ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТР 34.10 2012

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Издание официальное

Москва
Стандартинформ
2013

Предисловие

Цели и принципы стандартизации е Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 РАЗРАБОТАН Центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст

4 ВЗАМЕН ГОСТ Р 34.10—2001

Информация об изменениях *к настоящему стандарту публикуется в ежегодно* издаваемом *информационном указателе «Национальные стандарты». а текст* изменений *и поправок* — е *ежемесячно издаваемых информационных указателях* «Национальные *стандарты». В случае пересмотра (замены) или* отмены *настоящего стандарта соответствующее* уведомление будет *опубликовано в ежемесячно издаваемом информационном* указателе «*Национальные стандарты».* Соответствующая *информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства* по *техническому регулированию и метрологии в сети Интернет*

Содержание

Введение

Настоящий стандарт содержит описание процессов формирования и проверки электронной цифровой подписи (ЭЦП), реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.

Необходимость разработки настоящего стандарта вызвана потребностью в реализации электронной цифровой подписи разной степени стойкости в связи с повышением уровня развития вычислительной техники. Стойкость электронной цифровой подписи основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11—2012.

Настоящий стандарт разработан с учетом терминологии и концепций международных стандартов ИСО 2382-2 [1). ИСО/МЭК 9796 f2)— [3]. ИСО/МЭК 14888 [4]—ГП и ИСО/МЭК 10118 [8]—[11J.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Information technology. Cryptographic data security.
Generation and verification processes of electronic digital signature

Дата введения — 2013—01—01

1 Область применения

Настоящий стандарт определяет схему электронной цифровой подписи (ЭЦП) (далее — цифровая подпись), процессы формирования и проверки цифровой подписи под заданным сообщением (документом). передаваемым по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения.

Внедрение цифровой подписи на основе настоящего стандарта повышает по сравнению с ранее действовавшей схемой цифровой подписи уровень защищенности передаваемых сообщений от подделок и искажений.

Настоящий стандарт рекомендуется применять при создании, эксплуатации и модернизации систем обработки информации различного назначения.

2 Нормативные ссылки

8 настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р 34.11—2012 Информационная технология. Криптографическая защита информации. Функция хэширования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего годе, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен {изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим {измененным) стандартом. Если ссылочный стандарт отменен без замены, то положенно, а котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и обозначения

3.1 Термины и определения

8 настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1

дополнение (appendix): Строка бит. формируемая из цифровой подписи и произвольного текстового поля.

[ИСО/МЭК 14888-1:2008, [4Q

3.1.2

ключ подписи (signature key): Элемент секретных данных, специфичный для субъекта и ислользуэмый только данным субъектом в процессе формирования цифровой подписи.

(ИСО/МЭК 14886-1:2008. {4Ц

Издание официальное

3.1.3

ключ проверки подписи (verification key): Элемент данных, математически связанный с ключок ■юдписи и используемый проверяющей стороной в процессе проверки цифровой подписи.
(ИСО/МЭК 14888-1:2008, [4]]

3.1.4

параметр схемы ЭЦП (domain parameter): Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам.
(ИСО/МЭК 14888-1:2008. [4Ц

3.1.5

подписанное сообщение (signed message): Набор элементов данных, состоящий из сообщения t дополнения, являющегося частью сообщения.
(ИСО/МЭК 14888-1:2008. (4)]

3.1.6

последовательность псевдослучайных чисел (pseudo-random number sequence): Поспелова гельмость чисел, полученная в результате выполнения некоторого арифметического (вычислительного; процесса, используемая в конкретном случае вместо последовательности случайных чисел.
(ИСО 2382-2:1976. [1]]

3.1.7

последовательность случайных чисел (random number sequence): Последовательность чисел <аждое из которых не может быть предсказано (вычислено) только на основе знания предшествующи) эму чисел данной последовательности.
(ИСО 2382-2:1976, (1]]

3.1.8

процесс проверки подписи (verification process): Процесс, в качестве исходных данных которогс используются подписанное сообщение, ключ проверки подписи и параметры схемы ЭЦП, результатов (второго является заключение о правильности или ошибочности цифровой подписи.
(ИСО/МЭК 14888-1:2008. (4]]

3.1.9

процесс формирования подписи (signature process): Процесс, в качестве исходных данных кото эого используются сообщение, ключ подписи и параметры схемы ЭЦП. а в результате формируете* цифровая подпись.
(ИСО/МЭК 14888-1:2008. (4]]

3.1.10 свидетельство (witness): Элемент данных, представляющий соответствующее доказательство достоверности (недостоверности) подписи проверяющей стороне.

3.1.11

случайное число (random number): Число, выбранное из определенного набора чисел таким обраюм. что каждое число из данного набора может быть выбрано с одинаковой вероятностью.
(ИСО 2382-2:1976. (1Ц

3.1.12

сообщение (message): Строка бит произвольной конечной длины.
(ИСО/МЭК 14888-1:2008, (4]]

3.1.13

хэш-код (hash-code): Строка бит. являющаяся выходным результатом хэш-функции.
(ИСО/МЭК 14888-1:2008, (4]]

3.1.14

хэш-функция (cotlision-resistant hash-function): Функция, отображающая строки бит е строки бит фиксированной длины и удовлетворяющая следующим свойствам:

1) поданному значению функции сложно вычислить исходные данные, отображаемые в это значение;

2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в го же значение функции:

3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.

[ИСО/МЭК 14886-1:2008. [4Д

Примечания

1 Применительно к области электронной цифровой подписи свойство ло перечислению 1) подразумевает, что по известной электронной цифровой подписи невозможно восстановить исходное сообщение; свойство по перечислению 2) подразумевает, что для заданного подписанного сообщения трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же электронную цифровую подпись; свойство по перечислению 3) подразумевает, что трудно подобреть какую-либо пару сообщений, имеющих одну и ту же подпись.

2 В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями установлено, что термины «хэш-функция», «криптографическая хэш-функция», «функция хэширования» и «криптографическая функция хэширования» являются синонимами.

3.1.15

[электронная цифровая] подпись (signature); ЭЦП: Строка бит. полученная в результате процесса формирования подписи.

(ИСО/МЭК 14886-1:2008. [4fl

Примечания

1 Строка бит. являющаяся подписью, может иметь внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

2 В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями установлено, что термины «электронная подпись», «цифровая подпись» и «электронная цифровая подпись» являются синонимами.

3.2 Обозначения

8 настоящем стандарте применены следующие обозначения:

V, — множество всех двоичных векторов длиной / бит:

V* — множество всех двоичных векторов произвольной конечной длины;

Z — множество всех целых чисел;

p — простое число, p > 3;

F. — конечное простое поле, представляемое как множество из p целых чисел (0.1.....p-1):

P(mod p) — минимальное неотрицательное число, сравнимое с P по модулю p;

M — сообщение пользователя. Me V*;

(Л, ||$Л_2$) — конкатенация (объединение) двух двоичных векторов:

a. O — коэффициенты эллиптической кривой;

m — порядок группы точек эллиптической кривой;

q — порядок подгруппы группы точек эллиптической кривой;

O — нулевая точка эллиптической кривой;

P — точка эллиптической кривой порядка *q:*

d — целое число — ключ подписи;

Q — точка эллиптической кривой — ключ проверки подписи;

Q — цифровая подпись под сообщением *M.*

4 Общие положения

Общепризнанная схема (модель) цифровой подписи (см. ИСО/МЭК 14888-1 [4]) охватывает следующие процессы:

• генерация ключей (подписи и проверки подписи):

- формирование подписи;
- проверка подписи.

В настоящем стандарте процесс генерации ключей (подписи и проверки подписи) не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами. которые устанавливают соответствующие параметры по взаимному согласованию.

Механизм цифровой подписи определяется посредством реализации двух основных процессов (см. раздел 6);

- формирование подписи (см. 6.1):
- проверка подписи (см. 6.2).

Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:

- осуществление контроля целостности передаваемого подписанного сообщения:
- доказательное подтверждение авторства лица, подписавшего сообщение:
- защита сообщения от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке 1.

Дополнение

СообиркмМ !ДОроавгМАПк«*С Темя j

Рисунок 1 — Схема подписанного сообщения

Поле «Текст», показанное на данном рисунке и дополняющее поле «Цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в настоящем стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем. а также хэш-функции.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритмы вычисления хэш-функции установлены в ГОСТ Р 34.11—2012.

Параметры схемы цифровой подписи, необходимые для ее формирования и проверки, определены в 5.2. В настоящем стандарте предусмотрена возможность выбора одного из двух вариантов требований к параметрам.

Настоящий стандарт не определяет процесс генерации параметров схемы цифровой подписи. Конкретный алгоритм (способ) реализации данного процесса определяется субъектами схемы цифровой подписи исходя из требований к аппаратно-программным средствам, реализующим электронный документооборот.

Цифровая подпись, представленная в виде двоичного вектора длиной 512 или 1024 бита, должна вычисляться с помощью определенного набора правил, изложенных в 6.1.

Набор правил, позволяющих принять либо отвергнуть цифровую подпись под полученным сообщением. установлен в 6.2.

5 Математические объекты

Для определения схемы цифровой подписи необходимо описать базовые математические объекты, используемые е процессах ее формирования и проверки. В данном разделе установлены основные математические определения и требования, предъявляемые к параметрам схемы цифровой подписи.

5.1 Математические определения

Эллиптической кривой Е, определенной над конечным простым полем F_p (где p > 3 — простое число). называется множество пар (x, y). x. *уе* F_p, удовлетворяющих уравнению

$$y^2 \text{ в } x^3 + ax \blacklozenge b \pmod p. \qquad (1)$$

где *a. be* F_p и 4a* * $27b^2$ не сравнимо с нулем по модулю p.

Инвариантом эллиптической кривой называется величина J(E), удовлетворяющая уравнению

$$J\{£) \text{ в } 1728\frac{4a^{3}*27b^{2}}{4a^{3}*27b^{2}}\{\text{mod p}). \quad (2)$$

Пары *(х.* у), где х. у — элементы поля F_p, удовлетворяющие уравнению (1). называются «точками эллиптической кривой Е»; х и у — соответственно х- и у-координатами точки.

Точка эллиптической кривой обозначается 0(х. у) или просто *Q.* Две точки эллиптической кривой равны, если равны их соответствующие х- и у-координаты.

На множестве точек эллиптической кривой *Е*определена операция сложения, обозначаемая знаком «+*. Для двух произвольных точек О,(х,,у,)и $0_2<x_2$, y_2) эллиптической кривой *Е* рассматривают несколько случаев.

Для точек Q, и $0_{2>}$ координаты которых удовлетворяют условию х, * x_2. их суммой называется точка $Q_3(x_3$, Уз), координаты которой определяются сравнениями

$$x_3 =>.^{2} -x, -x_2(\text{modp}).$$
$$y_3 *>.(x, -x_3)-y,(\text{modp}).$$

где $>. = \frac{}{x_2 - X,}$ (mod p).

Если выполнены равенства х, = x_2 и у, = y_2 * 0. то координаты точки 0_3 определяются следующим образом:

$$|x_3 \sim к^{3} -2x,(\text{modp}),$$
$$1Уз =X(x, -x_3)-y,(\text{modp})_t \quad (4)$$

где $к = \frac{3X1^{2} * }{2 y,}$ (mod p).

Если выполнены условия х, - x_2 и у, =-y_2(mod p), то сумма точек О, и 0_2 называется нулевой точкой О без определения ее х- и у-координиат. В этом случае точка Q_2 называется отрицанием точки Q,. Для нулевой точки О выполнены равенства

$$Q\,4\,o = O \blacklozenge Q = Q. \quad (5)$$

где О — произвольная точка эллиптической кривой *Е.*

Относительно введенной операции сложения множество точек эллиптической кривой *Е* вместе с нулевой точкой образуют конечную абелеву (коммутативную) группу порядка *m,* для которого выполнено неравенство

$$p + 1 - 2\sqrt{p} \le m \le p + 1 + 2\sqrt{p}. \quad (6)$$

Точка *Q* называется «точкой кратности *к»* или просто «кратной точкой эллиптической кривой Ев. если для некоторой точки Р выполнено равенство

$$Qsp+...+ psfcP. \quad (7)$$

к

5.2 Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:

- простое число р — модуль эллиптической кривой:
- эллиптическая кривая Е. задаваемая коэффициентами *a. b e* F_p;
- целое число *m* — порядок группы точек эллиптической кривой Е;
- простое число *q* — порядок циклической подгруппы группы точек эллиптической кривой Е. для которого выполнены следующие условия:

m®OQ.rt6Z.nai (8)

$2^{rM} < Q < 2^{r56}$ или $2^{508} < Q < 2^{513'}$

• точка *P * O* эллиптической кривой *E*. с координатами (x_p. y_p), удовлетворяющая равенству *qP* - О;

. хэш-функция V* -» $У_Г$ отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные векторы длины / бит. Хэш-функция определена в ГОСТ Р 34.11—2012. Если 2^{25}< < *q* < 2^{2}«. то / = 256. Если 2»* < *q* < 2^{512}. то / = 512.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

• ключом подписи — целым числом *d*, удовлетворяющим неравенству 0 < *d* < *q*;

• ключом проверки подписи — точкой эллиптической кривой О с координатами ($x_в$. $у_„$). удовлетворяющей равенству *dP* - О.

К приведенным выше параметрам схемы цифровой подписи предъявляют следующие требования:

• должно быть выполнено условие p' * 1 (mod g) для всех целых (= 1.2.... в. где *B* - 31. если $2^{3ь*} < q < 2^{246}$, и *B* = 131. если $2^{50®} < q < 2^{s12}$;

• должно быть выполнено неравенство *m*p:*

- инвариант кривой должен удовлетворять условиям: *J(E)* * 0 и *J(E)* * 1728.

5.3 Двоичные векторы

Для определения процессов формирования и проверки цифровой подписи необходимо установить соответствие между целыми числами и двоичными векторами длины / бит.

Рассмотрим следующий двоичный вектор длиной / бит. в котором младшие биты расположены справа, а старшие — слева:

& = {«/.,.....«о)- $^{heV}i<$ (9)

где$а_{(}$, /= 0..., / - 1 равно либо 1. либо 0.

Число а € *Z* соответствует двоичному вектору /Г. если выполнено равенство

а в £«, 2\ /-о (10)

Для двух двоичных векторов

1.....^{a}о)' М-|Ч

.....Ро>.

соответствующих целым числам аир. операция конкатенации (объединения) определяется следующим образом:

^11) Лг" (^{a}/. •••• ^{a}о* fy- 1* •••• Ро)- (^2)

Объединение представляет собой двоичный вектор длиной *21* бит. составленный из компонент векторовиЛ$_2$.

Формулы (11) и (12) определяют способ разбиения двоичного вектора ftj|/$Т_2$ длиной *21* бит на два двоичных вектора длиной *I* бит. конкатенацией которых он является.

6 Основные процессы

В данном разделе определены процессы формирования и проверки цифровой подписи под сообщением пользователя.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи, соответствующие требованиям 5.2.

Кроме того, каждый пользователь должен иметь ключ подписи *d* и ключ проверки подписи Q(x_a, $у_„$). которые также должны соответствовать требованиям 5.2.

6.1 Формирование цифровой подписи

Для получения цифровой подписи под сообщением Me V необходимо выполнить следующие действия (шаги) по алгоритму I:

Шаг 1 — вычислить хэш-код сообщения *M: K - h(M).* (13)

Шаг 2 — вычислить целое число а, двоичным представлением которого является вектор *h*. и определить

$$e = u \pmod{q}. \quad (14)$$

Если е - 0. то определить е = 1.

Шаг 3 — сгенерировать случайное (псевдослучайное) целое число *к,* удовлетворяющее неравенству

$$0 < k < q. \quad (15)$$

Шаг 4 — вычислить точку эллиптической кривой С = *кР* и определить

$$r = x \bmod Q), \quad (16)$$

где x_e — х-координата точки *С.*

Если г = 0, то вернуться к шагу 3.

Шаг 5 — вычислить значение

$$s = (rd * *e) \pmod{q}. \quad (17)$$

Если s = 0, то вернуться к шагу 3.

Шаг 6 — вычислить двоичные векторы *г* и s. соответствующие г и s. и определить цифровую подпись £ - HIS- как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи *d* и подписываемое сообщение *M,* а выходным результатом — цифровая подпись

Схема процесса формирования цифровой подписи приведена на рисунке 2.

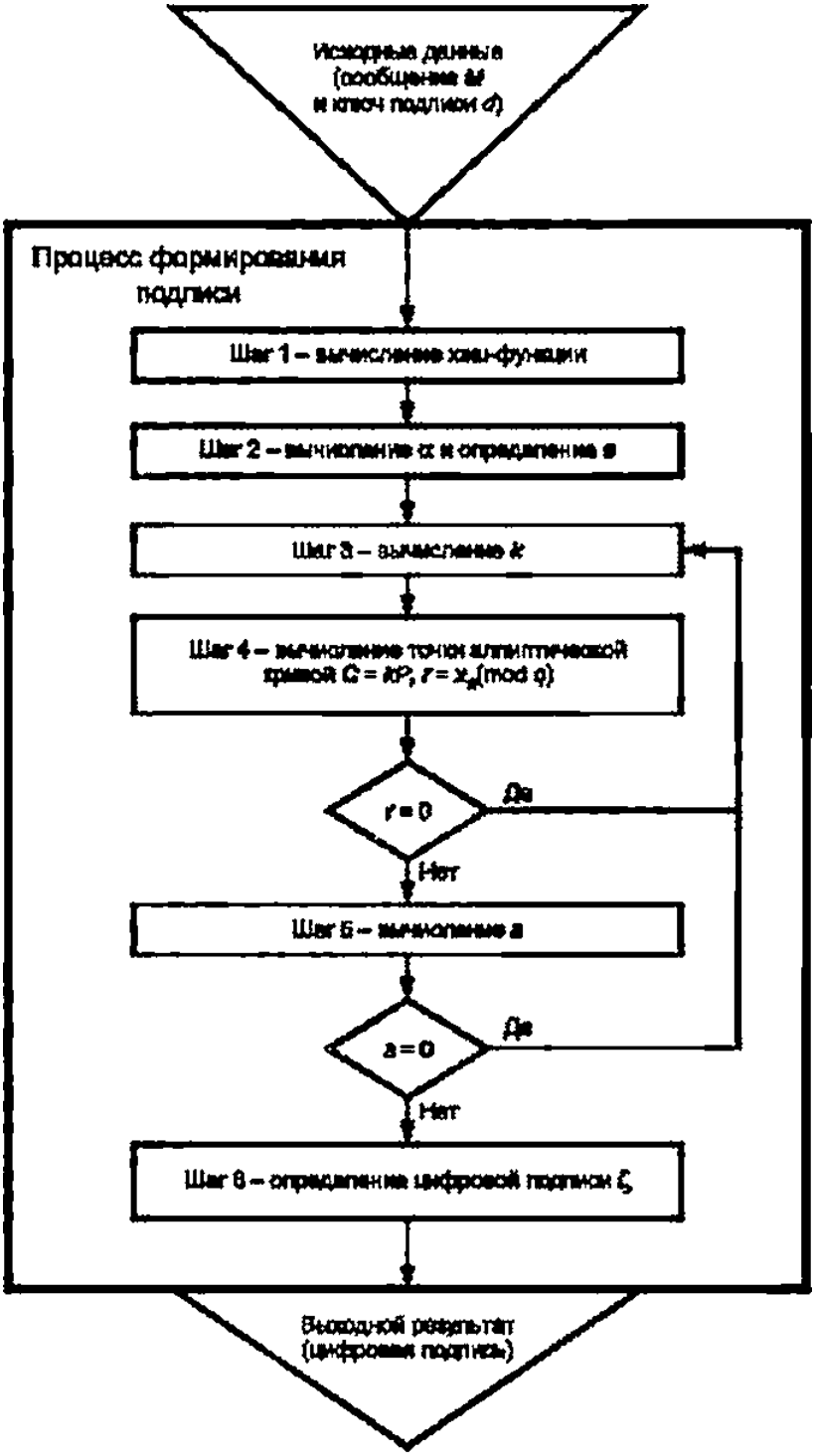

Рисунок 2 — Схема процесса формирования цифровой подписи

6.2 Проверка цифровой подписи

Для проверки цифровой подписи£ под полученным сообщением *M* необходимо выполнить следу* ющие действия (шаги) по алгоритму 11:

Шаг 1 — по полученной подписи *Q* вычислить целые числа г и а. Если выполнены неравенства 0 < г < д. 0 < s < д, то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2 — вычислить хэш-код полученного сообщения *M:*

$$h - h(M). \tag{18}$$

Шаг 3 — вычислить целое число *а*. двоичным представлением которого является вектор /Г. и опре- делить

$$esa(modp). \tag{19}$$

Если е = 0. то определить б = 1.

Ш а г 4 — еычислитьзначениеуве-' (mod д). (20)

Шаг 5 — вычислить значения

$$z, = sv \ (mod \ д). \ z_{г} = -rv \ (mod \ д). \tag{21}$$

Шаг 6 — вычислить точку эллиптической кривой С - $z,P \blacklozenge г_2 0$ и определить

$$R s x_t \ (mod \ д). \tag{22}$$

где x_e — х-координата точки С.

Шаг 7 — если выполнено равенство *R - г,* то подпись принимается, в противном случае — подпись неверна.

Исходными данными этого процесса являются подписанное сообщение *M*. цифровая подпись^ и ключ проверки подписи О. а выходным результатом — свидетельство о достоверности или ошибочнос- ти данной подписи.

Схема процесса проверки цифровой подписи приведена на рисунке 3.

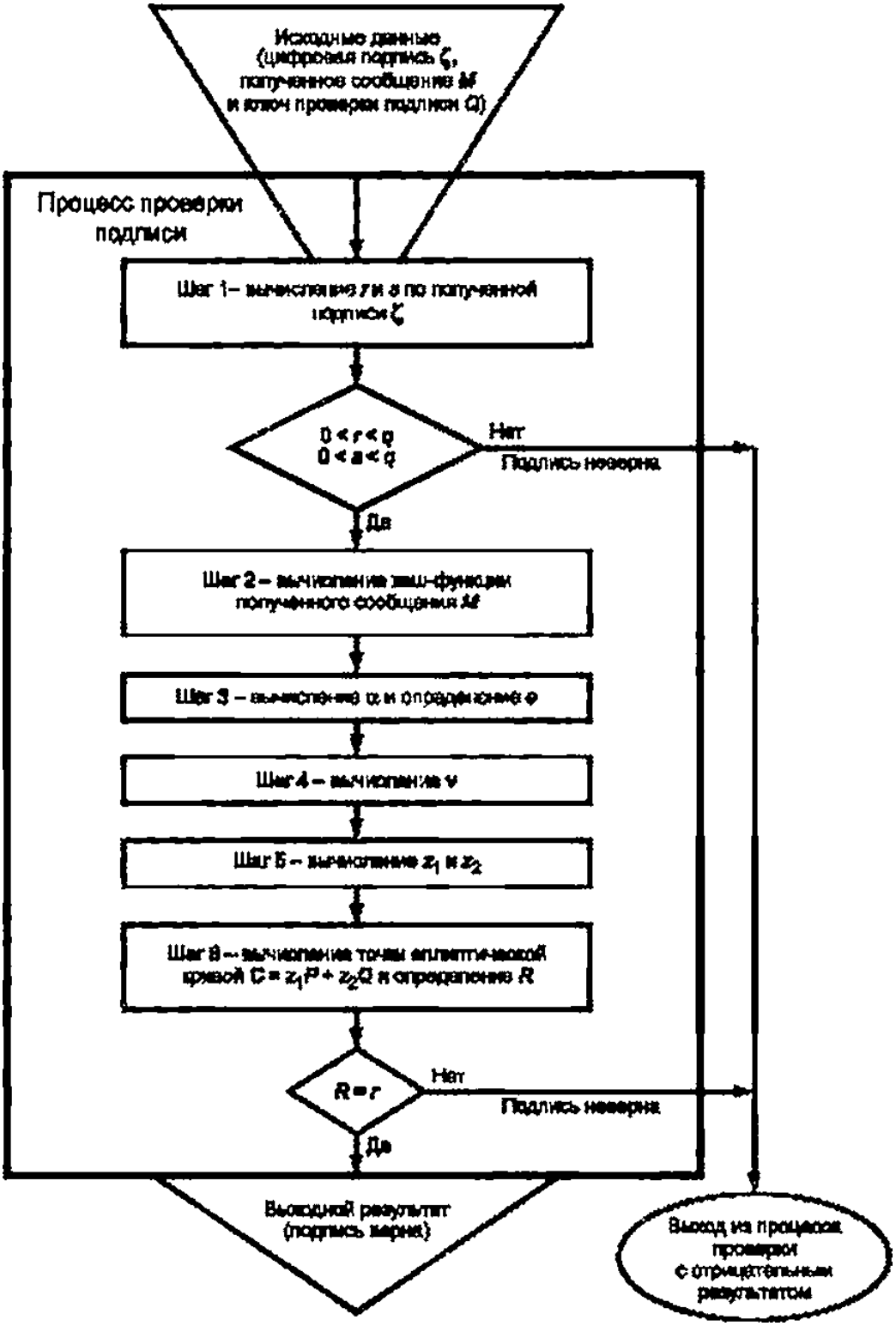

Рисунок 3 — Схема процесса проверки цифровой подписи

Приложение А
(справочное)

Контрольные примеры

Приводимые ниже значений параметров р. в. £>. *m, q, P.* а также значения ключей подписи и проверки подписи *а* и О рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящем стандарте.

Все числовые значения приведены в десятичной и шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления. Символ «и» обозначает перенос числа на новую строку. Например, запись

1234511
67690,р
49960202.$_{е}$

представляет целое число 1234567690 в десятичной и шестнадцатеричной системах счисления соответственно.

А.1 Пример 1

А.1.1 Параметры схемы цифровой подписи

Для формирования и проверки цифровой подписи должны быть использованы следующие параметры (см. S.2).

А.1.1.1 Модуль эллиптической кривой

В данном примере параметру р присвоено следующее значение.

р > 57896044618658097711785492504343953926116349923328202820197287920039565648210411$_{10}$
р ■ 8000000000000000000000000000000000000000000000000000000000000000000000000431,$_{в}$.

А.1.1.2 Коэффициенты эллиптической кривой

В данном примере параметры а и 6 принимают следующие значения.

а » 7,$_{0}$.
а » 7,$_{\#}$.
0 «433088765467672769057659045956509319951194211179445103958325296884203384958041 4,$_{с}$.
D« 5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514COCE9DAE23B7E,,.

А.1.1.3 Порядок группы точек эллиптической кривой

В данном примере параметр *m* принимает следующее значение.

/п > 57896044618658097711785492504343953921170829345837254506223809735921376310696 19.$_{0}$.
л> * 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3,$_{В}$.

А.1.1.4 Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр *q* принимает следующее значение:

р■ 57696044618656097711785492504343953921170829345837254506223609735921376310696 19.. ..
q * 8000000000000000000000000000000150FE 8A16929761S4C S9CFC193ACCF 583,,.

А.1.1.5 Коэффициенты точки эллиптической кривой

в данном примере координаты точки *P* принимают следующие значения:

x_p
X_p
y_p > 40189740S6539037S03335449422937059711
7563S739389905545080690979365213431566280,$_{0}$.
y„ > 8E2A8A0E65147D4BD6316030E16D19M
C85C97F0A9CA267122B96A8BCEA7E8FC8...

А.1.1.6 Ключ подписи

В данном примере считается, что пользователь обладает следующим ключом подписи О:

0 «55441196065363246126355624130324183111
96576709222340016572108097750006097525544, „.
tf * 7A929AOE789BB9BE10ED359DO39A72C11
11860961F49397EEE1D19CE9891EC3B28,*.

А.1.1.7 Ключ проверки подписи

8 денном примере считается, что пользователь обладает ключом проверки подписи *Q.* координаты которого имеют следующие значения:

x_9 ■ S7S2021612617680844363140502333807l\\
1766301049063136321828967413422066048594 03,$_0$.
x_e * 7F2B49E270D86D90D859S8EC458B5V\
OCS8S858A1D4E96768F6689DBD8E56FD808,$_B$.
y ■ 1761494 441921378154380939194 9654 060VV
0319426620453636392607098478594382867639 94,„.
y„ > 26F1B489O6701DD185C8413A977B3U
C8BAF6401C593D26627DFFB101 A87FF77DA.$_{fe}$.

А.1.2 Процесс формирования цифровой подписи (алгоритм I)

Пусть после выполнения шагов 1—3 по алгоритму I (см. 6.1) были получены следующие числовые значения:

e* 207988936744764520171340 61S6150827013W
0637142515379653289952617252661468872421,0.
e * 2DFBC1B372D89A1188C09C52E0EEU
C6lFC£52032AB1022E8E67ECE66728043EE5,$_e$.
к« 538541376773484637314038411479966192M
4150400343430202071296083852889319623339S.C.
к > 77105C9B20BCD3122623C6CF6FCCU
7B9S6DE33814E95B7FE64FE0924594DCEAB3,*.

При этом кратная точка С ■ *кР* имеет координаты:

x_c« 297009809158179528743712049839382569W
904227521079943196516326879820592109333 95, $_в$.
X_e * 41AA2802F1AB148260C09EDS6FE0W
A419740535S4A42767B83AD043FD39DC0493,».
y_e * 328425352786846634770046653225170845M
0680472103245454326813285455653927406091 0,$_e$.
y_e « 489C375A9941A3049E33B34361DDX1
204172AD98C3E5916OE2769SO22A61FAE46E,,.

Параметр *г* ■ x_c (mod g) принимает значение:

$_($*ж* 297009809158179S28743712049839382569U
904227521079943196516326879820592109333 95,,,
г * 41AA28D2F1AB148280CD9ED56FEOU
A41974053554A42767B83AD043FD39DC0493,,.

Параметр s ■ *{га ♦ кв)* (mod g) принимает значение:

a > 57497340027008465417692531001914703U
8455227042649098563933718999175515839552,,,.
S* 1456C64BA4642A165 3C235A98A60249BCO6D3F 74 6 8 631DF928014 F6C5BF9C40,$_e$.

А.1.3 Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1—3 по алгоритму II (см. 6.2) были получены следующие числовые значения:

e > 207988936744764520171340615615082701 3VV
0637142515379653289952617252661468872421, „.
в > 2DFBC1B372D89A1188C09C52EOEEU
C61FCE52032AB1022E8E67ECE6672B043EE5,..

При этом параметр *v* * e** (mod g) принимает значение:

v « 176866836059344686773017138249002685U
627468830806754967152880365724311457189 78,$_e$.
y > 271A4E6429F64EBC423E388964555B8U
29D3BA53C78F945E5FAC8F3817063S4C2,,.

Параметры г, • *av* (mod g) и z_3 • *-rv* (mod g) принимают значения:

2, > 37699167500901938556841057293512656 1M
0884134519049194261930453241274372099975 9,$_e$.
2, > 5358F8FFB38F7C09ABC782A2DF2AW
39270A4077007205F763662F3A76C901984F,$_B$.
$2_г$ • 1417199842 7343472112515917969500765 7W
69246655838972862114499932653333671092 21$_{le}$.
2; > 3221B4FBBF6D101074EC14AFAC2D4F7U
EFAC4CF9FEC1ED11BAE336D27D527665,,.

Точка C ■ $_{2}P + z_3Q$ имеет координаты.

x_c > 297006809158179528743712049839382569911
0422752107994319651832687982059210933395.$_0$.
X_c » 41AA28D2F1AB148280CD9EDS6FED11
A41974053554A42767B63AD043F039DC0493,,.
Xc « 32842535278664663477094665322517084501 1
6804721032454543268132854556539274060910.$_0$.
X_c > 489C375A9941A3049E33834361DD11
204172AD98C3E5916DE2769S022A61FAE46E,,.

Тогда параметр ■ x_c (mod q) принимает значение:

R > 267009809158179528743712049839362569 9П
0422752107994319651632687982059210933395, $_{и}$.
Я» 41AA28D2F1AB148280CD9ED56FE0U
A419740S3554A42767B83AD043FD39DC0493,,.

Поскольку выполнено равенство R ■ r, то цифровал подпись принимается.

А.2 Пример 2

А.2.1 Параметры схемы цифровой подписи

Для формирования и проверки цифровой подписи должны быть использованы следующие параметры (см. 5.2).

А.2.1.1 Модуль эллиптической кривой

В данном примере параметру р присвоено следующее значение.

p * 362398610222900363590778875368387430602132092553467860SOU
865461504508561666240024825884820222714968540250908236030511
873516373426382237196498722856290737240 3м.
р» 4531AC01FE0023C7550D26786B2FEE80922B14B2FFB90F0404EB7C09BS02015DM
F1D852741AF47Q4A0458G47E80E4S46D35B6336FAC224OD816648BF528BE6373$_{ie}$,.

А.2.1.2 Коэффициенты эллиптической кривой

в данном примере параметры а и 6 принимают следующие значения.

в * Лв-
в *
0 >151865506921082853450895003471404315492874752774020643611
194018823352809982443793732829756914785974674666041605397883677511
966263264139901369590474358118263 96,,.
Ь » 1CFF0806A31116OA29D8CFA54E57EB748BC5F377E49400FDO788B649ECA1AC411
361834013B2AD7322460A89CA58E0CF74BC9E 540C2ADD6897FAD0A3064F302AOC,,,.

А.2.1.3 Порядок группы точек эллиптической кривой

В данном примере параметр m принимает следующее значение.

m • 362398610222900363590776875368387430602132092553467860508654611 1
504508561666239691648963050328630684999614040794379365854558651922121 1
970734808812618120619743,„.
m ■ 4531ACD1FE0023C7550D267B6B2FEE60922B1482FFB90F04D4E87C09B5D2D15D11
A82F2D7ECB1DBAC719905C5EECC423F1D86E25EOBE23C595O644AAF187E6E6DF,,.

А.2.1.4 Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр q принимает следующее значение:

q « 362398610222900363590778675366367430602132092553467860508654611 1
504508561666239691648963050328630684909614040794379365854558651922121 1
970734808612618120619743,$_0$.
4531ACOlFE0023C75500267B6B2FEEa0922B14B2FF890F0404EB7C09B502015Dl\
A82F2D7ECB1DBAC71990SCSEECC423F1D86E25EOBE23C595D644AAF187E6E6DF,,.

А.2.1.5 Коэффициенты точки эллиптической кривой

В данном примере координаты точки P принимают следующие значения:

X, * 19283569440670228493993094012431375989977866354595079743570754913077665 11
9268583544106S5576810031848746196S8004903212332684252335830250729527632361 1
3493573274,,.
x_p * 24D19CC64S72EE30F396BF6E8BFO7A6CS21383B3D7O57CC825F91O93A68CD76211
F060611262C06380C6e60AA7EEE804E28BC849977FAC33B4B530FlB120248A9A,$_e$.
Xp > 228872869337107285997001215552947841635356232732950618031 1
144974259311026603015726141419970722717086070665938506503341523818 11

57347798885864807605098724013854,0,
28B312A43BD2CE6E0DO2O613C857ACODCFBF061E91E5F2C3F32447C2S9F398211
C83AB156D77F1496BF7EB3351E1EE4E43DC1A18B91B24640B6OBB92CB1ADD371E,,.

А.2.1.6 Ключ подписи

В денном примере считается, что пользователь обладает следующим ключом подписи *d:*

d • 610081804136373098219538153239847583006845519069531562982388135W
354890606301782255383608393423372379057665527595116827307025046458831 1
74407661211804 6687 5860,$_0$.
d » BA6048AAOAE241BA40936D47756D7C93091A0E8S14669700EE7508E508B10207211
E8123B2200A0563322OAD2827E2714A2636B7BFD18AAOFC62967821FA18OO4,,,

А.2.1.7 Ключ проверки подписи

в данном примере считается, что пользователь обладает ключом проверки подписи *Q.* координаты которого имеют следующие значения:

x, > 909546853002536596556690768669830310006929272546556281S963W
729653703124985631823204368928700528426G860826283245685822358 0U
713780290717986855863433431150561 ,$_c$.
x,« 11SDCSBC967S0C7B48598D6AB9E740D4C4A65A65BE33C181SB5C32OC854621OU
D5A51S8S6D13314AF69BC58924C8B4DOFF75C45415C1D9D09DD33612C0530EFE1,,.
$y_д$ * 29214572033744256206324497342484154556407008235594887051648956U
375095391342973273973802877414282460886266093291394418950168637 58W
984106326600572476822372076,^,
y_4> 37C7C9OCO4OBOF5621DC3AC1B751CFAOE2634FAO5O383D52639F507F872AFD611
1EA199441O943FFE7F0C70A2759A3CDB84C114E1F9339FDF27F35ECA93677BEEC,,.

А.2.2 Процесс формирования цифровой подписи (алгоритм 1)

Пусть после выполнения шагов 1—3 по алгоритму I (см. 6.1) были получены следующие числовые значения:

в» 2897963881682868575562827278553865049173745197871825199562947\\
419041388950970536661109553499954248733088719748844538964641281654 4W
635132969738277062720459 64.$_0$.
в « 3754F3CFACC9EO615C4F4A7C4O8DAB531809B6F9C17OC533A71O147O35B0C591U
7164EES36593F4414339976C64 7C5D5A407ADEDB1D560C4FC6777D2972075B8C,$_B$.
к ■ 17551635602585049954062827992112528033345103174773779165 02U
0814424318205707503444610298675096250890922723586612687247351680781 0541 П1
4 7529710309879958632945,0,
к ■ 359E7F481410FEACC570456C6801496946312120B39O019D455986E364F3U
65866748EO7A44B3E7944340060118422862122 73A6014CF70EA3AF71BB1AE679F I,^.

При этом кратная точка *С* • *кР* имеет координаты.

x_r> 248920447703134926507286464303214775366 74S131928213144402749863 73W
576110926102217951018714129288237168059598287083302842436534530 8S3U
22004442442534151761462$_{1C}$,
x_e* 2F86FA60A081091A23DD795E1E3C689EE512A3C82EEODCC2643C78EEA8FCAC1V
D35492558486B20F lC9£Cl97C9O699850260C93BCBCD9C5C3317E19344El73AE36$_{te}$,
y_c« 770173889928991836047844798780960441682062631876096137673946801 5011
24422293532765176528442837832456936422662546S13702148162933079517 11
084300501521086415063 10$_{1O}$,
y_c» EB488140F7E2F4E35CF220BOBC75AE44F26F9C7DF52E82436BOE80A91831DA27W
C81OOOAA876F9ADCOO28A82DO3826O4DC7F92E471DA23E55EOEBB3927C85BO6,0.

Параметрг*x_c(mod g> принимает значение:

г«24892044770313492650728646430321477S3667451319282131444027498637311
576110926102217951018714129288237168059598287083302842436534530653 11
22004442442534151761462,0,
г * 2F86FA60A081O91A23OO79SE1E3C689EES12A3C82EE0DCC2643C76EEA8FCAC11
D35492558486820F1C9EC197C90699850260C93BCBC09C5C3317E 19344E173AE36,$_C$.

Параметр *s* ■ (rtf ♦ *ке)* (mod 9) принимает значение:

а«864523221707669519038849297382936917075023735848431S799195987W
993133851805647486771956396724601794217607706932780309568076901 1511
82270990385368283183515937 0.0.
3 » 1081B394696FFE6E658SE 7A9362O26B6325F56778AADBC081C0BF8E933O52FF5811
23CE288E8C4F3625260800F7F70CE406A6EE81F56919CB92A9853BDE73E5B4A,,.

А.2.3 Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1—3 по алгоритму II {см. 6.2) было получено следующее числовое значение:

e> 2897963881682868575562827278S5386S04917374S197871825199562947\\
4190413869609705366611095534999542467330887197488445369646412816544»
635132969738277062720459641|0,
e ■ 3754F3CFACC9E0615C4F4A7C4D8DA8S31B09B6F9C170C533A71D14703S80CS91»
7184EE536593F4414339976C647C5O5A4O7AOEO81D560C4FC6777D2972075B8C,,.

При этом параметр *v* ■ e*' {mod a) принимает значение:

v«25569421S39460522226607408431640861538776922344007831911469284 9»
3561943457323447089240019252056962806881535340041458212439906061 36»
707223818593481596025267 1,
v « 30D212A9E25D1A80A0F238532CAOF3E64O7EF4E782B6AD140AAF8BBD9B84729»
84595EEC87B2F3446A1999D5F0A6DE0614A55AO875721EC8CFD504000B3A840FF,,.

Параметры *г,* * sv(mod d) и $г_3$ »-iv (mod d) принимают значения:

2, ■ 32064708273367686296869071018734752503433064460890303112144 84»
38587274320S045180345206826552901003496732941049780357793541942055»
60008495619817370719790257 5$_{ta}$.
2, > 3D38E7262D69BB2AD240D81EEA2F92E6348D619FA450078175837CF13B026079»
051A46A1A379188F37BA46CE12F7207F2A834 5459FF960E1EB05B4F2A34A6EEF$_{l8}$.
2_2 > 13667709118340031081429778480218 47S973204SS3475356412734827»
32082047028342168006031261814273230879203690726448631222679743757 5»
6163726695805660585960300820 3,
2_2> 1A18A31602E6EACOA9868C01941082AEFE296F8404S302603414C2A16E86FC529M
08O6372ES00C49O6C612CE1FF65BO58ElD2029F22690438CC36A76O0A444AC8,$_e$.

Точка С » 2,Р + $г_30$ имеет координаты.

x_c «24892044770313492650728646430321477536674513192821314440274986 37»
3576110928102217951018714129288237168059506267083302842436534530853»
220044424425341517614 62$_{10}$.
к, ■ 2F86FA60A081091A23OD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC»
D35492558466B20F1C9EC197C90690850260C93BC8C09C5C3317E19344E173AE36,,.
y_c« 770173689928991836047844798780960441682062631876096137673946 8015»
024422293532765176528442837832456936422662546513702146162033079517 0»
8430050152108641508310,$_e$.
y_c ■ £B486140F7E2F4E35CF2208O8C75AE44F26F9C7OF52Ed2436BDEeOA9l631DA27»
C6l00DAA676F9AOC0D28A620D3826O4OC7F92E471OA23E5SE0EB83927C85BO6$_{ie}$.

Тогда параметр *R* » x_c (mod d) принимает значение:

R«24892044770313492650728646430321477536674513192821314440274986»
373S7611092810221795Ю187141292882371680595982870833028424365345 3085W
322004442442534151761462,
*R** 2F86FA60AO81091A23D0795E1E3C689EE512A3C82EE0OCC2643C78EEA8FCAC»
035492558486820F1C9EC197C90699850260C93BC8CD9CSC3317E19344E173AE36,,.

Поскольку выполнено равенство *R* ■ г. то цифровая подпись принимается.

Библиография*

(1)	ИСО 2382-2:1976	Системы обработки информации. Словарь. Часть 2. Арифметические и логические операции
	(ISO 2382-2:1976)	(Data processing — Vocabulary — Part 2: Antnmetic and logic operations}
(2)	ИСО/МЭК 9796-2:2010	Информационные технологии. Методы обеспечений безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации
	(ISO/IEC 9796-2:2010)	(Information technology — Security techniques — Digital signature schemes giving message recovery— Part 2: Integer factorization based mechanisms)
(3)	ИСО/МЭК 9796-3:2006	Информационные технологии. Методы обеспечений безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 3. Механизмы на основе дискретного логарифма
	(ISO/IEC 9796-3:2006)	(information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms)
(4)	ИСО/МЭК 14888-1:2008	Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения
	(ISO/IEC 14888-1.2008}	(Information technology — Security techniques—Digital signatures with appendix — Part 1: General)
(5)	ИСО/МЭК 14888-2:2008	Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 2. Механизмы, основанные не разложении на множители
	(ISO/IEC 14888-2:2008}	(Information technology — Security techniques—Digital signatures with appendix — Part 2: integer factorization based mechanisms)
(6)	ИСО/МЭК 14888-3:2006	Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма
	(ISO/IEC 14888-3:2006}	(Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms)
(7)	ИСО/МЭК 14888-3:2006/Изм. 1:2010	Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма. Изменение 1. Алгоритм русской цифровой подписи эллиптической кривой, алгоритм цифровой подписи Шнора. алгоритм цифровой подписи Шнора для эллиптической кривой и полный алгоритм цифровой подписи Шнора для эллиптической кривой
	(ISO/IEC 14888-3.2006/Amd 1:2010}	(Information technology — Security techniques—Digital signatures with appendix— Part 3: Discrete logarithm based mechanisms. Ammendment 1. Elliptic Curve Russian Digital Signature Algorithm. Schnorr Digital Signature Algorithm. Eliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digitel Signature Algonthm)
(8)	ИСО/МЭК 10118-1:2000	Информационные технологии. Методы защиты информации. Хэш-функции. Часть 1. Общие положения
	(ISO/IEC 10116-1:2000}	(Information technology — Security techniques — Hash-functions — Part 1: General)
(9)	ИСО/МЭК 10118-2:2010	Информационные технологии. Методы защиты информации. Хэш-функции. Часть 2. Хэш-функции с использованием алгоритма шифрования л-битными блоками
	(ISO/IEC 10118-2:2010}	(information technology — Secunty techniques — Hash-functions — Part 2: Hash-functions using an n-blt block cipher)
(10)	ИСО/МЭК 10118-3:2004	Информационные технологии. Методы защиты информации. Хэш-функции. Часть 3. выделенные хэш-функции
	(ISO/IEC 10118-3:2004)	(Information technology — Secunty techniques — Hash-functions — Part 3: Dedicated hash-functions)
(11)	ИСО/МЭК 10118-4:1998	Информационные технологии. Методы защиты информации. Хэш-функции. Часть 4. Хэш-функции с применением арифметики в остаточных классах
	(ISO/IEC 10118-4:1998)	(Information technology — Secunty techniques — Hash-functions—Part 4: Hash-functions using modular anthmetlc)

* Оригиналы международных стандартов ИСО/МЭК находятся а ФГУП «Стандартинформ» Федерального агентства по техническому регулированию и метрологии.

УДК 681.3.06:006.354 ОКС 35.040 ОКСТУ 5001 П85

Ключевые слова: обработка данных, передача данных, обмен информацией, сообщения, цифровые подписи, защита информации, формирование цифровой подписи, проверка цифровой подписи

Редактор *в.Н.* Кооыоое
Технический редактор *в.Н.* /7ру<свкоеа
Корректор *РА. Ментова*
Компьютерная верстка *В.Н.* Грищенко

Сдано а набор 25.12.2012. Подписано в печать 00.02.2013. Формат в0хО4'/|. Гарнитура Ариал. Уел. пен. *я.* 2.79.
Уч.-иаа. л. 2.40. Тираж ЭДэкэ. Зак. 121.

ФГУП «СТАНДАРТИНФОРМ». 123095 Москва. Гранатный лер.. 4
«vw1v.9o1tnfo.ru info^goslinforu
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник». 105002 Москва. Лялин пер.. 0.

Федеральное агентство
по техническому регулированию
и метрологии

Федеральное агентство
по техническому регулированию
и метрологии

Федеральное агентство
по техническому регулированию
и метрологии

Федеральное агентство
по техническому регулированию
и метрологии