2p, 3p, \ldots, p^{\alpha-1}p\}$, не являются взаимно простыми с p^{α}. Мощность последнего множества равна $p^{\alpha-1}$. Следовательно: $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

86. В множестве последовательных натуральных чисел $\{1, 2, \ldots, 50\}$ имеется $\varphi(50) = 20$ ($\varphi(n)$ — функция Эйлера от n) чисел, взаимно простых с числом 50. Эти 20 чисел являются минимальными положительными представителями 20 классов по модулю 50. Каждому из этих классов в множестве $\{1, 2, \ldots, 5000\}$ принадлежат $5000 : 50 = 100$ различных чисел. Полное количество чисел, взаимно простых с числом 50, равно $20 \cdot 100 = 2000$.

87. В множестве последовательных натуральных чисел $\{1, 2, \ldots, 50\}$ имеется $\varphi(50) = 20$ ($\varphi(n)$ — функция Эйлера от n) чисел, взаимно простых с числом 50. Следовательно, в указанном интервале имеется $50 - \varphi(50) = 30$ чисел, которые не являются взаимно простыми с числом 50. Эти 30 чисел являются минимальными положительными представителями 30 классов по модулю 50. Каждому из этих классов в множестве

$\{1, 2, \ldots, 30\,000\}$ принадлежат $30\,000 : 50 = 600$ различных чисел. Полное количество чисел, не являющихся взаимно простыми с числом 50, равно $30 \cdot 600 = 18\,000$.

88. Сформировать простое число q длины $|q| \approx \frac{1}{2}|p|$ и произвольное четное число N длины $|N| \approx \frac{1}{4}|p|$, такое что $N\gamma < q$. Выполнить следующую процедуру: 1) вычислить $r = N\gamma q + 1$; 2) проверить условия $N\gamma < q$, $2^{N\gamma} \bmod r \neq 1$ и $2^{N\gamma q} \bmod r = 1$; 3) если хотя бы одно из условий шага 2 не выполняется, то увеличить значение N на два ($N := N + 2$) и перейти к шагу 1; 4) принять r в качестве искомого простого числа p.

89. По условию имеем $a^{\gamma} \equiv 1 \bmod p^{\alpha} \Rightarrow p^{\alpha} | (a^{\gamma} - 1)$. Из последнего соотношения следует $p | a^{\gamma} - 1 \Rightarrow a^{\gamma} \equiv 1 \bmod p$. Поскольку γ есть простое число, то оно является показателем по модулю p числа a.

90. Пусть число a является первообразным корнем по модулю p. Тогда для любого нетривиального делителя $d | p - 1$ имеет место $a^{(p-1)/d} \bmod p \neq 1$, следовательно, p не делит $a^{(p-1)/d}$. Учитывая соотношение $a \equiv a^{p} \equiv a^{p^{\alpha - i}} \bmod p$, где $i = 1, 2, \ldots, \alpha$, получаем: $a^{p^{\alpha-1}(p-1)/d} \bmod p \neq 1$, т. е. p не делит $a^{p^{\alpha-1}(p-1)/d} - 1$ ни для какого нетривиального делителя d числа $p - 1$. Следовательно, p^{α} не делит $a^{p^{\alpha-1}(p-1)/d} - 1$ ни для какого нетривиального делителя d числа $p - 1$. Таким образом, при некотором значении i число $\gamma = p^{\alpha - i}(p - 1)$ есть минимальный показатель, для которого выполняется соотношение $a^{\gamma} \equiv 1 \bmod p^{\alpha}$ (по теореме Эйлера имеем: $a^{\varphi(p^{\alpha})} \equiv a^{p^{\alpha-1}(p-1)} \equiv 1 \bmod p^{\alpha}$).

91. Из условия $a^{\gamma} \equiv 1 \bmod p \Rightarrow p | a^{\gamma} - 1$ не следует $p^{\alpha} | a^{\gamma} - 1 \Rightarrow a^{\gamma} \equiv 1 \bmod p^{\alpha}$. Рассмотрим, например, число a, вычисляемое по формуле $a = b^{\frac{p-1}{\gamma}} \bmod p^{\alpha} \neq 1$, где b есть первообразный корень по модулю p^{α}. Для этого числа имеем: $a^{\gamma} \equiv \left(b^{(p-1)/\gamma}\right)^{\gamma} \equiv b^{(p-1)} \equiv 1 \bmod p$ и $a^{\gamma} \equiv \left(b^{(p-1)/\gamma}\right)^{\gamma} \equiv b^{(p-1)} \bmod p^{\alpha} \neq 1$, т. е. число a не относится по модулю p^{α} к показателю γ.

92. Представим число a в виде некоторой степени ε числа b, являющегося первообразным корнем по модулю p^{α}: $a \equiv b^{\varepsilon} \bmod p^{\alpha}$. По условию имеем:

$a^{p^l} \equiv b^{\varepsilon p^l} \equiv 1 \bmod p^\alpha \Rightarrow \varepsilon p^l \equiv 0 \bmod p^{\alpha-1}(p-1)$, т. е. $\varepsilon p^l = kp^{\alpha-1}(p-1)$ $\Rightarrow$ $\varepsilon = kp^{\alpha-1-l}(p-1)$, где k — целое число. Таким образом, $a \equiv$ $\equiv b^{kp^{\alpha-1-l}(p-1)} \bmod p^\alpha \Rightarrow a \equiv b^{kp^{\alpha-1-l}(p-1)} \equiv 1 \bmod p$, ч.т.д.

93. Представим число a в виде некоторой степени ε числа b, являющегося первообразным корнем по модулю p^α: $a \equiv b^\varepsilon \bmod p^\alpha$. По условию имеем: $a^\delta \equiv b^{\varepsilon\delta} \equiv 1 \bmod p^\alpha \Rightarrow \varepsilon\delta \equiv 0 \bmod p^{\alpha-1}(p-1)$, т. е. $\varepsilon\delta = kp^{\alpha-1}(p-1)$ $\Rightarrow$ $\varepsilon = kp^{\alpha-1-l}(p-1)/\gamma$, где k — целое число. Таким образом, $a \equiv$ $\equiv b^{kp^{\alpha-1-l}(p-1)/\gamma} \bmod p^\alpha \Rightarrow a \equiv b^{kp^{\alpha-1-l}(p-1)/\gamma} \bmod p$. Из последней формулы следует: $a^\gamma \equiv b^{kp^{\alpha-1-l}(p-1)} \equiv 1 \bmod p$. Поскольку γ простое число, то оно является по модулю p показателем числа a.

94. Возводя $(p-1)$ в квадрат, получаем: $(p-1)^2 \equiv (-1)^2 \equiv 1 \bmod p$, ч.т.д. Поскольку $\varphi(2) = 1$, то по простому модулю существует только одно число, относящееся к показателю 2. Следовательно, по любому простому модулю p имеется единственное число $(p-1)$, относящееся к показателю 2.

95. Функция Эйлера от чисел 13, 79 и 89 равна 12, 78 и 88 соответственно. Число 3 делит только 12 и 78, поэтому существуют числа, относящиеся к показателю 3, только по модулям 13 и 79, причем количество таких чисел для любого простого модуля равно либо нулю, либо $\varphi(3) = 2$. Таким образом, по модулям 13 и 79 имеем два таких числа, а по модулю 89 таких чисел не существует.

96. Согласно условию имеется некоторое число x, такое что $x^2 \equiv a \bmod m$. Следовательно, $m \mid x^2 - a$, но тогда и каждый делитель модуля m делит значение $x^2 - a$, т. е. $p_1 \mid x^2 - a$, $p_2 \mid x^2 - a$, ..., $p_s \mid x^2 - a$. Из последних соотношений получаем: $x^2 \equiv a \bmod p_1$, $x^2 \equiv a \bmod p_2$, ..., $x^2 \equiv a \bmod p_s$, ч.т.д.

97. Число 12 относится по модулю 13 к показателю 2. Все числа, сравнимые с 12 по модулю 13, также относятся к этому показателю. Множество этих чисел записывается в виде формулы $x' = 12 + 13i$ (1), где $i = 0, \pm1, \pm2, \pm3$ ... Число 42 относится по модулю 43 к показателю 2. Все числа сравнимые, с 42 по модулю 43, также относятся к показателю 2. Эти числа представляются в следующем общем виде $x'' = 42 + 43j$ (2), где $j = 0, \pm1, \pm2, \pm3$ ... Нас интересуют значения, присутствующие одновременно в множествах $\{12 + 13i\}$ и $\{42 + 43j\}$. Их можно найти, решая неоднородное диофантово уравнение вида $12 + 13i = 42 + 43j$ или $13i -$

$-43j = 30$ относительно неизвестных i и j. Так как НОД(13, 43) = 1, то решение существует. НОД(13, 43) = $10 \cdot 13 - 3 \cdot 43$, откуда получаем частное решение приведенного выше неоднородного уравнения: $i = 300$, $j = 90$. Для нахождения всех решений запишем общее решение однородного уравнения $13i - 43j = 0$: $j = 13t$ и $i = 43t$, где $t = 0, \pm1, \pm2, \pm3$ ... Общее решение неоднородного уравнения представимо в виде суммы частного решения неоднородного и общего решения однородного уравнений: $j = 90 + 13t$ и $i = 300 + 43t$, где $t = 0, \pm1, \pm2, \pm3$ ... Подставляя эти значения i в (1) или значения j в (2), получим множество искомых чисел: $x = 12 + 13(300 + 43t) = 42 + 43(90 + 13t) = 3912 + 559t$. Например, при $t = -6$ имеем число 558.

98. Данные модули являются составными: $77 = 7 \cdot 11$ и $119 = 7 \cdot 17$. Если некоторое число относится к показателю 2 по составному модулю, то оно относится к такому же показателю и по всем простым модулям, которые делят составной модуль. Число -1 есть единственное число, которое относится к показателю 2 по любому простому модулю. Легко доказать, что -1 относится к показателю 2 по модулям 77 и 119. Все числа, сравнимые с -1 по модулю 77, также относятся к показателю 2 по модулю 77. Эти числа представляются в виде $x' = -1 + 77i$ (1), где $i = 0, \pm1, \pm2, \pm3$ ... Все числа, сравнимые с -1 по модулю 119, также относятся к показателю 2 по модулю 119. Эти числа представляются в виде $x'' = -1 + 119j$ (2), где $j = 0, \pm1, \pm2, \pm3$ ... Нас интересуют значения, присутствующие одновременно в множествах $\{-1 + 77i\}$ и $\{-1 + 119j\}$. Их можно найти, решая однородное диофантово уравнение вида $-1 + 77i = -1 + 119j \Rightarrow 77i - 119j = 0 \Rightarrow 11i - 17j = 0$ относительно неизвестных i и j. Общее решение этого уравнения записывается в виде: $i = 17t$ и $j = 11t$, где $t = 0, \pm1, \pm2, \pm3$.... Подставляя эти значения i в (1) или значения j в (2), получим множество искомых чисел: $x = -1 + 17 \cdot 77t = -1 + 11 \cdot 119t = -1 + 1309t$. Например, при $t = 1$ имеем число 1308.

99. Пусть $y = a^x \bmod pq$, где $a \neq p$ и $a \neq q$. Требуется вычислить x по известному y. Очевидно, что выполняются следующие сравнения: $y \equiv a^x \bmod p = a^{x_1} \bmod p$, где $x_1 = x \bmod p - 1$, и $y \equiv a^x \bmod q = a^{x_2} \bmod q$, где $x_2 = x \bmod q - 1$. Решив задачу дискретного логарифмирования по модулю p и модулю q, можно найти значения x_1 и x_2, которые связаны с искомым значением x, в соответствии со сравнениями $x \equiv x_1 \bmod p - 1$ и $x \equiv x_2 \bmod q - 1$. Данная система сравнений легко решается с использованием китайской теоремы об остатках (предварительно обе части этих сравнений делятся на НОД$(q - 1, p - 1) = \varepsilon$ и осуществляется переход к неизвестной $x' = x/\varepsilon$). Трудоемкость нахождения решения этой системы сравнений много меньше сложности вычисления значений x_1 и x_2.

100. Стандартным методом решения подобных систем сравнений является использование китайской теоремы об остатках. При малом числе сравнений, входящих в решаемую систему, более простым оказывается метод последовательного исключения. Решение системы есть часть решения сравнения (1), которое можно представить в виде $x = a + km_1$ (3), где $k = 0, \pm1, \pm2, \pm3 \ldots$ Из этого множества чисел следует исключить все значения, не удовлетворяющие сравнению (2). Иными словами, должно выполняться сравнение $a + km_1 \equiv b \bmod m_2$, где неизвестной величиной является k. Поскольку НОД$(m_1, m_2) = 1$, то получаем $k \equiv (b-a)\mu \bmod m_2$ $\Rightarrow k = (b-a)\mu + gm_2$, где $\mu = m_1^{-1} \bmod m_2$ и $g = 0, \pm1, \pm2, \pm3 \ldots$ Подставляя полученное выражение для значений k, удовлетворяющих соотношению (2), в формулу (3), получаем решение заданной системы: $k = a + (b-a)\mu m_1 + g m_2 m_1$.

101. Учитывая, что $\varphi(19) = 18$ и $\varphi(18) = 6$, получаем: $\left(3^{57^{127}}\right) \equiv$

$$\equiv \left(3^{\left(57^{127}\right) \bmod 18}\right) \equiv \left(3^{\left(57^{127 \bmod 6}\right) \bmod 18}\right) \equiv \left(3^{57^1 \bmod 18}\right) \equiv \left(3^3\right) \equiv 8 \bmod 19.$$

Таким образом, $\left(3^{57^{127}}\right) \bmod 19 = 8$.

102. *Указание*: второе сравнение имеет два решения $x \equiv 16 \bmod 79$ и $x \equiv 63 \bmod 79$. Поэтому решением заданной системы сравнений является объединение решений двух следующих систем сравнений: $\begin{cases} x \equiv 17 \bmod 39, \\ x \equiv 16 \bmod 79 \end{cases}$ и $\begin{cases} x \equiv 17 \bmod 39, \\ x \equiv 63 \bmod 79. \end{cases}$

103. *Указание*: второе сравнение имеет единственное решение $x \equiv 35 \bmod 47$. Поэтому решением заданной системы сравнений является решение следующей системы сравнений первой степени: $\begin{cases} x \equiv 11 \bmod 51, \\ x \equiv 35 \bmod 47. \end{cases}$

104. *Указание*: второе сравнение не имеет решений, так как 11 является квадратичным невычетом по модулю 47: $11^{\frac{47-1}{2}} \bmod 47 = 46$. Поэтому заданная система не имеет решений.

105. *Указание*: второе сравнение представить в виде $(x^2)^5 \equiv 37 \bmod 127$ (*а*). Так как НОД$(5, 126) = 1$, то сравнение (*а*) эквивалентно сравнению $x^2 \equiv 37^{1/5} \equiv 99 \bmod 127$ (*б*), которое имеет два решения: $x \equiv 37 \bmod 127$ и

$x \equiv 90 \bmod 127$. Решением заданной системы сравнений является объединение решений двух следующих систем сравнений: $\begin{cases} x \equiv 37 \bmod 137, \\ x \equiv 37 \bmod 127 \end{cases}$

и $\begin{cases} x \equiv 37 \bmod 137, \\ x \equiv 90 \bmod 127. \end{cases}$

106. Первое сравнение не имеет решений, поскольку 37 по модулю 79 является невычетом. Число 76 является вычетом, поэтому сравнение (2) распадается на следующие два сравнения $x^2 \equiv 47 \bmod 79$ и $x^2 \equiv 32 \bmod 79$, в которых 47 — невычет и 32 — вычет, поэтому (2) имеет два решения. Число 9 является вычетом, поэтому сравнение (3) выполняется, если выполняется хотя бы одно из следующих двух сравнений: $x^2 \equiv 76 \bmod 79$ и $x^2 \equiv 3 \bmod 79$, в которых 76 — вычет и 3 — невычет, поэтому (3) имеет два решения.

107. Разлагая n, получаем $5963 = 67 \cdot 89$. Некоторое число является квадратичным вычетом по модулю n, если оно является одновременно вычетом по модулю 67 и по модулю 89. Проверка (возведение в степень $(p-1)/2$ по модулю p) показывает, что вычетами по модулю 67 являются числа 1034, 1959, 2477, 3074 и 4179. Из них вычетами по модулю 89 являются числа 1034, 1959 и 4179. Следовательно, последние три числа являются вычетами по модулю 5963.

108. Разлагая заданные числа на множители, получаем: $2301 = 11 \cdot 41 \cdot 51$, $\varphi(2301) = 10 \cdot 40 \cdot 50 = 20\,000$, $L(2301) = \text{НОК}[10, 40, 50] = 200$; $900 = 2^2 \cdot 3^2 \cdot 5^2$, $\varphi(900) = 2 \cdot 6 \cdot 20 = 240$, $L(900) = \text{НОК}[2, 6, 20] = 60$; $10965 = 5 \cdot 17 \cdot 129$, $\varphi(10\,965) = 4 \cdot 16 \cdot 128 = 8192$, $L(10\,965) = \text{НОК}[4, 16, 128] = 128$.

109. Учитывая, что $2^{16} + 1$ есть число простое, и разлагая число 254 на множители, получаем: $\varphi(2(2^{16} + 1)) = 1 \cdot 2^{16} = 2^{16}$, $L(2(2^{16} + 1)) = 2^{16}$; $254 = 2 \cdot 127$, $\varphi(254) = 1 \cdot 126 = 126$, $L(254) = 126$; $\varphi(2^k) = 2^{k-1}$, $L(2^k) = 2^{k-1}$.

110. $\text{НОД}(13, 87) = 1 = -20 \cdot 13 + 3 \cdot 87$.

111. $\text{НОД}(11, 97) = 1 = -44 \cdot 13 + 5 \cdot 87$.

112. $\text{НОД}(23, 121) = 1 = -21 \cdot 13 + 4 \cdot 87$.

113. $\text{НОД}(35, 169) = 1 = 29 \cdot 13 - 6 \cdot 87$.

114. Найдем частное решение заданного диофантова уравнения $34x + 289y = 187$ (1). Для этого найдем наибольший общий делитель коэффициентов в левой части уравнения и его линейное представление: $\text{НОД}(34, 289) = 17$. Поскольку число в правой части уравнения делится на 17, то решения существуют. Делим обе части (1) на 17 и получаем

равносильное уравнение $2x + 17y = 11$ (2). Находим линейное представление НОД(2, 17) = $1 = -8 \cdot 2 + 1 \cdot 17$, т. е. 11 представляется в виде $11 = -88 \cdot 2 + 11 \cdot 17$. Отсюда получаем частное решение уравнения (1): $x = -88$, $y = 11$. Общее решение уравнения (1) может быть представлено как сумма найденного частного решения и общего решения однородного уравнения $2x + 17y = 0$ (2), которое записывается в виде $y = 2t$ и $x = -17y/2 = -17t$, где $t = 0, \pm 1, \pm 2, \pm 3 \ldots$ Получаем $x = -88 - 17t$ и $y = 11 + 2t$.

115. Найдем значение $3^{-1} \bmod 40 = 27$, следовательно, кубический корень из чисел 5, 21, 31, 32, 36, 37 и 39 по модулю 41 можно найти возведением их в степень 27 по модулю 41, что дает значения 20, 33, 23, 9, 21, 16, 36 соответственно.

116. Выполняя операцию возведения в степень $(p-1)/2$ по модулю $p = 139$, определяем, что среди заданных чисел квадратичными вычетами являются 11, 51, 99 и 121. Поскольку $139 \equiv 3 \bmod 4$, то квадратные корни из последних четырех чисел можно найти, возводя их в степень $(p+1)/4$ по модулю $p = 139$. Получаем следующие пары значений корней: (122, 17); (107, 32); (51, 88) и (11, 128) соответственно. Квадратных корней по модулю 139 из чисел 17, 105 и 132 не существует.

117. Число 81 является вычетом четвертой степени по модулю 137, поскольку выполняется условие $81^{\frac{137-1}{4}} \equiv 1 \bmod 137$. Подбором легко найти: $\sqrt[4]{81} \equiv 3 \bmod 137$. Далее на основе известной теоремы воспользуемся тем, что все корни можно получить, умножая один корень из числа 81 на все корни из единицы по модулю 137. Для нахождения корней четвертой степени из единицы найдем число α, относящееся по модулю 137 к показателю 4. Испытав несколько различных чисел β и используя формулу $\alpha = \beta^{34} \bmod 137$, найдем: $100^4 \equiv 1 \bmod 137$, следовательно, 100 есть искомое число. Возводя число 100 по модулю 137 в степень 2, 3 и 4, получаем следующие корни из 1: 100, 136, 37 и 1. Умножая последние на 3, получаем все корни $\sqrt[4]{81} \bmod 137$: 26, 134, 111 и 3.

118. Число 8 является вычетом третьей степени по модулю 19, так как $2^3 \equiv 8 \bmod 19$. Далее на основе известной теоремы воспользуемся тем, что все корни можно получить, умножая один корень из числа 8 на все корни третьей степени из единицы по модулю 19. Для нахождения этих корней найдем число α, относящееся по модулю 19 к показателю 3. Испытав несколько различных чисел β и используя формулу $\alpha = \beta^6 \bmod 19$, найдем: $11^3 \equiv 1 \bmod 19$, следовательно, 11 есть искомое число. Возводя число 11 по модулю 19 в степень 2 и 3, получаем сле-

дующие корни третьей степени из 1: 11, 7 и 1. Умножая последние на 2, получаем все корни $\sqrt[3]{8} \bmod 19$: 3, 14 и 2. Классы $\overline{3}, \overline{14}, \overline{2}$ составляют решение заданного сравнения.

119. Число 32 является вычетом пятой степени по модулю 101, поскольку существует корень $\sqrt[5]{32} \bmod 101$: $\sqrt[5]{32} \equiv 2 \bmod 101$. Далее на основе известной теоремы воспользуемся тем, что все корни можно получить, умножая один корень из числа 32 на все корни пятой степени из единицы по модулю 101. Для нахождения этих корней найдем число α, относящееся по модулю 101 к показателю 5. Испытав несколько различных чисел β и используя формулу $\alpha = \beta^{20} \bmod 101$, найдем: $87^5 \equiv 1 \bmod 19$. следовательно, 87 есть искомое число. Возводя число 87 по модулю 101 в степень 2, 3, 4 и 5, получаем следующие корни пятой степени из 1: 87, 95, 84, 36 и 1. Умножая последние на 2, получаем все корни $\sqrt[5]{32} \bmod 101$: 73, 89, 67, 72 и 2. Классы $\overline{73}, \overline{89}, \overline{67}, \overline{72}$ и $\overline{2}$ составляют решение заданного сравнения.

120. По одному известному корню n-й степени остальные корни могут быть найдены в соответствии со следующим алгоритмом: 1) Найти число w, относящееся к n как к показателю по модулю p. 2) Вычислить значения $wx_0 \bmod p$, $wx_0^2 \bmod p$, $wx_0^3 \bmod p$, ..., $wx_0^{n-1} \bmod p$ (все эти значения попарно различны и не равны 1). Корнями заданного сравнения являются классы $\overline{wx_0}$, $\overline{wx_0^2}$, $\overline{wx_0^3}$, ..., $\overline{wx_0^{n-1}}$ и $\overline{x_0}$.

121. Число 89 является невычетом третьей степени по модулю 139, поскольку не выполняется условие $89^{\frac{139-1}{3}} \equiv 1 \bmod 139$. Поэтому первое сравнение не имеет решений. Число 33 является вычетом третьей степени по модулю 139, поскольку выполняется условие $33^{\frac{139-1}{3}} \equiv 1 \bmod 139$. Поэтому второе сравнение имеет 3 решения. Число 3 не делит 136, поэтому сравнение (3) имеет одно решение.

122. *Указание*: поскольку $45^{\frac{139-1}{3}} \equiv 1 \bmod 139$, то 45 является вычетом 3-й степени и сравнение $x^3 \equiv 45 \bmod 139$ имеет три решения. которые обозначим как классы $\overline{x_1}$, $\overline{x_2}$ и $\overline{x_3}$. Заданная система имеет решения, если число a принадлежит одному из этих классов. В противном случае решений нет. Методом подбора легко найти $31^3 \equiv 45 \bmod 139$, т. е. 31 есть один из корней. Остальные корни (51 и 57) легко найти путем умножения числа 31 на кубические корни из единицы (42, 96 и 1) по мо-

дулю 139. Таким образом, заданная система имеет решения, если $a \in \{\overline{31}, \overline{51}, \overline{57}\}$. Решением системы является тот класс, которому принадлежит a.

123. Разложим заданное число на множители: $1521 = 3^2 \cdot 13^2$. Поскольку 1521 является квадратом, то оно является квадратичным вычетом по произвольному простому модулю $p \notin \{3, 13\}$ (понятие квадратичного вычета определяется для чисел a, таких что p не делит a).

124. Поскольку заданное число является квадратом числа $x = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_k^{s_k}$, то оно является квадратичным вычетом по произвольному простому модулю $p \notin \{p_1, p_2, \ldots, p_k\}$ (понятие квадратичного вычета определяется для чисел a, таких что p не делит a).

125. Функция Эйлера от 67 имеет следующие делители: $66 = 2 \cdot 3 \cdot 11$, поэтому для всех n, не содержащих делители 2, 3 и 11, имеется единственный корень из числа 58. Для остальных значений n следует воспользоваться формулой $58^{\overline{66}/n} \equiv 1 \bmod 67$, которой должны удовлетворять вычеты степени n. Имеем: $58^{\overline{66}/2} \equiv 66 \bmod 67$, следовательно, квадратного корня из 58 не существует; $58^{\overline{66}/3} \equiv 1 \bmod 67$, следовательно, существуют три корня третьей степени; $58^{\overline{66}/11} \equiv 64 \bmod 67$, следовательно, не существует корня 11-й степени. Аналогично можно показать, что для других значений $n \mid 66$ ($n = 6, 22, 33, 66$) корней нет. Для значений n, таких что НОД$(n, 66) = \delta \neq 1$, следует воспользоваться известной теоремой, согласно которой вычеты n-й степени по простому модулю $p > 2$ совпадают с вычетами степени δ по этому же модулю. Так как δ может принимать только значения 2, 3, 6, 11, 22, 33 и 66, то легко видеть, что корни из 58 по модулю 67 существуют только для нечетных значений n, которые делятся на 3 и не делятся на 11 (для каждого из этих значений степени имеем три корня) или не делятся ни на 3, ни на 11 (для каждого из этих значений степени имеем один корень).

126. Для числа a, являющегося вычетом степени n по простому модулю p, выполняется условие $a^{\overline{p-1}/n} \equiv 1 \bmod p$, которое означает, что число a не является первообразным корнем.

7.2. Схемы ЭЦП

7.2.1. ЭЦП на основе сложности факторизации

1. $d_1 = 49$ (в случае $n_1 = 299$) и $d_2 = 193$ (для $n_2 = 527$).
2. $e_1 = 141$ (в случае $n_1 = 187$) и $e_2 = 61$ (для $n_2 = 319$).
3. $d_1 = 7$ (в случае $n_1 = 299$) и $d_2 = 247$ (для $n_2 = 551$).
4. Значения $M = 67$ и $M = 69$ относятся по модулю $n = 187$ к некоторому показателю $\gamma < \varphi(n) = 160$. Значения $e = 141$ и $e = 101$ сравнимы с 1 по модулю γ. Легко проверить, что числа 67 и 69 относятся по модулю 187 к показателям 2 и 5 соответственно.
5. Открытый ключ должен представлять собой число, относящееся к показателю 7 по модулю $\varphi(n)$, где n есть RSA-модуль. Следовательно, модуль n должен быть таким, чтобы число 7 содержалось как делитель в числе $\varphi(\varphi(n))$, что может иметь место, например, если число $p - 1$ содержит множитель 7^g, где p один из двух простых делителей модуля n и $g \geq 2$.
6. Число e, выбираемое в качестве шифрующей экспоненты, должно быть взаимно простым с функцией Эйлера от модуля, которая является четной. Следовательно, число e должно быть нечетным и отличным от единицы. Поэтому минимальным значением веса Хемминга у шифрующей экспоненты в криптосистеме RSA является два.
7. По условию $n = pq$, следовательно, $\varphi(n^2) = \varphi(p^2 q^2) = p(p-1)q(q-1) = pq(p-1)(q-1) = n\varphi(n)$.
8. Возврат исходного значения сообщения M после пятикратного шифрования в общем случае будет иметь место, если открытый ключ e относится к показателю 5 по модулю $\varphi(n) = \varphi(5963)$, однако проверка показывает, что это не так. Особенность ситуации, описываемой в задаче, состоит в том, что число $e = 157$ относится к показателю 5 по модулю $\gamma = 66$, являющемуся делителем числа $\varphi(5963) = \varphi(67 \cdot 89) = 66 \cdot 88 = 5808$, а число 57 относится к γ как к показателю по модулю 5963. При этом число $e = 157$ не относится к показателю 5 по модулю $\varphi(5963)$, поэтому для значений сообщения M, не относящихся к показателю $\gamma = 66$, пятикратное шифрование не возвращает значение M. Для этих значений M четырехкратное шифрование не будет эквивалентно возведению в степень секретного ключа $d = 37$ (т. е. формированию подписи к сообщению).

9. Может, поскольку $\varphi(\varphi(190\,847)) = \varphi(\varphi(1373 \cdot 139)) = \varphi(2^3 \cdot 3 \cdot 7^3 \cdot 23) = 2^5 \cdot 3 \cdot 7^2 \cdot 11 = 51\,744$, т. е. $\varphi(\varphi(n))$ содержит множитель 7. Это может произойти, если в качестве открытого ключа выбрано число, относящееся по модулю $\varphi(n) = 1372 \cdot 138 = 189\,336$ к показателю 7. Таким числом, например, является $e = 27\,049$. Ответы для остальных случаев: а) нет, б) да, в) да, г) да.

10. Имеем $\varphi(n) = (p-1)(q-1) = 2^s t$, где p и q — делители RSA-модуля n. С большой вероятностью число 2 входит в каноническое разложение чисел $p-1$ и $q-1$ в различной степени. Пусть 2 входит в разложение $p-1$ с большей степенью. Тогда при некотором натуральном числе k имеем: $(q-1) = 2^{s-k} t$, но $p-1$ не делит $2^{s-k} t$, и при случайном выборе a с большой вероятностью будем иметь $a^{2^{s-k}t} \bmod n = Z$ (1), где $Z \neq 1$ ($Z < n$) и $a^{2^{s-k}t} \equiv 1 \bmod q$ (2). Последнее соотношение означает, что $q \mid a^{2^{s-k}t} - 1$. Следовательно, $\text{НОД}(a^{2^{s-k}t} - 1, n) = q$. Однако длина числа $a^{2^{s-k}t} - 1$ обычно является чрезвычайно большой, поэтому для разложения модуля n следует воспользоваться формулой $\text{НОД}(a^{2^{s-k}t} \bmod n - 1, n) = q$. Покажем, что $q \mid (a^{2^{s-k}t} \bmod n - 1)$. Из (1) и (2) следует: $a^{2^{s-k}t} \equiv Z \bmod q \Rightarrow Z \equiv 1 \bmod q$, т. е. $q \mid (Z-1)$.

11. Схема ЭЦП с заданным уравнением проверки подписи может быть рассмотрена как система RSA с общим значением открытого ключа. Схема слепой подписи может быть построена аналогично схеме Чаума для случая $e = 3$.

12. Для генерации подписи требуется выполнить операцию извлечения квадратного корня по модулю n, что можно сделать с приемлемой для подписывающего сложностью, если делители n являются сравнимыми с числом 3 по модулю 4 (аналогично криптосхеме Рабина). Параметр R задает вероятностный характер рассматриваемой схемы ЭЦП и может служить для того, чтобы снять проблему «переформатирования документа» для получения значения H, являющегося квадратичным вычетом. Для произвольного H можно подобрать такое R, что $H \| R$ является квадратичным вычетом, т. е. для произвольных значений H можно сформировать подпись, подбирая соответствующие значения R.

13. Нет. Для произвольного H можно подобрать S, взаимно простое с модулем n, для которого легко вычисляется R, удовлетворяющее уравнению проверки ЭЦП.

14. Нет. Для произвольного H можно легко подобрать значение S, такое что НОД$(S^2, n) = 1$. Для него легко вычисляется $R = S^{-2}(H - S^3) \bmod n$, удовлетворяющее уравнению проверки ЭЦП.

15. Схема представляется стойкой, так как при предварительном выборе одного из значений R и S для нахождения второго требуется решить задачу извлечения квадратного корня по модулю RSA. Для генерации подписи требуется выполнить операцию извлечения квадратного корня по модулю n, что можно сделать с приемлемой для подписывающего сложностью, если делители n являются сравнимыми с числом 3 по модулю 4 (аналогично криптосхеме Рабина). Параметр R задает вероятностный характер рассматриваемой схемы ЭЦП и может служить для того, чтобы снять проблему «переформатирования документа» для получения значения H, являющегося квадратичным вычетом. Для произвольного H подпись может быть вычислена путем предварительного выбора такого значения R, что НОД$(R, n) = 1$ и $R^{-1}(H - R^2)$ — квадратичный вычет. Расчетная формула имеет вид $S = [R^{-1}(H - R^2)]^{1/2} \bmod n$.

16. Уравнение генерации подписи имеет вид: $S = (\alpha^{H^{-1}} - H) \bmod n$. Схема с исходным уравнением проверки подписи $S^H = \alpha \bmod n$ допускает формирование подписей S_1 и S_2 к значениям хэш-функций H_1 и H_2 соответственно, по известной подписи S к $H = H_1 H_2$: $S_1 = S^{H_2} \bmod n$ и $S_2 = S^{H_1} \bmod n$. Действительно, имеем $S_1^{H_1} = S^H \equiv \alpha \bmod n$ и $S_2^{H_2} = S^H \equiv \alpha \bmod n$. Однако модифицированная схема ЭЦП также имеет этот недостаток. Действительно, если известна подпись S, соответствующая значению $H = H_1 H_2$, то $S_1 = [(S + H)^{H_2} - H_1] \bmod n$ и $S_2 = [(S + H)^{H_1} - H_2] \bmod n$ есть подписи к H_1 и H_2 соответственно.

17. Уравнение генерации подписи имеет вид: $S = (\alpha^{U}/H) \bmod n$, где $U = H^{-1} \bmod \gamma$, γ — показатель числа α по модулю n (γ — секретный ключ). Сравниваемые варианты модифицированных уравнений проверки ЭЦП аналогичны по замыслу, однако оба не устраняют исходный недостаток. Если известна подпись S, соответствующая значению $H = H_1 H_2$, то $S_1 = [(SH)^{H_2}/H_1] \bmod n$ и $S_2 = [(SH)^{H_1}/H_2] \bmod n$ есть подписи к H_1 и H_2 соответственно. Специфика состоит в использовании операции модульного умножения вместо сложения. Недостаток использования умножения подписи на значение хэш-функции состоит в необходимости «переформатирования документа», если текущее полученное значение H не является взаимно простым с модулем (это связано с тем, что при генерации подписи выполняется деление на H). Однако вероятность этого случая пренебрежимо мала.

18. Уравнение генерации подписи имеет вид: $S = \alpha^{(H^2 + H)^{-1}} \bmod n$. Схема с исходным уравнением проверки подписи $S^H = \alpha \bmod n$ допускает фор-

мирование подписей S_1 и S_2 к значениям хэш-функций H_1 и H_2 соответственно, по известной подписи S к $H = H_1 H_2$: $S_1 = S^{H_2} \bmod n$ и $S_2 = S^{H_1} \bmod n$. Действительно, имеем $S_1^{H_1} \equiv S^H \equiv \alpha \bmod n$ и $S_2^{H_2} \equiv S^H \equiv \alpha \bmod n$. В модифицированной схеме ЭЦП этот недостаток устраняется. Время генерации подписи практически не изменяется. Время проверки подписи увеличивается примерно в 2 раза. Проверяющий предварительно вычисляет значение $U = H^2 + H$, где $|U| \approx 2|H|$, а затем выполняет модульное возведение в степень: $S^U \bmod n = \alpha$. Проверка подписи по формуле $[(S^{H^2} \bmod n)(S^H \bmod n)] \bmod n = \alpha$ является менее эффективной с вычислительной точки зрения.

19. Уравнение генерации подписи имеет вид: $S = \alpha^{(H \operatorname{div} 2^{64} + (H \bmod 2^{64}) 2^{64}) H^{-1}} \bmod n$. Схема с исходным уравнением проверки подписи $S^H = \alpha \bmod n$ допускает формирование подписей S_1 и S_2 к значениям хэш-функций H_1 и H_2 по известной подписи S к $H = H_1 H_2$: $S_1 = S^{H_2} \bmod n$ и $S_2 = S^{H_1} \bmod n$. Модифицированная схема ЭЦП свободна от этого недостатка. Время генерации подписи изменяется несущественно. Время проверки подписи увеличивается примерно в 2 раза, поскольку требуется осуществить два возведения в степень по модулю n. Вычисление значения $U = H \operatorname{div} 2^{64} + (H \bmod 2^{64}) \cdot 2^{64}$ вносит несущественный вклад в повышение сложности процедуры проверки подписи.

20. В качестве α используется число, относящееся к некоторому показателю $\gamma | \varphi(n)$. Секретным ключом является значение γ. Размер подписи в исходной схеме ЭЦП равен сумме длин секретного ключа и модуля: $|R| + |S| \approx |n| + |\gamma|$. Заметим, что уравнение проверки преобразуется к виду $R = \alpha^{SR/H} \bmod n$, из которого вытекает следующий вариант схемы ЭЦП с сокращенной подписью: $R' = \alpha^{SR'/H} \bmod n$, где $R' = F(R)$ и F — некоторая сжимающая функция, например, $R' = R \bmod \delta$, $|\delta| = 128$ бит.

21. Определяем делители модуля: $n = p \cdot q = 3631 \cdot 5003 = 18\,165\,893$. Вычисляем функцию Эйлера от модуля n: $\varphi(n) = \varphi(3631 \cdot 5003) = \varphi(3631) \cdot \varphi(5003) = 3630 \cdot 5002 = 18\,157\,260$. Находим разложение функции Эйлера от каждого из делителей модуля n: $p - 1 = 3630 = 2 \cdot 3 \cdot 5 \cdot 121$ и $q - 1 = 5002 = 2 \cdot 41 \cdot 61$. Выбираем в качестве секретного ключа число $\gamma = \gamma' \gamma'' = 121 \cdot 61 = 7381$, которое содержит делители $\gamma' | p - 1$ и $\gamma'' | q - 1$. Затем вычисляем открытый ключ как число, относящееся к показателю γ по модулю n: $\alpha = 13^{\varphi(n)/\gamma} \bmod n = 13^{\varphi(n)/7381} \bmod 18165893 = 13^{2460} \bmod 18\,165\,893 = 7\,985\,177$. Проверяем выполнимость условия НОД$(\alpha - 1, n) = 1$: НОД$(7\,985\,176, 18\,165\,893) = 1$. Эта проверка подтверждает, что число 7 985 177 действительно относится по модулю n к

показателю 7381 (если бы число α относилось по модулю n к показателю γ' или γ'', то мы бы имели НОД$(\alpha-1, n)\neq 1$).

22. Определяем делители модуля: $n=p\cdot q=9\,205\,579\cdot 246\,319=$ $=2\,267\,509\,013\,701$. Вычисляем функцию Эйлера от модуля n: $\varphi(n)=$ $=\varphi(9\,205\,579\cdot 246\,319)=\varphi(9\,205\,579)\cdot\varphi(246\,319)=9\,205\,578\cdot 246\,318=$ $=2\,267\,499\,561\,804$. Находим разложение функции Эйлера от каждого из делителей модуля n: $p-1=9205\,578=2\cdot 3^2\cdot 137\cdot 3733$ и $q-1=246\,318=$ $=2\cdot 3\cdot 61\cdot 673$. Выбираем в качестве секретного ключа число $\gamma=$ $=\gamma'\gamma''=137\cdot 61=8357$, которое содержит делители $\gamma'|p-1$ и $\gamma''|q-1$. Затем вычисляем открытый ключ как число, относящееся к показателю γ по модулю n: $\alpha=7^{\varphi(n)^{-1}\gamma}\bmod n=7^{\varphi(n)^{-1}8357}\bmod n=7^{271329372}$ $\bmod 2\,267\,509\,013\,701=1\,663\,233\,398\,713$. Проверяем выполнимость условий $\alpha^{\gamma/\gamma'}\bmod n\neq 1$ и $\alpha^{\gamma/\gamma''}\bmod n\neq 1$: $\alpha^{\gamma/\gamma'}\bmod n=\alpha^{61}\bmod n=$ $1\,539\,413\,696\,326\neq 1$, $\alpha^{\gamma/\gamma''}\bmod n=\alpha^{137}\bmod n=503\,112\,509\,088\neq 1$. Проверяем выполнимость условия НОД$(\alpha-1,n)=1$: НОД$(1\,663\,233\,398\,712,$ $2\,267\,509\,013\,701)=1$.

23. Определяем делители модуля: $n=p\cdot q=19\,433\cdot 14\,869=288\,949\,277$. Вычисляем функцию Эйлера от модуля n: $\varphi(n)=\varphi(19\,433\cdot 14\,869)=$ $\varphi(19\,433)\cdot\varphi(14\,869)=19\,432\cdot 14\,868=288\,914\,976$. Находим разложение функции Эйлера от каждого из делителей модуля n: $p-1=19\,432=2^3\cdot 7\cdot 347$ и $q-1=14\,868=2^2\cdot 3^2\cdot 7\cdot 59$. Выбираем в качестве секретного ключа число $\gamma=\gamma'\gamma''=347\cdot 59=20\,473$, которое содержит делители $\gamma'|p-1$ и $\gamma''|q-1$. Затем вычисляем открытый ключ как число, относящееся к показателю γ по модулю n: $\alpha=$ $=2^{\varphi(n)^{-1}\gamma}\bmod n=2^{\varphi(n)^{-1}20473}\bmod n=2^{2460}\bmod 288\,949\,277=240\,433\,559$.

Проверяем выполнимость условия НОД$(\alpha-1, n)=1$: НОД$(240\,433\,558,$ $288\,949\,277)=1$. Эта проверка подтверждает, что число 240 433 559 действительно относится по модулю n к показателю 20 473 (если бы число α относилось по модулю n к показателю γ' или γ'', то мы бы имели НОД$(\alpha-1, n)\neq 1$).

24. Нет. Возможна подделка подписи следующим способом. Берем $k=H$ и $S=1/\alpha^H\bmod n$. Усиления схемы можно добиться, потребовав выполнения дополнительного условия $k\neq H\bmod\gamma$. Однако γ есть секретный ключ, поэтому проверку этого неравенства надо задать «скрытно», а именно через проверку неравенства $\alpha^H\neq\alpha^k\bmod n$.

25. Обе схемы построены на основе сложности задачи факторизации числа, представляющего собой произведение двух больших простых чисел. В первой схеме эта задача возникает при попытке разложения $\varphi(p')=$ $=p'-1$. Поскольку в разложении n' имеется только два больших множи-

теля, то длина элемента подписи g не может быть существенно меньше чем $0.5\,|p|$ (это некоторый недостаток по сравнению со второй схемой), однако использование в первом проверочном уравнении вычислений по простому модулю p' снимает проблему, связанную с выработкой числа α', показателем которого по модулю p' является простое число q'. Во второй схеме число α должно относиться к составному показателю, содержащему, по крайней мере, по одному достаточно большому делителю чисел $p-1$ и $q-1$. Это должно учитываться при выборе секретных множителей p и q модуля n. Размер каждого из этих сомножителей должен быть достаточно большим, например, 128 бит, что задает длину $|g| \approx 256$ бит, т. е. размер подписи во второй схеме ЭЦП будет несколько меньше. Это будет особенно заметно при длинах $|n| \approx |p'|$, превышающих 2000 бит с целью повышения стойкости. В первой схеме одновременно с ростом сложности задачи факторизации (за счет увеличения длины числа n') будет в соответствующей пропорции расти размер элемента g, а во второй схеме размер как элемента k, так и элемента g может сохраняться неизменным при увеличении размера модуля n. Еще одним небольшим преимуществом второй схемы является отсутствие необходимости проверки дополнительного проверочного неравенства.

26. Процедура генерации подписи основана на предварительном случайном выборе значений сумм $k+g \equiv U_1 \bmod \gamma_1$ (1) и $\nu+g \equiv U_2 \bmod \gamma_2$ (2). Если значения этих сумм считать заданными (фиксированными), то значение элемента подписи k предопределено: $k = (\alpha_1^{U_1}\alpha_2^{U_2 H} \bmod n) \bmod \delta$. Значения двух оставшихся элементов подписи вычисляются исходя из условий (1) и (2): $g = U_1 - k \bmod \gamma_1$ и $\nu \equiv U_2 - g \bmod \gamma_2$. Если числа γ_1 и γ_2 неизвестны, то подделать подпись вычислительно сложно. Специфические требования к выбору секретных чисел γ_1 и γ_2 состоят в том, что они должны иметь такую структуру, при которой вычисление делителей модуля n как НОД$(n, \alpha_1 - 1) \neq 1$ или НОД$(n, \alpha_2 - 1) \neq 1$ было бы неосуществимо. Кроме того, следует учесть, что для простого значения γ_i ($i = 1, 2$), которое является одновременно делителем обоих чисел $p-1$ и $q-1$, выполняется условие $\gamma_i | n-1$, что может быть использовано атакующим для вычисления γ_i. Для того чтобы не допустить указанных выше уязвимостей схемы ЭЦП, каноническое разложение каждого из показателей γ_1 и γ_2 должно содержать, по крайней мере, по одному достаточно большому (например, длиной 128 бит и более) простому делителю как числа $p-1$, так и числа $q-1$.

27. Процедура генерации подписи основана на представлении числа S в виде $S = M\alpha^g \bmod n$ и предварительном случайном выборе значения

суммы $k+g \equiv U \bmod \gamma$ (1). Если значение этой суммы считать заданным (фиксированным), то значение выражения в скобках в правой части проверочного уравнения оказывается предопределенным и равным $Z = \alpha^{U} \bmod n$. Выполнение проверочного уравнения в таком случае требует выполнения сравнения $g + Z \equiv 0 \bmod \gamma$, откуда следует, что для выбранного значения суммы имеем $g \equiv -Z \bmod \gamma$ и $S = M\alpha^{K} \bmod n$. Теперь из (1) можно найти второй элемент подписи (k, S): $k \equiv U - g \bmod \gamma$. Специфические требования к выбору секретного числа γ и открытого числа α состоят в том, что они должны иметь такую структуру, при которой вычисление делителей модуля n как НОД$(n, \alpha - 1) \neq 1$ или нахождение самого числа γ как делителя $\gamma | n - 1$ было бы неосуществимо. Для этого показатель γ должен содержать, по крайней мере, по одному достаточно большому (128 бит и более) простому делителю как числа $p - 1$, так и числа $q - 1$. С учетом желательности минимизации размера подписи при сохранении достаточной стойкости в качестве γ можно выбрать составное число $\gamma = \gamma'\gamma''$, где $\gamma' | p - 1$ и $\gamma'' | q - 1$, причем γ' не делит $q - 1$ и γ'' не делит $p - 1$.

28. При указанном проверочном уравнении процедура генерации подписи может быть основана на предварительном случайном выборе значений сумм $k + g \equiv U_1 \bmod \gamma_1$ (1) и $vM + gM \equiv U_2 \bmod \gamma$ (2). Если значения этих сумм считать заданными (фиксированными), то значение элемента подписи k предопределено: $k = (\alpha^{U_1} \bmod n)(\alpha^{U_2} \bmod n) \bmod \delta$. Значения двух оставшихся элементов подписи вычисляются исходя из условий (1) и (2): $g = U_1 - k \bmod \gamma$ и $v = (U_2 - gM)M^{-1} \bmod \gamma$.

29. При указанном проверочном уравнении процедура генерации подписи может быть основана на предварительном случайном выборе значений сумм $k + g - v \equiv U_1 \bmod \gamma$ (1) и $vM + gM \equiv U_2 \bmod \gamma$ (2). Если значения этих сумм считать заданными, то значение элемента подписи k предопределено: $k = (\alpha^{U_1} \bmod n)(\alpha^{U_2} \bmod n) \bmod \delta$. Значения двух оставшихся элементов подписи вычисляются путем совместного решения системы сравнений (1) и (2): $g = \dfrac{MU_1 - Mk + U_2}{2M} \bmod \gamma$ и $v = \dfrac{U_2 - MU_1 + Mk}{2M} \bmod \gamma$.

30. Процедура генерации подписи предполагает фиксирование каждого из выражений, стоящих в двух скобках в правой части проверочного сравнения, и состоит в следующем. Предварительно выбираются случайные числа $U_1 < \gamma$ и $U_2 < \delta$. Вычисляется значение $Z \equiv (\alpha^{U_1} \bmod n) \bmod \delta$. За-

тем совместно решаются следующие два сравнения: $k - v \equiv U_2 \bmod \delta$ (1) и $k + v \equiv Z^{U_2} \bmod \delta$ (2). В результате решения этой системы сравнений получаем формулы для вычисления двух элементов подписи: $k = \frac{U_2 + Z^{U_2}}{2} \bmod \delta$ и $v = \frac{Z^{U_2} - U_2}{2} \bmod \delta$. Третий элемент подписи вычисляем с учетом сравнения $kg \vee M \equiv U_1 \bmod \gamma$: $g = \frac{U_1}{Mkv} \bmod \gamma$.

31. Предварительно генерируют достаточно большие простые числа p и q, такие что простые числа γ' и γ'' требуемой длины являются делителями чисел $p-1$ и $q-1$ соответственно. Затем находят число α, относящееся к показателю γ по модулю n, используя формулу $\alpha = \beta^{\frac{\varphi(n)}{\gamma}} \bmod n \neq 1$, где $\gamma = \gamma'\gamma''$. Для вычисленного по этой формуле значения α проверяют выполнимость условий $\alpha^{\gamma'} \bmod n \neq 1$ и $\alpha^{\gamma''} \bmod n \neq 1$. Вычисление подписи осуществляется следующим образом. Выбирается случайное число $U < \gamma$, по которому вычисляется значение $Z = (\alpha^U \bmod n) \bmod \delta$. После этого определяют элементы подписи: $k = Z^H \bmod \delta$ и $g = \frac{U}{k} \bmod \gamma$.

32. Простые числа p и q генерируют таким образом, чтобы числа $p-1$ и $q-1$ содержали простые делители γ' и γ'' соответственно. Число α находят, выбирая произвольное число β и используя формулы $\alpha = \beta^{\frac{\varphi(n)}{\gamma}} \bmod n \neq 1$, $\alpha^{\gamma'} \bmod n \neq 1$ и $\alpha^{\gamma''} \bmod n \neq 1$, где $\gamma = \gamma'\gamma''$. Вычисление подписи осуществляется следующим образом. Выбирается случайное число $U < \gamma$, по которому вычисляется значение $Z = (\alpha^U \bmod n) \bmod \delta$. После этого определяют элементы подписи: $k = MZ^{-1} \bmod \delta$ и $g = (U - k) \bmod \gamma$.

33. Предварительно находят число α, относящееся к некоторому показателю $\gamma \mid \varphi(n)$, где γ содержит достаточно большие простые делители чисел $p-1$ и $q-1$. Затем выбираются случайные значения k' и g', по которым вычисляются значения $S' = \alpha^{g'} \bmod n$ и $R' = \alpha^{k'} \bmod n$. Далее вычисляют $U = g' + k' \bmod \gamma$ и $Z = (R'S' \bmod n) \bmod \gamma$. После этого решают систему из следующих двух уравнений: $g + k \equiv U \bmod \gamma$ и $gZ \equiv kH \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчет-

ные формулы: $k = \frac{ZU}{Z+H} \bmod \gamma$ и $g = \frac{UH}{Z+H} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. (Отметим, что можно взять в качестве α произвольное число. Тогда в качестве γ следует использовать значение $\varphi(n)$. Если для выбранных k' и g' имеет место НОД$(Z + H, \varphi(n)) \neq 1$, то берут другие значения k' и g' и снова проверяют указанные условия.)

34. В данной схеме ЭЦП в качестве α используется (см. решение предыдущей задачи) число, относящееся по модулю n к некоторому показателю $\gamma | \varphi(n)$, где γ содержит достаточно большие простые делители чисел $p-1$ и $q-1$. Это число используется при вычислении параметров подписи: $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. В случае использования простого числа в качестве показателя γ возникают некоторые проблемы. Например, если мы сформируем параметр α в соответствии с формулой $\alpha = \beta^{\varphi(n)\gamma/\gamma} \bmod n \neq 1$, где γ делит $p-1$, но не делит $q-1$, то будем иметь: $\alpha = \beta^{\varphi(n)\cdot\gamma} = (\beta^{(q-1)})^{(p-1)\gamma/\gamma} \bmod n \Rightarrow \alpha \equiv (\beta^{(q-1)})^{(p-1)\gamma/\gamma} \equiv 1^{(p-1)\gamma} \equiv 1 \bmod q \Rightarrow$ $\Rightarrow \alpha - 1 \equiv 0 \bmod q \Rightarrow q \mid \alpha - 1 \Rightarrow$ НОД$(\alpha - 1, n) = q$. Следовательно, при известном параметре α разложение модуля сводится к нахождению наибольшего общего делителя двух чисел $\alpha - 1$ и n. Аналогичным образом параметры S и R могут быть использованы для разложения модуля. Например, $\alpha \equiv 1 \bmod q \Rightarrow \alpha^k \equiv 1 \bmod q \Rightarrow R \equiv 1 \bmod q \Rightarrow R - 1 \equiv 0 \bmod q \Rightarrow$ $\Rightarrow q \mid R - 1 \Rightarrow$ НОД$(R - 1, n) = q$. Таким образом, для обеспечения высокого уровня стойкости требуется ввести некоторые ограничения на выбор параметров p, q и промежуточного числа α. Числа p и q могут быть сформированы таким образом, чтобы числа $p-1$ и $q-1$ содержали одинаковый большой простой делитель γ заданного размера. При этом требуется выполнение следующего условия: число γ^2 не делит ни $p-1$, ни $q-1$. Параметр α может формироваться в соответствии с формулой $\alpha = \beta^{L(n)\gamma/\gamma} \bmod n \neq 1$, где $L(n) =$ НОК$[p-1, q-1]$ — обобщенная функция Эйлера, или по формуле $\alpha = \beta^{\frac{(p-1)(q-1)}{\gamma^2}} \bmod n \neq 1$. В последнем случае имеем: $\alpha = \beta^{uv} \bmod n \neq 1$, где $u = (p-1)/\gamma$ и $v = (q-1)/\gamma$. Из последней формулы видно, что при выборе в качестве β числа, являющегося первообразным корнем одновременно по $\bmod p$ и по $\bmod q$, выполняются неравенства $\alpha \neq 1 \bmod q$ и $\alpha \neq 1 \bmod p$. Действительно, сравнение $\alpha \equiv$ $\equiv \beta^{uv} \equiv 1 \bmod q$ или $\alpha \equiv \beta^{uv} \equiv 1 \bmod p$ может выполняться только в случае, если $uv \equiv 0 \bmod (q-1)$ или $uv \equiv 0 \bmod (p-1)$ соответственно. Однако последние соотношения не выполняются, поскольку по по-

строению чисел p и q значение uv не делится ни на $q-1$, ни на $p-1$. Однако может быть осуществлена другая атака, не связанная с разложением модуля. Поскольку секретным параметром является γ, то можно попытаться вычислить γ, минуя проблему разложения модуля. В случае $\gamma | p-1$ и $\gamma | q-1$ имеем $n=(u\gamma+1)(v\gamma+1)=uv\gamma^2+(u+v)\gamma+1$, следовательно, $n-1=(uv\gamma+u+v)\gamma$. В общем случае разложение числа $n-1$ не будет сложной задачей, поэтому следует использовать составной показатель, включающий в качестве своих множителей большие делители обоих чисел $q-1$ и $p-1$.

35. По условию имеем $\alpha^{\gamma} \equiv 1 \bmod m\delta \Rightarrow \alpha^{\gamma} \equiv 1 \bmod m$ и $\alpha^{\gamma} \equiv 1 \bmod \delta$. Поскольку число γ не может быть показателем по модулю δ (показателями по модулю δ могут быть только делители $\varphi(\delta)$), то последнее сравнение может иметь место, только если $\alpha \equiv 1 \bmod \delta$. Для произвольного γ утверждение не верно. Например, числа γ и $\varphi(\delta)$ могут содержать общие нетривиальные делители. Число α может относиться к такому делителю как к показателю по модулю δ, благодаря чему будет выполняться условие $\alpha^{\gamma} \equiv 1 \bmod \delta$.

36. Заметим, что в качестве α используется число, относящееся к некоторому показателю $\gamma | \varphi(n)$, где γ содержит в качестве своих множителей, по крайней мере, по одному достаточно большому простому делителю чисел $p-1$ и $q-1$. Генерация подписи осуществляется следующим образом. Выбираются случайные значения k' и g', по которым вычисляются значения $S'=\alpha^{g'} \bmod n$ и $R'=\alpha^{k'} \bmod n$. Далее вычисляют $U=g'+k' \bmod \gamma$ и $Z=(R'S' \bmod n) \bmod \gamma$. После этого решают систему из следующих двух уравнений: $g+k \equiv U \bmod \gamma$ и $k+gZ \equiv H \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k=\dfrac{ZU-H}{Z-1} \bmod \gamma$ и $g=\dfrac{H-U}{Z-1} \bmod \gamma$. Если для выбранных k' и g' имеет место НОД$(Z-1, \gamma) \neq 1$, то берут другие значения k' и g' и снова проверяют это условие. По полученным значениям k и g вычисляются значения $S=\alpha^{g} \bmod n$ и $R=\alpha^{k} \bmod n$. Возможен вариант генерации подписи для различных сообщений по фиксированным значениям U и Z, которые вычисляются один раз по некоторым выбранным значениям k' и g'. При этом числа U и Z следует держать в секрете. Подпись можно подделать, осуществив замену переменных. Введем переменную $Z=RS \bmod n$. Тогда проверочное уравнение приобретает вид $ZS^{Z-1} = \alpha^{H} \bmod n$. Для произвольного Z параметр S выражается формулой $S=(\alpha^{H} / Z)^{\frac{1}{Z-1}} \bmod n$. При дробном значении степе-

ни трудно вычислить значение S, однако, принимая значение $Z = 2$, вычисляем элементы подписи $S = \alpha^H / Z \bmod n$ и $R = Z / S \bmod n$.

37. В качестве α используется число, относящееся к некоторому показателю $\gamma | \varphi(n)$. Из уравнения проверки вытекает следующая процедура генерации подписи. Выбираются случайные значения k' и g', по которым вычисляются значения $S' = \alpha^{g'} \bmod n$ и $R' = \alpha^{k'} \bmod n$. Далее вычисляют $U = k' - g' \bmod \gamma$ и $Z = (R'/S' \bmod n) \bmod \gamma$. После этого решают систему из следующих двух уравнений: $k - g \equiv U \bmod \gamma$ и $k + gZ \equiv HZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{ZU + ZH}{Z + 1} \bmod \gamma$ и $g = \dfrac{HZ - U}{Z + 1} \bmod \gamma$. Если для выбранных k' и g' имеет место НОД$(Z + 1, \gamma) \neq 1$, то берут другие значения k' и g' и снова проверяют это условие. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. Попытки подделать подпись, вводя новую переменную $Z = R/S \bmod n$, приводят к проверочному уравнению $ZS^{Z-1} = \alpha^{HZ} \bmod n$. Для произвольного Z параметр S выражается формулой $S = (\alpha^{HZ} / Z)^{\frac{1}{Z+1}} \bmod n$. При $Z \geq 1$ получаем в степени дробное значение, поэтому вычислительно сложно найти «правильное» значение элемента подписи S. Значение $Z = 0$ не может быть использовано, так как в скобках выполняется деление на Z.

38. В качестве α используется число, относящееся к некоторому показателю $\gamma | \varphi(n)$. Из уравнения проверки вытекает следующая процедура генерации подписи. Выбираются случайные значения k' и g', по которым вычисляются значения $S' = \alpha^{g'} \bmod n$ и $R' = \alpha^{k'} \bmod n$. Далее вычисляют $U = k' + 2g' \bmod \gamma$ и $Z = (R'(S')^2 \bmod n) \bmod \gamma$. После этого решают систему из следующих двух уравнений: $k + 2g \equiv U \bmod \gamma$ и $k + gH \equiv Z \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{HU - 2Z}{H - 2} \bmod \gamma$ и $g = \dfrac{Z - U}{H - 2} \bmod \gamma$.

Исходя из последних двух формул делаем вывод, что при вычислении хэш-функции от подписываемого документа требуется осуществить проверку НОД$(H - 2, \gamma) = 1$ и $H \neq 2$. Если значения γ и $H - 2$ не являются взаимно простыми, то следует модифицировать документ пока не будет выполнено это условие. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$, которые удовлетворяют уравнению проверки подписи. Попытки подделать подпись с использованием новой переменной $Z = RS^2 \bmod n$ приводят к проверочному уравнению

$ZS^{H-2} = \alpha^Z \bmod n$. Для произвольного Z параметр S выражается формулой $S = (\alpha^Z / Z)^{\frac{1}{H-2}} \bmod n$. В общем случае выражение в скобках возводится в дробную степень, поэтому без знания секрета γ или функции Эйлера от модуля вычислительно сложно найти «правильное» значение элемента подписи S. Однако в крайне маловероятном случае $H = 3$ подделка подписи возможна. Чтобы исключить эту возможность, следует к основному проверочному уравнению добавить проверку выполнимости неравенства $H \neq 3$. Однако это представляется излишним, так как при использовании стойкой хэш-функции вычислительно невозможно подобрать документ, хэш-функция от которого равна значению 3.

39. Вычисляют число α, относящееся к некоторому показателю $\gamma | \varphi(n)$. Затем выбираются случайные значения k' и g', по которым вычисляются значения $S' = \alpha^{g'} \bmod n$ и $R' = \alpha^{k'} \bmod n$. Далее вычисляют $U = g' + k' \bmod \gamma$ и $Z = (R'S' \bmod n) \bmod \gamma$. После этого решают систему из следующих двух уравнений: $g + k \equiv U \bmod \gamma$ и $k \equiv gHZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{HZU}{ZH+1} \bmod \gamma$ и $g = \dfrac{U}{HZ+1} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. Если для выбранных k' и g' имеет место НОД$(ZH + 1, \gamma) \neq 1$, то берут другие значения k' и g' и снова проверяют это условие. Попытка подделать подпись с использованием новой переменной $Z = RS \bmod n$ приводит к проверочному уравнению $Z = S^{HZ+1} \bmod n$. Для произвольного Z параметр S выражается формулой $S = Z^{\frac{1}{ZH+1}} \bmod n$. В общем случае выражение в скобках возводится в дробную степень, поэтому без знания секрета γ или разложения модуля трудно вычислить «правильное» значение S. Таким образом, подделка подписи вычислительно нереализуема.

40. Вычисляют число α, относящееся к некоторому показателю $\gamma | \varphi(n)$. Затем выбираются случайные значения k' и g', по которым вычисляются значения $S' = \alpha^{g'} \bmod n$ и $R' = \alpha^{k'} \bmod n$. Далее вычисляют $U = g' + k' \bmod \gamma$ и $Z = [(R'S')^H \bmod n] \bmod \gamma$. После этого решают систему из следующих двух сравнений: $g + k \equiv U \bmod \gamma$ и $k \equiv gZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{ZU}{Z+1} \bmod \gamma$ и $g = \dfrac{U}{Z+1} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. Если для

выбранных значений k' и g' имеет место НОД$(Z+1, \gamma) \neq 1$, то следует взять другие значения k' и g' и снова проверить последнее условие. (На самом деле следует сразу случайно выбрать значение U, а затем вычислить $Z = [\alpha^{U'H} \bmod n] \bmod \gamma$.) Если показатель γ содержит только два достаточно больших множителя, то с большой вероятностью будет выполняться НОД$(Z+1, \gamma) = 1$, поэтому операция деления при вычислении степеней k и g практически не будет вносить дополнительной сложности в процедуру формирования подписи.

41. Формулы генерации подписи аналогичны соотношениям, приведенным в решении предыдущей задачи. Проверка подписи даст корректный результат, однако данная схема практически неприменима. Это связано с тем, что проверяющий должен осуществить H возведений числа S в степень $Z = RS \bmod n$, так как он не знает значение модуля γ, по которому можно было бы предварительно вычислить $(RS \bmod n)^{U} \bmod \gamma$. Требование достаточно большой длины чисел R и S состоит в том, чтобы исключить возможность несанкционированного подбора подписи к заданному документу путем перебора всех возможных значений подписи. При этом также исключаются тривиальные подписи, например, $R = 1$ и $S = 1$.

42. В качестве α используется число, относящееся по модулю n к некоторому показателю $\gamma \mid \varphi(n)$, в частности, может быть использовано число, относящееся к показателю $L(n)$, где $L(n)$ — обобщенная функция Эйлера. Из уравнения проверки вытекает следующая процедура генерации подписи. Выбираются случайные значения k' и g', по которым вычисляются значения $S' = \alpha^{g'} \bmod n$ и $R' = \alpha^{k'} \bmod n$. Далее вычисляют $U = k' + Hg' \bmod \gamma$ и $Z = (R'(S')^{H} \bmod n) \bmod \gamma$. После этого решают систему из следующих двух уравнений: $k + Hg \equiv U \bmod \gamma$ и $k + g \equiv Z \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{ZH - U}{H - 1} \bmod \gamma$ и $g = \dfrac{U - Z}{H - 1} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^{g} \bmod n$ и $R = \alpha^{k} \bmod n$, которые удовлетворяют уравнению проверки подписи. Требование достаточно большой длины чисел R и S состоит в том, чтобы исключить возможность несанкционированного подбора подписи к заданному документу путем перебора возможных значений подписи при относительно малом значении H.

43. Например, находят число α, относящееся к обобщенной функции Эйлера $L(n)$ как к показателю по модулю n. Затем выбирается случайное значение $U < \gamma = L(n)$. Далее вычисляют $Z = (\alpha^{U} \bmod n) \bmod \gamma$. После

этого решают систему из следующих двух уравнений: $g + Hk \equiv U \bmod \gamma$ и $k \equiv gZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{ZU}{HZ+1} \bmod \gamma$ и $g = \dfrac{U}{HZ+1} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. Если для выбранного значения U имеет место НОД$(HZ+1, L(n)) \neq 1$, то берут другие значения k' и g' и снова проверяют это условие. В этой схеме ЭЦП одинаковые значения параметров U и Z могут быть использованы для генерации подписей к нескольким различным документам. Если для какого-то документа будет иметь место неравенство НОД$(HZ+1, L(n)) \neq 1$, то упомянутые параметры потребуется изменить.

44. Вычисляют число α, относящееся к некоторому показателю $\gamma \mid \varphi(n)$, где $\gamma = \gamma'\gamma''$. Для обеспечения стойкости делители (модуля n) p и q следует выбрать так, что $\gamma' \mid p-1$ и $\gamma'' \mid q-1$, причем γ' не делит $q-1$ и γ'' не делит $p-1$. Затем выбирается случайное значение U, по которому вычисляется параметр $Z = (\alpha^U \bmod n) \bmod \gamma$. После этого решают систему из следующих двух сравнений: $U = (Tg + Hk) \bmod \gamma$, где $T = H^{-1} \bmod \gamma$, и $k \equiv gZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{ZU}{HZ+T} \bmod \gamma$ и $g = \dfrac{U}{HZ+T} \bmod \gamma$.

По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. Данная схема ЭЦП некорректна, так как проверяющий не может вычислить $\varphi(n)$, а следовательно и $H^{-1} \bmod \varphi(n)$, что необходимо для проверки подлинности подписи.

45. Вычисляют число α, относящееся к некоторому показателю $\gamma \mid \varphi(n)$. Затем выбираются случайные значения k' и g', по которым вычисляются значения $S' = \alpha^{g'} \bmod n$ и $R' = \alpha^{k'} \bmod n$. Далее вычисляют $U = (k' + Hg') \bmod \gamma$ и $Z = [R'(S')^H \bmod n] \bmod \gamma$. После этого решают систему из следующих двух сравнений: $U = (k + Hg) \bmod \gamma$ и $kH \equiv gZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{ZU}{H^2+Z} \bmod \gamma$, $g = \dfrac{HU}{H^2+Z} \bmod \gamma$.

По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. Если для выбранных значений k' и g' имеет место

НОД$(H^2 + Z, \varphi(n)) \neq 1$, то берут другие значения k' и g' и снова проверяют это условие.

46. Открытый ключ $n = pq$ генерируется таким образом, чтобы числа $p - 1$ и $q - 1$ содержали достаточно большие простые делители γ' и γ'' соответственно. Следует выбрать некоторое число α, относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$. Это значение α будет использовано в дальнейшем для вычисления элементов подписи. Вычисление подписи осуществляется следующим образом. Выбираются случайные значения U_1 и $U_2 \neq U_1$, не превышающие значения $\gamma - 1$, затем вычисляются значения $Z_1 = (\alpha^{U_1} \bmod n) \bmod \gamma$ и $Z_2 = (\alpha^{U_2} \bmod n) \bmod \gamma$. После этого решают систему из следующих трех сравнений: $g + l \equiv U_1 \bmod \gamma$, $g + k \equiv U_2 \bmod \gamma$ и $kZ_1 \equiv gH + lZ_2 \bmod \gamma$, где неизвестными являются k, l и g. Система сравнений легко решается методом последовательного исключения неизвестных. Решение системы дает следующие расчетные формулы: $k = \dfrac{U_2 H + Z_2(U_1 - U_2)}{Z_1 - Z_2 + H} \bmod \gamma$, $l = \dfrac{2U_2 H - U_2 Z_1 + U_1(Z_1 + H)}{Z_1 - Z_2 + H} \bmod \gamma$ и $g = \dfrac{UZ_1 - U_1 Z_2}{Z_1 - Z_2 + H} \bmod \gamma$. Данная схема ЭЦП не является стойкой, поскольку допускает практически реализуемую возможность подделки подписи путем представления проверочного уравнения в новом виде, использующем переменные $Z = SV \bmod n$ и $Z' = RS \bmod n$: $Z'^{Z} \equiv S^{H+Z-Z'} Z^{Z'} \bmod n$. Для произвольно выбранных чисел Z и Z' значение $S = \left(Z'^{Z} Z^{-Z'}\right)^{\frac{1}{H+Z-Z'}} \bmod n$ удовлетворяет модифицированному проверочному уравнению. В общем случае вычисление параметра S связано с нахождением разложения модуля, однако, выбирая значение $Z' = H + Z - 1$, можно обойти задачу вычисления корней по модулю. Тройка чисел (Z, Z', S) может быть легко пересчитана в тройку значений (R, S, V), удовлетворяющих исходному уравнению проверки подписи.

47. Открытый ключ $n = pq$ генерируется таким образом, чтобы числа $p - 1$ и $q - 1$ содержали достаточно большие простые делители γ' и γ'' соответственно. Следует выбрать некоторое число α, относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$. Это значение α будет использовано в дальнейшем для вычисления элементов подписи. Вычисление подписи осуществляется следующим образом. Выбираются случайные значения U_1 и $U_2 \neq U_1$, не превышающие значения $\gamma - 1$, затем вычисляются значения $Z_1 = (\alpha^{U_1} \bmod n) \bmod \gamma$ и $Z_2 = (\alpha^{U_2} \bmod n) \bmod \gamma$. После этого решают

систему из следующих трех сравнений: $l+g+k \equiv U_1 \bmod \gamma$, $l+g-k \equiv U_2 \bmod \gamma$ и $lH+kZ_1 \equiv gZ_2 \bmod \gamma$, где неизвестными являются k, l и g. Решение системы дает следующие расчетные формулы: $k=\frac{U_1-U_2}{2} \bmod \gamma$, $l=\frac{U_1(Z_1+Z_2+2H)+U_2(Z_2-Z_1+2H)}{2(H+Z_2)} \bmod \gamma$ и $g=$ $=\frac{H(U_1+U_2)+Z_1(U_1-U_1)}{2(H+Z_2)} \bmod \gamma$. По полученным значениям k, l и g вычисляются значения $V=\alpha^l \bmod p$, $S=\alpha^g \bmod p$ и $R=\alpha^k \bmod p$. Данная схема ЭЦП представляется стойкой, поскольку не допускает практически реализуемую возможность подделки подписи путем представления проверочного уравнения в новом виде, использующем переменные $Z=SV \bmod n$ и $Z'=RSV \bmod n$: $\left(\frac{Z}{S}\right)^H \left(\frac{Z'}{Z}\right)^{Z'} = S^{(Z^2/Z' \bmod n)} \bmod n$. Из последнего соотношения получаем формулу для вычисления параметра S: $S=\left(\frac{Z^H Z'^{Z'}}{Z^{Z'}}\right)^{\frac{1}{(Z^2/Z' \bmod n)+H}} \bmod n$ (для произвольно выбранных чисел Z и Z'). При $H>0$ подделка подписи требует вычисления дробей по неизвестному модулю.

48. Предполагается, что открытый ключ $n=pq$ генерируется таким образом, чтобы числа $p-1$ и $q-1$ содержали достаточно большие делители γ. Следует выбрать некоторое число α, относящееся по модулю n к достаточно большому делителю $\gamma \mid \varphi(n)$. Причем проверяется условие НОД$(\alpha-1, n)=1$. Если это условие не выполняется, то генерируется другое значение α. Это значение α предполагается использовать в дальнейшем для вычисления элементов подписи. Формирование подписи связано с выбором трех взаимно не равных значений U_1, U_2 и U_3, по которым вычисляются параметры $Z_1=(\alpha^{U_1} \bmod n) \bmod \gamma$, $Z_2=$ $=(\alpha^{U_2} \bmod n) \bmod \gamma$ и $Z_3=(\alpha^{U_3} \bmod n) \bmod \gamma$. Предполагается найти значения k, l и g, которые удовлетворяют системе сравнений: $g+l \equiv$ $\equiv U_1 \bmod \gamma$, $l+k \equiv U_2 \bmod \gamma$, $g+k \equiv U_3 \bmod \gamma$ и $kZ_1 \equiv gZ_2+lHZ_3 \bmod \gamma$, где неизвестными являются k, l и g. Система сравнений в общем случае не имеет решений, поскольку включает четыре сравнения при трех неизвестных. Поэтому рассматриваемая схема ЭЦП не является корректной.

49. Предполагается, что открытый ключ $n=pq$ генерируется таким образом, чтобы числа $p-1$ и $q-1$ содержали достаточно большие простые делители γ' и γ'' соответственно. Следует выбрать некоторое число α.

относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$. Это значение α предполагается использовать в дальнейшем для вычисления элементов подписи. Формирование подписи связано с выбором двух неравных значений U_1 и U_2, по которым вычисляются параметры $Z_1 = (\alpha^{U_1} \bmod n) \bmod \gamma$ и $Z_2 = (\alpha^{U_2} \bmod n) \bmod \gamma$. Предполагается найти значения k, l и g, которые удовлетворяют системе сравнений: $g + l \equiv U_1 \bmod \gamma$, $l + k \equiv \equiv U_2 \bmod \gamma$ и $kZ_1 \equiv gZ_2 + lH \bmod \gamma$, где неизвестными являются k, l и g. Система из трех сравнений с тремя неизвестными имеет решение. Поэтому рассматриваемая схема ЭЦП является корректной. Данная схема ЭЦП допускает практически реализуемую возможность подделки подписи путем представления проверочного уравнения в новом виде, использующем переменные $Z = SV \bmod n$ и $Z' = RV \bmod n$: $(Z'/V)^Z = (Z/V)^{Z'} V^H \bmod n$. Для произвольно выбранных чисел Z и Z' значение параметра S, вычисленное по формуле $V = (Z'^Z Z^{-Z'})^{\frac{1}{Z+H-Z'}} \bmod n$, будет удовлетворять модифицированному проверочному уравнению. Значения Z и Z' могут быть выбраны произвольно, поэтому можно воспользоваться выбором, удовлетворяющим соотношению $Z + H - Z' = 1$. В этом случае можно обойти задачу вычисления корней по модулю. Тройка чисел (Z, Z', V) может быть легко пересчитана в тройку значений (R, S, V), удовлетворяющих исходному уравнению проверки подписи.

50. Подпись вычисляется по формуле $S = H/x \bmod \gamma$, которая накладывает ограничение на выбор секретного ключа НОД$(x, \gamma) = 1$, если показатель γ является составным числом. Рассматриваемая схема уязвима, поскольку без введения специальных ограничений позволяет по нескольким известным подписям S_1, S_2, ..., S_k и соответствующим им хэш-функциям H_1, H_2, ..., H_k определить γ. Действительно, имеем $x \equiv \equiv H_i/S_i \bmod \gamma$ и $x \equiv H_j/S_j \bmod \gamma$, следовательно, $S_i H_j \equiv S_j H_i \bmod \gamma \Rightarrow \Rightarrow \gamma | S_i H_j - S_j H_i$. Разлагая на множители значения $S_i H_j - S_j H_i$ при различных i и j, можно выбрать одинаковые встречающиеся множители. Перемножая последние в различных сочетаниях, в общем случае можно определить значение γ. Данная схема может быть усилена путем использования второго элемента подписи аналогично тому, как это имеет место в случае схемы подписи Эль-Гамаля. Проверочное уравнение в усиленном варианте схемы приобретает, например, следующий вид $\alpha^H = y^R R^S \bmod n$ или вид $R = y^{R \cdot S} \alpha^{HS} \bmod n$.

51. Подпись вычисляется по формуле $S = k/HR \bmod \varphi(n)$, где R предварительно генерируется по формуле $R = \alpha^k \bmod n$ (k — случайно выбирае-

мое число). Параметр α должен быть числом, для которого должно выполняться условие НОД(α, n) = 1. Кроме того, число α должно относиться к достаточно большому показателю для различных значений n. При формировании открытого ключа выполнение этого условия можно проверить, рассматривая все малые делители $\delta | \varphi(n)$ и проверяя соотношение $\alpha^{\delta} \bmod n \neq 1$. Вероятность того, что для сгенерированного значения n число α будет относиться по модулю n к малому показателю, пренебрежимо мала.

52. Элементы подписи (R, S) следует искать в виде $R = (\alpha^k \bmod n) \bmod z$ и $S = \alpha^g \bmod n$, где α — число, относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$. Длина z выбирается, например, равной 128–256 бит, что дает существенное сокращение длины параметра R. Для обеспечения стойкости делители модуля p и q следует выбирать так, что простые числа γ' и γ'' входят в разложение только одного из чисел $p - 1$ и $q - 1$. Формирование подписи осуществляется следующим образом. Выбирается случайное значение k, вычисляется R, после чего определяются $g = k(HR)^{-1} \bmod \gamma$ и $S = \alpha^g \bmod n$.

53. При фиксировании одного из элементов подписи (g, R) даже по известному секретному ключу q сложно вычислить второй элемент. Для вычисления подписи следует представить число R в виде $R = \alpha^k \bmod p$. После этого можно выбрать некоторое произвольное значение $U < q$ и рассмотреть область пар значений k и g, удовлетворяющих условию $kg \equiv U \bmod \gamma$ (1). Последнее условие задает некоторый фиксированный параметр $Z = (\alpha^U \bmod p) \bmod q$. Для выполнения проверочного соотношения следует найти пару (k, g), удовлетворяющую также и сравнению $k \equiv HZ \bmod q$ (2). С учетом сравнений (1) и (2) получаем формулы для вычисления подписи (g, R): $g = \dfrac{U}{HZ} \bmod q$ и $R = \alpha^{HZ} \bmod p$. Использование проверочного неравенства $|g| < 610$ бит связано с возможностью формирования подписи (g', R'), удовлетворяющей проверочному сравнению, путем вычисления чисел g' и k' по модулю n с использованием формул $g' = \dfrac{U}{HZ} \bmod n$ и $k' \equiv HZ \bmod n$, где $Z' = \alpha^{U'} \bmod p$.

54. При фиксировании одного из элементов подписи (g, R) даже по известному секретному ключу q сложно вычислить второй элемент. Для вычисления подписи следует представить число R в виде $R = \alpha^k \bmod p$. После этого можно выбрать некоторое произвольное значение $U < q$ и рассмотреть область пар значений k и g, удовлетворяющих условию

$kg \equiv U \bmod q$ (1). Последнее условие фиксирует значение степени в правой части проверочного сравнения. Для выполнения проверочного соотношения следует найти пару (k, g), удовлетворяющую также и сравнению $g \equiv kHZ \bmod q$ (2), где $Z = (\alpha^{l'} \bmod p) \bmod q$. С учетом сравнений (1) и (2) получаем формулы для вычисления подписи (g, R): $g = \pm\sqrt{UHZ} \bmod q$, $k = \pm\sqrt{U/HZ} \bmod q$ и $R = \alpha^k \bmod p$. Трудоемкость процедуры генерации подписи можно снизить, если простое число q выбрать таким образом, что выполняется соотношение $q \equiv 3 \bmod 4$. Использование проверочного неравенства $|g| < 770$ бит необходимо для подтверждения подлинности подписи, поскольку элемент подписи g длиной, примерно равной длине числа n, можно сформировать без использования секретного ключа. Например, подпись (g', R'), удовлетворяющая проверочному сравнению, может быть вычислена с использованием формул $g = \pm\sqrt{UHZ} \bmod n$ и $k = \pm\sqrt{\frac{U}{HZ}} \bmod n$.

55. При фиксировании одного из элементов подписи (g, R) даже по известному секретному ключу γ сложно вычислить второй элемент. Для вычисления подписи следует представить число R в виде $R = \alpha^k \bmod n$. Теперь зафиксируем некоторое произвольное значение $U < \gamma$, такое что НОД$(U, \gamma) = 1$. и рассмотрим область пар значений k и g, удовлетворяющих условию $kg \equiv U \bmod \gamma$ (1). Последнее условие задает некоторый фиксированный параметр $Z = \alpha^{U'} \bmod n$ (при этом будем брать различные значения U до тех пор, пока не получим НОД$(Z, \gamma) = 1$). Для выполнения проверочного соотношения следует найти пару (k, g), удовлетворяющую также и сравнению $kHg^2 \equiv Z \bmod \gamma$ (2). Искомая пара значений может быть найдена как решение системы из сравнений (1) и (2): $g = \frac{Z}{HU} \bmod \gamma$ и $k = \frac{HU^2}{Z} \bmod \gamma$.

56. Процедура генерации подписи (g, R) состоит в следующем. Число R представляется в виде $R = \alpha^k \bmod p$. Затем выбирается некоторое произвольное значение $U < q$ и решается система сравнений $kg \equiv U \bmod q$ (1) и $H \equiv kZ \bmod q$ (2), где $Z = (\alpha^{U'} \bmod p) \bmod q$. Решение системы сравнений (1) и (2) дает следующие формулы для вычисления подписи (g, R): $g = UZ/H \bmod q$ и $R = \alpha^{H/Z} \bmod p$. Дополнительное проверочное соотношение $|g| < 520$ бит используется потому, что без знания секретного ключа можно сформировать подпись (g', R'), удовлетворяющую проверочному сравнению, путем вычисления чисел g' и k' по формулам $g' = UZ/H \bmod n$ и $k' = H/Z \bmod n$.

57. Процедура генерации подписи (g, R) состоит в следующем. Выбирается некоторое случайное значение $k < q$ и вычисляется число R: $R = \alpha^k \bmod p$. Затем решается сравнение $k \equiv HRg \bmod q$, из которого вытекает формула $g = k/HR \bmod q$. Использование проверочного неравенства $|g| < 520$ бит связано с возможностью формирования подписи (g', R'), удовлетворяющей проверочному сравнению, путем вычисления элемента g' по модулю n с использованием формулы $g' = k/HR \bmod n$. Сократить размер подписи в заданной схеме ЭЦП можно путем задания в проверочном уравнении не самого значения параметра R, а значения некоторой сжимающей функции $F(R)$, вычисленной от R. В этом случае проверочное уравнение имеет вид: $F(R) = F(\alpha^{H^{-1}(R)g})$ mod p. Подписью является пара чисел $(g, F(R))$. В частности, можно использовать следующую функцию $F(R) = R \bmod \delta$, где δ есть некоторое простое число заданного размера, например, $|\delta| \approx 160$ бит.

58. Следует выбрать модуль $p = 2n + 1$, где n — число, удовлетворяющее требованиям, предъявляемым к модулю RSA. В этом случае криптоаналитик, решивший задачу дискретного логарифмирования и определивший значение секретного ключа x, сможет выбрать случайное k, вычислить $R = \alpha^k \bmod p$, а затем найти значение $S^2 \equiv ((H - xR)/k) \bmod 2n$, но, чтобы подделать подпись (R, S) к документу, соответствующему значению хэш-функции H, ему понадобится также извлечь квадратный корень по составному модулю, что требует факторизации числа n.

59. Процедура генерации подписи состоит в выборе такой пары значений k и g, что выполняется проверочное соотношение. Если предварительно зафиксировать одно из значений k или g, то второе значение будет найти вычислительно сложно (даже если знать секретный ключ γ). Однако владелец секретного ключа может реализовать другой способ генерации подписи, который является вычислительно эффективным. Этот способ состоит в предварительном задании значения разности $k - Hg$, вычислении значения правой части проверочного сравнения и приравнивании его по модулю δ к сумме $k + Hg$. Детально процедура генерации подписи описывается следующим образом. Предварительно выбирается случайное число $U < \gamma$ и вычисляется значение $Z \equiv \alpha^U \bmod n$. Затем совместно решаются следующие два сравнения: $k - Hg \equiv U \bmod \gamma$ (1) и $k + Hg \equiv Z \bmod \delta$ (2). При решении системы сравнений (1) и (2) следует учесть, что модули в них различаются. В связи с этим от этой системы сравнений следует перейти к следующей системе уравнений:

$$\begin{cases} k - Hg = U + N_1\gamma, \\ k + Hg = Z + N_2\delta. \end{cases}$$

Очевидно, что целочисленные решения этой систе-

мы уравнений при любых значениях натуральных чисел N_1 и N_2 будут удовлетворять также и системе сравнений (1) и (2). Решение системы уравнений в общем виде дает: $\begin{cases} k = (U + N_1\gamma + Z + N_2\delta)/2, \\ g = (Z + N_2\delta - U - N_1\gamma)H^{-1}/2. \end{cases}$ Теперь зафиксируем значение N_2 (т. е. приравняем его к нулю или некоторому небольшому натуральному числу) и запишем диофантово уравнение относительно неизвестных N_1 и g: $2Hg + \gamma N_1 = Z - U + N_2\delta$. Это уравнение с большой вероятностью имеет целочисленные решения (значение γ обычно выбирается равным произведению двух больших простых чисел, поэтому с большой вероятностью имеем НОД$(2H, \gamma) = 1$)), которые могут быть найдены с помощью расширенного алгоритма Евклида. Зафиксированное значение N_2 и вычисленное N_1 подставляем в уравнение $k = (U + N_1\gamma + Z + N_2\delta)/2$. Если получим целочисленное значение k, то подпись вычислена. В противном случае выберем новое значение U, для которого повторим описанную выше процедуру. После нескольких таких попыток с достаточно большой вероятностью будет получено целочисленное значение для k. В результате получим положительные целочисленные значения k и g, которые составят искомую подпись.

60. *Первый механизм* основан на предварительном выборе случайного значения произведения $Hgk \equiv U \bmod \gamma$ (1). Согласно проверочному сравнению задание значения U предопределяет значение k: $k = Z = (\alpha^{U} \bmod n) \bmod \delta$ (2). Второй элемент подписи вычисляется из сравнения (1): $g = (U / HZ) \bmod \gamma$. *Второй механизм* основан на предварительном вычислении значения k по формуле $k = (\alpha^{w} \bmod n) \bmod \delta$, где w — случайное значение, и решении сравнения $\alpha^{w} = \alpha^{Hgk} \bmod n$ относительно g: $g = \dfrac{w}{Hk} \bmod \gamma$. Большей общностью обладает первый механизм, так как он дает возможность сформировать подпись в ряде схем ЭЦП, для которых второй механизм непригоден. Например, в случае проверочных уравнений вида $k^2 H + k \equiv (\alpha^{gk} \bmod n) \bmod \delta$ и $k + Hg \equiv (\alpha^{k \cdot Hg} \bmod n) \bmod \delta$.

61. Поскольку значения $F(n)$ могут представлять собой числа, относящиеся к различным показателям, то вычисление значения, обратного к H, следует осуществлять по модулю $\varphi(n)$. Таким образом, приходим к следующему уравнению формирования подписи: $S = [F(n)]^{H^{-1} \bmod \varphi(n)} \bmod n$. Длина подписи соответствует длине модуля. Стойкость схемы обусловлена сложностью извлечения корней большой

степени по составному модулю без знания его разложения на простые множители. При формировании открытого ключа в соответствии с требованиями к RSA-модулю рассматриваемая схема подписи является стойкой. Время формирования подписи можно несколько уменьшить, переходя от φ к обобщенной функции Эйлера $L(n)$, т. е. формируя подпись по формуле: $S = [F(n)]^{H^{-1} \bmod L(n)} \bmod n$. Недостатком схемы является то, что значение хэш-функции H от текущего подписываемого документа может оказаться не взаимно простым с $\varphi(n)$, поэтому потребуется видоизменить документ, чтобы обеспечить выполнение условия НОД(H, $\varphi(n)$) = 1.

62. Генерация подписи путем последовательного вычисления значений k и g является проблематичной. Действительно, если предварительно зафиксировать одно из значений k или g, то второе значение будет найти вычислительно сложно (даже если знать секретный ключ γ). При использовании секретного ключа можно реализовать следующий вычислительно эффективный способ генерации подписи: 1) предварительно задаем произвольное значение выражения $Hk - g$, 2) вычисляем значение правой части проверочного сравнения и приравниваем его по модулю δ к сумме $Hk + g$, 3) подпись вычисляем как пару значений k и g. удовлетворяющих сравнениям, возникающим на шагах 1 и 2. Детально процедура генерации подписи описывается следующим образом. Предварительно выбирается случайное число $U < \gamma$ и вычисляется значение $Z \equiv \alpha^U \bmod n$. Затем совместно решаются следующие два сравнения: $Hk - g \equiv U \bmod \gamma$ (1) и $Hk + g \equiv Z \bmod \delta$ (2). При решении системы сравнений (1) и (2) следует учесть, что модули в них различаются. В связи с этим от этой системы сравнений следует перейти к следующей системе уравнений: $\begin{cases} Hk - g = U + N_1\gamma, \\ Hk + g = Z + N_2\delta. \end{cases}$ Очевидно, что целочисленные решения этой системы уравнений при любых значениях натуральных чисел N_1 и N_2 будут удовлетворять также и системе сравнений (1) и (2). Решение системы уравнений в общем виде дает: $\begin{cases} 2Hk = U + N_1\gamma + Z + N_2\delta, & (1) \\ g = (Z + N_2\delta - U - N_1\gamma)/2. & (2) \end{cases}$ Теперь зафиксируем значение N_2 (т. е. приравняем его к нулю или некоторому небольшому натуральному числу) и запишем диофантово уравнение относительно неизвестных N_1 и k: $2Hk - \gamma N_1 = Z + U + N_2\delta$. Это уравнение с большой вероятностью имеет целочисленные решения (значение γ обычно выбирается равным произведению двух больших простых чисел, поэтому с большой веро-

ятностью имеем НОД$(2H, \gamma) = 1$), которые могут быть найдены с помощью расширенного алгоритма Евклида. Фиксированное значение N_2 и вычисленное N_1 подставляем в уравнение (2). Если получим целочисленное значение g, то подпись вычислена. В противном случае выберем новое значение U, для которого повторим процедуру. После нескольких таких попыток с достаточно большой вероятностью будет получено целочисленное значение для g. В результате получим положительные целочисленные значения k и g, которые составят искомую подпись.

63. Генерация подписи состоит в выполнении следующей процедуры: 1) предварительно выбирается случайное число $U < \gamma$, 2) вычисляется значение $Z \equiv H(\alpha^U \bmod n) \bmod \delta$, 3) решается система сравнений: $k - g \equiv$ $\equiv U \bmod \gamma$ (1) и $k \equiv gZ \bmod \delta$ (2). При решении системы сравнений (1) и (2) следует учесть, что модули в них различаются. В связи с этим от этой системы сравнений следует перейти к следующей системе уравнений: $\begin{cases} k - g = U + N_1\gamma, & (1') \\ k = gZ + N_2\delta. & (2') \end{cases}$ Очевидно, что целочисленные решения этой системы уравнений при любых значениях натуральных чисел N_1 и N_2 будут удовлетворять также и системе сравнений (1) и (2). Вычитая первое уравнение из второго, получаем: $g(Z-1) + N_2\delta = U + N_1\gamma$ (3). Фиксируя значение N_1 и решая диофантово уравнение (3) относительно неизвестных g и N_2, можно определить положительное значение элемента подписи g. Полученное значение g подставляем в уравнение (1') и получаем значение второго элемента подписи: $k = U + N_1\gamma + g$. Более простым способом является совместное решение уравнения $k = gZ$, где $Z = [H(\alpha^U \bmod n)] \bmod \delta$, и сравнения (1), что дает следующие формулы: $g = U/(Z-1) \bmod \gamma$ и $k = gZ$.

7.2.2. ЭЦП на основе сложности дискретного логарифмирования

64. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому нечетному делителю $\gamma | p-1$ как к показателю по модулю p. Во втором случае сложность процедуры генерации подписи может быть уменьшена в несколько раз. Вычисление подписи по секретному ключу осуществляется следующим образом. Выбирается случайное значение $U < \gamma$, далее вычисляют $Z = \alpha^U \bmod p$. После этого решают систему из следующих двух сравнений: $U \equiv (k+g) \bmod \gamma$ и $xH + g \equiv k + Z \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы:

$g = \frac{U + Z - xH}{2} \bmod \gamma$ и $k = \frac{U + xH - Z}{2} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod p$ и $R = \alpha^k \bmod p$. В этой схеме ЭЦП можно один раз вычислить параметры U и Z для генерации подписей к многим различным документам, поскольку осуществляется операция деления на число 2, которое является взаимно простым с модулем γ. Данная схема ЭЦП не является стойкой, поскольку допускает практически реализуемую возможность подделки подписи путем представления проверочного уравнения в новом виде, использующем переменную $Z = RS \bmod n$: $S^2 \equiv y^{-H} Z \alpha^Z \bmod p$. Легко найти значения Z, для которых правая часть последнего сравнения будет равна значению, являющемуся квадратичным вычетом по модулю p. Значение S может быть получено путем извлечения квадратного корня по простому модулю p, что не представляется вычислительно сложной задачей. Другой способ подделки подписи связан с выбором следующего представления элементов подписи S и R: $S = \alpha^g \bmod p$ и $R = y^H \alpha^k \bmod p$. Подделка подписи выполняется следующим образом. Выбирается случайное значение $U < \gamma$, вычисляется число $Z = y^H \alpha^U \bmod p$. После этого решают систему из следующих двух сравнений: $U = (k' + g') \bmod \gamma$ и $g' \equiv k' + Z \bmod \gamma$, где неизвестными являются k' и g'. Решая совместно последние два сравнения, получаем: $g' = \frac{U + Z}{2} \bmod \gamma$ и $k' = \frac{U - Z}{2} \bmod \gamma$. Подпись (R', S'), где $S' = \alpha^{g'} \bmod p$ и $R' = \alpha^{k'} \bmod p$, удовлетворяет проверочному уравнению.

65. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p - 1$ как к показателю по модулю p. В последнем случае сложность процедуры генерации подписи может быть уменьшена в несколько раз. Вычисление подписи осуществляется следующим образом. Выбирается случайное число $U < \gamma$ и вычисляется $Z = (\alpha^U \bmod p) \bmod \gamma$. После этого решают систему из следующих двух сравнений: $U = (k + g) \bmod \gamma$ и $xH + g \equiv ky + Z \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $g = \frac{yU + Z - xH}{y + 1} \bmod \gamma$ и $k = \frac{U - Z + xH}{y + 1} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod p$ и $R = \alpha^k \bmod p$. В этой схеме ЭЦП можно один раз

вычислить параметры U и Z для генерации подписей ко многим различным документам. Данная схема ЭЦП не является стойкой, поскольку допускает практически реализуемую возможность подделки подписи путем представления проверочного уравнения в новом виде, использующем переменную $Z = RS \bmod n$: $R \equiv (Zy^H / \alpha^Z)^{\frac{1}{v+1}} \bmod p$. Если НОД$(v+1, \gamma) = 1$, то с помощью расширенного алгоритма Евклида легко найти целочисленное значение $(v+1)^{-1} \bmod \gamma$, а затем вычислить «правильные» значения R и $S = Z/R \bmod p$. Если в процедуру генерации открытого ключа включить требование НОД$(v+1, \gamma) = d \neq 1$, то это несколько усложняет подделку подписи, однако схема ЭЦП все равно не может рассматриваться как стойкая. Выбирая различные значения Z, можно задать значение выражения в скобках равным некоторому вычету степени d. Проверочное уравнение представляется в виде $R^d \equiv$ $\equiv (Zy^H/\alpha^Z)^w \bmod p$, где $w = \dfrac{d}{v+1} \bmod \gamma$ — легко вычислимое целочисленное значение. Таким образом, подделка подписи сводится к вычислению корня d-й степени по простому модулю. Процедура подделки существенно усложнилась, однако не в такой мере, чтобы рассматриваемую схему ЭЦП признать стойкой. Тем более что имеется еще один вычислительно эффективный способ формирования правильной подписи без знания секретного ключа. Второй способ подделки подписи связан с выбором следующего представления элементов подписи S и R: $S = y^{-H}\alpha^g \bmod p$ и $R = \alpha^k \bmod p$. Подделка подписи выполняется следующим образом. Выбирается случайное значение $U < \gamma$, вычисляется число $Z = y^{-H}\alpha^U \bmod p$. После этого решают систему из следующих двух сравнений: $U = (k' + g') \bmod \gamma$ и $g' \equiv k'y + Z \bmod \gamma$, где неизвестными являются k' и g'. Решая совместно последние два сравнения, получаем: $g' = \dfrac{Uy + Z}{1+y} \bmod \gamma$ и $k' = \dfrac{U - Z}{1+y} \bmod \gamma$. Подпись (R', S'), где $S' = y^{-H}\alpha^{g'} \bmod p$ и $R' = \alpha^{k'} \bmod p$, удовлетворяет проверочному уравнению.

66. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p-1$ как к показателю по модулю p. В последнем случае сложность процедуры генерации подписи может быть уменьшена в несколько раз. Вычисление подписи осуществляется следующим образом. Выбирается случайное число $U < \gamma$, по которому вычисляется значение $Z = (\alpha^U \bmod p) \bmod \gamma$. После этого решается система из следующих двух

сравнений: $U=(k+g) \bmod \gamma$ и $xZ+g \equiv kH+1 \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $g=\frac{UH-xZ+1}{H+1} \bmod \gamma$ и $k=\frac{U+xZ-1}{H+1} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S=\alpha^g \bmod p$ и $R=\alpha^k \bmod p$. В этой схеме ЭЦП при использовании простого числа в качестве γ можно один раз вычислить параметры U и Z для генерации подписей ко многим различным документам. Данная схема ЭЦП допускает практически реализуемую возможность подделки подписи путем представления проверочного уравнения в новом виде, использующем переменную $Z=RS \bmod n$: $R \equiv (Zy^Z / \alpha)^{\frac{1}{H+1}} \bmod p$. С большой вероятностью подписываемому сообщению соответствует значение H, удовлетворяющее условию НОД$(H+1, \gamma)=1$, поэтому легко можно найти целочисленное значение $(H+1)^{-1} \bmod p$, а затем вычислить «правильные» значения R и $S=Z/R \bmod p$. Подделка подписи может быть осуществлена еще одним способом. Он связан с представлением элементов подписи S и R в виде: $S=\alpha y^g \bmod p$ и $R=y^k \bmod p$. Подделка подписи выполняется следующим образом. Выбирается случайное значение $U<\gamma$, вычисляется число $Z=\alpha y^U \bmod p$. После этого решают систему из следующих двух сравнений: $U=(k'+g') \bmod \gamma$ и $Z+g' \equiv k'H \bmod \gamma$, где неизвестными являются k' и g'. Решая совместно последние два сравнения, получаем: $g'=\frac{HU-Z}{1+H} \bmod \gamma$ и $k'=\frac{U+Z}{1+H} \bmod \gamma$. Подпись (R', S'), где $S'=\alpha y^{g'} \bmod p$ и $R'=\alpha^{k'} \bmod p$, удовлетворяет проверочному уравнению.

67. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p-1$ как к показателю по модулю p. В последнем случае сложность процедуры генерации подписи может быть уменьшена в несколько раз. Значение α будет использовано в дальнейшем для вычисления элементов подписи. Вычисление подписи осуществляется следующим образом. Выбираются случайные значения U_1 и $U_2 \neq U_1$, не превышающие значения $\gamma-1$, затем вычисляются значения $Z_1=(\alpha^{U_1} \bmod n) \bmod \gamma$ и $Z_2=(\alpha^{U_2} \bmod n) \bmod \gamma$. После этого решают систему из следующих трех сравнений: $g+k+l \equiv U_1 \bmod \gamma$, $g+k-l \equiv U_2 \bmod \gamma$ и $l+kZ_1 \equiv gZ_2+xH+1 \bmod \gamma$, где неизвестными являются k, l и g. Решение системы дает следующие расчетные формулы: $k=\frac{U_1(Z_2-1)+U_2(Z_2+1)+2xH+2}{2(Z_2+Z_1)} \bmod \gamma$.

$l = \dfrac{U_1 - U_2}{2} \bmod \gamma$ и $g = \dfrac{Z_1(U_1 + U_2) + U_1 - U_2 - 2xH - 2}{2(Z_1 + Z_2)} \bmod \gamma$. По полученным значениям k, l и g вычисляются значения $V = \alpha^l \bmod p$, $S = \alpha^g \bmod p$ и $R = \alpha^k \bmod p$. Подделка подписи может быть осуществлена путем представления элементов подписи в виде $V = y^H \alpha^l \bmod p$, $S = \alpha^g \bmod p$ и $R = \alpha^k \bmod p$ или в виде $V = \alpha y^l \bmod p$, $S = y^g \bmod p$ и $R = y^k \bmod p$. В обоих вариантах значения k, l и g вычисляются из системы из трех сравнений, в которые не входит значение секретного ключа (устранена необходимость решения задачи дискретного логарифмирования). Подделка подписи может быть осуществлена также и с помощью метода замены переменных. Введем переменные $Z = SR/V \bmod n$ и $Z' = RSV \bmod n$. Выразим V и R через Z, Z' и S: $V = (Z'/Z)^{1/2} \bmod p$ и $R = (ZZ)^{1/2}/S \bmod p$. Теперь проверочное уравнение приобретает вид $\left(\dfrac{Z'}{Z}\right)^{1/2}\left(\dfrac{\sqrt{ZZ'}}{S}\right)^{Z'} = S^Z y^H \alpha \bmod p$. Из последнего соотношения получаем формулу для вычисления параметра S: $S = (Z'^{(Z'+1)/2} Z^{(Z'-1)/2} y^{-H} \alpha^{-1})^{1/(Z+Z')} \bmod p$. Второй способ подделки подписи по сравнению с первым имеет большее значение трудоемкости, поэтому первый вариант подделки подписи является предпочтительным для потенциального нарушителя.

68. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p-1$ как к показателю по модулю p. В последнем случае сложность процедуры генерации подписи может быть уменьшена в несколько раз. Вычисление подписи осуществляется следующим образом. Выбираются случайные значения U_1 и $U_2 \neq U_1$, не превышающие значения $\gamma - 1$, затем вычисляются значения $Z_1 = (\alpha^{U_1} \bmod p) \bmod \gamma$ и $Z_2 = (\alpha^{U_2} \bmod p) \bmod \gamma$. После этого решают систему из следующих трех сравнений: $g + kH + l \equiv U_1 \bmod \gamma$, $g + k + lH \equiv U_2 \bmod \gamma$ и $kZ_1 \equiv gZ_2 + x + H \bmod \gamma$, где неизвестными являются k, l и g. Решение системы сравнений дает значения k, l и g, по которым вычисляются значения $V = \alpha^l \bmod p$, $S = \alpha^g \bmod p$ и $R = \alpha^k \bmod p$, удовлетворяющие проверочному уравнению. Попытки подделать подпись путем представления значений R и S в виде $R = \alpha^t y^u \bmod p$ и $S = \alpha^z y^w \bmod p$ приводят к вычислительно сложным процедурам, поскольку трудно использовать переменную V в качестве подгоночного параметра (благодаря тому, что значение V используется в правой и левой частях проверочного уравнения, причем в степени правой части оно возводится в степень H). Однако эта схема ЭЦП не

является безопасной. Подделка подписи легко осуществляется, представляя элементы подписи в виде $R = (y\alpha^H)^k \bmod p$, $S = (y\alpha^H)^g \bmod p$ и $V = (y\alpha^H)^l \bmod p$.

69. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p-1$ как к показателю по модулю p. В последнем случае сложность процедуры генерации подписи может быть уменьшена в несколько раз. Вычисление подписи осуществляется следующим образом. Выбираются случайные значения k' и g', по которым вычисляются значения $U = (k' + yg') \bmod \gamma$ и $Z = (\alpha^U \bmod p) \bmod \gamma$. После этого решают систему из следующих двух сравнений: $H + g = kZ + x \bmod \gamma$ и $k + yg = U \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $k = \dfrac{U + yH - xy}{1 + yZ} \bmod \gamma$ и $g = \dfrac{UZ - H + x}{1 + yZ} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod p$ и $R = \alpha^k \bmod p$. В этой схеме ЭЦП можно один раз вычислить параметры U и Z для генерации подписей ко многим различным документам. Подделка подписи может быть осуществлена путем представления элементов подписи в виде $S = y\alpha^g \bmod p$ и $R = \alpha^k \bmod p$ или в виде $S = \alpha^{-H} y^g \bmod p$ и $R = y^k \bmod p$. В обоих вариантах значения k и g вычисляются из системы из двух сравнений, в которые не входит значение секретного ключа (тем самым обходится сложная задача дискретного логарифмирования). Подделка подписи может быть осуществлена также и с помощью метода замены переменных. Введем переменную $Z = RS^v \bmod p$ и выразим R через Z и S: $R = Z / S^v \bmod p$. Теперь проверочное уравнение приобретает вид $\alpha^H S = y(Z / S^v)^Z \bmod p$. Из последнего соотношения получаем формулу для вычисления параметра S:

$S = \left(\dfrac{yZ^Z}{\alpha^H} \right)^{\frac{1}{Zy+1}} \bmod p$. Легко выбрать значение Z, удовлетворяющее условию НОД$(Zy + 1, p - 1) = 1$. В этом случае легко вычисляется значение S, а затем и R. Два последних значения образуют подпись (R, S), удовлетворяющую исходному проверочному уравнению. Таким образом, рассмотренная схема подписи не является безопасной.

70. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p-1$ как к показателю по модулю p. В последнем случае сложность процедуры генерации подписи может быть уменьшена в несколько раз.

Вычисление подписи осуществляется следующим образом. Выбираются случайные значения k' и g', по которым вычисляются значения $U = (k' + g') \bmod \gamma$ и $Z = (\alpha^{U'} \bmod p) \bmod \gamma$. После этого решают систему из следующих двух сравнений: $(k + g) = U \bmod \gamma$ и $H + g \equiv kyZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $g = \dfrac{yUZ - H}{1 + yZ} \bmod \gamma$ и $k = \dfrac{H + U}{1 + yZ} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod n$ и $R = \alpha^k \bmod n$. Данная схема ЭЦП не является стойкой. Это видно из того, что при формировании подписи не используется секретный ключ. Возможны и другие варианты формирования подписи без использования секретного ключа.

71. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p - 1$ как к показателю по модулю p. В последнем случае сложность процедуры генерации подписи может быть уменьшена в несколько раз. Вычисление подписи осуществляется следующим образом. Выбираются случайные значения k' и g', по которым вычисляются значения $U = (k' + g') \bmod \gamma$ и $Z = (\alpha^{U'} \bmod p) \bmod \gamma$. После этого решают систему из следующих двух сравнений: $(k + g) = U \bmod \gamma$ и $H + g \equiv kZ + xZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $g = \dfrac{ZU + xZ - H}{Z + 1} \bmod \gamma$ и $k = \dfrac{U - xZ + H}{Z + 1} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod p$ и $R = \alpha^k \bmod p$. В этой схеме ЭЦП можно один раз вычислить параметры U и Z для генерации подписей ко многим различным документам. Подделка подписи может быть осуществлена путем представления элементов подписи в виде $S = \alpha^{-H} y^g \bmod p$ и $R = y^k \bmod p$. Значения k и g вычисляются из системы из двух сравнений, в которые не входит значение секретного ключа (тем самым обходится проблема дискретного логарифмирования). Подделка подписи может быть осуществлена также и с помощью метода замены переменных. Введем переменную $Z = RS \bmod p$ и выразим R через Z и S: $R = Z / S \bmod p$. Теперь проверочное уравнение приобретает вид $\alpha^H S = (yZ/S)^Z \bmod p$. Из последнего соотношения получаем формулу для вычисления параметра S: $S = \left(\dfrac{y^Z Z^Z}{\alpha^H} \right)^{\frac{1}{Z+1}} \bmod p$. Легко выбрать значение Z, удовлетворяющее условию НОД$(Z + 1, p - 1) = 1$. После этого легко вычислить S, а затем и

R, т. е. «правильную» подпись (R, S), удовлетворяющую исходному проверочному уравнению. Таким образом, рассмотренная схема допускает подделку подписи.

72. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p-1$ как к показателю по модулю p. Вычисление подписи осуществляется следующим образом. Выбирается случайное значение $U < \gamma$ и вычисляется $Z = (\alpha^U \bmod p) \bmod \gamma$. После этого решают систему из следующих двух сравнений: $(k+g) = U \bmod \gamma$ и $H + g \equiv k + xZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы: $g = \dfrac{U + xZ - H}{2} \bmod \gamma$ и $k = \dfrac{H + U - xZ}{2} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S = \alpha^g \bmod p$ и $R = \alpha^k \bmod p$. В этой схеме ЭЦП можно один раз вычислить параметры U и Z для генерации подписей ко многим различным документам. Рассматриваемая схема ЭЦП небезопасна. Имеется несколько вариантов подделки подписи. Например, без знания секретного ключа «правильные» значения элементов подписи можно найти, представляя их в виде $S = \alpha^{-H} y^g \bmod p$ и $R = y^k \bmod p$ или в виде $S = y^g \bmod p$ и $R = \alpha^H y^k \bmod p$. В обоих вариантах значения k и g вычисляются из системы из двух сравнений, в которые не входит значение секретного ключа, что устраняет проблему дискретного логарифмирования. Подделка подписи может быть осуществлена также и с помощью метода замены переменных. Введем переменную $Z = RS \bmod p$ и выразим R через Z и S: $R = Z/S \bmod p$. Теперь проверочное уравнение приобретает вид $\alpha^H S = (Z/S) y^Z \bmod p$. Из последнего соотношения получаем формулу для вычисления параметра S: $S = \left(\dfrac{y^Z Z}{\alpha^H} \right)^{\frac{1}{2}} \bmod p$.

73. В качестве числа α можно использовать первообразный корень по модулю p или число, относящееся к достаточно большому делителю $\gamma | p-1$ как к показателю по модулю p. В последнем случае сложность процедуры генерации подписи может быть уменьшена в несколько раз. Вычисление подписи осуществляется следующим образом. Выбираются случайные значения k' и g', по которым вычисляются значения $U = (yk' + g') \bmod \gamma$ и $Z = (\alpha^U \bmod p) \bmod \gamma$. После этого решают систему из следующих двух сравнений: $yk + g = U \bmod \gamma$ и $g + k = H + xZ \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие

расчетные формулы: $g=\dfrac{xyZ+Hy-U}{y-1} \bmod \gamma$ и $k=\dfrac{U-xZ-H}{y-1} \bmod \gamma$. По полученным значениям k и g вычисляются значения $S=\alpha^g \bmod n$ и $R=\alpha^k \bmod n$. В этой схеме ЭЦП можно один раз вычислить параметры U и Z для генерации подписей ко многим различным документам. Рассматриваемая схема ЭЦП небезопасна. Например, без знания секретного ключа «правильные» значения элементов подписи можно найти, представляя их в виде $S=\alpha^H y^g \bmod p$ и $R=y^k \bmod p$. Значения k и g вычисляются из системы из двух сравнений, в которые не входит значение секретного ключа, что устраняет проблему дискретного логарифмирования. Подделка подписи может быть осуществлена также и с помощью метода замены переменных. Введем переменную $Z=R^x S \bmod p$ и выразим S через Z и R: $S=Z/R^x \bmod p$. Теперь проверочное уравнение приобретает вид $ZR^{1-x}=\alpha^H y^Z \bmod p$. Из последнего соотношения получаем формулу для вычисления параметра R: $R=\left(\dfrac{\alpha^H y^Z}{Z}\right)^{\frac{1}{1-x}} \bmod p$. Если потребовать выбор такого секретного ключа, для которого НОД$(y-1, p-1)\neq 1$, то это несколько усложняет задачу подделки подписи по второму варианту, но не затрагивает трудоемкость первого варианта подделки подписи. Первый способ подделки подписи может быть предотвращен, если несколько модифицировать проверочное уравнение, например, можно задать в виде: $RS=\alpha^{H(RS^x \bmod p) y^{(RS^x \bmod p) \bmod q}} \bmod p$, где q -- достаточно большое простое число, не являющееся делителем $p-1$ (предполагается, что по размеру число q существенно меньше модуля p). Смысл такой модернизации состоит в том, что теперь оба множителя, представляющие степени чисел α и y, являются зависимыми от R и S. Однако рассмотренная модернизация схемы ЭЦП не устраняет второй способ подделки подписи.

74. Перепишем проверочное уравнение в виде $R=S(\alpha^H y)^{(RS \bmod p)} \bmod p$. Теперь видно, что проблему дискретного логарифмирования потенциальный нарушитель может обойти, если представит элементы подписи в виде $R=(\alpha^H y)^k \bmod p$ и $S=(\alpha^H y)^g \bmod p$. Далее вычисление подписи без знания секретного ключа может быть осуществлено следующим образом. Выбирается случайное значение $U<\gamma$, далее вычисляют $Z=(\alpha^H y)^U \bmod p$. После этого решают систему из следующих двух сравнений: $U=(k+g) \bmod \gamma$ и $k \equiv g+Z \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы:

$g = \frac{U - Z}{2} \bmod \gamma$ и $k = \frac{U + Z}{2} \bmod \gamma$. По полученным значениям k и g вычисляются значения S и R.

75. Чтобы сформировать подпись, удовлетворяющую данному проверочному уравнению, можно воспользоваться следующим путем: 1) выберем случайное значение $U < p - 1$; 2) вычислим $k = (y^H \alpha^U \bmod p) \bmod (p - 1)$; если НОД$(p - 1, k) \neq 1$, то перейти к шагу 1; 3) вычислим $S = U/k \bmod (p - 1)$ и $R = \alpha^k \bmod p$. Легко проверить, что полученная подпись (R, S) удовлетворяет проверочному уравнению. Поскольку при генерации подписи мы не использовали секретный ключ x, то это есть процедура подделки подписи, которой может воспользоваться нарушитель.

76. Первое проверочное уравнение допускает следующую процедуру подделки подписи. Будем искать элемент подписи R в виде $R = y^k \bmod p$. Если на выбор k и S наложить требование $k + S = U \bmod \gamma$ (1), где U — некоторое фиксированное значение, то тогда получаем $y^k = y^{(\alpha^H y^U \bmod p)} \bmod p$. Следовательно, в качестве k можно выбрать значение $k = (\alpha^H y^U \bmod p) \bmod \gamma$, а элемент S вычислить по k, воспользовавшись формулой (1). Этот способ формирования правильной подписи без использования секретного ключа неприменим ко второму проверочному уравнению, поскольку выражение в скобках требует представить элемент R как степень числа α, а само проверочное уравнение требует представления этого элемента в виде степени открытого ключа. При использовании секретного ключа x оба требования могут быть удовлетворены, т. е. имеется вычислительно эффективная процедура генерации подписи, тогда как подделка подписи требует решения задачи дискретного логарифмирования. Процедура генерации подписи может быть представлена в виде следующего алгоритма: 1) выбрать случайное значение $U < \gamma$; 2) вычислить $Z = (y^H \alpha^U \bmod p) \bmod \gamma$ и $k = xZ \bmod \gamma$; 3) вычислить $R = \alpha^k \bmod p$ и $S = U - k \bmod \gamma$.

77. Оба проверочных уравнения задают похожие схемы цифровой подписи. На первый взгляд вторая схема представляется более замысловатой, поскольку при представлении элемента R в виде степени α^k она предполагает выполнение вычислений над α^k по двум различным модулям p и γ. Однако эта проблема преодолевается при представлении R в виде $R = \alpha^k \bmod (p\gamma)$. Это приводит к соответствующему увеличению длины подписи за счет увеличения размера элемента R (при этом, очевидно, стойкость схемы определяется выбором модуля p). Рассмотрим процедуры формирования подписи в обеих схемах. В первой схеме форми-

рование подписи можно осуществить по алгоритму: 1) выбрать случайное значение $U < \gamma$; 2) вычислить $Z = (\alpha^{U'} \bmod p) \bmod \gamma$; 3) вычислить $k = (H - xZ) \bmod \gamma$; 4) сформировать элементы подписи $R = \alpha^k \bmod p$ и $S = U/k \bmod \gamma$. Во второй схеме формирование подписи можно осуществить по алгоритму: 1) выбрать случайное значение $U < \gamma$; 2) вычислить $Z = \alpha^{U'} \bmod \gamma$; 3) вычислить $k = (H - xZ) \bmod \gamma$; если НОД$(\gamma - 1, k) \neq 1$, то перейти к шагу 1; 4) сформировать элементы подписи $R = \alpha^k \bmod (p\gamma)$ и $S = U/k \bmod (\gamma - 1)$. Сравнение показывает, что во втором случае процедура генерации подписи имеет несколько более высокую трудоемкость. Таким образом, некоторое предпочтение можно отдать схеме ЭЦП, задаваемой первым проверочным уравнением.

78. При фиксировании одного из элементов подписи (g, R) даже по известному секретному ключу x сложно вычислить второй элемент. Для вычисления подписи следует представить число R в виде $R = \alpha^k \bmod p$ или в виде $R = y^k \bmod n$. Остановимся на первом варианте. Зафиксируем некоторое произвольное значение $U < \gamma$ и рассмотрим область пар значений k и g, удовлетворяющих условию $kg \equiv U \bmod \gamma$ (1). Последнее условие задает некоторый фиксированный параметр $Z = \alpha^{U'} \bmod p$. Подставляя $R = \alpha^k \bmod p$ в проверочное соотношение, видим, что оно выполняется, если пара значений (k, g) является также и некоторым решением сравнения $kHg^2 \equiv x + Z \bmod \gamma$ (2). Искомая пара значений может быть найдена как решение системы из сравнений (1) и (2): $g = \dfrac{x+Z}{HU} \bmod \gamma$ и $k = \dfrac{HU^2}{x+Z} \bmod \gamma$.

79. При фиксировании одного из элементов подписи (g, R) даже по известному секретному ключу x сложно вычислить второй элемент. Для вычисления подписи элемент R можно представить в виде $R = \alpha^k \bmod p$. В этом случае получаем следующую систему сравнений, которым должны удовлетворять значения k и g: $k + g \equiv U \bmod \gamma$ (1) и $k(H - g) \equiv xZ \bmod \gamma$ (2). Совместное решение этих сравнений приводит к следующему квадратному сравнению: $g^2 - (U + H) \equiv xZ - UH \bmod \gamma$ (3). Решение этого сравнения потребует выполнения операции извлечения квадратных корней по модулю. Эта задача существенно упрощается, если модуль γ является сравнимым с числом 3 по модулю 4. Если это требование выполнено, то решение задачи извлечения корня сводится к выполнению операции возведения в степень (см., например, схему ЭЦП Рабина). Решение сравнения (3) дает два корня:

$$g \equiv \sqrt{xZ + (U-H)^2/4} + (U+H)/2 \bmod \gamma \text{ или}$$

$$g \equiv -\sqrt{xZ + (U-H)^2/4} + (U+H)/2 \bmod \gamma.$$

Значения k, соответствующие этим корням, легко найти по (1). Если параметры схемы ЭЦП выбраны таким образом, что выполняется условие $\gamma \equiv 3 \bmod 4$, то решения сравнения (3) вычисляются по формулам:

$$g \equiv \left(xZ + \frac{(U-H)^2}{4} \right)^{\frac{\gamma+1}{4}} + \frac{U+H}{2} \bmod \gamma \text{ или}$$

$$g \equiv \frac{U+H}{2} - \left(xZ + \frac{(U-H)^2}{4} \right)^{\frac{\gamma+1}{4}} \bmod \gamma.$$

80. Первая схема не является стойкой, поскольку допускает возможность формирования подписи без использования секретного ключа. Подделка подписи может быть осуществлена с использованием представления элемента подписи R в виде $R = y^k \bmod p$. В этом случае при условии $kS \bmod \gamma = U = \text{const}$ имеем $Z = (\alpha y^U \bmod p) \bmod \gamma$ и два сравнения: $kS \equiv U \bmod \gamma$ (1′) и $k \equiv HZ \bmod \gamma$ (2′). Совместное решение этой пары сравнений позволяет найти правильное значение подписи без использования секретного ключа. Для второй схемы ЭЦП такой подход к формированию подписи не может быть применен, поскольку значение α не может быть «устранено» путем представления параметра R в виде $R = \alpha y^k \bmod p$, так как в этом случае имеются проблемы с фиксированием значения Z, которое равно $Z = (\alpha^S y^{kS} \bmod p) \bmod \gamma$. При использовании секретного ключа процедура генерации подписи достаточно проста и может использовать представление R в виде $R = y^k \bmod p$, $R = (\alpha y)^k \bmod p$ или $R = \alpha^k \bmod p$. Например, в последнем случае приходим к следующему алгоритму формирования подписи: 1) выбрать случайное значение $U < \gamma$; 2) вычислить $Z = (\alpha^U \bmod p) \bmod \gamma$; 3) решить систему сравнений $kS \equiv U \bmod \gamma$ (1) и $k \equiv 1 + xHZ \bmod \gamma$ (2); 4) используя значения S и k, удовлетворяющие системе сравнений (1) и (2), сформировать подпись (R, S), где $R = \alpha^k \bmod p$.

81. В исходной схеме подпись формируется с использованием представления элемента R в виде $R = \alpha^k \bmod p$. В этом случае при условии $k + xg \bmod \gamma = U = \text{const}$ имеем $Z = (\alpha^U \bmod p) \bmod \gamma$ и два совместно решаемых сравнения: $k + xg \equiv U \bmod \gamma$ (1) и $k \equiv HZ \bmod \gamma$ (2). Второе сравнение позволяет сразу вычислить значение степени k, соответствующее «правильному» значению элемента R. Второй элемент подписи

(R, g) определяется по формуле: $g = \frac{U - HZ}{x} \bmod \gamma$. Необходимость выполнения операции деления на значение секретного ключа обусловливает требование НОД$(\gamma, x) = 1$. Если использовать простое значение γ, то при выборе секретного ключа достаточно выполнить условие $x < \gamma$. Преобразование исходной схемы в схему с восстановлением сообщения может быть осуществлено, если сообщение M встраивать в параметр R, который следует перенести в правую часть и формировать его как произведение M и некоторой степени числа α: $R = M\alpha^k \bmod p$. В этом случае произведение всех степеней числа α в правой части сократится, оставив значение M. Таким образом, мы приходим к следующему проверочному уравнению, задающему схему ЭЦП с восстановлением сообщения: $M = R\alpha^{(R^{-1}g \bmod p)} \bmod p$ (значение хэш-функции может не фигурировать в проверочном уравнении, поскольку сообщение появится непосредственно в процессе проверки подлинности подписи). Для формирования подписи решается система сравнений $k + xg \equiv U \bmod \gamma$ (1′) и $k \equiv -Z \bmod \gamma$ (2′), где $Z = (M\alpha^{H} \bmod p) \bmod \gamma$. Элементы подписи (R, g) вычисляются по формулам $R = M\alpha^{-Z} \bmod p$ и $g = \frac{U + Z}{x} \bmod \gamma$.

82. В исходной схеме подпись формируется, используя представление элемента R в виде $R = y^k \bmod p$. В этом случае при условии $xk + g \bmod \gamma = U = \text{const}$ имеем $Z = (\alpha^{H} \bmod p) \bmod \gamma$ и два совместно решаемых сравнения: $xk + g \equiv U \bmod \gamma$ (1) и $kH \equiv Z \bmod \gamma$ (2). Второе сравнение позволяет сразу вычислить значение степени k, соответствующее «правильному» значению элемента R: $k \equiv Z / H \bmod \gamma$. Второй элемент подписи (R, g) определяется по формуле: $g = U - xZ / H \bmod \gamma$. Необходимость выполнения операции деления на значение хэш-функции от подписываемого документа обусловливает требование НОД$(\gamma, H) = 1$. Если использовать простое значение γ, то при выборе секретного ключа достаточно выполнить условие $H < \gamma$. Преобразование исходной схемы в схему с восстановлением сообщения может быть осуществлено, если сообщение M встраивать в параметр R, который следует перенести в правую часть и формировать как произведение M и некоторой степени числа α: $R = M^{y^{-1}}\alpha^k \bmod p$ (учитываем, что в исходном уравнении значение R возводится в степень H, которую мы предполагаем заменить на y). В этом случае при правильном значении подписи произведение всех степеней числа α в правой части сократится, оставив значение M. Таким образом, мы приходим к следующему

проверочному уравнению, задающему схему ЭЦП с восстановлением сообщения: $M = R^y y^{(R\alpha^g \bmod p)} \bmod p$ (3). Процедура формирования подписи может быть основана на решении системы сравнений $k + g \equiv U \bmod \gamma$ (1′) и $ky \equiv -xZ \bmod \gamma$ (2′), где $Z = (M^{y^{-1}} \alpha^{U} \bmod p) \bmod \gamma$. Элементы подписи (R, g) вычисляются по формулам $R = M^{1/y} \alpha^{-xZ/y} \bmod p$ и $g = \dfrac{yU + xZ}{y} \bmod \gamma$. Значение хэш-функции от подписываемого документа можно использовать как один из параметров проверочного уравнения, например, заменяя в (3) y на H: $M = R^H y^{(R\alpha^g \bmod p)} \bmod p$. В этом случае проверка подлинности сообщения совмещается с проверкой подлинности подписи.

83. В заданной схеме ЭЦП подпись формируется, используя представление элемента R в виде $R = H^{-1} M \alpha^k \bmod p$. Для формирования подписи решается система сравнений $k + xg \equiv U \bmod \gamma$ (1) и $k \equiv -(x+1)Z \bmod \gamma$ (2), где $Z = (H^{-1} M \alpha^{U} \bmod p) \bmod \gamma$. Элементы подписи (R, g) вычисляются по формулам: $R = H^{-1} M \alpha^{-(x+1)Z} \bmod p$ и $g = \dfrac{U + (x+1)Z}{x} \bmod \gamma$. Контроль подлинности сообщения обеспечивается проверкой равенства полученного значения H и хэш-функции, вычисленной от восстановленного (в процессе проверки подписи) сообщения M. Проверочное уравнение $M = HRy\alpha^{(Ry^g \bmod p)} \bmod p$ задает схему, которая по стойкости примерно эквивалентна рассмотренному выше варианту. Вычисление подписи можно осуществлять, используя представление параметра R в виде $R = H^{-1} M \alpha^k \bmod p$ или в виде $R = y^{-1} H^{-1} M \alpha^k \bmod p$. Схема ЭЦП, соответствующая проверочному уравнению $M = HR\alpha y^{(Ry^g \bmod p)} \bmod p$, имеет явную слабость, которая заключается в возможности подделки подписи, т. е. подпись можно сформировать без использования секретного ключа. Для этого параметр R представляется в виде $R = \alpha^{-1} H^{-1} M y^k \bmod p$.

84. Указанное в условии задачи преобразование предполагает, что при генерации подписи элемент подписи R будет представляться в виде $R = M\alpha^k \bmod p$. Однако в степени при основании α параметр R возводится в степень g, которая будет определена только после выполнения процедуры генерации подписи. В свою очередь без фиксирования значения в скобках генерация «правильного» значения подписи является трудной задачей. Наличие множителя M в выражении $R = M\alpha^k \bmod p$

не позволяет зафиксировать значение $R^g y^\varepsilon \bmod p$ заданием достаточно простого соотношения между значениями k и g. Учитывая это, можно сделать вывод, что указанная модификация в проверочном соотношении несостоятельна. В схеме ЭЦП, соответствующей заданному проверочному равенству, подпись формируется, используя представление элемента R в виде $R = \alpha^k \bmod p$. Для формирования подписи решается система сравнений $kg + xg \equiv U \bmod \gamma$ (1) и $k \equiv -H - Z \bmod \gamma$ (2), где $Z = (\alpha^l \bmod p) \bmod \gamma$. Решение системы сравнений (1) и (2) приводит к следующим формулам для вычисления подписи (R, g): $R = \alpha^{-H-Z} \bmod p$ и $g = \dfrac{U}{x - H - Z} \bmod \gamma$.

85. Подпись к некоторому документу, представленному хэш-функцией H, формируется следующим образом. Значение R представляется в виде $R = Hy^k \bmod p$. Берется некоторое произвольное значение $U < \gamma$. Затем составляется система сравнений $k + g \equiv U \bmod \gamma$ (1) и $xk \equiv Z \bmod \gamma$ (2), где $Z = Hy^l \bmod p$, из которой вычисляются элементы подписи $g = U - Z/x \bmod \gamma$ и $R = H\alpha^Z \bmod p$. При необходимости формирования подписи вслепую выбирается случайное число $0 < \varepsilon < \gamma$ и вычисляется коэффициент $K = y^\varepsilon \bmod p$. После этого значение H маскируется: $H' = HK \bmod p$. Полученное значение H' представляется для формирования подписи (R', g'). По подписи к H' вычисляется подпись (R, g), соответствующая значению хэш-функции H: $R = R'/K \bmod p$ и $g = g' + \varepsilon \bmod \gamma$. Полученная таким образом подпись (R, g) и значение H удовлетворяют проверочному уравнению. Действительно, из $R' = H'\alpha^{(R'y^{g'} \bmod p)} \bmod p$ следует $Ry^\varepsilon = Hy^\varepsilon \alpha^{(Ry^\varepsilon y^{g-\varepsilon} \bmod p)} \bmod p$, т. е. выполняется равенство $R = H\alpha^{(Ry^g \bmod p)} \bmod p$. Рассмотренная схема слепой подписи не обеспечивает решения задачи анонимности, поскольку подписывающий может определить, что подпись (R, g), соответствующая значению H, была восстановлена из подписи (R', g'), соответствующей значению H' (предполагаем, что подписывающий регистрирует все доступные ему данные, связанные с процедурой слепой подписи). Критерием для установления этого факта может служить выполнение соотношения $H'/H = R'/R = y^{g-g'} \bmod p$.

86. Подпись к некоторому документу, представленному хэш-функцией H, формируется следующим образом. Подписывающий, используя известное ему разложение модуля, проверяет, является ли значение H квадратичным вычетом по модулю n. Если нет, то он модифицирует документ без изменения его смыслового содержания или просит это сделать того,

кто подготовил документ к подписи. После нескольких таких попыток будет получено значение H, которое является квадратичным вычетом. Подпись формируется как один из четырех корней из H. Если требуется получить подпись вслепую, то выбирается случайное число t, вычисляется маскирующий коэффициент $K = t^2 \bmod n$, который по построению является квадратичным вычетом, и значение $H' = HK \bmod n$. Значение H' представляется для формирования подписи к нему. Если окажется, что H' не является квадратичным вычетом, то документ модифицируется и по новому значению H формируется новое значение H'. Когда будет получено H', являющееся квадратичным вычетом, подписывающий формирует подпись S', извлекая из H' квадратный корень. Подпись к H восстанавливается из S' по формуле $S = S'/t \bmod n$. Действительно, такое значение S удовлетворяет проверочному уравнению: $S^2 = (S'/t)^2 = S'^2/K = H'/K = H \bmod n$. Имея образцы хэш-функций H и H' и соответствующих им подписей S и S', подписывающий не может раскрыть анонимность процедуры слепой подписи, поскольку пара значений H и S может быть сопоставлена произвольной паре значений S'' и $H'' = (S'')^2 \bmod n$ из множества подписей, сформированных вслепую. Однако практического значения эта схема слепой подписи не имеет, поскольку нарушитель может специальным образом подготовить значение H' и после получения подписи S' легко факторизовать модуль. Действительно, выбрав произвольное значение k и вычислив $H = k^2 \bmod n$, нарушитель восстанавливает значение S, которое с высокой вероятностью не равно $\pm k \bmod n$. Если это произойдет, то он вычислит один из делителей модуля как НОД$(k \pm S, n) > 1$. Таким образом, рассмотренная схема не имеет практического значения, так как она не является стойкой.

87. При формирования подписи вслепую выбирается случайный коэффициент $K < p$, с помощью которого осуществляется маскирование хэш-функции H, соответствующей документу, к которому формируется подпись: $H' = HK \bmod p$. Полученное значение H' представляется для формирования подписи (R', g'). По подписи к H' вычисляется подпись (R, g), соответствующая значению хэш-функции H: $R = R'K \bmod p$ и $g = g'$. Полученная таким образом подпись (R, g) и значение H удовлетворяют проверочному уравнению. Однако рассмотренная схема слепой подписи не обеспечивает решения задачи анонимности, поскольку подписывающий может легко определить, что подпись (R, g), соответствующая значению H, была восстановлена из подписи (R', g'), соответствующей значению H' (очевидным критерием для установления этого факта является равенство $g = g'$).

88. Подпись к некоторому документу, представленному хэш-функцией H ($H < \gamma$), формируется следующим образом. Значение R представляется в виде $R = H^{-1}y^{k} \bmod p$. Берется некоторое произвольное значение $U < \gamma$. Затем составляется система сравнений $2k + g \equiv U \bmod \gamma$ (1) и $xk \equiv Z \bmod \gamma$ (2), где $Z = H^{-1}y^{l} \bmod p$, из которой вычисляются элементы подписи $g = U - 2Z/x \bmod \gamma$ и $R = H^{-1}\alpha^{Z} \bmod p$. Формирование подписи вслепую осуществляется следующим путем. Выбирается случайное число $0 < \varepsilon < \gamma$ и вычисляется коэффициент $K = y^{\varepsilon} \bmod p$. После этого значение H маскируется: $H' = HK \bmod p$. Полученное значение H' представляется для формирования подписи (R', g'). По подписи к H' вычисляется подпись (R, g), соответствующая значению хэш-функции H: $R = R'K \bmod p$ и $g = g' - \varepsilon \bmod \gamma$. Полученная таким образом подпись (R, g) и значение H удовлетворяют проверочному уравнению. Действительно, из $R'H' = \alpha^{(R'^{2}H'y^{g'} \bmod p-1} \bmod p$ следует $(R/K)HK = \alpha^{(R^{2}y^{-2\varepsilon}Hy^{\varepsilon}y^{g+\varepsilon} \bmod p-1)} \bmod p$, т. е. проверочное соотношение выполняется. Анонимность данной схемой не обеспечивается, так как подписывающий может определить, что подпись (R, g), соответствующая значению H, была восстановлена из подписи (R', g'), соответствующей значению H' (предполагается, что подписывающий регистрирует сформированные им подписи). Критерием для установления этого факта может служить выполнение соотношения $H'/H = R/R' = y^{g'-g} \bmod p$.

89. Подпись к некоторому документу, представленному хэш-функцией H, формируется следующим образом. Значение R представляется в виде $R = H\alpha^{k} \bmod p$. Берется некоторое произвольное значение $U < \gamma$. Затем из системы сравнений $k + g \equiv U \bmod \gamma$ (1) и $k \equiv xZ \bmod \gamma$ (2), где $Z = H\alpha^{l} \bmod p$, вычисляются значения $g = U - xZ \bmod \gamma$ и $R = H\alpha^{xZ} \bmod p$. При формировании подписи вслепую выбирается случайное число $\varepsilon < \gamma$ и вычисляется коэффициент $K = \alpha^{\varepsilon} \bmod p$, а затем значение H зашифровывается: $H' = HK \bmod p$. Полученное значение H' представляется для формирования подписи (R', g'). По подписи к H' вычисляется подпись (R, g), соответствующая значению хэш-функции H: $R = R'/K \bmod p$ и $g = g' + \varepsilon \bmod \gamma$. Полученная таким образом подпись (R, g) и значение H удовлетворяют проверочному уравнению. Действительно, из $R' = H'y^{(R'\alpha^{g'} \bmod p)} \bmod p$ следует $R\alpha^{\varepsilon} = H\alpha^{\varepsilon}y^{(R\alpha^{\varepsilon}\alpha^{g-\varepsilon} \bmod p)} \bmod p$ и $R = Hy^{(R\alpha^{g} \bmod p)} \bmod p$. Рассмотренная схема слепой подписи не обеспечивает решения задачи анонимности, поскольку подписывающий мо-

жет определить, что подпись (R, g), соответствующая значению H, была восстановлена из подписи (R', g'), соответствующей значению H'. Критерием для установления этого факта может служить выполнение соотношения $H'/H = R'/R = \alpha^{g-g'} \bmod p$.

90. Рассмотрим процедуру формирования подписи к некоторому документу, представленному хэш-функцией H ($H < \gamma$). Значение R представляется в виде $R = H^2 y^k \bmod p$. Берется некоторое произвольное значение $U < \gamma$ и составляется система сравнений $k + g \equiv U \bmod \gamma$ (1) и $xk \equiv Z \bmod \gamma$ (2), где $Z = H^3 y^U \bmod p$, из которой вычисляются элементы подписи (R, g): $g = U - Z/x \bmod \gamma$ и $R = H^2 \alpha^Z \bmod p$. Формирование подписи вслепую осуществляется следующим путем. Выбирается случайное число $0 < \varepsilon < \gamma$ и вычисляется коэффициент $K = y^\varepsilon \bmod p$. После этого маскируется значение H: $H' = HK \bmod p$. Значение H' представляется для формирования подписи (R', g'), из которой восстанавливается подпись (R, g), соответствующая значению хэш-функции H: $R = R'K^{-2} \bmod p$ и $g = g' + 3\varepsilon \bmod \gamma$. Полученная таким образом подпись (R, g) и значение H удовлетворяют проверочному уравнению. Действительно, из $R' = H'^2 \alpha^{(H'R' y^{g'} \bmod p)} \bmod p$ следует $Ry^{2\varepsilon} = H^2 y^{2\varepsilon} \times \times \alpha^{(Hy^\varepsilon Ry^{2\varepsilon} y^{g-3\varepsilon} \bmod p)} \bmod p$, т. е. проверочное соотношение выполняется. Анонимность данной схемой не обеспечивается, так как, используя в качестве критерия выполнимость соотношений $(H'/H)^2 = R'/R \bmod p$ и $(H'/H)^3 = \alpha^{g-g'} \bmod p$, подписывающий может определить, что подпись (R, g), соответствующая значению H, была восстановлена из подписи (R', g'), соответствующей значению H'.

91. В указанных схемах вычисление секретного ключа по известной подписи является вычислительно сложной задачей. Подделка подписи в схеме, соответствующей первому уравнению проверки, вычислительно невозможна, а во второй схеме осуществляется достаточно просто. Выбираются случайные числа $U < \gamma$ и $U' < \gamma$, вычисляются значения $Z = \alpha^U \bmod p$ и $Z' = y^{U'} \bmod p$. После этого последовательно вычисляются элементы подписи: $k = Z'^{Z'} \bmod \gamma$, $g = U - k \bmod \gamma$ и $v = \dfrac{U'}{gk} \bmod \gamma$. Возможность такой подделки подписи определяется тем, что значения α и y разнесены в разные скобки, благодаря чему вычисление значений g и v, обеспечивающих «фиксирование» значений U и U', не требует использования секретного ключа. В первой схеме ЭЦП генерация подписи выполняется следующим образом. Выбираются случайные числа $U < \gamma$ и

$U' < \gamma$ и вычисляются значения $Z = \alpha^{U'} \bmod p$ и $Z' = y^{U'} \bmod p$. После этого вычисляют $k = ZZ' \bmod \gamma$ и находят значения g и v, обеспечивающие «фиксирование» значений U и U', т. е. решают систему сравнений $k + g \equiv U \bmod \gamma$ и $v + xkg \equiv U' \bmod \gamma$.

92. Выбирается случайное число k и вычисляется параметр $R = m(\alpha^k \bmod p) \bmod q$ и второй элемент подписи $S = \dfrac{-k}{1 + xHR} \bmod \gamma$.

Последнее соотношение выводится следующим образом. $R(y^{HRS}\alpha^S \bmod p) \bmod q = [m(\alpha^k \bmod p) \bmod q](y^{HRS}\alpha^S \bmod p) \bmod q =$ $= m(\alpha^k \bmod p)(y^{HRS}\alpha^S \bmod p) \bmod q = m(\alpha^k y^{HRS}\alpha^S \bmod p) \bmod q \Rightarrow$ $\Rightarrow \alpha^k y^{HRS}\alpha^S \bmod p = 1 \Rightarrow k + xHRS + S = 0 \bmod \gamma$.

93. Уравнение проверки подписи можно переписать в виде $\alpha' = y^{\frac{-H}{R}} R^{\frac{1}{R}} \bmod p$, из которого видно, что сложность формирования подписи без знания секретного ключа не превышает сложности задачи дискретного логарифмирования по $\bmod p$ при основании α. В другом варианте решения открытый ключ можно представить в виде $y = \alpha^{x'} \bmod p$. Тогда видно, что, решая задачу дискретного логарифмирования, можно вычислить x', а затем параметр S вычислить из уравнения $S = R^{-1}(k - Hx') \bmod p - 1$.

94. Данное проверочное уравнение допускает следующую попытку подделки подписи. Введем новую переменную $Z = SR \bmod (prq)$, с использованием которой проверочное сравнение приобретает вид $Zy^{H(Z \bmod q)} \equiv S^2\alpha^{(Z \bmod r)} \bmod p$. Теперь элемент подписи S не входит ни в одну из степеней модифицированного сравнения проверки, поэтому можно взять произвольное значение Z, такое что $\max(p, r, q) < Z < prq$, и решить сравнение относительно S. Эта задача не является вычислительно трудной, поскольку p есть простой модуль. По найденному значению $S \bmod p$ вычисляется значение $R = Z/S \bmod p$. Если в качестве p использовать составной модуль n, который теперь вместе с параметром α будет задавать открытый ключ (n, α, y), то задача вычисления квадратного корня станет достаточно сложной, обеспечивая безопасность модифицированной схемы ЭЦП.

95. Данное проверочное уравнение не позволяет осуществить подделку подписи путем введения переменной $Z = S\alpha^k \bmod (prq)$, которая позволяет по произвольно выбранному значению Z вычислить $S \bmod p$ и $\alpha^k \bmod p$, однако вычисление значения k потребует решения сложной задачи дискретного логарифмирования по модулю p, значение которого

по предположению (предполагаемому замыслу, положенному в основу рассматриваемой схемы ЭЦП) достаточно велико. Генерация подписи по секретному ключу осуществляется следующим образом. Представим S в виде $S = \alpha^{\xi} \bmod (pqr)$. Запишем систему сравнений $k + g \equiv U \bmod \gamma$ (1), где U есть случайно выбираемое число, и $k + xHZ \equiv g + Z' \bmod \gamma$ (2). Решив эту систему, найдем k и g, а затем S. Параметры α, p, q и r следует выбирать таким образом, что α должно быть несравнимым с 1 по модулю p, по модулю q и по модулю r (выполнение этого условия на самом деле задано в условии задачи, поскольку, говоря о числе, относящемся к какому-либо показателю, имеется в виду число, несравнимое с 1 по заданному модулю). Если $\alpha \equiv 1 \bmod q$ и $\alpha \equiv 1 \bmod r$, то проверочное уравнение преобразуется к виду $\alpha^k y^{H(S \bmod q)} \equiv S\alpha^{(S \bmod r)} \bmod p$, которое уже будет задавать схему ЭЦП с другим механизмом формирования подписи, хотя эта версия также представляется стойкой. Если $\alpha \bmod q \neq 1$ и $\alpha \equiv 1 \bmod r$ или $\alpha \bmod r \neq 1$ и $\alpha \equiv 1 \bmod q$, то проверочное уравнение преобразуется к виду $\alpha^k y^{H(S\alpha^k \bmod q)} \equiv S\alpha^{(S \bmod r)} \bmod p$ или $\alpha^k y^{H(S \bmod q)} \equiv S\alpha^{(S\alpha^k \bmod r)} \bmod p$ соответственно. Схемы ЭЦП с двумя последними проверочными соотношениями неработоспособны, поскольку даже при использовании секретного ключа генерация подписи является вычислительно сложной процедурой, так как значение одной из скобок нельзя зафиксировать.

96. Первая схема ЭЦП внешне представляется более замысловатой, однако она допускает следующую простую процедуру подделки подписи. Выберем случайное значение $k < \gamma$ и вычислим $R = y^{\alpha^k} \bmod p$. Затем представим значение S в виде $S = \alpha^g \bmod \gamma$. Подставляя эти значения в первое проверочное уравнение, имеем: $y^{\alpha^k \alpha^g} \equiv y^{\alpha^{HR}} \bmod p \Rightarrow k + g \equiv HR \bmod \gamma - 1$. Из последнего соотношения легко вычислить g, по которому определим второй элемент подписи (R, S), удовлетворяющей проверочному соотношению. Заметим, что в этой процедуре формирования подписи знания секретного ключа не потребовалось. Во втором уравнении подделка подписи, соответствующая заданному значению хэш-функции H, является вычислительно сложной задачей. Генерация подписи осуществляется так: генерируется случайное значение $k < \gamma$, и вычисляется элемент подписи $R = \alpha^k \bmod p$. Значение S определяется из сравнения $x + HR = kS \bmod \gamma$.

97. При фиксировании одного из элементов подписи (g, R) даже по известному секретному ключу x сложно вычислить второй элемент. Для вычисления подписи следует представить число R в виде $R = \alpha^k \bmod n$ (альтернативным вариантом является использование представления

$R = y^k \bmod n$). Выбирается некоторое произвольное значение $U < \gamma$, и решается система сравнений $k + xg \equiv U \bmod \gamma$ (1) и $k \equiv Z \bmod \gamma$ (2), где $Z = H\alpha^U \bmod n$, относительно неизвестных k и g. Найденное решение определяет подпись (g, R), где $R = \alpha^k \bmod n$. Предложенное проверочное соотношение может быть значительно упрощено, поскольку вместо RSA-модуля можно использовать простое число, что приведет к схеме с проверочным уравнением $R = \alpha^{(R^{-g}H \bmod p)} \bmod p$, где p и α — общие для всех пользователей параметры криптосистемы, а секретный ключ включает только число x. При этом задача дискретного логарифмирования, лежащая в основе схемы, становится существенно сложнее, ввиду того что теперь она относится к простому, а не к составному модулю той же длины. Однако при раскрытии исходной схемы в первую очередь требуется решить задачу разложения модуля на множители. Трудоемкость этой задачи примерно равна сложности дискретного логарифмирования по простому модулю p (при одинаковых размерах модулей p и n). Легко указать способ сокращения подписи, если заметить, что по подписи в процессе проверки ее подлинности восстанавливается значение k как степень при числе α. Действительно, ввиду отмеченного нет никакого смысла переходить от k к $R = \alpha^k \bmod n$ с точки зрения стойкости. Если такого перехода не делать, то получаем эквивалентные исходному проверочные уравнения вида $\alpha^k = \alpha^{(\alpha^k y^g H \bmod p)} \bmod p$ и $k = (\alpha^k y^g H \bmod p) \bmod \gamma$, которые при сравнительно малом размере числа γ определяют схемы ЭЦП с сокращенной длиной подписи.

98. Если используется простой модуль p, то подпись можно сформировать без знания секретного ключа по формуле $R = y^{-\frac{1}{S}} R^{\frac{H}{S}} \bmod p$. Выбрав произвольное S, являющееся взаимно простым с $p - 1$, можно легко вычислить целые числа $t = -1/S \bmod p - 1$ и $u = H/S \bmod p - 1$, а затем параметр R, который вместе с выбранным S удовлетворяет уравнению проверки подписи. Для обеспечения стойкости в качестве модуля следует выбрать RSA-модуль n. В этом случае вычисление параметров t и u потребует знания разложения модуля для вычисления функции Эйлера $\varphi(n)$. Такой выбор модуля предполагает, что он является элементом открытого ключа (y, n).

99. Из уравнения проверки вытекает следующая процедура генерации подписи. Выбирается случайное значение $U < \gamma$. Далее вычисляют $Z = (\alpha^U \bmod p) \bmod \gamma$. После этого решают систему из следующих двух уравнений: $k + g \equiv U \bmod \gamma$ и $k + gH \equiv xH + Z \bmod \gamma$, где неизвестными являются k и g. Решение системы дает следующие расчетные формулы:

$k = \dfrac{UH - xH - Z}{H - 1} \bmod \gamma$ и $g = \dfrac{xH + Z - U}{H - 1} \bmod \gamma$. По полученному значению g вычисляется значение $S = \alpha^g \bmod n$, которое вместе с k удовлетворяет уравнению проверки подписи. Открытый ключ и элемент α можно представить в виде $y = \pi^{x'} \bmod p$ и $\alpha = \pi^u \bmod p$, где π — первообразный корень по модулю p (заметим, что в общем случае невозможно представить y в виде степени α). Решая задачу дискретного логарифмирования, можно вычислить a и x', по которым затем легко вычисляются параметры S и k (аналогично тому, как генерируется подпись при известном секретном ключе). В определенном смысле можно сказать, что стойкость заданной схемы ЭЦП вдвое превышает сложность задачи дискретного логарифмирования.

100. Пусть дан некоторый документ, хэш-функция от которого равна H. Далее действуем по следующему алгоритму.

1. Выбрать некоторое значение z.
2. Вычислить $R = \alpha^z y^H \bmod p$.
3. Если НОД$(R, p - 1) > 1$, то повторить шаги 1 и 2, пока не выполнится условие НОД$(R, p - 1) = 1$.
4. Вычислить $S = z / R \bmod p - 1$, т. е. получаем $z = SR \bmod p - 1$.
5. Предъявить в качестве подписи к хэш-функции H пару чисел (R, S).

Подставляя в левую часть уравнения проверки подписи значение $R = \alpha^{SR} y^H \bmod p$, видим, что правая и левая части совпадают, т. е. сформированная подпись является правильной.

101. Пусть дан некоторый документ, хэш-функция от которого равна H. Злоумышленник может действовать по следующей схеме.

1. Выбрать некоторое значение z, такое что НОД$(z, p - 1) = 1$.
2. Вычислить $R = \alpha^z y^{-H} \bmod p$.
3. Вычислить $S = R / z \bmod p - 1$.
4. Предъявить в качестве подписи к хэш-функции H пару чисел (R, S).

Подставляя в правую часть уравнения проверки подписи значения $R = Sz \bmod p - 1$ и $R = \alpha^z y^{-H} \bmod p$, получаем $y^{HS} \alpha^{zS} y^{-HS} \equiv \alpha^R \bmod p$, т. е. правая часть совпадает с левой. Это означает, что сформированная подпись правильная.

102. Подделка подписи к документу, хэш-функция от которого равна H, может быть осуществлена по следующей схеме.

1. Выбрать некоторое значение w, такое что НОД$(w, p - 1) = 1$.

2. Вычислить $R = \alpha^{H} y^{-w} \bmod p$.

3. Вычислить $S = R/w \bmod p - 1$.

4. Предъявить в качестве подписи к хэш-функции H пару чисел (R, S).

Подставляя в правую часть уравнения проверки подписи значение $R = wS \bmod p - 1$ и $R = \alpha^{H} y^{-w} \bmod p$, получаем $y^{wS}\alpha^{HS}y^{-wS} \equiv \alpha^{HS} \bmod p$. Совпадение левой и правой частей уравнения проверки показывает, что сформированная (без знания секретного ключа) подпись является правильной.

103. Пусть дан некоторый документ, хэш-функция от которого равна H. Подделка подписи осуществляется в соответствии со следующим алгоритмом.

1. Выбрать некоторое значение w, такое что НОД$(w, p-1) = 1$.

2. Вычислить $R = \alpha^{H} y^{-w} \bmod p$.

3. Вычислить $S = Rf(H)/w \bmod p - 1$.

4. Предъявить в качестве подписи к хэш-функции H пару чисел (R, S).

Подставляя в правую часть уравнения проверки подписи значение произведения $Rf(H) \equiv wS \bmod p - 1$ и $R = \alpha^{H} y^{-w} \bmod p$, получаем $y^{wS}\alpha^{HS}y^{-wS} \equiv \equiv \alpha^{HS} \bmod p$. Совпадение левой и правой частей уравнения проверки показывает, что сформированная подпись (R, S) является правильной.

104. Для того чтобы подделать подпись к некоторому документу, нарушитель может действовать следующим образом.

1. Вычислить хэш-функцию H от документа.

2. Если НОД$(f(H), p-1) > 1$, то модифицировать документ, сохраняя его смысловое содержание, и повторить шаг 1, в противном случае перейти к следующему шагу алгоритма.

3. Выбрать произвольное $w < p - 1$ и вычислить значение $z = H/f(H) \bmod p - 1$.

4. Вычислить $R = \alpha^{z} y^{w} \bmod p$. Если НОД$(R, p-1) > 1$, то выбрать случайное $w < p - 1$ и перейти к началу шага 4, в противном случае перейти к шагу 5.

5. Вычислить $S = wf(H)/R \bmod p - 1$.

6. Предъявить в качестве подписи к хэш-функции H пару чисел (R, S).

Подставляя в левую часть уравнения проверки подписи значение $R = \alpha^{z} y^{w} \bmod p$, получаем $R^{f(H)} \equiv \alpha^{zf(H)} y^{wf(H)} \equiv \alpha^{H} y^{RS} \bmod p$. Совпадение левой и правой частей уравнения проверки показывает правильность сформированной подписи (R, S).

105. Для того чтобы подделать подпись к некоторому документу, нарушитель может действовать следующим образом.

1. Вычислить хэш-функцию H от документа.
2. Если НОД$(f(H), p-1) > 1$, то модифицировать документ, сохраняя его смысловое содержание, и повторить шаг 1, в противном случае перейти к следующему шагу алгоритма.
3. Выбрать пару значений z и w, таких что $z/w = H/f(H)$.
4. Вычислить $R = \alpha^z y^w \bmod p$ и $F(R)$.
5. Если НОД$(F(R), p-1) > 1$, то повторить шаги 3 и 4, в противном случае перейти к следующему шагу алгоритма.
6. Вычислить $S = wF(R)/f(H) \bmod p - 1$.
7. Предъявить в качестве подписи к хэш-функции H пару чисел (R, S).

Из выражения в п. 6 легко получить $w = Sf(H)/F(R) \bmod p - 1$ и $z = wH/f(H) \bmod p - 1 = SH/F(R) \bmod p - 1$. Подставляя в левую часть уравнения проверки подписи значение $R = \alpha^t y^w \bmod p$, получаем $R^{F(R)} \equiv \alpha^{zF(R)} y^{wF(R)} \equiv \alpha^{SH} y^{Sf(H)} \bmod p$. Сравнимость левой и правой частей по модулю p показывает правильность сформированной подписи (R, S) к документу.

106. Проверочное уравнение в криптосистеме DSA можно представить в виде $R' \equiv (\alpha^{H/S} y^{R'/S} \bmod p) \bmod q$, где α — число, относящееся к показателю q по модулю p. Представим значение R' в виде $R' \equiv (\alpha^t y^u \bmod p) \bmod q$. Приравнивая правые части приведенных выражений, получаем: $\alpha^t y^u \equiv \alpha^{H/S} y^{R'/S} \bmod p$, откуда следуют «подгоночные» формулы для вычисления параметров S и H: $S = R'/u \bmod q$ и $H = tR'/u \bmod q$. Следовательно, для нахождения случайного значения H и правильной подписи к нему можно выполнить следующую процедуру. Взять произвольные значения t и u. Затем последовательно вычислить следующие параметры: $R' \equiv (\alpha^t y^u \bmod p) \bmod q$, $S = R'/u \bmod q$ и $H = tR'/u \bmod q$. Легко показать, что сформированная подпись (R, S) и значение H удовлетворяют проверочному уравнению.

107. Проверочное уравнение в схеме ЭЦП по стандарту ГОСТ Р 34.10-94 можно представить в виде $R' = (\alpha^{S/H} y^{-R'/H} \bmod p) \bmod q$, где α — число, относящееся к показателю q по модулю p. Представим значение R' в виде $R' = (\alpha^t y^u \bmod p) \bmod q$. Приравнивая правые части приведенных выражений, получаем: $\alpha^t y^u \equiv \alpha^{S/H} y^{-R'/H} \bmod p$, откуда следуют «подгоночные» формулы для вычисления параметров S и H: $H = -R'/u \bmod q$ и $S = -tR'/u \bmod q$. Следовательно, для нахождения случайного значения

H и правильной подписи к нему можно выполнить следующую процедуру. Взять произвольные значения t и u. Затем последовательно вычислить следующие параметры: $R' \equiv (\alpha^t y'' \bmod p) \bmod q$, $H = -R'/u \bmod q$ и $S = -tR'/u \bmod q$. Легко показать, что сформированная подпись (R, S) и значение H удовлетворяют проверочному уравнению.

108. Способ подделки подписи к документу, хэш-функция от которого равна H, может быть найден путем представления значения R в виде $R = \alpha^t y'' \bmod p$. Подставляя это значение в формулу проверки подписи, получаем: $\alpha^H \equiv y^{RS} \alpha^t y'' \bmod p$. Отсюда видно, что проверочное уравнение удовлетворяется, если $H \equiv t \bmod p-1$ и $RS \equiv -u \bmod p-1$. Следовательно, выбирая произвольное значение u, легко вычисляем элементы подписи (R, S) к заданной хэш-функции: $R = \alpha^H y'' \bmod p$ и $S \equiv -u/R \bmod p-1$.

109. Данное уравнение есть своего рода усиленный вариант схемы ЭЦП Эль-Гамаля, которая допускает вычисление без знания секретного ключа тройки чисел R, S и H, таких что (R, S) является правильной подписью к значению хэш-функции H. Это может быть осуществлено, представляя значение R в виде $R = \alpha^t y'' \bmod p$ и вычисляя S и H как «подгоночные» значения. В большинстве применений это не является критичным, поскольку получаемое таким образом значение H является случайным. Однако в заданной схеме ЭЦП нахождение указанной тройки чисел является вычислительно нереализуемым, поскольку открытый ключ возводится в степень $R' = R^H \bmod p-1$, в результате чего теперь требуется найти значения S и H, удовлетворяющие сравнениям $H \equiv tS \bmod p-1$ и $R^H \equiv -uS \bmod p-1$, т. е. требуется решить уравнение вида $R'^S \equiv -uS \bmod p-1$. Однако в рассматриваемой схеме ЭЦП при генерации и проверке подписи выполняется на одну операцию возведения в степень больше, чем в схеме Эль-Гамаля.

110. Выбирается некоторое произвольное значение $U < \gamma$. Затем, принимая в качестве неизвестных значения k и g, решается система сравнений $k + xg \equiv U \bmod \gamma$ (1) и $k \equiv M^{U+t} Z^{-1} \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Найденное решение определяет подпись (k, g).

111. Выбирается некоторое произвольное значение $U < \gamma$. Затем, принимая в качестве неизвестных значения k и g, решается система сравнений $k + xg \equiv U \bmod \gamma$ (1) и $k + g \equiv MZ^{-1} \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Найденное решение определяет подпись (k, g).

112. Выбирается некоторое произвольное значение $U < \gamma$. Затем, принимая в качестве неизвестных значения k и g, решается система сравнений $k + xg \equiv U \bmod \gamma$ (1) и $k - g \equiv MZ \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Найденное решение определяет подпись (k, g).

113. Формирование подписи осуществляется следующим образом. Выбирается некоторое произвольное значение $U < \gamma$. Затем, принимая в качестве неизвестных значения k и g, решается система сравнений $k + xg \equiv U \bmod \gamma$ (1) и $k + g \equiv (MZ)^{1-H} \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Найденное решение определяет подпись (k, g). Необходимость использования значения хэш-функции от сообщения, до того как последнее будет восстановлено из подписи, определяет необходимость представления проверяющему значения H одновременно с подписью. Это означает, что H имеет значение некоторой контрольной суммы, которая позволяет одновременно с проверкой подписи выполнить также и проверку подлинности восстанавливаемого сообщения.

114. Формирование подписи осуществляется следующим образом. Выбирается некоторое произвольное значение $U < \gamma$. Затем, принимая в качестве неизвестных значения k и g, решается система сравнений $Hk + x(g + H) \equiv U \bmod \gamma$ (1) и $g \equiv MZ^{-1} \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Найденное решение определяет подпись (k, g). Необходимость использования значения хэш-функции от сообщения, до того как последнее будет восстановлено из подписи, определяет необходимость представления проверяющему значения H одновременно с подписью. Значение H играет роль некоторой контрольной суммы, обеспечивающей одновременное выполнение проверки подлинности подписи и подлинности восстанавливаемого сообщения.

115. Формирование подписи осуществляется следующим образом. Выбирается некоторое произвольное значение $U < \gamma$. Затем, принимая в качестве неизвестных значения k и g, решается система сравнений $k + xg \equiv U \bmod \gamma$ (1) и $g \equiv M - HZ \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Найденное решение определяет подпись (k, g). Значение H позволяет одновременно с выполнением проверки подлинности подписи осуществить и проверку подлинности восстанавливаемого сообщения.

116. Подпись может быть подделана в схеме ЭЦП, соответствующей первому проверочному сравнению. Это может быть реализовано с помощью замены переменных. Введем переменную $w \equiv kg \bmod \gamma$ и перепишем проверочное сравнение в виде $g + w/g \equiv (\alpha^w y^H \bmod p) \bmod \gamma$. Для произвольно выбранного значения w вычисляем значение g как один из корней квадратного сравнения $g^2 - g(\alpha^w y^H \bmod p) + w \equiv 0 \bmod \gamma$. Затем определяем вторую часть подписи $k \equiv w/g \bmod \gamma$. Таким образом. подпись подделана. Во второй схеме подписание заданного сообщения требует знания секретного ключа. Подпись определяется решением системы сравнений $g + xk \equiv U \bmod \gamma$ (1), где $U < \gamma$ — случайно выбираемое значение, и $gk \equiv MZ \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Второе сравне-

ние допускает экзистенциальную подделку подписи, т. е. возможность сопоставить произвольно выбранной паре значений (k, g) некоторое случайное сообщение M', такое что указанная пара воспринимается как подлинная подпись к M'. Возможность экзистенциальной подделки подписи не означает слабость схемы ЭЦП, хотя и является нежелательным свойством. В схемах, допускающих экзистенциальную подделку подписи, в проверочное уравнение вместо значения сообщения обычно входит значение хэш-функции, что устраняет это свойство.

117. Подпись может быть подделана в схеме ЭЦП, соответствующей второму проверочному сравнению. Это может быть реализовано с помощью замены переменных. Введем переменную $w \equiv g/k \bmod \gamma$ и перепишем проверочное сравнение в виде $g^2 \equiv w(\alpha^w y^{1-w} \bmod p) \bmod \gamma$. Для произвольно выбранного значения w вычисляем значение g как один из квадратных корней от правой части, а затем определяем вторую часть подписи $k \equiv g/w \bmod \gamma$. Таким образом, подделка подписи имеет весьма низкую сложность. В схеме ЭЦП, заданной первым сравнением, формирование подписи к заданному сообщению требует знания секретного ключа. Подпись определяется решением системы сравнений $g + xk \equiv U \bmod \gamma$ (1), где $U < \gamma$ — случайно выбираемое значение, и $g + M \equiv Z \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Первое сравнение допускает экзистенциальную подделку подписи, т. е. возможность сопоставить произвольно выбранной паре значений (k, g) некоторое случайное сообщение M', такое что указанная пара удовлетворяет проверочному сравнению как подлинная подпись к M'. Возможность экзистенциальной подделки подписи является нежелательным свойством, но не означает слабость схемы ЭЦП. В практических приложениях это учитывается. В схемах, допускающих экзистенциальную подделку подписи, в проверочное уравнение вместо значения сообщения обычно входит значение хэш-функции, что устраняет это свойство. В некоторых случаях вычисление хэш-функции от сообщения вносит нежелательное усложнение в протоколы с проверкой подписи к часто передаваемым сообщениям малого размера. В этих случаях желательно использование схем ЭЦП, которые не допускают экзистенциальной подделки подписи.

118. Представим значение R в виде $R = m\alpha^t y^u \bmod p$. В соответствии с проверочным уравнением имеем: $m = \alpha^{RS} y m \alpha^t y^u \pmod p$. Проверка будет положительной, если будут выполняться соотношения: $t \equiv -RS \bmod p - 1$ и $u \equiv -1 \bmod p - 1$, т. е. при формировании R следует выбрать $u = p - 2$ при произвольном t, затем по R вычислить $S \equiv -t/R \bmod p - 1$. Если НОД$(p - 1, R) \neq 1$, то выбрать новое значение t и повторить вычисления.

119. Представим значение R в виде $R = m\alpha^t y^u \bmod p$. В соответствии с проверочным уравнением имеем: $m = \alpha^{f(R)S} y m \alpha^t y^u \pmod p$. Проверка будет положительной, если будут выполняться соотношения: $t \equiv -f(R)S \bmod p-1$ и $u \equiv -1 \bmod p-1$, т. е. при формировании R следует выбрать $u = p-2$ при произвольном t, затем найти значение $f(R)$ и по $f(R)$ вычислить $S \equiv -t/f(R) \bmod p-1$. Если НОД$(p-1, f(R)) \neq 1$, то выбрать новое значение t и повторить вычисления.

120. Представим значение R в виде $R = \alpha^t y^u \bmod p$. В соответствии с проверочным уравнением имеем: $\alpha^{HS} \equiv y^R \alpha^{tS} y^{uS} \bmod p$. Проверка будет положительной, если будут выполняться соотношения: $H \equiv t \bmod p-1$ и $uS \equiv -R \bmod p-1$, т. е. при формировании R следует выбрать $t = H$ и произвольное u, такое что НОД$(p-1, u) \neq 1$. После этого легко найти требуемое значение $S \equiv -R/u \bmod p-1$.

121. Представим значение R в виде $R = \alpha^t y^u \bmod p$. В соответствии с проверочным уравнением имеем: $\alpha^{HR} \equiv y^S \alpha^t y^u \bmod p$. Проверка будет положительной, если будут выполняться соотношения: $HR \equiv t \bmod p-1$ и $S \equiv -u \bmod p-1$, т. е. для $H \equiv t/R \bmod p-1$ правильная подпись (R, S) получена. Однако полученное значение хэш-функции является случайным и вычислительно сложно найти документ, который якобы подписан. Если окажется, что НОД$(p-1, R) \neq 1$, то следует выбрать новое значение t или u и вычислить новое значение R, а затем и новое значение S.

122. Представим значение R в виде $R = \alpha^t y^u \bmod p$. В соответствии с проверочным уравнением имеем: $\alpha^{RS} \equiv y^H \alpha^t y^u \bmod p$. Проверка будет положительной, если будут выполняться соотношения: $RS \equiv t \bmod p-1$ и $H \equiv -u \bmod p-1$, где значение R уже вычислено. Значение $S \equiv t/R \bmod p-1$ будет соответствовать правильной подписи (R, S) к произвольному заданному значению H, если при генерации R было использовано значение $u = p-1-H$. Если окажется, что НОД$(p-1, R) \neq 1$, то следует выбрать новое значение t и вычислить новое значение R, а затем и новое значение S.

123. ЭЦП с сокращенной длиной подписи задается проверочным уравнением $R' = F(\alpha^{H/S} y^{-R'/S} \bmod p)$, где $R' = F(\alpha^k \bmod p)$, α — число, относящееся по модулю p к показателю $q \mid p-1$ сравнительно малого размера, F — сжимающая функция, k — случайное число. Уравнение генерации подписи имеет вид $S = \dfrac{H - xR'}{k} \bmod q$.

124. ЭЦП с сокращенной длиной подписи задается проверочным уравнением $R' = F(\alpha^{S/H} y^{-R'/H} \bmod p)$, где $R' = F(\alpha^k \bmod p)$, α — число, относя-

щееся по модулю p к показателю $q \mid p-1$ сравнительно малого размера, F — сжимающая функция, k — случайное число. Уравнение генерации подписи имеет вид $S = kH + xF(R) \bmod q$.

125. Заданная схема ЭЦП преобразуется в схему с сокращенной длиной подписи, описываемую проверочным уравнением $R' = F(\alpha^{H^{-1}S} y^{-R'^{-1}S} \bmod p)$, где $R' = F(\alpha^k \bmod p)$, α — число, относящееся по модулю p к показателю $q \mid p-1$ сравнительно малого размера, F — сжимающая функция, k — случайное число. Для придания свойства «восстановления сообщения» в качестве сжимающей функции выберем операцию взятия остатка от деления на простое число q ($|q| = 160-256$ бит), а параметр R' будем вычислять по формуле $R' = m(\alpha^k \bmod p) \bmod q$, где m — подписанное сообщение. С учетом этих изменений уравнение проверки приобретает вид $m = R'(\alpha^{H^{-1}S} y^{-R'^{-1}S} \bmod p)^{-1} \bmod q$, а уравнение генерации подписи: $S = \dfrac{H - xR'}{k} \bmod q$.

126. Если одно и то же значение $U < \gamma$ будет использовано при формировании подписей к двум сообщениям, соответствующим значениям хэш-функции H_1 и $H_2 \neq H_1$, то потенциальный нарушитель может легко вычислить ключ, совместно решая сравнения $H_1 k_1 + x g_1 \equiv U \bmod \gamma$ и $H_2 k_2 + x g_2 \equiv U \bmod \gamma$ с неизвестными U и x. Уточнение процедуры генерации подписи состоит в том, что после вычисления значения Z нужно убедиться, что оно является квадратичным вычетом по модулю γ, т. е. убедиться, что выполняется сравнение $Z^{\frac{\gamma-1}{2}} \equiv 1 \bmod \gamma$. Если это не так, то нужно выбрать новое значение U и повторить указанную проверку для нового значения Z. Поскольку элемент подписи k вычисляется как квадратный корень из Z, то целесообразно снизить сложность этой операции путем выбора параметра γ, удовлетворяющего сравнению $\gamma \equiv 3 \bmod 4$. В этом случае имеем $k \equiv Z^{\frac{\gamma+1}{4}} \bmod \gamma$.

127. Чтобы обеспечить свойство восстановления сообщения, вместо хэш-функции H в проверочном соотношении будем использовать само сообщение M (предполагается, что $M < \gamma$). Значение k^2 переместим в правую часть как множитель, в который можно встроить информацию о сообщении. Последнее можно сделать, задавая вычисление k по формуле $k^2 \equiv \dfrac{M}{(\alpha^U \bmod p)} \bmod \gamma$ (1), где U — произвольное число ($U < \gamma$), которая вместе со сравнением $k + xg \equiv U \bmod \gamma$ (2) образует систему, ре-

шение которой дает значение подписи в схеме ЭЦП с проверочным равенством $M \equiv k^2(\alpha^k y^g \bmod p) \bmod \gamma$. Проверка подлинности сообщения непосредственно при проверке подлинности подписи в построенной схеме не обеспечивается. При использовании такой схемы ЭЦП предполагается, что подлинность сообщения проверяется самой структурой сообщения (это осмысленный текст или в конце текста приведено заранее оговоренное слово, или к сообщению присоединена некоторая контрольная сумма, которая проверяется с использованием дополнительной процедуры уже после восстановления сообщения).

128. Требуемая модернизация схемы ЭЦП связана с перенесением значения хэш-функции H в степень при α и/или y. В этом случае без использования значения секретного ключа решение проверочного сравнения относительно H при заданных значениях k и g становится вычислительно сложным. Таким образом, приходим к следующим трем вариантам $k \equiv (\alpha^{Hk} y^g \bmod p) \bmod \gamma$ (1), $k \equiv (\alpha^k y^{g+H} \bmod p) \bmod \gamma$ (2) и $k \equiv (\alpha^{k+H} y^{g+H} \bmod p) \bmod \gamma$ (3). При этом во втором и третьем вариантах сложность процедуры проверки подписи даже снижается, поскольку вместо одной операции умножения по модулю γ вводится не более двух операций сложения по тому же модулю. Генерация подписи осуществляется путем выбора случайного числа $U < \gamma$ и последующего решения системы сравнений: 1) $Hk + xg \equiv U \bmod \gamma$ и $k = \alpha^U \bmod p$, 2) $k + xg + xH \equiv U \bmod \gamma$ и $k = \alpha^U \bmod p$, 3) $k + H + xg + Hx \equiv U \bmod \gamma$ и $k = \alpha^U \bmod p$, соответственно в первом, втором и третьем вариантах.

129. Для генерации подписи представим параметр R в виде $R = \alpha^{\alpha^k} \bmod p$, где k — случайно выбираемое число (маскирующий разовый секрет). Подставляя в проверочное сравнение значения R, y и y', выраженные через соответствующие степени числа α, получаем следующее: $\alpha^{\alpha^x \alpha^{HR}} \equiv \alpha^{\alpha^k \alpha^{xS}} \bmod p \Rightarrow \alpha^x \alpha^{HR} \equiv \alpha^k \alpha^{xS} \bmod \gamma \Rightarrow x + HR \equiv k + xS \bmod \gamma - 1$. Из последнего сравнения выводим следующую формулу для вычисления второго элемента подписи: $S \equiv \dfrac{HR - k}{x} + 1 \bmod \gamma - 1$, из которой вытекает требование НОД$(x, \gamma - 1) = 1$, которое следует учитывать при выборе секретного ключа. Формирование подписи может быть осуществлено также с использованием представления параметра R в виде $R = y^{\alpha^k} \bmod p$. Тогда из проверочного соотношения получаем: $y^{\alpha^{HR}} \equiv y^{\alpha^k \alpha^{xS}} \bmod p \Rightarrow \alpha^{HR} \equiv \alpha^k \alpha^{xS} \bmod \gamma \Rightarrow HR \equiv k + xS \bmod \gamma - 1$. Из

последнего сравнения выводим следующую формулу для вычисления параметра S: $S \equiv \frac{HR - k}{x} \bmod \gamma - 1$. Легко заметить, что стойкость этой схемы ЭЦП определяется сложностью дискретного логарифмирования по модулю γ, поэтому сокращение длины γ приведет к резкому падению стойкости, так что предложенная модификация схемы с 256-битовым простым модулем γ недопустима. Сокращения размера параметра S можно достичь без снижения стойкости путем выбора такого числа α, которое относится по модулю p к показателю γ и одновременно относится по модулю γ к некоторому делителю $q \mid \gamma - 1$, который имеет размер 160÷256 бит. Такая модификация несостоятельна даже в случае, если использовать открытый ключ $y = \alpha^{x'} \bmod p$, где $x' \neq x$, поскольку параметр R можно вычислять по формуле $R = y^{\alpha^k} \bmod p$. В этом случае значение x' не используется при генерации подписи.

130. Схема ЭЦП, задаваемая указанным проверочным уравнением, представляется работоспособной при наложении определенных ограничений на выбор ее параметров, для рассмотрения которых следует пояснить идею, положенную в ее основу. Элементы подписи вычисляются с учетом того, что значение в каждой из двух скобок фиксируется путем задания определенной связи между элементами подписи. После этого значение элемента v оказывается заданным. Другие два элемента подписи подбираются такими, чтобы при полученном значении v значение выражения в каждой из скобок осталось прежним. Поскольку открытый ключ входит как множитель в два разных произведения, вычисляемые по разным модулям, причем возведенный в различную степень, то следует 1) либо наложить требование $\alpha_1 = \alpha_2 = \alpha$, 2) либо наложить ограничение $\alpha_1 \equiv 1 \bmod p_2$ и $\alpha_2 \equiv 1 \bmod p_1$. При этом открытый ключ следует вычислять по формуле $y \equiv \alpha^x \bmod (p_1 p_2)$ в первом случае или по формуле $y \equiv (\alpha_1 \alpha_2)^x \bmod (p_1 p_2)$ во втором, где x — секретный ключ. Для обоих вариантов можно указать алгоритмы, позволяющие сформировать параметры, которые отвечают требуемым условиям. В частном случае можно даже обеспечить условие $\gamma_1 = \gamma_2 = \gamma$. В предположении, что указанные ограничения учтены, процедура генерации подписи по секретному ключу по существу представляет собой решение следующей системы сравнений: $g + v + xk \equiv U_1 \bmod \gamma_1$ (1), где $U_1 < \gamma_1$ — случайно выбираемое значение, $k + vH + xg \equiv U_2 \bmod \gamma_2$ (2), где $U_2 < \gamma_2$ — случайно выбираемое значение и $v \equiv Z_1 Z_2 \bmod \gamma$ (3), где $Z_1 = \alpha_1^{U_1} \bmod p_1$, $Z_2 = \alpha_2^{U_2} \bmod p_2$ и в общем случае $\gamma_1 \neq \gamma_2 \neq \gamma$. Наиболее

простой вид процедура генерации подписи имеет в случае $\gamma_1 = \gamma_2 = \gamma$ и $\alpha_1 = \alpha_2 = \alpha$. Стойкость определяется сложностью логарифмирования по простому числу p_1 или p_2, имеющему большее значение. Недостатком этой схемы ЭЦП является то, что размер открытого ключа примерно вдвое больше по сравнению со схемами, использующими вычисления только по одному простому модулю p (при условии $|p_1| \approx |p_2| \approx |p|$).

131. Если $\delta = \gamma$, то возможен следующий способ подделки подписи. Выбрать случайное значение $U < \gamma$ и вычислить $Z = (\alpha y^H)^U \bmod p$. Взять в качестве одного элемента подписи значение $g = Z \bmod \gamma$. Другой элемент подписи вычислить по формуле $k = U/Z \bmod \gamma$. Если на выбор значений γ и δ наложить условие $\delta \neq \gamma$, то показатели степени при (y^H) и α представляют собой разные функции от произведения gk. Однако это не снимает проблему с возможностью подделки подписи. При указанном ограничении генерация подписи также не требует использования секретного ключа. Она состоит в решении следующей системы сравнений: $gk \equiv U \bmod \gamma$ (1), где $U < \gamma$ — случайно выбираемое значение, и $g \equiv Z \bmod \delta$ (2), где $Z = \alpha^U y^{(U \cdot H \bmod \gamma) \bmod \delta} \bmod p$.

132. Формулы (1) и (2) получены как результат решения системы сравнений $Mg \equiv kZ \bmod \gamma$ (3) и $g - kx \equiv U \bmod \gamma$ (4). При этом сравнение (3) связывает между собой значения k и g определенным соотношением, которое непосредственно не зависит ни от x, ни от U. Поэтому сравнение (3) не дает непосредственной дополнительной информации о значениях x и U, которая могла бы быть использована в вычислительно эффективных способах вычисления этих величин. Это означает, что формулы (1) и (2) не могут быть системой сравнений, из которых можно однозначно определить величины x и U. Таким образом, в силу сложности задачи дискретного логарифмирования неопределенность, которая присутствует в сравнении (4) относительно x и U, сохраняется и в системе (1) и (2).

133. Рассмотрим механизм формирования подписи. Для некоторых пар значений (k, g) выражение в скобках может быть одним и тем же, например равным некоторому числу Z. Мы не можем по заданному Z определить множество соответствующих ему пар чисел (k, g), так как для этого пришлось бы решать задачу дискретного логарифмирования. Однако легко записать условия, которым должны удовлетворять значения элементов подписи, чтобы значение выражения в скобках было «зафиксировано». Это выполняется, если $f(k, g) + xk \equiv U \bmod \gamma$ (1), где U есть некоторое произвольно выбираемое число ($U < \gamma$). По выбранному значению U можно вычислить соответствующее ему значение Z. Согласно проверочному уравнению элемент k равен Z. Таким образом, в (1) все значения оказываются заданными, кроме числа g. Поскольку мы вы-

числили k в предположении, что выполняется (1), то теперь нужно выбрать такое g, чтобы сравнение (1) выполнялось, т. е. значение второго элемента подписи находится как решение сравнения (1). Это означает, что 1) функция $f(k, g)$ должна быть такой, чтобы существовали решения для произвольных значений x, U и Z; 2) при этом сложность решения сравнения (1) не должна быть высокой. Первое требование учитывает принципиальную возможность нахождения подписи, а второе — эффективность процедуры формирования подписи. Первое требование выполняется, если выбрать такую функцию $f(k, g)$, которая задает биективное отображение множества значений g в множество значений $f(k, g) \bmod \gamma$ при произвольном k ($0 < k < \gamma$). Учитывая первое и второе требования, можно предложить следующий вид рассматриваемой функции: $f(k, g) = g * f'(k) \bmod \gamma$, где $f'(k)$ — произвольная эффективно вычислимая функция от k и $* \in \{+_\gamma, -_\gamma, \times_\gamma, \div_\gamma\}$ ($+_\gamma, -_\gamma, \times_\gamma, \div_\gamma$ обозначают сложение по mod γ, вычитание по mod γ, умножение по mod γ, деление по mod γ соответственно). Таким образом, мы можем записать такой обобщенный вид проверочного уравнения, которое задает приемлемую схему ЭЦП: $k = (H\alpha^{g*f'(k)} y^k \bmod p) \bmod \gamma$. Процедура генерации подписи такова: 1) выбираем случайное $U < \gamma$; 2) вычисляем $k = (H\alpha^U \bmod p) \bmod \gamma$; 3) вычисляем $g = (U - xk) \overline{*} f'(k) \bmod \gamma$, где $\overline{*}$ есть операция, обратная операции $*$.

134. Выражение $(\alpha^{Hg} y^{f(k,g)} \bmod p) \bmod \gamma$ равно одному и тому же значению $Z = \alpha^U \bmod p$, если выполняется условие $Hg + xf(k, g) \equiv U \bmod \gamma$ (1). Следовательно, мы можем сформировать подпись, предварительно выбрав случайное число $U < \gamma$, по которому затем вычислим $k = Z \bmod \gamma = (\alpha^U \bmod p) \bmod \gamma$. Теперь первый элемент подписи определен. Второй элемент подписи нужно будет определить из сравнения (1). Отсюда следует требование, чтобы (1) имело решение относительно неизвестного g почти для всех возможных значений x, U и k и нахождение этого решения обладало относительно невысокой сложностью. Учитывая эти требования, можно предложить следующий вид рассматриваемой функции: $f(k, g) = g * f'(k) \bmod \gamma$, где $f'(k)$ — некоторая эффективно вычислимая функция от k и $* \in \{+_\gamma, -_\gamma, \times_\gamma, \div_\gamma\}$ ($+_\gamma, -_\gamma, \times_\gamma, \div_\gamma$ обозначают сложение по mod γ, вычитание по mod γ, умножение по mod γ, деление по mod γ соответственно). На функцию $f'(k)$ не накладывается жестких требований, хотя желательно, чтобы она задавала биективное отображение $\{k\} \to \{f'(k)\}$. В частности, ее можно выбрать из множества $\{k, k^2, k^{-1}, k^{-2}, k + k^{-1}, k + k^2\}$. Существенным

требованием к выбору $f'(k)$ является реализация низкой вероятности коллизий, т. е. получения двух одинаковых значений функции, соответствующих двум различным значениям аргумента. Таким образом, мы можем записать такой обобщенный вид проверочного уравнения, которое задает приемлемую схему ЭЦП: $k = (\alpha^{Hg} y^{g*f'(k)} \bmod p) \bmod \gamma$. Процедура генерации подписи такова: 1) выбираем случайное $U < \gamma$; 2) вычисляем $k = (\alpha^U \bmod p) \bmod \gamma$; 3) вычисляем g из сравнения $Hg + x(g*f'(k)) = U \bmod \gamma$.

135. Введем новую переменную $t = g/k \bmod \gamma$. Тогда проверочное уравнение приобретает вид $tk^2 = [(\alpha^{Ht} y)^t \bmod p] \bmod \gamma$. Испытывая несколько различных значений t, найдем некоторое t', такое что выражение $[(\alpha^{Ht'} y)^{t'} \bmod p]\, t'^{-1} \bmod \gamma$ имеет значение T, которое является квадратичным вычетом. Элемент подписи k находим, извлекая квадратный корень из T: $k = \sqrt{T} \bmod \gamma$, что не является сложной задачей. После этого вычисляем второй элемент подписи $g = kt \bmod \gamma$.

136. Введем новую переменную $t = (g + k^{-1}) \bmod \gamma$. Тогда проверочное уравнение приобретает вид $\dfrac{g}{t-g} = (\alpha^t y^H \bmod p) \bmod \gamma$. Выбираем произвольное отличное от нуля значение t и вычисляем элемент подписи $g = \dfrac{Zt}{1+Z} \bmod \gamma$, где $Z = (\alpha^t y^H \bmod p) \bmod \gamma$. После этого вычисляем элемент подписи $k = (1/(t-g)) \bmod \gamma$. Другой способ подделки подписи основан на решении системы уравнений $g + k^{-1} \equiv U \bmod \gamma$ и $kg \equiv Z \bmod \gamma$, где $Z = \alpha^U y^H \bmod p$.

137. Рассмотрим первую схему. Генерация подписи включает следующие шаги: 1) выбираем два случайных числа U и U' ($U, U' < \gamma$); 2) вычисляем значения $Z = (\alpha^U \bmod p) \bmod \gamma$, $Z' = (\alpha^U \bmod p) \bmod \gamma$ и $k = ZZ' \bmod \gamma$; 3) вычисляем значение $g = U/k \bmod \gamma$; 4) из сравнения $g + v + xkH \equiv U' \bmod \gamma$ находим третий элемент подписи: $v \equiv U' - g - xkH \bmod \gamma$. Теперь рассмотрим вторую схему. Здесь в каждую из скобок входят значения α и y, однако в каждую из скобок один из этих параметров входит как константа, поэтому становится возможной подделка подписи: 1) выбираем два случайных числа U и U' ($U, U' < \gamma$); 2) вычисляем значения $Z = (\alpha^U y \bmod p) \bmod \gamma$, $Z' = (\alpha^H y^U \bmod p) \bmod \gamma$ и $k = Z^{Z'} \bmod \gamma$; 3) вычисляем значение $g = U/k \bmod \gamma$; 4) из сравнения $vk \equiv U' \bmod \gamma$ находим третий элемент подписи: $v \equiv U'/k \bmod \gamma$. Таким образом, во второй схеме формирование подписи можно осуществить без использования секретного ключа.

138. Идея механизма формирования подписи состоит в том, чтобы выбрать некоторую величину произведения значений k и g, которое обозначим U. Поскольку U задано, то это, согласно проверочному уравнению, однозначно зафиксирует значение k. После этого значение g рассчитывается таким, чтобы произведение k и g было равно выбранной вначале величине U. Очевидно, что эту схему формирования пары значений (k, g) можно легко реализовать, используя значение функции Эйлера от модуля, которое равно $p-1$. Однако в этом случае длина $|g|$ будет примерно равна длине $|p|$. Вероятность случайно получить g, для которого выполняется условие $|g| < \frac{2}{3}|p|$, пренебрежимо мала. Выполнение последнего соотношения реализуется при использовании того обстоятельства, что число α относится по модулю p к показателю q. Использование секретного значения q определяет следующие вычисления при формировании подписи: 1) выбираем случайное число U ($U < q$); 2) вычисляем значения $Z = (\alpha^{UH} \bmod p) \bmod \delta$ и $k = Z \bmod \gamma$; 3) вычисляем значение $g = U/k \bmod q$. Таким образом, мы сформировали подпись (k, g), в которой длина $|g|$ будет примерно равна длине $|q| \approx 0.5|p|$.

139. При указанном проверочном уравнении процедура генерации подписи может быть основана на предварительном случайном выборе значений сумм $k + g \equiv U_1 \bmod \delta - 1$ (1) и $\nu + kH \equiv U_2 \bmod \gamma$ (2). Если значения этих сумм считать заданными (фиксированными), то значение элемента подписи k предопределено: $k = \alpha^{U_1}(\alpha^{U_2} \bmod n) \bmod \delta$. Значения двух оставшихся элементов подписи вычисляются исходя из условий (1) и (2): $g = U_1 - k \bmod \delta - 1$ и $x\nu = (U_2 - kH)x^{-1} \bmod \gamma$. Таким образом, при произвольных простых модулях p и δ указанное уравнение является корректным как проверочное в смысле возможности вычисления подписи к заданному сообщению при известном секретном ключе. Однако в плане безопасности схемы ЭЦП числа α, p и δ должны быть такими, что α относится к достаточно большому показателю как по модулю p, так и по модулю δ. При этом число α должно относиться по модулю p к простому показателю $\gamma | p-1$. Если в качестве γ выбрать составное число, то при выборе секретного ключа потребуется осуществлять проверку НОД$(x, \gamma) = 1$. Если γ есть сравнительно малое число, то можно сравнительно легко подобрать значение $x' \equiv x \bmod \gamma$, которое является эквивалентным секретному ключу в смысле возможности вычислительно эффективного нахождения правильной подписи к заданному документу. Если α будет относиться к достаточно большому показателю по модулю p и к сравнительно малому показателю $\gamma' | \delta - 1$ по модулю δ, то путем нахождения значений $g' \equiv g \bmod \gamma'$ потенциальный нарушитель

сможет достаточно легко модифицировать известную подпись, хотя подделка подписи будет оставаться для него вычислительно неосуществимой задачей.

140. При указанном проверочном сравнении процедура генерации подписи может быть основана на предварительном случайном выборе значения суммы $g + xkH \equiv U \bmod \gamma$ (1). При фиксировании этой суммы значение элемента подписи k предопределено: $k = \pm\sqrt{(\alpha^U \bmod p)} \bmod \gamma$. Значение второго элемента подписи вычисляется исходя из условия (1): $g = U \mp xH\sqrt{(\alpha^U \bmod p)} \bmod \gamma$.

141. Процедура генерации подписи включает предварительный выбор случайного значения суммы $g^2H + xk \equiv U \bmod \gamma$ (1). Задание значения этой суммы предопределяет значение элемента подписи k: $k = \pm\sqrt{(\alpha^U \bmod p)} \bmod \gamma$. Значение второго элемента подписи вычисляется исходя из условия (1): $g = \pm\sqrt{H^{-1}(U \mp x\sqrt{(\alpha^U \bmod p)})} \bmod \gamma$ (т. е. для заданного значения $U < \gamma$ имеем четыре различных значения подписи (k, g)).

142. Процедура генерации подписи включает предварительный выбор случайного значения суммы $kg + xk + xg \equiv U \bmod \gamma$ (1). Согласно проверочному сравнению задание значения U предопределяет значение суммы $k + g$: $k + g \equiv HZ \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Следовательно, значение подписи вычисляется как решение системы сравнений (1) и (2):

$$k = \frac{HZ}{2} \pm \sqrt{\frac{H^2Z^2}{4} + xHZ - U} \bmod \gamma \quad \text{и} \quad g = \frac{HZ}{2} \mp \sqrt{\frac{H^2Z^2}{4} + xHZ - U} \bmod \gamma$$

(т. е. для заданного значения $U < \gamma$ имеем два различных значения подписи (k, g)). Если выражение под корнем окажется квадратичным невычетом, то процедуру формирования подписи следует повторить при новом случайном значении $U < \gamma$.

143. При указанном проверочном сравнении процедура генерации подписи может быть основана на предварительном случайном выборе значения суммы $k + xg \equiv U \bmod \gamma$ (1). При фиксировании этой суммы значение элемента подписи k предопределено: $k = H + Z \bmod \gamma$, где $Z = H\alpha^U \bmod p$. Значение второго элемента подписи легко определяется с учетом условия (1): $g = \dfrac{U - H - Z}{x} \bmod \gamma$.

144. Процедура генерации подписи осуществляется следующим образом. Предварительно выбирается случайное значение суммы $gH + xk \equiv$

$\equiv U \bmod \gamma$ (1). Затем вычисляется значение элемента подписи k: $k = Z - H \bmod \gamma$, где $Z = \alpha^U \bmod p$. Значение второго элемента подписи определяется с учетом условия (1): $g = \dfrac{U - xZ + xH}{H} \bmod \gamma$.

145. Процедура генерации подписи включает предварительный выбор случайного значения суммы $k + xg \equiv U \bmod \gamma$ (1). Согласно проверочному сравнению, задание значения U предопределяет значение суммы $k + g$: $k + g \equiv HZ \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Следовательно, значение подписи вычисляется как решение системы сравнений (1) и (2): $k = \dfrac{U - xHZ}{1 - x} \bmod \gamma$ и $g = \dfrac{HZ - U}{1 - x} \bmod \gamma$.

146. Процедура генерации подписи включает предварительный выбор случайного значения суммы $H(k - g) + xk \equiv U \bmod \gamma$ (1). Согласно проверочному сравнению, задание значения U предопределяет значение суммы $k + g$: $k + g \equiv Z \bmod \gamma$ (2), где $Z = \alpha^U \bmod p$. Следовательно, значение подписи вычисляется как решение системы сравнений (1) и (2): $k = \dfrac{U + HZ}{2H + x} \bmod \gamma$ и $g = \dfrac{HZ + xZ - U}{2H + x} \bmod \gamma$.

147. *Первый механизм* основан на предварительном выборе случайного значения суммы $Hg + xk \equiv U \bmod \gamma$ (1). Согласно проверочному сравнению задание значения U предопределяет значение k: $k = Z = (\alpha^U \bmod p) \bmod \gamma$ (2). Второй элемент подписи вычисляется из сравнения (1): $g = \dfrac{U - xZ}{H} \bmod \gamma$. *Второй механизм* основан на предварительном вычислении значения k по формуле $k = (\alpha^w \bmod p) \bmod \gamma$, где w — случайное значение, и решении сравнения $\alpha^w \equiv \alpha^{Hg} y^k \bmod p$ относительно g: $g = \dfrac{w - xk}{H} \bmod \gamma$. Большей общностью обладает первый механизм, так как он дает возможность сформировать подпись в ряде схем ЭЦП, для которых второй механизм непригоден. Например, в случае проверочных уравнений вида $k \equiv g(\alpha^{Hg} y^k \bmod p) \bmod \gamma$ и $g + k \equiv (H\alpha^g y^k \bmod p) \bmod \gamma$.

148. Процедура генерации подписи включает предварительное формирование числа $R = \alpha^k \bmod p$, после чего вычисляются значения $E = HR \bmod \gamma$ и $S = k - xE \bmod \gamma$.

149. Процедура генерации подписи основана на представлении числа R в виде $R = \alpha^k \bmod p$ и предварительном выборе случайного значения

суммы $g + kH \equiv U \bmod \gamma$ (1), что задает значение $E = (\alpha^U \bmod p) \bmod \gamma$. Согласно проверочному сравнению должно выполняться сравнение $k \equiv xE + g \bmod \gamma$ (2). Решая систему сравнений (1) и (2), находим g.

150. Процедура генерации подписи включает предварительное формирование случайного числа U, по которому вычисляются значения $Z = (H\alpha^U \bmod p) \bmod \gamma$ и $Z' = (\alpha^U \bmod p) \bmod \gamma$. Затем решается система из следующих трех сравнений: $k = xZ \bmod \gamma$ (1); $g = vZ' \bmod \gamma$ (2) и $k + g \equiv U \bmod \gamma$ (3). Соотношение (1) позволяет непосредственно вычислить степень k, по которой находим элемент подписи R: $R = \alpha^k \bmod p$. Из выражения (3) находим степень g: $g = (U - xZ) \bmod \gamma$, по которой вычисляем элемент подписи S: $S = \alpha^g \bmod p$. Значение v находим по формуле: $v = \dfrac{U - xZ}{Z'} \bmod \gamma$.

151. Процедура генерации подписи включает предварительное формирование случайных чисел U_1 и U_2, по которым вычисляются значения $Z_1 = (\alpha^{U_1} \bmod p) \bmod \gamma$ и $Z_2 = (\alpha^{U_2} \bmod p) \bmod \gamma$. Затем решается система из следующих трех сравнений: $k + g \equiv U_1 \bmod \gamma$ (1); $k - g \equiv U_2 \bmod \gamma$ (2) и $k \equiv g + Z_1 H + xvZ_2 \bmod \gamma$ (3). Решение системы дает следующие формулы: $k = \dfrac{U_1 + U_2}{2} \bmod \gamma$, $g = \dfrac{U_1 - U_2}{2} \bmod \gamma$ и $v = \dfrac{U_2 - Z_1 H}{xZ_2} \bmod \gamma$. По степеням k и g находим: $R = \alpha^k \bmod p$ и $S = \alpha^g \bmod p$.

7.2.3. Комбинированные схемы ЭЦП

152. Структура простого модуля p должна быть следующей: $p = 2rq + 1$, где r и q есть два больших простых числа. Число α можно выбрать таким, чтобы по модулю p оно относилось к показателю r или q. При этом следует задать ограничение размера элемента подписи S: $|S| < \dfrac{|p|}{2} + 1$.

Процедура генерации подписи включает следующие шаги. Представим R в виде $R = \alpha^t \bmod p$. Значение t выбирается случайным образом. Затем вычисляются значения R и $E = F(R, H)$. Второй элемент подписи вычисляется по формуле: $S = t - xE \bmod q$. Процедура проверки подписи состоит в вычислении значения R, по которому затем определяется значение $E' = F(R, H)$. Если $E' = E$, то подпись признается подлинной.

153. Простой модуль p можно сформировать в виде $p = 2rq + 1$, где r и q есть два больших простых числа. Число α можно выбрать таким, чтобы по модулю p оно относилось к показателю, равному меньшему из чисел r и q. При этом следует задать ограничение размера элемента подписи S:

$|S| < \frac{|p|}{2} + 1$. Далее предположим, что $r > q$. Процедура генерации подписи включает следующие шаги. Представим R в виде $R = \alpha^k \bmod p$. Выберем случайное число U и вычислим значение $E = F(\alpha^U \bmod p)$, используя которое определим $g = \frac{U - xE}{H + 1} \bmod q$ (последняя формула получается как решение системы сравнений $k + g = U \bmod q$ и $k = xE + gH \bmod q$). Процедура проверки подписи состоит в вычислении значения R, по которому затем определяется значение $E' = F(R\alpha^g \bmod p)$. Если $E' = E$, то подпись признается подлинной.

154. Для понимания процедуры генерации подписи представим R в виде $R = \alpha^k \bmod p$. Выберем случайное число U и вычислим значение $E = F(\alpha^U \bmod n)$, используя которое определим $g = \pm\sqrt{\frac{U}{EH}} \bmod \gamma$ (последняя формула получается как решение системы сравнений $kg = U \bmod \gamma$ и $k = EgH \bmod \gamma$). Процедура проверки подписи состоит в вычислении значения R, по которому затем определяется значение $E' = F(R^g \bmod n)$. Если $E' = E$, то подпись признается подлинной.

155. Для понимания процедуры генерации подписи представим R в виде $R = \alpha^k \bmod p$. Выберем случайное число U и вычислим значение $E = F(\alpha^U \bmod p)$, используя которое определим $g = \pm\sqrt{\frac{U}{EH}} \bmod \gamma$ (последняя формула получается как решение системы сравнений $kgH = u \bmod \gamma$ и $k = Eg \bmod \gamma$). Процедура проверки подписи состоит в вычислении значения R, по которому затем определяется значение $E' = F(R^g \bmod n)$. Если $E' = E$, то подпись признается подлинной.

156. Для понимания процедуры генерации подписи представим R в виде $R = \alpha^k \bmod p$. Выберем случайное число U и вычислим значение $E = F(\alpha^U \bmod p)$, используя которое определим значение g: $g = -\frac{H}{2} \pm \sqrt{\frac{H^2}{4} + \frac{U}{EH}} \bmod \gamma$ (последняя формула получается как решение системы сравнений $kg + kH = U \bmod \gamma$ и $k = EgH \bmod \gamma$). Процедура проверки подписи состоит в вычислении значения R, по которому затем определяется значение $E' = F(R^{g \cdot H} \bmod n)$. Если $E' = E$, то подпись признается подлинной.

157. Представим элемент подписи k в виде $k = F(\alpha_1^{t_1} \bmod n_1 + \alpha_2^{t_2} \bmod n_2)$. Значения t_1 и t_2 выбираются предварительно, после чего вычисляется

значение k. Проверочное уравнение выполнится, если будет иметь место соотношение $\alpha_1^{t_1} \bmod n_1 + \alpha_2^{t_2} \bmod n_2 = \alpha_1^{kgH} \bmod n_1 + \alpha_2^{kg+H} \bmod n_2$. Приравнивая соответствующие слагаемые, получаем: $t_1 \equiv kgH \bmod \gamma \Rightarrow$ $\Rightarrow g = \frac{t_1}{kH} \bmod \gamma$ (1) и $t_2 \equiv kg + H \bmod \gamma \Rightarrow g = \frac{t_2 - H}{k} \bmod \gamma$ (2). Легко видеть, что значения t_1 и t_2 следует выбирать такими, чтобы выполнялось условие $t_2 - H \equiv \frac{t_1}{H} \bmod \gamma \Rightarrow t_2 \equiv \frac{t_1}{H} + H \bmod \gamma$ (3). Значение k вычисляется по t_1 и t_2, удовлетворяющим условию (3). Затем вычисляется значение второго элемента подписи g по формуле (1) или (2). (Другой вариант решения связан с использованием фиксирующего сравнения $kg \equiv U \bmod \gamma$.)

158. Процедура генерации подписи основана на возможности одновременного фиксирования значений $\alpha_1^{kgH} \bmod n_1$ и $\alpha_2^{kg+H} \bmod n_2$ при выполнении условия $kg \equiv U \bmod \gamma$ (1), где U — произвольное число. При формировании подписи к сообщению, хэш-функция от которого имеет значение H, следует решить систему соотношений, состоящую из сравнения (1) и следующего уравнения: $g - k = Z$, где $Z = F(\alpha_1^{UH} \bmod n_1 +$ $+ \alpha_2^{U+H} \bmod n_2)$. Решение дает: $k = -\frac{Z}{2} \pm \sqrt{\frac{Z^2}{4} + U} \bmod \gamma$ и $g = Z + k$.

159. Выберем сравнительно большое произвольное значение U и вычислим значение $k = F(\alpha^U \bmod n)$. Элемент подписи g вычислим по формуле $g = U - H - k$. После нескольких попыток с большой вероятностью мы получим положительное значение g. Усиления заданной схемы можно достичь, например, придавая проверочному соотношению вид $k - g =$ $= F(\alpha^{k+g+H} \bmod n)$ или $k = F(\alpha^{kgH} \bmod n)$.

160. Процедура генерации подписи основана на решении следующей системы соотношений: $\begin{cases} k + g = Z, \\ kgH \equiv U \bmod \gamma, \end{cases}$ из которой можно получить следующие формулы: $k = \frac{Z}{2} \pm \sqrt{\frac{Z^2}{4} - \frac{U}{H}} \bmod \gamma$ и $g = Z - k$, где $Z =$ $F(\alpha^U \bmod n)$. Чтобы избежать отрицательных значений, следует выбрать сжимающую функцию, которая с достаточно малой вероятностью принимает значения, меньшие γ. (На практике выполнения последнего условия удобнее добиваться выбором соответствующего размера числа γ.)

161. Процедура генерации подписи основана на представлении параметра R в виде $R = \alpha^k \bmod n$ и решении следующей системы сравнений: $\begin{cases} kg \equiv U \bmod \gamma, \\ k \equiv EH + g \bmod \gamma, \end{cases}$ из которой можно получить следующие формулы: $k = \frac{EH}{2} \pm \sqrt{\frac{E^2H^2}{4} + U} \bmod \gamma$ и $g = k^{-1} U \bmod \gamma$. Формирование подписи начинается с выбора случайного значения U и последующего вычисления значений $E = F(\alpha^U \bmod n)$, k и g.

162. Процедура генерации подписи основана на решении следующей системы сравнений: $\begin{cases} ks + vH \equiv u \bmod p, \\ k + v \equiv t \bmod p, \end{cases}$ где $t = \psi(u * G)$, из которой можно получить следующие формулы: $k = \frac{tH - u}{H - s} \bmod p$ и $v = \frac{u - ts}{H - s} \bmod p$. Формирование подписи начинается с выбора случайного значения u и последующего вычисления значений t, k и v.

163. Процедура генерации подписи основана на решении следующей системы сравнений: $\begin{cases} ks + vH \equiv u \bmod p, \\ k \equiv vt \bmod p, \end{cases}$ где $t = \psi(u * G)$, из которой можно получить следующие формулы: $k = \frac{ut}{ts + H} \bmod p$ и $v = \frac{u}{ts + H} \bmod p$. Формирование подписи начинается с выбора случайного значения u и последующего вычисления значений t, k и v.

164. Процедура генерации подписи основана на решении следующей системы сравнений: $\begin{cases} k = t, \\ kgH \equiv u_1 \bmod \gamma, \\ ks + vH \equiv u_2 \bmod p, \end{cases}$ где $t = (\alpha^{u_1} \bmod n) + \psi(u_2 * G)$, из которой можно получить формулы: $g = \frac{u_1}{tH} \bmod \gamma$ и $v = \frac{u_2 - ts}{H} \bmod p$. Формирование подписи начинается с выбора случайных значений u_1 и u_2, после чего вычисляются значения $t = k$, g и v.

165. Процедура генерации подписи основана на решении следующей системы сравнений: $\begin{cases} k = t, \\ ks_1 + vH \equiv u_1 \bmod p_1, \\ ks_2 + w + H \equiv u_2 \bmod p_2, \end{cases}$ где $t = \psi_1(u_1 * G_1) + \psi_2(u_2 * G_2)$,

из которой можно получить следующие формулы: $v = \frac{u_1 - s_1 t}{H} \bmod p_1$ и $w = u_2 - s_2 t - H \bmod p_2$. Формирование подписи начинается с выбора случайных значений u_1 и u_2 и последующего вычисления значений $t = k$, v и w.

166. Процедура генерации подписи основана на решении следующей системы сравнений: $\begin{cases} k = t, \\ xkH + g \equiv u_1 \bmod \gamma, \\ ks + vH \equiv u_2 \bmod p, \end{cases}$ где $t = \{(\alpha^{u_1} \bmod p') + \psi(u_2 * G)\} \bmod p$, из которой можно получить следующие формулы: $g = (u_1 - xtH) \bmod \gamma$ и $v = \frac{u_2 - ts}{H} \bmod p$. Формирование подписи начинается с выбора случайных значений u_1 и u_2, после чего вычисляются значения $t = k$, g и v.

167. Процедура генерации подписи основана на представлении параметра R в виде $R = \alpha^k \bmod p$ и совместном решении следующих двух сравнений: $k + S^2 \equiv U \bmod q$ (1) и $k \equiv xS^2 + EH \bmod q$ (2), где в качестве U выбирается случайное число и $E = (\alpha^U \bmod p) \bmod \gamma$. Решение системы дает следующие формулы для вычисления элементов подписи: $k = \frac{Ux + EH}{x + 1} \bmod q$ и $S^2 \bmod q = \frac{U - EH}{x + 1} \bmod q$. Если в последней формуле значение правой части является квадратичным невычетом по модулю q, то следует выбрать новое значение U и повторить вычисление значения $Z = S^2 \bmod q$. Извлекая квадратный корень по модулю q из найденного значения Z, можно определить элемент подписи S. Решение задачи дискретного логарифмирования по простому модулю позволяет определить значение секретного значения x, что дает возможность вычислить пару (E, Z), однако для нахождения правильного значения S требуется еще вычислить квадратный корень из Z. Для этого нужно определить значение модуля, по которому следует извлечь квадратный корень. Однако атакующему нет необходимости решать задачу факторизации числа n. Найти значение q можно, используя значения $x = \log_\alpha y (\bmod p)$ и $k = \log_\alpha R (\bmod p)$, получаемые в результате решения задачи дискретного логарифмирования. Поскольку $k \equiv xS^2 + EH \bmod q$ и $W \overset{def}{=} [(xS^2) \bmod n] \equiv xS^2 \bmod q$, то $q | (W + EH - k)$, поэтому, разлагая число $W + EH - k$, которое легко вычисляется по известной подписи, на множители, значение q можно найти как один из сомножителей указанного

разложения. Таким образом, безопасность заданной схемы ЭЦП определяется сложностью задачи логарифмирования по модулю p. Нет необходимости непосредственного решения задачи факторизации числа n.

168. Процедура генерации подписи состоит в следующем. Выбирается случайное число k, вычисляется значение $R = \alpha^k \bmod p$, определяется значение $E = (R^H \bmod p) \bmod \gamma$ и решается следующее сравнение: $k \equiv xS^2 + E \bmod q$. В результате решения имеем: $Z = S^2 \bmod q = x^{-1}(k - E) \bmod q$. Если в последней формуле значение правой части является квадратичным невычетом по модулю q, то следует выбрать новое значение k и повторить вычисление значения $Z = S^2 \bmod q$. Извлекая квадратный корень по модулю q из найденного значения Z, определяем элемент подписи S. Решение задачи дискретного логарифмирования по простому модулю позволяет определить значение секретного значения x, что дает возможность вычислить пару (E, Z), однако для нахождения правильного значения S требуется еще вычислить квадратный корень из Z. Для этого нужно определить значение модуля q, по которому следует выполнить операцию извлечения квадратного корня. Потенциальному атакующему нет необходимости решать задачу факторизации числа n непосредственно. Он может воспользоваться результатами решения задачи дискретного логарифмирования. Действительно, найти значение q можно, используя значения $x = \log_\alpha y \pmod p$ и $k = \log_\alpha R \pmod p$, следующим образом. Поскольку $k \equiv xS^2 + E \bmod q$ и $W \overset{def}{=} [(xS^2) \bmod n] \equiv xS^2 \bmod q$, то $q \mid (W + E - k)$, поэтому q можно найти как один из сомножителей числа $W + E - k$, которое легко вычисляется по известной подписи. Таким образом, безопасность заданной схемы ЭЦП определяется только сложностью задачи логарифмирования по модулю p (решение задачи факторизации числа n не приводит к взлому рассмотренной схемы ЭЦП). Взлом рассмотренной схемы ЭЦП не требует одновременного решения двух трудных математических задач.

169. Процедура генерации подписи состоит в следующем. Выбирается случайное число k, вычисляется значение $R = \alpha^k \bmod p$, определяется значение $E = R^H \bmod \gamma$ и решается следующее сравнение: $k \equiv S^2 + E \bmod q$. В результате решения имеем: $Z = S^2 \bmod q = (k - E) \bmod q$. Если в последней формуле значение правой части является квадратичным невычетом по модулю q, то следует выбрать новое значение k и повторить вычисление значения $Z = S^2 \bmod q$. Извлекая квадратный корень по модулю q из квадратичного вычета Z, определяем элемент подписи S. Решение задачи дискретного логарифмирования по простому модулю позволяет определить значение секретного значения x, что дает возмож-

ность вычислить пару (E, Z), однако для нахождения правильного значения S требуется еще вычислить квадратный корень из Z. Это можно сделать без осуществления непосредственного разложения на множители числа n (чтобы определить значение модуля, по которому следует извлечь квадратный корень). Если в качестве подписи использовать пару чисел (E, Z), то сложность процедуры генерации подписи уменьшается в среднем вдвое. Для взлома исходной и модифицированной схемы ЭЦП достаточно разработать эффективный метод дискретного логарифмирования. Действительно, определив значения $x = \log_\alpha y \pmod p$ и $k = \log_\alpha R \pmod p$, мы получаем следующий вид проверочного соотношения $\alpha^k \equiv \alpha^{(xE+S^2) \bmod n} \bmod p$, где $k \equiv [(xE + S^2) \bmod n] \bmod q$. Из последнего соотношения следует $k \equiv xE + S^2 \bmod q$, поэтому $q \mid (xE + S^2 - k)$. Последнее соотношение показывает, что, получив образец некоторой подписи и решив задачу дискретного логарифмирования, атакующий может определить секретное число q как один из простых делителей числа $E + S^2 - k$. Так как атакующий может получить большое число различных подписей, то он может выбрать те из них, для которых разложение числа $xE + S^2 - k$ имеет сравнительно низкую трудоемкость. Замена исходного проверочного уравнения на $R = y^E \alpha^Z \bmod p$ практически не изменяет исходного уровня ее безопасности, однако вдвое снижает сложность процедуры генерации подписи.

170. Процедура генерации подписи основана на представлении параметра R в виде $R = \alpha^k \bmod p$ и совместном решении следующих двух сравнений: $k + S \equiv U \bmod q$ (1) и $k \equiv xEH + S^2 \bmod q$ (2), где в качестве U выбирается случайное число и $E = (\alpha^U \bmod p) \bmod \gamma$. Решение системы дает следующие формулы для вычисления элементов подписи: $S = -\frac{1}{2} \pm \sqrt{\frac{1}{4} + U - xEH} \bmod q$ и $k = U - S \bmod q$. Если в первой формуле подкоренное выражение является квадратичным невычетом по модулю q, то следует выбрать новое значение U и повторить вычисление значения S. Для вычисления квадратного корня нужно определить значение модуля q, что можно сделать, минуя проблему факторизации числа n. Действительно, найти значение q можно, используя значения $x = \log_\alpha y \pmod p$ и $k = \log_\alpha R \pmod p$, следующим путем. Согласно процедуре генерации подписи имеем $k \equiv xEH + S^2 \bmod q$, поэтому $q \mid (xEH + S^2 - k)$, поэтому q можно найти как один из сомножителей числа $xEH + S^2 - k$, которое легко вычисляется по известной подписи. Приходим к выводу, что взлом рассмотренной схемы ЭЦП не требует одновременного решения двух трудных математических задач — дис-

кретного логарифмирования и факторизации составного числа, содержащего два больших неизвестных простых делителя. Безопасность заданной схемы ЭЦП определяется только сложностью задачи логарифмирования по модулю p (решение задачи факторизации числа n не приводит к взлому рассмотренной схемы ЭЦП).

171. Процедура генерации подписи включает следующую последовательность шагов: 1) выбирается случайное число U; 2) вычисляется значение $k = Z = (\alpha^U \bmod p) \bmod \delta$; 3) решается сравнение $xZH + g \equiv U \bmod q$, что дает значение $g \equiv U - xZH \bmod q$; 4) в качестве подписи берется пара найденных чисел (k, g). Для взлома рассматриваемой схемы ЭЦП достаточно иметь эффективный метод вычисления дискретных логарифмов. Действительно, определив значение $x = \log_\alpha y \pmod p$, мы получаем следующий вид проверочного соотношения $k = (\alpha^{xkH+g} \bmod p) \bmod \delta$, которое можно представить в виде $(\alpha^t \bmod p) \bmod \delta = (\alpha^{xkH+g} \bmod p) \bmod \delta$, следовательно, $t \equiv xkH + g \bmod q$ и $q \mid (xkH + g - t)$. Последнее соотношение показывает, что, получив образец некоторой подписи, вычислив $Z = \alpha^{xkH+g} \bmod p$ и $t = \log_\alpha Z \pmod p$, атакующий может определить секретное число q как один из простых делителей числа $xkH + g - t$. Так как атакующий может получить большое число различных подписей, то он может выбрать те из них, для которых разложение числа $xkH + g - t$ имеет сравнительно низкую трудоемкость. Таким образом, взлом модифицированной схемы ЭЦП требует решения только одной трудной математической задачи — задачи дискретного логарифмирования. Если в процедуру генерации подписи включить вычисления, обеспечивающие высокую сложность разложения числа $xkH + g - t$, то это неоправданно усложнит формирование подписи, делая рассматриваемую схему ЭЦП малопригодной для практического применения (заметим, что при формировании подписи число k можно вычислять в виде $k = (\alpha^t \bmod p) \bmod \delta$, что дает следующую формулу для вычисления второго элемента подписи: $g = (t - xkH) \bmod q$).

172. Сокращение размера подписи обеспечивается тем, что в качестве параметра α в модифицированной схеме ЭЦП выбирается значение, относящееся к показателю q по модулю p. В качестве параметра β следует выбрать число, относящееся по модулю q к некоторому простому делителю $\gamma \mid q - 1$ (пара чисел (γ, q) есть секретный ключ), причем по модулю n число β должно относиться к показателю $\delta = \gamma\gamma'$, где $\gamma' \mid r - 1$ и $|\gamma'| > |\gamma|$, причем γ не делит $r - 1$ (последнее требование предотвращает возможность вычисления секретного числа γ как делителя числа $n - 1$). Генерация подписи состоит в вычислении значений $t = H^{-1} \bmod \gamma$ и $S = \beta^t \bmod q$. Из последней формулы видно, что размер подписи S при-

мерно равен размеру модуля q, т. е. сокращение размера подписи в модифицированной схеме обеспечивается за счет того, что ее вычисление осуществляется по модулю q. Покажем, что сформированная указанным способом подпись удовлетворяет проверочному соотношению. Пусть $Z = S^H \bmod n$, тогда $Z \equiv S^H \equiv \beta^{H-1H} \equiv \beta \bmod q$. Поскольку α представляет собой число, относящееся по модулю p к показателю q, то из условия $Z = (S^H \bmod n) \equiv \beta \bmod q$ следует $\alpha^{\beta} \equiv \alpha^{S^H \bmod n} \bmod p$. Рассматриваемая схема ЭЦП не является стойкой. Значение может быть найдено по двум подписям S_1 и S_2, соответствующим значениям хэш-функции H_1 и H_2, как делитель числа $S_1^{H_1} \bmod n - S_2^{H_2} \bmod n$.

173. Формирование подписи осуществляется следующим образом. Выбирается случайное число k и вычисляется значение $R = \alpha^{\beta^k \bmod q} \bmod p$. Затем вычисляются элементы подписи: $E = R^H \bmod \delta$ и $S = \dfrac{k - E}{x} \bmod \gamma$.

Рассмотрим варианты подделки подписи. *Первый вариант* основан на разложении числа n, что позволяет вычислить q и γ. Третий секретный элемент определяется вычислением дискретного логарифма $x = \log_{\beta} y \pmod q$, сложность которого определяется размером чисел γ и q. Во *втором варианте* предполагается, что предварительно будет решаться задача дискретного логарифмирования. По известной подписи атакующий вычисляет $K = \log_{\alpha} R \pmod p$, затем определяет значение $Z = \beta^E y^S \bmod n \Rightarrow Z \equiv \beta^E y^S \bmod q$. В соответствии с процедурой генерации подписи имеем: $K \equiv \beta^E y^S \bmod q$, поэтому $K \equiv Z \bmod q$. Поскольку $q \mid Z - K$, то, разлагая значение $Z - K$ на множители, легко определить q. Заметим, что атакующий может иметь большое число различных подписей, поэтому он с достаточно большой вероятностью найдет пару значений $Z - K$ и $Z' - K'$, таких что НОД$(Z - K, Z' - K')$ содержит только один большой делитель q. Определив q, атакующий вычисляет $x = \log_{\beta} y \pmod q$. Разлагая значение $q - 1$ на множители, легко определить секретное значение γ. Учитывая известные в настоящее время алгоритмы факторизации и дискретного логарифмирования и то, что размеры чисел n и p примерно равны, можно сделать заключение, что оба указанных выше варианта атаки имеют примерно одинаковую трудоемкость. Для взлома заданной схемы ЭЦП достаточно решить только одну из упомянутых сложных задач.

174. В схеме ЭЦП с проверочным сравнением $\alpha^{\beta^H \bmod n} \equiv \alpha^{y^S R \bmod n} \bmod p$ генерация подписи осуществляется следующим образом. Выбирается случайное число $k < \gamma$ и вычисляется значение $R \equiv \beta^k \bmod q$, а затем и

значение $S = \frac{H - K}{x} \bmod \gamma$. На первый взгляд эта схема ЭЦП представляется стойкой, поскольку вычисление параметра $R \equiv \beta^H y^{-S} \bmod n$ при произвольно выбранном числе S дает значение $|R| \approx |n| \approx 1200$ бит. Для того, чтобы получить требуемый размер $|R| < 610$ бит, нужно выполнить разложение модуля n. Однако последнее может быть сравнительно легко реализовано по одной или нескольким известным подписям. Пусть $V \overset{def}{=} \beta^H \bmod n \Rightarrow V \equiv \beta^H \bmod q$ и $W = y^S R \bmod n \Rightarrow W \equiv$ $\equiv y^S R \bmod q$. В соответствии с процедурой генерации подписи имеем: $\beta^H \equiv y^S R \bmod q$, следовательно, $V \equiv W \bmod q \Rightarrow q \mid W - V$. Разлагая значение $W - V$ на множители, легко определить значение q (заметим, что в общем случае $W \neq V$). При наличии у атакующего нескольких подлинных подписей он с большой вероятностью найдет пару значений $W - V$ и $W' - V'$, таких что НОД$(W - V, W' - V')$ содержит только один большой делитель q. Таким образом, для вычисления секретных значений не требуется решения какой-либо трудной математической задачи. Рассмотренная схема ЭЦП не является безопасной.

175. Формирование подписи осуществляется следующим образом. Выбирается случайное число k и вычисляется первый элемент подписи: $R \equiv \beta^k \bmod q$, длина которого составит $|R| \approx |q| \approx 600$ бит. Затем вычисляется второй элемент подписи: $S = \frac{k + x}{H} \bmod \gamma$, длина которого составит $|S| \approx |\gamma| \approx 128$ бит. Последняя формула определяется соотношением $k + x \equiv SH \bmod \gamma$, которое обеспечивает выполнимость уравнения проверки подписи. Действительно, из него следует: $\beta^{k+x} \equiv \beta^{HS} \bmod q \Rightarrow$ $\Rightarrow \alpha^{\beta^{k+x} \bmod q} \equiv \alpha^{\beta^{HS} \bmod q} \bmod p \Rightarrow y^R \equiv \alpha^{\beta^{HS} \bmod q} \bmod p$. Еще следует показать, что из $y^R \equiv \alpha^{\beta^{HS} \bmod q} \bmod p$ следует $y^R \equiv \alpha^{\beta^{HS} \bmod n} \bmod p$ (проверяющий пользуется этим сравнением для проверки подписи, поскольку он не знает числа q). Поскольку $\beta^x R \equiv \beta^{HS} \bmod q$ и $W \overset{def}{=} (\beta^{HS} \bmod n) \equiv$ $\equiv \beta^{HS} \bmod q$, то $\beta^x R \equiv W \bmod q \Rightarrow y^R \equiv \alpha^{\beta^x R} \equiv \alpha^{\beta^{HS} \bmod n} \bmod p$, что требовалось показать. Рассмотрим вопрос стойкости заданной схемы ЭЦП. Для ее взлома достаточно решить одну из двух следующих трудных математических проблем — задачу факторизации числа n или задачу дискретного логарифмирования по простому модулю. Пусть атакующий умеет эффективно вычислять дискретные логарифмы по простому модулю p. Тогда он может вычислить $X = \log_\alpha y \,(\bmod p)$ и $x =$

$= \log_\beta X (\mathrm{mod}\, q)$. Зная некоторую правильную подпись, можно составить соотношение $XR \equiv (\beta^{HS} \bmod n) \bmod q$, т. е. $q \mid [XR - (\beta^{HS} \bmod n)]$. В общем случае $XR \neq \beta^{HS} \bmod n$, поэтому значение q может быть определено разложением числа $XR - (\beta^{HS} \bmod n)$ на множители. Если имеется несколько подлинных подписей, то с большой вероятностью будет найдена пара подписей (R, S) и (R', S'), для которой наибольший общий делитель чисел $XR - (\beta^{HS} \bmod n)$ и $X'R' - (\beta^{H'S'} \bmod n)$ содержит только один большой простой делитель q. В этом случае вычисление q не представляет сложностей. После определения q секретное число γ находится как один из делителей числа $q - 1$. Таким образом, решение задачи дискретного логарифмирования позволяет по известной подписи найти все секретные параметры. Рассмотрим теперь другой случай, когда атакующий знает эффективный способ факторизации числа n, т. е. атакующий может вычислить q, а затем и γ. По q он может определить $X = \log_\alpha y (\mathrm{mod}\, p)$, используя формулу $X = R^{-1}\beta^{HS} \bmod q$. Теперь вычисление секретного значения x сведено к дискретному логарифмированию по простому модулю q, длина которого примерно вдвое меньше длины p: $x = \log_\beta X (\mathrm{mod}\, q)$. Однако для подделки подписи нет необходимости знать значение x, поскольку генерация подписи выполняется на основе сравнения $k + x \equiv SH \bmod \gamma$. Это позволяет по известной подписи (R, S) сформировать подпись (R, S') к некоторому другому документу, соответствующему хэш-функции H', по формуле $S' = \dfrac{SH}{H'} \bmod \gamma$ (заметим, что в новой подписи сохраняется значение параметра R).

176. Формирование подписи осуществляется следующим образом. Выбирается случайное число k и вычисляется первый элемент подписи: $R \equiv \beta^k \bmod q$, длина которого составит $|R| \approx |q| \approx 600$ бит. Затем вычисляется второй элемент подписи: $S = \dfrac{H - x}{k} \bmod \gamma$, длина которого составит $|S| \approx |\gamma| \approx 128$ бит. Последняя формула определяется соотношением $x + kS \equiv H \bmod \gamma$, которое обеспечивает выполнимость уравнения проверки подписи. Действительно, из него следует: $\beta^{x+kH} \equiv \beta^H \bmod q \Rightarrow$

$$\Rightarrow \alpha^{\beta^{x+kS} \bmod q} \equiv \alpha^{\beta^H \bmod q} \bmod p \Rightarrow \left(\alpha^{\beta^x}\right)^{\beta^{kS} \bmod q} \equiv \alpha^{\beta^H \bmod q} \Rightarrow y^{R^S \bmod q} \equiv$$

$$\equiv \alpha^{\beta^H \bmod q} \bmod p.$$

Покажем, что из $y^{R^S \bmod q} \equiv \alpha^{\beta^H \bmod q} \bmod p$ следует $y^{R^S \bmod n} \equiv \alpha^{\beta^H \bmod n} \bmod p$ (проверяющий пользуется этим сравнением для проверки подписи, поскольку он не знает числа q). Введем

переменные W и V: $W \overset{def}{=} (\beta^H \bmod n) \equiv \beta^H \bmod q$ и $V \overset{def}{=} (R^S \bmod n) \equiv$ $\equiv R^S \bmod q$. В соответствии с процедурой генерации подписи имеем $\beta^r R^S \equiv \beta^H \bmod q$, поэтому: $\beta^r V \equiv W \bmod q \Rightarrow \alpha^{\beta^r} \equiv \alpha^{W} \bmod p \Rightarrow$ $\Rightarrow (\alpha^{\beta^r})^{\frac{1}{r}} \equiv \alpha^{W} \bmod p \Rightarrow y^{R^S \bmod n} \equiv \alpha^{\beta^H \bmod n} \bmod p$, что и требовалось показать. Проанализируем безопасность заданной схемы ЭЦП. Пусть атакующий умеет эффективно вычислять дискретные логарифмы по простому модулю p. Тогда он может вычислить $X = \log_\alpha y (\bmod p)$ и, зная некоторую правильную подпись, получить соотношение $X(R^S \bmod n) \equiv (\beta^H \bmod n) \bmod q$, т. е. $q \mid [X(R^S \bmod n) - (\beta^H \bmod n)]$ и значение q может быть определено разложением числа $X(R^S \bmod n) -$ $-(\beta^H \bmod n)$ на множители. После определения q секретное число γ легко определяется как один из делителей числа $q - 1$. Значение x вычисляется по формуле $x = \log_\beta X (\bmod q)$. Таким образом, решение задачи дискретного логарифмирования позволяет по известной подписи найти все секретные параметры. Рассмотрим теперь другой случай, когда атакующий знает эффективный способ факторизации числа n, т. е. атакующий может вычислить q, а затем и γ. По q он может определить $X = \log_\alpha y (\bmod p)$, используя формулу $X = R^{-S} \beta^H \bmod q$. Теперь вычисление секретного значения x сведено к дискретному логарифмированию по простому модулю q, длина которого примерно вдвое меньше длины p: $x = \log_\beta X (\bmod q)$. Учитывая лучшие известные в настоящее время алгоритмы дискретного логарифмирования и факторизации, можно сделать вывод, что если длина чисел p и n составляет 1000 бит и более, то рассмотренная схема ЭЦП может считаться безопасной.

177. Схема ЭЦП, заданная вторым сравнением, детально охарактеризована в предыдущей задаче. Схема, соответствующая первому проверочному сравнению, является очень похожей на вторую по конструктивным идеям и выполняемым вычислениям при генерации и проверке подписи. Безопасность обеих схем основана на том, что задача дискретного логарифмирования и задача факторизации числа $n = rq$ являются вычислительно неразрешимыми в настоящее время. Формирование подписи в первой схеме начинается с выбора случайного числа k и вычисления параметра $R \equiv \alpha^{\beta^k \bmod q} \bmod p$, длина которого составит $|R| \approx |p| \approx$ ≈ 1200 бит (во второй схеме длина параметра R вдвое меньше). Затем вычисляется параметр $S = \dfrac{H - k}{x} \bmod \gamma$, длина которого составит $|S| \approx |\gamma| \approx 128$ бит. Последняя формула определяется соотношением $k + xS \equiv H \bmod \gamma$, которое обеспечивает выполнимость уравнения про-

верки подписи. Доказательство этого факта выполняется аналогично тому, как это сделано в предыдущей задаче. Атака на первую схему на основе вычисления дискретного логарифма начинается с вычисления значения $K = \log_\alpha R \pmod p$, где $K = \beta^k \bmod q$. Если длина чисел p и n составляет 1000 бит и более, то обе рассмотренные схемы ЭЦП могут считаться безопасными.

178. Процедура генерации подписи включает выбор случайного числа k и вычисление параметра $R = \alpha^{\beta^k \bmod q} \bmod p$. Затем вычисляются значения $E = R^H \bmod \delta$ и $S = \dfrac{k - E}{H} \bmod \gamma$, т. е. размеры элементов подписи S и E составляют $|S| \approx |\gamma| \approx 96$ бит и $|E| \approx |\delta| \approx 96$ бит. Особенностью этой схемы ЭЦП является формирование подписи с возведением числа β в степень по модулю q, являющемуся секретным значением. Выполнение этой операции при проверке подлинности подписи реализуется косвенно следующим путем. Вычисления ведутся по модулю $n = rq$, но благодаря тому, что параметр α представляет собой число, относящееся по модулю p к показателю q, операция возведения числа α в некоторую степень W автоматически обрезает значение W по модулю q, т. е. фактически получаем результат возведения числа α в степень $W' = W \bmod q$. Например, пусть $R = \alpha^{\beta^k \bmod q} \bmod p$ и $R' = \alpha^{\beta^k \bmod n} \bmod p$, тогда $R' = R$. Действительно, $Z \overset{def}{=} \beta^k \bmod n \Rightarrow Z \equiv \beta^k \bmod n \Rightarrow \alpha^{Z \bmod q} \equiv \equiv \alpha^{\beta^k \bmod q} \bmod p$. То, что проверяющий получает значения степеней W, вычисленные по модулю n, обеспечивает «маскирование» соответствующих результатов W', которые формируются при вычислении по модулю q, благодаря чему обеспечивается «маскирование» числа q. Решение задачи факторизации числа n дает непосредственное значение q, а разложение на множители числа $q - 1$ позволяет определить значение γ. После этого можно сформировать подпись к любому сообщению. Решение задачи дискретного логарифмирования также позволяет определить секретные параметры. Пусть имеется эффективный алгоритм дискретного логарифмирования по простому модулю, т. е. реально можно вычислить значения $K = \log_\alpha R \pmod p$ и $k = \log_\beta K \pmod q$. Тогда, зная некоторую правильную подпись, можно составить соотношение $K \equiv (\beta^{SH+E} \bmod n) \bmod q$, т. е. $q \mid [K - (\beta^{SH+E} \bmod n)]$. В общем случае $K \neq \beta^{SH+E} \bmod n$, поэтому значение q может быть определено разложением числа $K - (\beta^{SH+E} \bmod n)$ на множители. Если имеется несколько подлинных подписей, то с большой вероятностью будет найдена пара подписей (E, S) и (E', S'), для которой наибольший общий делитель чи-

сел $K-(\beta^{SH\cdot 1} \bmod n)$ и $K'-(\beta^{S'H'\cdot 1'} \bmod n)$ содержит только один большой простой делитель q. В этом случае вычисление q может быть существенно упрощено. После определения q секретное значение γ находится как один из делителей числа $q-1$. Таким образом, решение задачи дискретного логарифмирования позволяет по известной подписи найти все секретные параметры.

179. Процедура генерации подписи включает выбор случайного числа k и вычисление параметра $R=\alpha^{\beta^k \bmod q} \bmod p$. Затем вычисляются значения $E=R \bmod \delta$ и $S=\dfrac{k}{HE} \bmod \gamma$, т. е. размеры элементов подписи S и E составляют $|S| \approx |\gamma| \approx 96$ бит и $|E| \approx |\delta| \approx 96$ бит. Особенностью этой схемы ЭЦП является то, что при проверке подписи используются «скрытные» вычисления по модулю q, являющемуся секретным значением. Скрытность обеспечивается тем, что вычисления ведутся по модулю $n=rq$ и получаемые результаты сравнимы по модулю q с результатами вычислений по модулю q. Безопасность заданной схемы ЭЦП нарушается, если будет решена либо задача дискретного логарифмирования, либо задача факторизации чисел, представляющих собой произведение двух больших простых неизвестных чисел. Решение задачи факторизации числа n дает непосредственное значение q, а разложение на множители числа $q-1$ позволяет определить значение γ. Решение задачи дискретного логарифмирования также позволяет определить секретные параметры. Рассмотрим, как эффективный алгоритм дискретного логарифмирования по простому модулю может быть использован для вычисления секретных значений q и γ. Пусть вычислено значение $K=\log_\alpha R(\bmod p)$. Тогда, зная некоторую правильную подпись, можно составить соотношение $K \equiv (\beta^{SHE} \bmod n) \bmod q$, т. е. $q \mid [K-(\beta^{SHE} \bmod n)]$. В общем случае $K \neq \beta^{SHE} \bmod n$, поэтому значение q может быть определено разложением числа $K-(\beta^{SHE} \bmod n)$ на множители. Задача вычисления числа q еще проще при наличии нескольких подписей. Тогда с большой вероятностью будет найдена пара подписей (E, S) и (E', S'), для которой наибольший общий делитель чисел $K-(\beta^{SHE} \bmod n)$ и $K'-(\beta^{S'H'E'} \bmod n)$ содержит только один большой простой делитель q. После определения q секретное значение γ находится как один из делителей числа $q-1$.

180. Процедура генерации подписи может быть получена на основе представления числа R в виде $R=\alpha^{\beta^k \bmod q} \bmod p$. Это позволяет зафиксировать параметр E, т. е. значение первого элемента подписи, накладывая следующую связь на переменные S и k: $S+k=U \bmod \gamma$ (1), где U есть

случайно выбираемое число ($U < \gamma$). Первое проверочное уравнение выполняется, если имеет место соотношение $k = SHE \bmod \gamma$ (2), где E вычисляется по формуле $E = (\alpha^{\beta^{U} \bmod q} \bmod p) \bmod \delta$. Видно, что формирование подписи можно осуществить, выбирая случайное значение U, вычисляя E и решая систему сравнений (1) и (2). Решение этой системы дает следующие формулы: $S = \dfrac{U}{HE+1} \bmod \gamma$ и $k = \dfrac{UHE}{HE+1} \bmod \gamma$. Вычисление значения S завершает процедуру формирования подписи (E, S) (значение k нас не интересует).

181. Процедура генерации подписи может быть получена на основе представления чисел R и S в виде $R = \alpha^{\beta^{k} \bmod q} \bmod p$ и $S = \beta^{g} \bmod q$. Это позволяет зафиксировать параметр E, т. е. значение первого элемента подписи, накладывая следующую связь на переменные g и k: $g + k = U \bmod \gamma$ (1), где U есть случайно выбираемое число ($U < \gamma$). Первое проверочное уравнение выполняется, если имеет место соотношение $k = gHE \bmod \gamma$ (2), где E вычисляется по формуле $E = (\alpha^{\beta^{U} \bmod q} \bmod p) \bmod \delta$. Видно, что формирование подписи можно осуществить, выбирая случайное значение U, вычисляя E и решая систему сравнений (1) и (2). Решение этой системы дает следующую формулу: $g = \dfrac{U}{HE+1} \bmod \gamma$ для определения значения g, по которому вычисляется элемент $S = \beta^{g} \bmod q$, что завершает процедуру формирования подписи (E, S).

182. Процедура генерации подписи может быть получена на основе представления числа R в виде $R = \alpha^{\beta^{k} \bmod q} \bmod p$. Это позволяет зафиксировать параметр E, т. е. значение первого элемента подписи, накладывая следующую связь на переменные S и k: $S + k = U \bmod \gamma$ (1), где U есть случайно выбираемое число ($U < \gamma$). Первое проверочное уравнение выполняется, если имеет место соотношение $k = HS + E^2 \bmod \gamma$ (2), где E вычисляется по формуле $E = (\alpha^{\beta^{U} \bmod q} \bmod p) \bmod \delta$. Видно, что формирование подписи можно осуществить, выбирая случайное значение U, вычисляя E и решая систему сравнений (1) и (2). Решение этой системы дает следующие формулы: $S = \dfrac{U - E^2}{H+1} \bmod \gamma$ и $k = \dfrac{UH + E^2}{H+1} \bmod \gamma$. Вычисление значения S завершает процедуру формирования подписи (E, S) (значение k нас не интересует).

183. Процедура генерации подписи может быть получена на основе представления числа R в виде $R = \alpha^{\beta^{k} \bmod q} \bmod p$. Это позволяет зафиксиро-

вать значение первого элемента подписи E, накладывая следующую связь на переменные S и k: $k + HS = U \bmod \gamma$ (1), где U есть случайно выбираемое число ($U < \gamma$). Первое проверочное уравнение выполняется, если имеет место соотношение $k = SE \bmod \gamma$ (2), где E вычисляется по формуле $E = (\alpha^{\beta^{U} \bmod q} \bmod p) \bmod \delta$. Видно, что формирование подписи можно осуществить, выбирая случайное значение U, вычисляя E и решая систему сравнений (1) и (2). Решение этой системы дает следующую формулу $S = \dfrac{U}{H + E} \bmod \gamma$, по которой вычисляется значение S, что завершает процедуру формирования подписи (E, S).

184. Процедура генерации подписи может быть получена на основе представления числа R в виде $R = \alpha^{\beta^{k} \bmod q} \bmod p$ (1). Она начинается с выбора случайного числа k ($k < \gamma$), по которому вычисляется R с использованием формулы (1). Затем по полученному значению R вычисляется значение E: $E = R^{H} \bmod \delta$. Второй элемент подписи (E, S) определяется по формуле $S = kE^{-1} \bmod \gamma$.

185. Процедура генерации подписи может быть получена на основе представления чисел R и S в виде $R = \alpha^{\beta^{k} \bmod q} \bmod p$ и $S = \beta^{g} \bmod q$. Это позволяет представить проверочное соотношение в виде $\alpha^{\beta^{k} \bmod q} \equiv \equiv \alpha^{\beta^{E+g} \bmod q} \bmod p$ (1). Если сравнение (1) выполняется, то выполняется и первое заданное проверочное уравнение $R = \alpha^{(S\beta^{E} \bmod n)} \bmod p$ (проверяющий осуществляет вычисление параметра $W = S\beta^{E} \bmod n$ по модулю n; поскольку $W \equiv S\beta^{E} \bmod q$ и число α относится по модулю p к показателю q, то $\alpha^{S\beta^{E} \bmod q} \equiv \alpha^{(S\beta^{E} \bmod n)} \bmod p$). Из сравнения (1) вытекает следующая формула для вычисления значения $g = k - E \bmod \gamma$, где $E = R^{H} \bmod \delta$. Вычисление второго элемента подписи (E, S) выполняется по формуле $S = \beta^{g} \bmod q$. Размеры элементов подписи равны $|E| \approx \approx |\delta| \approx 96$ бит и $|S| \approx |q| \approx 512$ бит, т. е. длина подписи составляет около 608 бит.

186. Процедура генерации подписи может быть получена на основе представления чисел R и S в виде $R = \alpha^{\beta^{k} \bmod q} \bmod p$ и $S = \beta^{g} \bmod q$. Это позволяет зафиксировать значение первого элемента подписи E, накладывая на переменные g и k следующее условие: $g + k = U \bmod \gamma$ (1), где U есть случайно выбираемое число ($U < \gamma$). Первое проверочное уравнение выполняется, если g и k удовлетворяют сравнению $k = g + E \bmod \gamma$ (2), где E вычисляется по формуле $E = (H\alpha^{\beta^{U} \bmod q} \bmod p) \bmod \delta$. Видно, что формирование подписи можно осуществить, выбирая случайное

значение U, вычисляя E и решая систему сравнений (1) и (2). Решение этой системы дает следующие формулы: $g = \frac{U-E}{2} \bmod \gamma$ и $k = \frac{U+E}{2} \bmod \gamma$. Вычисление значения S по формуле $S = \beta^g \bmod q$ завершает процедуру формирования подписи (E, S) (значение k нас не интересует). Размеры элементов подписи равны $|E| \approx |\delta| \approx 96$ бит и $|S| \approx |q| \approx 512$ бит, т. е. длина подписи составляет около 608 бит.

187. В первой схеме ЭЦП размер подписи определяется длинами чисел γ и δ и составляет $|E| + |S| \approx |\gamma| + |\delta| \approx 192$ бит, а во второй схеме — длинами чисел ε и δ и составляет $|E| + |S| \approx |\varepsilon| + |\delta|$. Вопрос состоит в оценке безопасного размера числа ε. Чтобы предотвратить возможность вычисления разложения модуля n путем нахождения НОД$(\varepsilon - 1, n) \neq 1$, число ε следует выбирать таким, что $\varepsilon = \varepsilon'\varepsilon''$, где $\varepsilon' | (r-1)$ и $\varepsilon'' | (q-1)$. При этом возможно использование (*см. разд. 4.3*) соотношения НОД$(b^{\varepsilon'} - 1, n) \neq 1$ или НОД$(b^{\varepsilon''} - 1, n) \neq 1$ для разложения числа n путем угадывания или перебора возможных значений числа ε' или ε''. Поэтому каждое из чисел ε' и ε'' должно быть достаточно большой длины, чтобы сделать эту атаку практически нереализуемой. Представляется возможным использование значений $|\varepsilon'| \approx |\varepsilon''| \approx 96$ бит. При этом имеем $|\varepsilon| = |\varepsilon'| + |\varepsilon''| \approx 192$ бит и размер подписи 288 бит. Таким образом, вторая схема ЭЦП требует использования подписи большего размера.

188. Для реализации заданной цели можно выбрать модуль, имеющий структуру $p = 2n + 1$, где $n = qr$, q и r — большие простые числа, сравнимые с числом 3 по модулю 4 (это обеспечит возможность легко выполнять операцию извлечения квадратного корня по модулю n). В качестве параметра α можно выбрать первообразный корень или число, относящееся по модулю p к показателю n. Это делается следующим образом. Выбирается случайное число β, вычисляется число $z = \beta^2 \bmod p$. Если $z \neq 1$, $z^q \bmod p \neq 1$ и $z^r \bmod p \neq 1$, то z берется в качестве элемента α. Если нарушитель решит задачу дискретного логарифмирования и найдет логарифм от y по модулю p при основании α, то для генерации подписи $S = \pm\sqrt{\frac{k}{H + xR}} \bmod n$ ему еще потребуется выполнить операцию извлечения квадратного корня по модулю n. Последнее, как известно, эквивалентно (по сложности) разложению n на множители.

189. Если известна подпись S, соответствующая значению $H = H_1 H_2$, то $S_1 = S^{H_2} \bmod n$ и $S_2 = S^{H_1} \bmod n$ есть подписи к H_1 и H_2 соответственно.

Если нарушителю требуется получить подпись к документу, соответствующему значению хэш-функции H, то он может представить на подпись значение $H' = HK$, где K — маскирующий множитель. Получив подпись к H', нарушитель без труда вычисляет правильную подпись к H по формуле $S = (S')^K \bmod n$.

190. Для вычисления подписи следует представить число R в виде $R = \alpha^k \bmod n$. Это позволяет зафиксировать некоторое произвольное значение $U < \gamma$, такое что НОД$(U, \gamma) = 1$, и рассматривать область пар значений k и g, удовлетворяющих условию $kg \equiv U \bmod \gamma$ (1). Это условие задает некоторый фиксированный параметр $Z = \alpha^U \bmod n$ (при этом будем брать различные значения U до тех пор, пока не получим НОД$(Z, \gamma) = 1$). Для выполнения проверочного соотношения следует найти пару (k, g), удовлетворяющую также и сравнению $kHg^3 \equiv Z \bmod \gamma$ (2). Искомая пара значений может быть найдена как решение системы из сравнений (1) и (2): $g = \pm\sqrt{\frac{Z}{HU}} \bmod \gamma$ и $k = \pm U\sqrt{\frac{HU}{Z}} \bmod \gamma$. Вычисление квадратных корней значительно упрощается, если оба множителя модуля $\gamma = \gamma'\gamma''$ сравнимы с числом 3 по модулю 4, т. е. если $\gamma' \equiv \gamma'' \equiv 3 \bmod 4$. В этом случае извлечение корней по модулю $\gamma = \gamma'\gamma''$ сводится к извлечению корней по модулям γ' и γ'' и использованию китайской теоремы об остатках (см. схему ЭЦП Рабина).

191. В обеих схемах для вычисления подписи следует представить число R в виде $R = \alpha^k \bmod n$. Это позволяет зафиксировать некоторое произвольное значение $U < \gamma$, такое что НОД$(U, \gamma) = 1$, и рассматривать область пар значений k и g, удовлетворяющих условию $kg^2 \equiv U \bmod \gamma$ (1а) и $kg \equiv U \bmod \gamma$ (1б), соответственно для первого и второго проверочных сравнений. Это условие задает некоторый фиксированный параметр $Z = \alpha^U \bmod n$ (при этом берутся новые значения U до тех пор, пока не получим НОД$(Z, \gamma) = 1$). Для выполнения проверочного соотношения следует найти пару (k, g), удовлетворяющую также и сравнению $kHg^3 \equiv Z \bmod \gamma$ (2), которое является одинаковым для обеих рассматриваемых схем. Искомая пара значений может быть найдена как решение системы из сравнений (1а) и (2) для первой схемы ЭЦП и (1б) и (2) для второй. Для первой схемы ЭЦП имеем: $g = \frac{Z}{HU} \bmod \gamma$ и $k = \frac{H^2U^3}{Z^2} \bmod \gamma$. Вторая схема требует выполнения операции извлечения квадратных кор-

ней: $g = \pm\sqrt{\frac{Z}{HU}} \bmod \gamma$ и $k = \pm U\sqrt{\frac{HU}{Z}} \bmod \gamma$. Это определяет более высокую трудоемкость генерации подписи в случае второй схемы.

192. Оба варианта проверочных уравнений основаны на сложности разложения составного числа, являющегося произведением двух больших простых чисел, удовлетворяющих, например, критериям, предъявляемым к сильным простым числам. Задача факторизации считается сложной, если размер множителей r и q равен 512 и более бит. Значение хэш-функции обычно имеет размер от 128 до 256 бит. Поэтому в первом проверочном уравнении имеется возможность подделать подпись, выбрав некоторое произвольное число U, такое что $|U| \le 200$ бит. Подпись (S, R) вычисляется следующим образом: $R = \alpha^{U} \bmod p$ и $S = UH$. Легко видеть, что сформированная таким образом подпись удовлетворяет проверочному уравнению. Усилить первое проверочное уравнение можно, если в него встроить некоторую операцию, выполнение которой потребует знания секретного ключа q. Этого можно достичь, если в качестве степени при R использовать не H, а H^t, где t выбирается с учетом того, что после возведения значения хэш-функции в степень с вероятностью, очень близкой к 1, будет получено значение, размер которого значительно больше размера секретного ключа, например, $t = 10$. Проверочное сравнение приобретает вид $R^{H^t} = \alpha^{S} \bmod p$. При этом в процедуру проверки подлинности подписи следует добавить дополнительное проверочное неравенство: $|S| < |q'|$, где $|q'| \ge |q| + 8$ бит. Это неравенство будет обеспечивать контроль того, что при вычислении S был использован секретный ключ. В построенной таким образом схеме ЭЦП генерация подписи осуществляется следующим образом. Выбирается случайное число $k < q - 1$, вычисляются $R = \alpha^{k} \bmod p$ и $S = kH^t \bmod q$. Из последнего соотношения видно, что случайное число k играет роль маскирующего параметра. При проверке подписи проверяющий вычисляет значение H^t по модулю $p - 1$, поэтому в качестве t можно выбирать достаточно большие числа. Второе проверочное уравнение имеет еще более явную слабость. Подделка подписи тривиальна: выбирается произвольное число S, вычисляются $R = \alpha^{S^2 H} \bmod p$ и $R' = R \bmod \delta$. Исправить этот недостаток можно, вводя множитель $R \bmod \delta$ в степень при α: $R \bmod \delta = (\alpha^{S^2 H(R \bmod \delta)} \bmod p) \bmod \delta$.

Заключение

В данном учебном пособии дается краткое изложение математических результатов, используемых при синтезе и анализе криптосистем с открытым ключом, и ряда классических и новых криптосистем этого типа, включая достаточно большое число схем электронной цифровой подписи (ЭЦП). Основная часть книги содержит методические материалы для проведения практических занятий: формулировки заданий для курсовых работ и проектов и достаточно большое число задач, сопровождаемых подробными указаниями и решениями. Некоторые из задач могут быть взяты за основу при формировании новых задач или курсовых заданий. Задачи являются в большей части оригинальными и связанными с новыми схемами ЭЦП или вопросами, касающимися синтеза и анализа последних. Приведенные краткие теоретические сведения призваны служить в качестве справочного материала. Более подробно затронутые теоретические вопросы рассматриваются в книге **Н. А. Молдовяна и А. А. Молдовяна «Введение в криптосистемы с открытым ключом» (БХВ-Петербург, 2005)**, однако теоретическая часть, касающаяся оригинальных схем построения ЭЦП на основе сложности задач факторизации и дискретного логарифмирования, является новой. Она подготовлена на основании ряда недавно опубликованных работ [62, 63, 65, 66, 67, 69] и статей, подготовленных в печать [64, 68, 71], авторы которых любезно дали согласие на использование их результатов при написании данного учебного пособия. Они также приняли участие в подготовке части материала, касающегося заданий для курсового проектирования, формулировки условий задач и их решений. Благодаря использованию новых механизмов построения схем ЭЦП удалось сформировать достаточно большой список задач и заданий.

Настоящая книга не включает вопросы, задачи и упражнения, относящиеся к симметричным криптосистемам. Достаточное число вопросов и задач можно найти в книгах [6, 9, 15, 21, 22], однако в большей части указания и решения к ним отсутствуют. Указанные книги включают достаточно обшир-

ный теоретический материал по симметричной криптографии. Для еще более широкого и глубокого ознакомления с этой областью криптографии можно воспользоваться книгами [14, 16, 24, 26, 31]. Читателям, интересующимся детальным изложением вопросов синтеза симметричных шифров на основе управляемых операций, можно рекомендовать книги [38, 40]. Вопросы разработки программных и гибких шифров подробно рассмотрены в книгах [38, 39], зарубежные алгоритмы — в [15, 22, 26, 29, 31], прикладные аспекты — в [18, 33–37]. Широкий круг вопросов по криптосистемам с открытым и секретным ключом представлен в книгах [18, 24, 25, 29, 32]. Читатели, желающие более подробно ознакомиться с математическим аппаратом, используемым в криптографии, могут воспользоваться книгами [10, 12, 25, 27, 30].

Автор надеется, что настоящее учебное пособие окажет существенную помощь изучающим вопросы криптографии с открытым ключом и преподавателям при подготовке практических, а возможно, и теоретических занятий со студентами вузов.

Литература

Теория чисел и математические основы криптографии

1. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. Пер. с англ. — М.: Мир, 1987. — 416 с.
2. Бухштаб А. А. Теория чисел. — М.: Просвещение. 1966. — 384 с.
3. Виноградов И. М. Основы теории чисел. — М.: Наука, 1972. — 167 с.
4. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. — М.: Постмаркет, 2001. — 323 с.
5. Московский университет и развитие криптографии в России. Материалы конференции в МГУ 17–18 октября 2002 г. — М.: МЦНМО, 2003. — 270 с.
6. Ростовцев А. Г. Алгебраические основы криптографии. — СПб.: Мир и Семья, 2000. — 353 с.
7. Степанов С. А. Арифметика алгебраических кривых. — М.: Наука. Гл. ред. физ.-мат. лит., 1991. — 388 с.
8. Сэвидж Д. Э. Сложность вычислений. — М.: Факториал, 1998. — 368 с.
9. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 381 с.
10. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.
11. Шеннон К. Э. Теория связи в секретных системах // В кн.: Шеннон К.Э. Работы по теории информации и кибернетике. — М.: 1963. С.333–402.
12. Koblitz N. A Course in Number Theory and Cryptography. — Berlin, Heidelberg, New York: Springer, 1994. — 235 p.
13. Cohen H. A Course in Computational Algebraic Number Theory. — Berlin, Heidelberg, New York: Springer, 1996. — 545 p.

Введение в проблематику и методы криптографии

14. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. — М.: Гелиос АРВ, 2002. — 480 с.

15. Венбо Мао. Современная криптография. Теория и практика. — М., СПб., Киев: Издательский дом «Вильямс», 2005. — 763 с.

16. Грущо А. А., Применко Э. А, Тимонина Е. Е. Анализ и синтез криптоалгоритмов. — Йошкар-Ола, 2000. — 110 с.

17. Диффи У., Хеллман М. Э. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР, 1979. Т. 67. № 3. С. 71–109.

18. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. —СПб.: Лань, 2000. — 218 с.

19. Молдовян А. А., Молдовян Н. А. Введение в криптосистемы с открытым ключом. — СПб.: БХВ-Петербург, 2005. — 286 с.

20. Молдовян Н. А. Проблематика и методы криптографии. —СПб.: СПбГУ, 1998. — 212 с.

21. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. — М.: Горячая линия телеком, 2005. — 229 с.

22. Смарт Н. Криптография. — М.: Техносфера, 2005. — 528 с.

23. Специальный выпуск. — ТИИЭР, 1988. Т. 76. № 5.

24. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. — М.: ТРИУМФ, 2002. — 816 с.

25. Фомичев В. М. Дискретная математика и криптология. — М.: ДИАЛОГ-МИФИ, 2003. — 397 с.

26. Pieprzyk J., Hardjono Th., Seberry J. Fundumentals of Computer Security. Springer-Verlag. Berlin, 2003. — 677 p.

27. Welsh D. Codes and Cryptography. — Oxford, Clarendon Press, 1998. — 257 p.

28. Lecture on Data Security: Modern Cryptology in Theory and Practice / I. Damgard (ed.). — Lecture Notes in Computer Science. Springer-Verlag, 1999. — V. 1561. — 250 p.

29. Menezes A. J., Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996. — 780 p.

30. Delfs H., Knebl H. Introduction to Cryptography. Principles and Applications. — Berlin, Heidelberg, New York, Milan. Paris, Tokyo: Springer, 2002. — 310 p.

31. State of the Art in Applied Cryptography : revised lectures / Course on Computer Security and Industrial Cryptography, Leuven, Belgium, June 3-6, 1997 / B. Preneel, V.Rijmen (eds.). — Lecture Notes in Computer Science. Springer-Verlag, 1998. —V. 1528. — 393 p.

32. Stinson D.R. Cryptography Theory and Practice. — N.Y.: CRC Press., Inc, 1995. — 434 p.

Криптографические методы защиты информации в вычислительных системах и сетях

33. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. — М.: Кудиц-Образ. 2001. — 368 с.

34. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. — М.: ДМК, 2000. — 445 с.

35. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 1999. — 328 с.

36. Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах — М.: ДМК, 2002. — 328 с.

37. Столлингс В. Криптография и защита сетей: принципы и практика., 2-е изд.: Пер. с англ. — М.: Изд. дом «Вильямс», 2001. — 672 с.

Программные и скоростные шифры

38. Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В. Криптография: скоростные шифры. — СПб.: БХВ-Петербург, 2002. — 495 с.

39. Молдовян Н. А. Скоростные блочные шифры. — СПб.: СПбГУ, 1998. — 230 с.

40. Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов. — СПб.: БХВ-Петербург, 2004. — 446 с.

41. Moldovyan A. A., Moldovyan N. A. A cipher based on data-dependent permutations. *Journal of Cryptology*. — 2002. — N. 1. — P. 61–72.

42. Moldovyan A. A., Moldovyan N. A. Flexible block ciphers with provably inequivalent cryptalgorithm modifications // *Cryptologia*. — 1998. — V.XXII. — N. 2. — P. 134–140.

43. Moldovyan A. A., Moldovyan N. A. Software encryption algorithms for transparent protection technology // *Cryptologia*. — 1998. — V. XXII. —N. 1. — P. 56–68.

44. Moldovyan A. A., Moldovyan N. A. Fast Software Encryption Systems for Secure and Private Communication // Twelfth International Conference on Computer Communication. Seoul, Korea, 21–24 August 1995. Proceedings. — P. 415–420.

45. Moldovyan N. A. On Cipher Design Based on Switchable Controlled Operations Int. // Workshop MMM-ANCS'2003 Proc. LNCS, Springer-Verlag, Berlin. — 2003. — V. 2776. — P. 316–327.

46. Rogaway Ph., Coppersmith D. A software-optimized encryption algorithm // Journal of Cryptology. — 1998. — V. 11. — N. 4. — P. 273–287.

47. Rivest R. L. The RC5™ Encryption Algorithm // Fast Software Encryption, Second International Workshop // Lecture Notes in Computer Science. Springer-Verlag. — 1995. — V. 1008. — P. 86–96.

48. Schneier B. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) // «Fast Software Encryption», Cambridge Security Workshop Proc. LNCS, Springer-Verlag. — 1994. — V. 809. — P. 191–204.

Классические схемы ЭЦП (отправные работы)

49. Chaum D. Blind Signature Systems. U.S. Patent # 4.759.063. — Jul.19.1988.

50. Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology: Proc. of CRYPTO'82. Plenum Press. — 1983. — P. 199–203.

51. Chaum D. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Communication of the ACM. —Oct. 1985. — V. 28. — N. 10. — P. 1030–1044.

52. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Transactions on Information Theory. — 1976. — V. IT–22. — P. 644–654.

53. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. — 1985. — V. IT–31. — N. 4. — P. 469–472.

54. Gordon J. Strong primes are easy to find, *Advances in cryptology — EUROCRYPT'84, Springer-Verlag LNCS.* — 1985. — V. 209. — P. 216–223.

55. Lieberherr K. Uniform Complexity and Digital Signatures // Theoretical Computer Science. — Oct. 1981. — V. 16. — N. 1. — P. 99–110.

56. Schnorr C. P. Efficient signature generation by smart cards // J. Cryptology. — 1991. — V. 4. — P. 161–174.

57. Schnorr C. P. Efficient identification and signatures for smart cards // Advances in cryptology — CRYPTO'89, Springer-Verlag LNCS. — 1990. — V. 435. — P. 239–252.

58. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems // Advances in cryptology — CRYPTO'86, Springer-Verlag LNCS. — 1987. — V. 263. — P. 186–194.

59. Pollard J. M., Schnorr C. P. «An efficient solution of the congruence $x^2+ky^2=m$ (mod n)», IEEE Transactions on Information Theory. — 1987. — V. IT–33. — N. 5. — P. 702–709.

60. Rabin M. O. Digitalized signatures and public key functions as intractable as factorization. — Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Science. — 1979.

61. Rivest R., Shamir A., Adleman A. A method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communication of the ACM. — 1978. — V. 21. — N. 2. — P. 120–126.

Нетрадиционные схемы ЭЦП

62. Гортинская Л. В., Молдовян Д. Н., Молдовян А. А. Требования к выбору параметров криптосхем на основе RSA-модуля // Вопросы защиты информации. — 2005. — № 3 (70). — С. 34–38.

63. Гортинская Л. В., Молдовян Д. Н. Основанная на сложности факторизации схема ЭЦП с простым модулем // Вопросы защиты информации. — 2005. — № 4 (71). — С. 7–11.

64. Гортинская Л. В., Молдовян Д. Н., Молдовян А. А. Обоснование требований к выбору параметров схем цифровой подписи // Известия вузов. Приборостроение (в печати).

65. Костин А. А., Молдовян Д. Н., Молдовян Н. А. Новая криптосистема с открытым ключом на основе RSA-модуля // Вопросы защиты информации. — 2005 (68). — № 1. — С. 8–12.

66. Молдовян Д. Н. Схемы цифровой подписи на основе сложности факторизации модуля // Вопросы защиты информации. — 2004. — № 4 (67). — С. 6–11.

67. Молдовян Д. Н. Новый механизм формирования подписи в схемах ЭЦП, основанных на сложности дискретного логарифмирования и факторизации // Вопросы защиты информации. — 2005. — № 4 (71). — С. 2–7.

68. Молдовян Д. Н., Молдовян Н. А. Новые схемы ЭЦП с сокращенной длиной подписи // Вопросы защиты информации. — 2006. — № 3. — С. 7–12.

69. Молдовян Д. Н. Схема ЭЦП с проверкой подлинности по длине // В кн. Инновационная деятельность в вооруженных силах Российской Федерации. Труды всеармейской научно-практической конференции. СПб., 17–18 ноября 2005 г. СПб. — 2005. — С. 196–199.

70. Estes D., Adleman L. M., Konpella K., McCurley K. S., Miller G. L. Breaking the Ong-Schnorr-Shamir signature schemes for quadratic number

fields // Advances in Cryptology — CRYPTO'85 Proceedings. Springer Verlag. — 1986. — P. 3–13.

71. Moldovyan A. A., Moldovyan D. N., Gortinskaya L. V. Cryptoschemes Based on New Signature Formation Mechanism // Computer Science Journal of Moldova (in publishing).

72. Pollard J. M., Schnorr C. P. An efficient solution of the congruence $x^2+ky^2=m \pmod{n}$ // IEEE Transactions on Information Theory. — 1987. — V. IT–33. — N. 5. — P. 702–709.

73. Shimada M. Another Practical Public-key Cryptosystem // Electronics Letters. — 1992. — V. 28. — N. 23. — P. 2146–2147.

Молдовян Николай Андреевич, доктор технических наук, профессор, заслуженный изобретатель РФ, главный научный сотрудник Научного филиала ФГУП НИИ «Вектор» — СЦПС «Спектр». Известный специалист, ведущий открытые исследования в области криптографии.

Автор более 250 печатных работ в области защиты информации и криптографии и более 60-ти патентов на изобретения, которые патентуются в 21 стране (Россия, США, Германия, Франция, Великобритания, Китай и др.). Его новые подходы к построению скоростных шифров опубликованы в ведущих научных журналах мира.

Специализированный центр программных систем «Спектр»
nmold@cobra.ru
www.cobra.ru

ПРАКТИКУМ ПО КРИПТОСИСТЕМАМ С ОТКРЫТЫМ КЛЮЧОМ

Среди большого обилия книг, посвященных теоретическим вопросам классической и современной криптографии, трудно найти материал для практических занятий. Целью данной книги является восполнение этого пробела по отношению к криптосистемам с открытым ключом. В ней приводится около 200 вариантов заданий для выполнения курсовых работ и проектов.

На основе многолетнего преподавательского опыта автором составлен список задач по элементам теории чисел и двухключевой криптографии, включая тематику анализа и синтеза систем электронной различного типа, для которых приводятся ответы, указан

БХВ-ПЕТЕРБУРГ
191036, Санкт-Петербург, Гончарная ул., 20
Тел.: (812) 717-10-50, 339-54-17, 339-54-28
E-mail: mail@bhv.ru
Internet: www.bhv.ru

bhv

ISBN 978-5-9775-3524-3