НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Процессы формирования и проверки электронной цифровой подписи

Information technology. Cryptographic data security.

Signature and verification processes of [electronic] digital signature

Дата введения – 20__-__-__

1 Область применения

Настоящий стандарт определяет схему электронной цифровой подписи (ЭЦП) (далее по тексту – 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 базе настоящего стандарта повышает, по сравнению с действующей схемой цифровой подписи, уровень защищенности передаваемых сообщений от подделок и искажений.

Стандарт рекомендуется использовать в новых системах обработки информации различного назначения, а также при модернизации действующих систем.

2 Нормативные ссылки

В настоящем стандарте использована ссылка на следующий стандарт:

ГОСТ Р 34.11-20__(проект) Информационная технология. Криптографическая защита информации. Функции хэширования

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

3 Определения и обозначения

3.1 Определения

В настоящем стандарте применены следующие термины:

3.1.1

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

[ИСО/МЭК 14888-1].

3.1.2

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

[ИСО/МЭК 14888-1]

3.1.3

ключ проверки (verification key): Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи.

[ИСО/МЭК 14888-1]

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].

3.1.5

подписанное сообщение (signed message): Набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения.

[ИСО/МЭК 14888-1]

3.1.6

последовательность псевдослучайных чисел (pseudo-random number sequence): Последовательность чисел, полученная в результате выполнения некоторого арифметического (вычислительного) процесса, используемая в конкретном случае вместо последовательности случайных чисел.

[ИСО 2382-2]

3.1.7

последовательность случайных чисел (random number sequence): Последовательность чисел, каждое из которых не может быть предсказано (вычислено) только на основе знания предшествующих ему чисел данной последовательности.

[ИСО 2382-2]

3.1.8

процесс проверки подписи (verification process): Процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки и параметры схемы ЭЦП, результатом которого является заключение о правильности или ошибочности цифровой подписи.

[ИСО/МЭК 14888-1].

3.1.9

процесс формирования подписи (signature process): Процесс, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы ЭЦП, а в результате формируется цифровая подпись.

[ИСО/МЭК 14888-1]

3.1.10

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

[ИСО/МЭК 148881-1]

3.1.11

случайное число (random number): Число, выбранное из определенного набора чисел таким образом, что каждое число из данного набора может быть выбрано с одинаковой вероятностью.

[ИСО 2382-2]

3.1.12

сообщение (message): Строка бит ограниченной длины

[ИСО/МЭК 9796-3]

3.1.13

хэш-код (hash-code): Строка бит, являющаяся выходным результатом хэш-функции.

[ИСО/МЭК 10118-1]

3.1.14

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

1 по данному значению функции сложно вычислить исходные данные, отображенные в это значение;

2 для заданных исходных данных трудно найти другие исходные данные, отображаемые с тем же результатом;

3 трудно найти какую-либо пару исходных данных с одинаковым значением хэш-функции.

[ИСО/МЭК 10118-1]

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

3.1.15

[электронная] цифровая подпись (digital signature); ЭЦП: Строка бит, полученная в результате процесса формирования подписи. Данная строка имеет внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

[ИСО/МЭК 14888-1]

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

3.2 Обозначения

В настоящем стандарте используются следующие обозначения:

V_l – множество всех двоичных векторов длиной l бит

V_∞ – множество всех двоичных векторов произвольной конечной длины;

Z – множество всех целых чисел;

p – простое число, $p > 3$;

F_p – конечное простое поле, представляемое как множество из p целых чисел {0,1, … , *p*-1}

$b(\mathrm{mod}\, p)$ – минимальное неотрицательное число, сравнимое с b по модулю p;

M – сообщение пользователя, $M \in V_\infty$

$(\overline{h_1} \parallel \overline{h_2})$ – конкатенация (объединение) двух двоичных векторов;

a, b – 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;

ζ – цифровая подпись под сообщением *M*.

4 Общие положения

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

- генерация ключей (подписи и проверки);
- формирование подписи;

- проверка подписи.

В настоящем стандарте процесс генерации ключей (подписи и проверки) 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:

- осуществить контроль целостности передаваемого подписанного сообщения,
- доказательно подтвердить авторство лица, подписавшего сообщение,
- защитить сообщение от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке 1.

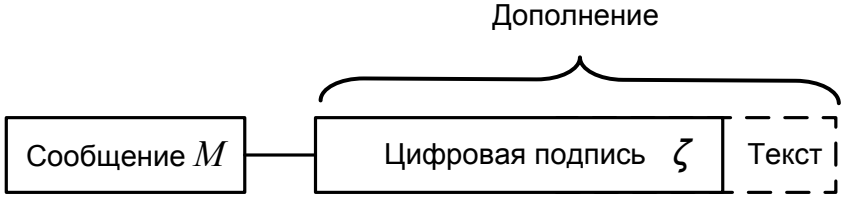

Рисунок 1 – Схема подписанного сообщения

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, определённой 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 34.11-20__(проект).

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

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

5 Математические соглашения

Для определения схемы цифровой подписи необходимо описать базовые математические объекты, используемые в процессах ее формирования и проверки. В данном разделе установлены основные математические определения и требования, накладываемые на параметры схемы цифровой подписи.

5.1 Математические определения

Пусть задано простое число $p > 3$. Тогда *эллиптической кривой* E, определённой над конечным простым полем F_p, называется множество пар чисел (x,y), $x,y \in F_p$, удовлетворяющих тождеству

$$y^2 \equiv x^3 + ax + b \pmod{p}, \tag{1}$$

где $a,b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю p.

Инвариантом эллиптической кривой называется величина $J(E)$, удовлетворяющая тождеству

$$J(E) \equiv 1728 \frac{4a^3}{4a^3+27b^2} \pmod{p} \tag{2}$$

Коэффициенты a,b эллиптической кривой E, по известному инварианту $J(E)$, определяются следующим образом

$$\begin{cases} a \equiv 3k \pmod{p}, \\ b \equiv 2k \pmod{p}, \text{где } k \equiv \frac{J(\mathrm{E})}{1728 - J(\mathrm{E})} \pmod{p},\ J(\mathrm{E}) \neq 0 \text{ или } 1728 \end{cases} \tag{3}$$

Пары (x,y), удовлетворяющие тождеству (1), называются *точками эллиптической кривой* E, x и y - соответственно x- и y-координатами точки.

Точки эллиптической кривой будем обозначать $Q(x,y)$ или просто Q. Две точки эллиптической кривой равны, если равны их соответствующие *x*- и *y*-координаты.

На множестве всех точек эллиптической кривой E введем операцию сложения, которую будем обозначать знаком "+". Для двух произвольных точек $Q_1(x_1, y_1)$ и $Q_2(x_2, y_2)$ эллиптической кривой E рассмотрим несколько вариантов.

Пусть координаты точек Q_1 и Q_2 удовлетворяют условию $x_1 \neq x_2$. В этом случае их суммой будем называть точку $Q_3(x_3, y_3)$ координаты которой определяются сравнениями

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}, \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}, \end{cases} \quad \text{где } \lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} \tag{4}$$

Если выполнены равенства $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то определим координаты точки Q_3 следующим образом

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 \pmod{p}, \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}, \end{cases} \quad \text{где } \lambda \equiv \frac{3x_1^2 + a}{2y_1} \pmod{p} \tag{5}$$

В случае, когда выполнено условие $x_1 = x_2$ и $y_1 \equiv -y_2 \pmod{p}$, сумму точек Q_1 и Q_2 будем называть *нулевой точкой* O, не определяя ее x- и y-координаты. В этом случае, точка Q_2 называется *отрицанием* точки Q_1. Для нулевой точки O выполнены равенства

$$Q + O = O + Q = Q, \tag{6}$$

где Q – произвольная точка эллиптической кривой *E.*

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

$$p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p} \tag{7}$$

Точка Q называется точкой кратности k, или просто – кратной точкой эллиптической кривой E, если для некоторой точки P выполнено равенство:

$$Q = \underbrace{P + \cdots + P}_{k} = kP \tag{8}$$

5.2 Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:

- простое число p - модуль эллиптической кривой;
- эллиптическая кривая E, задаваемая своим инвариантом J (E) или коэффициентами $a,b \in F_p$;
- целое число m – порядок группы точек эллиптической кривой E;
- простое число q - порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} m = nq, \ n \in Z, \ n \geq 1 \\ 2^{254} < q < 2^{256} \text{ или } 2^{508} < q < 2^{512} \end{cases} \tag{9}$$

- точка $P \neq O$ эллиптической кривой E, с координатами (x_p,y_p), удовлетворяющая равенству $qP=O$.
- хэш-функция $h(\cdot) : V_\infty \to V_l$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные вектора длины l бит. Хэш-функция определена в ГОСТ Р 34.11-20__(проект). Если $2^{254} < q < 2^{256}$, то $l = 256$. Если $2^{508} < q < 2^{512}$, то $l = 512$.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

- ключом подписи – целым числом d, удовлетворяющим неравенству $0 < d < q$;
- ключом проверки – точкой эллиптической кривой Q с координатами (x_q, y_q), удовлетворяющей равенству $dP=Q$.

На приведенные выше параметры схемы цифровой подписи накладываются следующие требования:

- должно быть выполнено условие $p^t \neq 1 \pmod q$, для всех целых t = 1,2, … B, где B удовлетворяет неравенству $B \geq 31$;
- должно быть выполнено неравенство $m \neq p$;
- инвариант кривой должен удовлетворять условию J (E) $\neq 0$ или 1728.

5.3 Двоичные векторы

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

Рассмотрим следующий двоичный вектор длиной l бит, в котором младшие биты расположены справа, а старшие – слева

$$\bar{h} = (\alpha_{l-1}, \dots, \alpha_0), \ \ \bar{h} \in V_l \tag{10}$$

где α_i, i= 0,..,$l-1$ равно либо 1, либо 0. Будем считать, что число $\alpha \in$ Z *соответствует* двоичному вектору $\bar{h}$, если выполнено равенство

$$\alpha = \sum_{i=0}^{l-1} \alpha_i 2^i \tag{11}$$

Для двух двоичных векторов $\bar{h}_1$ и $\bar{h}_2$, соответствующих целым числам α и β, определим операцию *конкатенации* (объединения) следующим образом. Пусть

$$\bar{h}_1 = (\alpha_{l-1}, \dots, \alpha_0),$$
$$\bar{h}_2 = (\beta_{l-1}, \dots, \beta_0) \tag{12}$$

тогда их объединение имеет вид

$$(\bar{h}_1 \parallel \bar{h}_1 = (\alpha_{l-1}, \dots, \alpha_0, \beta_{l-1}, \dots, \beta_0) \quad (13)$$

и представляет собой двоичный вектор длиной $2l$ бит, составленный из коэффициентов векторов $\bar{h}_1$ и $\bar{h}_2$.

С другой стороны, приведенные формулы определяют способ разбиения двоичного вектора $\bar{h}_1$ длиной $2l$ бит на два двоичных вектора длиной l 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, удовлетворяющие требованиям 5.2.

Кроме того, каждый пользователь должен иметь ключ подписи d и ключ проверки подписи $Q(x_q, y_q)$, которые также должны удовлетворять требованиям 5.2.

6.1 Формирование цифровой подписи

Для получения цифровой подписи под сообщением $M \in V_\infty$ необходимо выполнить следующие действия (шаги) по алгоритму I:

Шаг 1 – вычислить хэш-код сообщения $M : \overline{h} = h(M)$ (14)

Шаг 2 – вычислить целое число α, двоичным представлением которого является вектор $\overline{h}$, и определить

$$e \equiv \alpha \pmod q \quad (15)$$

Если *e* = 0, то определить *e* = 1.

Шаг 3 – сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству

$$0 < k < q \quad (16)$$

Шаг 4 – вычислить точку эллиптической кривой $C = kP$ и определить

$$r \equiv x_c \pmod q \quad (17)$$

где x_c – x-координата точки *C*. Если $r = 0$, то вернуться к шагу 3.

Шаг 5 – вычислить значение

$$s \equiv (rd + ke) \pmod q \quad (18)$$

Если $s = 0$, то вернуться к шагу 3.

Шаг 6 – вычислить двоичные векторы $\overline{r}$ и $\overline{s}$, соответствующие r и s, и определить цифровую подпись $\zeta = (\overline{r} \parallel \overline{s})$ как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи d и подписываемое сообщение M, а выходным результатом – цифровая подпись ζ.

Схематическое представление процесса формирования цифровой подписи приведено на рисунке 2.

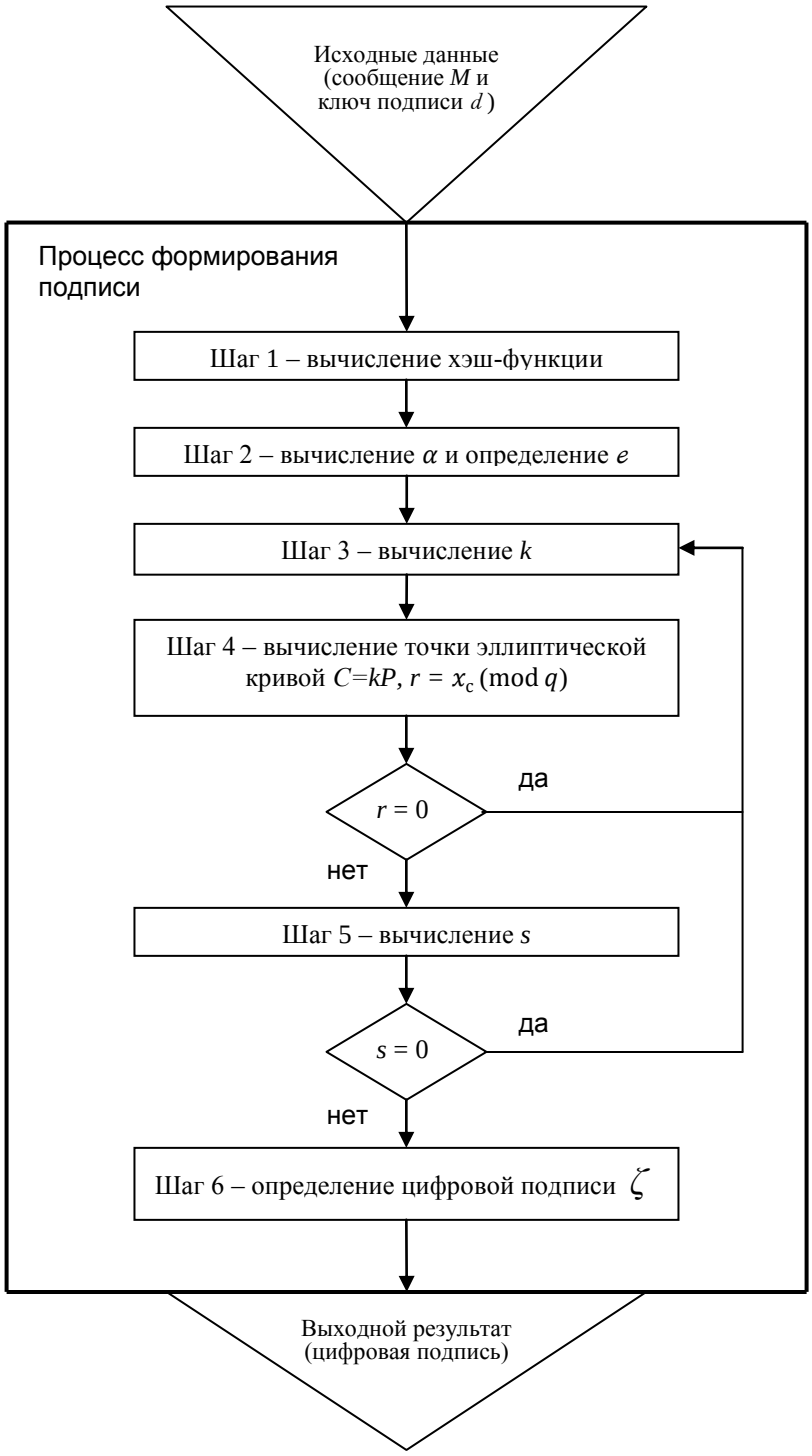

Рисунок 2 – Схема процесса формирования цифровой подписи

6.2 Проверка цифровой подписи

Для проверки цифровой подписи ζ под полученным сообщением M необходимо выполнить следующие действия (шаги) по алгоритму II:

Шаг 1 – по полученной подписи ζ вычислить целые числа r и s. Если выполнены неравенства $0 < r < q, \ \ 0 < s < q$, то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2 – вычислить хэш-код полученного сообщения M

$$\overline{h} = h(M) \tag{19}$$

Шаг 3 – вычислить целое число α, двоичным представлением которого является вектор $\overline{h}$ и определить

$$e \equiv \alpha \ (\mathrm{mod}\ q) \tag{20}$$

Если $e = 0$, то определить $e = 1$.

Шаг 4 – вычислить значение $v \equiv e^{-1} \ (\mathrm{mod}\ q)$. (21)

Шаг 5 – вычислить значения

$$z_1 \equiv sv \ (\mathrm{mod}\ q), \ \ z_2 \equiv -rv \ (\mathrm{mod}\ q) \tag{22}$$

Шаг 6 – вычислить точку эллиптической кривой $C = z_1 P + z_2 Q$ и определить

$$R \equiv x_c (\mathrm{mod}\ q) \tag{23}$$

где x_c – x-координата точки C.

Шаг 7 – если выполнено равенство $R = r$, то подпись принимается, в противном случае, подпись неверна.

Исходными данными этого процесса являются подписанное сообщение M, цифровая подпись ζ и ключ проверки Q, а выходным результатом – свидетельство о достоверности или ошибочности данной подписи.

Схематическое представление процесса проверки цифровой подписи приведено на рисунке 3.

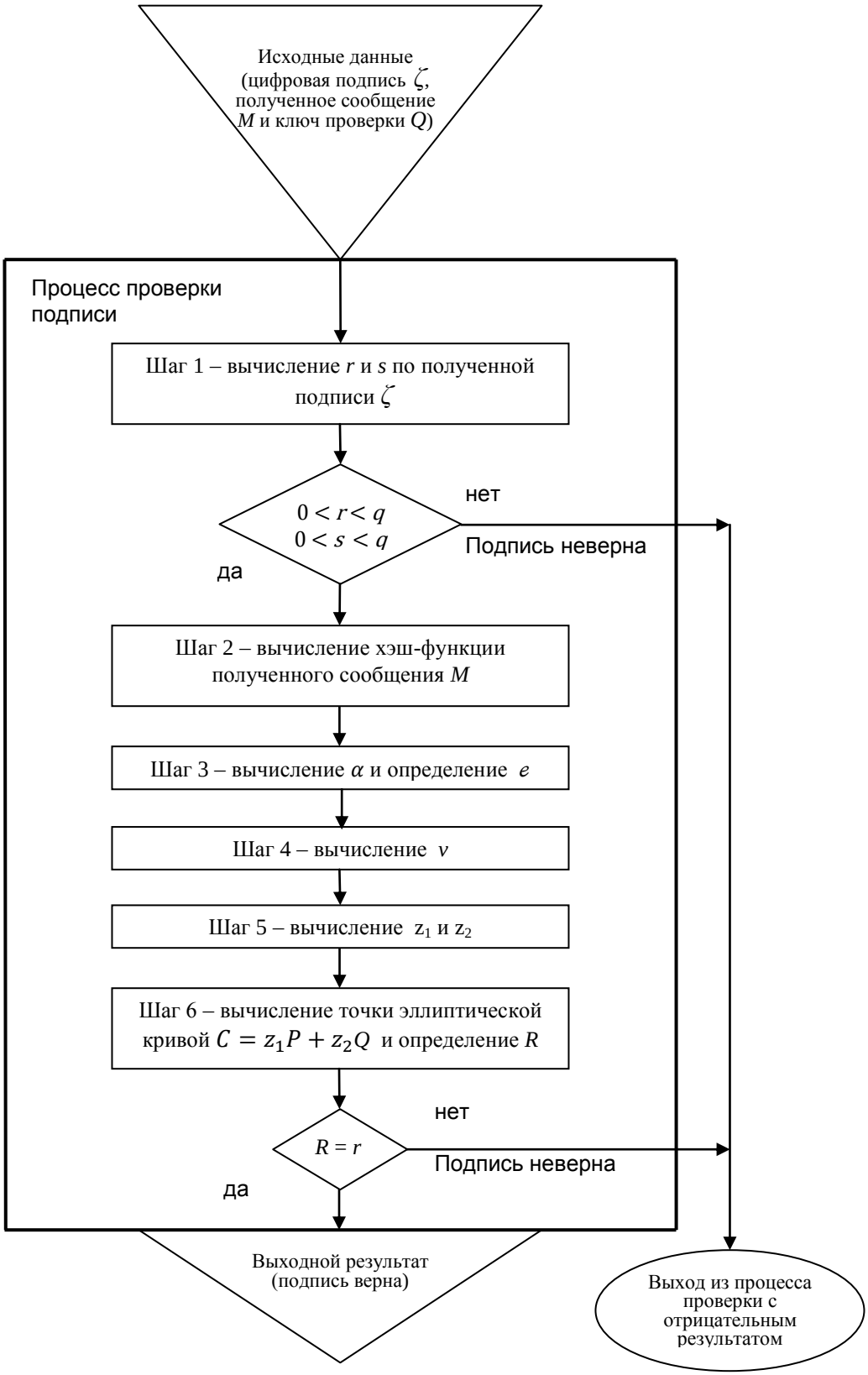

Рисунок 3 – Схема процесса проверки цифровой подписи

Приложение А
(справочное**)**

КОНТРОЛЬНЫЕ ПРИМЕРЫ

Данное приложение носит справочный характер и не является частью стандарта. Приводимые ниже значения параметров p, a, b, m, q, P, а также значения ключей подписи и проверки d и Q 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 "\\" обозначает перенос числа на новую строку. Например, запись

$$12345\backslash\backslash$$
$$67890_{10}$$
$$499602D2_{16}$$

представляет целое число 1234567890, соответственно, в десятичной и шестнадцатеричной системах счисления.

А.1 Пример 1

А.1.1 Параметры схемы цифровой подписи

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

А.1.1.1 Модуль эллиптической кривой

В данном примере параметру p присвоено следующее значение:

$$p = 57896044618658097711785492504343953926\backslash\backslash$$
$$634992332820282019728792003956564821041_{10}$$
$$p = 8000000000000000000000000000000000000000000000000000000000000431_{16}$$

А.1.1.2 Коэффициенты эллиптической кривой

В данном примере параметры a и b принимают следующие значения:

$$a = 7_{10}$$
$$a = 7_{16}$$
$$b = 43308876546767276905765904595650931995\backslash\backslash$$
$$94211179445103958325296884203384958041 4_{10}$$
$$b = 5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514C0CE9DAE23B7E_{16}$$

А.1.1.3 Порядок группы точек эллиптической кривой

В данном примере параметр m принимает следующее значение:

$$m = 57896044618658097711785492504343953 92\backslash\backslash$$
$$708293458372545062238097359213763106961 9_{10}$$

m = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3$_{16}$

А.1.1.4 Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр q принимает следующее значение:

q = 57896044618658097711785492504343953 92\\

7082934583725450622380973592137631069619$_{10}$

q = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3$_{16}$

А.1.1.5 Коэффициенты точки эллиптической кривой

В данном примере координаты точки P принимают следующие значения:

x_p = 2$_{10}$

x_p = 2$_{16}$

y_p = 4018974056539037503335449422937059 7\\

7563573938990554508069097936521343156628 0$_{10}$

y_p = 8E2A8A0E65147D4BD6316030E16D19\\

C85C97F0A9CA267122B96ABBCEA7E8FC8$_{16}$

А.1.1.6 Ключ подписи

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

d = 5544119606536324612635562413032418 31\\

9657670922234001657210809775000609752554 4$_{10}$

d = 7A929ADE789BB9BE10ED359DD39A72C\\

11B60961F49397EEE1D19CE9891EC3B28$_{16}$

А.1.1.7 Ключ проверки

В данном примере считается, что пользователь обладает ключом проверки Q, координаты которого имеют следующие значения:

x_q = 5752021612617680844363140502333807 1\\

1766301049063136321828967413422066048594 03$_{10}$

x_q = 7F2B49E270DB6D90D8595BEC458B5\\

0C58585BA1D4E9B788F6689DBD8E56FD80B$_{16}$

y_q = 1761494441921378154380939194965408 0\\

0319426620453636392607098478594382867639 94$_{10}$

y_q = 26F1B489D6701DD185C8413A977B3\\

CBBAF64D1C593D26627DFFB101A87FF77DA$_{16}$

А.1.2 Процесс формирования цифровой подписи (алгоритм I)

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

e = 2079889367447645201713406156150827 013\\

$$0637142515379653289952617252661468872421_{10}$$

$$e = 2DFBC1B372D89A1188C09C52E0EE\backslash\backslash$$

$$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$$

$$k = 538541376773484637314038411479966192\backslash\backslash$$

$$41504003434302020712960838528893196233395_{10}$$

$$k = 77105C9B20BCD3122823C8CF6FCC\backslash\backslash$$

$$7B956DE33814E95B7FE64FED924594DCEAB3_{16}$$

При этом кратная точка $C = kP$ имеет координаты:

$$x_c = 297009809158179528743712049839382569\backslash\backslash$$

$$90422752107994319651632687982059210933395_{10}$$

$$x_c = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$

$$A41974053554A42767B83AD043FD39DC0493_{16}$$

$$y_c = 328425352786846634770946653225170845\backslash\backslash$$

$$0680472103245454326813285455653927406091 0_{10}$$

$$y_c = 489C375A9941A3049E33B34361DD\backslash\backslash$$

$$204172AD98C3E5916DE27695D22A61FAE46E_{16}$$

Параметр $r = x_c \pmod q$ принимает значение:

$$r = 297009809158179528743712049839382569\backslash\backslash$$

$$90422752107994319651632687982059210933395_{10}$$

$$r = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$

$$A41974053554A42767B83AD043FD39DC0493_{16}$$

Параметр $s = (rd + ke) \pmod q$ принимает значение:

$$s = 57497340027008465417892531001914703\backslash\backslash$$

$$84552270426490985639337189991755158395 52_{10}$$

$$s = 1456C64BA4642A1653C235A98A60249BCD6D3F746B631DF928014F6C5BF9C40_{16}$$

А.1.3 Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1 – 3 по алгоритму II (6.2) были получено следующее числовое значение:

$$e = 207988936744764520171340615615082 7013\backslash\backslash$$

$$0637142515379653289952617252661468872421_{10}$$

$$e = 2DFBC1B372D89A1188C09C52E0EE\backslash\backslash$$

$$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$$

При этом параметр $v = e^{-1} \pmod q$ принимает значение:

$$v = 176866836059344686773017138249002685\backslash\backslash$$

$$62746883080675496715288036572431145718978_{10}$$

$$v = 271A4EE429F84EBC423E388964555BB\backslash\backslash$$

29D3BA53C7BF945E5FAC8F381706354C2$_{16}$

Параметры $z_1 \equiv sv \pmod q$ и $z_2 \equiv -rv \pmod q$ принимают значения:

z_1 = 37699167500901938556841057293512656 1\\

088413451904919426193045324127437209997 59$_{10}$

z_1 = 5358F8FFB38F7C09ABC782A2DF2A\\

3927DA4077D07205F763682F3A76C9019B4F$_{16}$

z_2 = 14171998427343472112515917969500765 7\\

692466558389728621144999326533336710922 1$_{10}$

z_2 = 3221B4FBBF6D101074EC14AFAC2D4F7\\

EFAC4CF9FEC1ED11BAE336D27D527665$_{16}$

Точка $C = z_1P + z_2Q$ имеет координаты:

x_c = 29700980915817952874371204983938256 99\\

042275210799431965163268798205921093339 5$_{10}$

x_c = 41AA28D2F1AB148280CD9ED56FED\\

A41974053554A42767B83AD043FD39DC0493$_{16}$

y_c = 32842535278684663477094665322517084 50\\

680472103245454326813285455653927406091 0$_{10}$

y_c = 489C375A9941A3049E33B34361DD\\

204172AD98C3E5916DE27695D22A61FAE46E$_{16}$

Тогда параметр $R = x_c \pmod q$ принимает значение:

R = 29700980915817952874371204983938256 99\\

042275210799431965163268798205921093339 5$_{10}$

R = 41AA28D2F1AB148280CD9ED56FED\\

A41974053554A42767B83AD043FD39DC0493$_{16}$

Поскольку выполнено равенство $R = r$, то цифровая 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 p присвоено следующее значение:

p = 36239861022290036359077887536838743060213209255346786050\\

865461504508561666240024825884820222714968540250908236030 5\\

873516373426382237196498722858290737240 3$_{10}$

p = 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\\

F1D852741AF4704A0458047E80E4546D35B8336FAC224DD81664BBF528BE6373$_{16}$

А.2.1.2 Коэффициенты эллиптической кривой

В данном примере параметры a и b принимают следующие значения:

a = 7$_{10}$

a = 7$_{16}$

b = 151865506921082853450895003471404315492874752774020643\\

194018823352809982443793732829756914785974674866041605397883677\\

9662632641399013695904743581182639$6_{10}$

b = 1CFF0806A31116DA29D8CFA54E57EB748BC5F377E49400FDD788B649ECA1AC4\\

361834013B2AD7322480A89CA58E0CF74BC9E540C2ADD6897FAD0A3084F302ADC$_{16}$

А.2.1.3 Порядок группы точек эллиптической кривой

В данном примере параметр m принимает следующее значение:

m = 362398610222900363590778875368387430602132092553467860508654\\

61\\

504508561666239691648983050328630684999614040794379365854558651922\\

12\\

970734808812618120619743$_{10}$

m = 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\\

A82F2D7ECB1DBAC719905C5EECC423F1D86E25EDBE23C595D644AAF187E6E6DF$_{16}$

А.2.1.4 Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр q принимает следующее значение:

q = 362398610222900363590778875368387430602132092553467860508654\\

61\\

504508561666239691648983050328630684999614040794379365854558651922\\

12\\

970734808812618120619743$_{10}$

q = 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\\

A82F2D7ECB1DBAC719905C5EECC423F1D86E25EDBE23C595D644AAF187E6E6DF$_{16}$

А.2.1.5 Коэффициенты точки эллиптической кривой

В данном примере координаты точки P принимают следующие значения:

x_p = 192835694406702284939930940124313759899778663545950797435707549130776\\

65\\

926858354410655576810031848748196580049032123328842523358302507295276323\\

8\\

3493573274$_{10}$

x_p = 24D19CC64572EE30F396BF6EBBFD7A6C5213B3B3D7057CC825F91093A68CD762\\

FD60611262CD838DC6B60AA7EEE804E28BC849977FAC33B4B530F1B120248A9A$_{16}$

y_p = 228872869337197285997001215552947841635356232732950618\\

03\\

144974259311028603015728141419970722717088070665938506503341523818\\

57347798885864807605098724013854$_{10}$

y_p = 2BB312A43BD2CE6E0D020613C857ACDDCFBF061E91E5F2C3F32447C259F39B2\\

C83AB156D77F1496BF7EB3351E1EE4E43DC1A18B91B24640B6DBB92CB1ADD371E$_{16}$

А.2.1.6 Ключ подписи

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

d = 610081804136373098219538153239847583006845519069531562982388135\\
35489060630178225538360839342337237905766552759511682730702504645883\\
7440766121180466875860$_{10}$

d = BA6048AADAE241BA40936D47756D7C93091A0E8514669700EE7508E508B102072\\
E8123B2200A0563322DAD2827E2714A2636B7BFD18AADFC62967821FA18DD4$_{16}$

А.2.1.7 Ключ проверки

В данном примере считается, что пользователь обладает ключом проверки Q, координаты которого имеют следующие значения:

x_q = 909546853002536596556690768669830310006929272546556281596 3\\
72965370312498563182320436892870052842808608262832456858223580\\
7137802907179868558634334311505610$_{10}$

x_q = 115DC5BC96760C7B48598D8AB9E740D4C4A85A65BE33C1815B5C320C854621D\\
D5A515856D13314AF69BC5B924C8B4DDFF75C45415C1D9DD9DD33612CD530EFE1$_{16}$

y_q = 292145720337442562063244973424841545564070082355948870516489 58\\
37509539134297327397380287741428246088626609329139441895016863758\\
9841063266005724768223720760$_{10}$

y_q = 37C7C90CD40B0F5621DC3AC1B751CFA0E2634FA0503B3D52639F5D7FB72AFD6\\
1EA199441D943FFE7F0C70A2759A3CDB84C114E1F9339FDF27F35ECA93677BEEC$_{16}$

А.2.2 Процесс формирования цифровой подписи (алгоритм I)

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

e = 2897963881682868575562827278553865049173745197871825199562947\\
41904138895097053666110955349995424873308871974884453896464128165 44\\
6351329697382770627204596 4$_{10}$

e = 3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C591\\
7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D2972075B8C$_{16}$

k = 1755163560258504995406282799211252803334510317477377916502\\
08144243182057075034446102986750962508909227235866126872473516807 8105417\\
4752971030987995863294 5$_{10}$

k = 359E7F4B1410FEACC570456C6801496946312120B39D019D455986E364F3\\
65886748ED7A44B3E794434006011842286212273A6D14CF70EA3AF71BB1AE679F1$_{16}$

При этом кратная точка $C = kP$ имеет координаты:

x_c = 248920447703134926507286464303214775366745131928213144402749 86373\\
57611092810221795101871412928823716805959828708330284243653453085 3\\
2200444244253415176146 2$_{10}$

x_c = 2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$

y_c = 770173889928991836047844798780960441682062631876096137673946801502\\
44422293532765176528442837832456936422662546513702148162933079517\\
08430050152108641508310$_{10}$

y_c = EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BDE80A91831DA27\\
C8100DAA876F9ADC0D28A82DD3826D4DC7F92E471DA23E55E0EBB3927C85BD6$_{16}$

Параметр $r = x_c(\mathrm{mod}\, q)$ принимает значение:

r = 24892044770313492650728646430321477536674513192821314440274986373\\
57611092810221795101871412928823716805959828708330284243653453085 3\\
22004442442534151761462$_{10}$

r = 2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$

Параметр $s = (rd + ke)\ (\mathrm{mod}\, q)$ принимает значение:

s = 864523221707669519038849297382936917075023735848431579919598 7\\
99313385180564748877195639672460179421760770893278030956807690115\\
82270990385368283183515937 0$_{10}$

s = 1081B394696FFE8E6585E7A9362D26B6325F56778AADBC081C0BFBE933D52FF58\\
23CE288E8C4F362526080DF7F70CE406A6EEB1F56919CB92A9853BDE73E5B4A$_{16}$

А.2.3 Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1 – 3 по алгоритму II (6.2) были получено следующее числовое значение:

e = 289796388168286857556282727855386504917374519787182519956294 7\\
41904138895097053666110955349995424873308871974884453896464128165 44\\
63513296973827706272045964$_{10}$

e = 3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C591\\
7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D2972075B8C$_{16}$

При этом параметр $v = e^{-1}(\mathrm{mod}\, q)$ принимает значение:

v = 255694215394605222266074084316408615387769223440078319114692849\\
35619434573234470892400192520569828068815353400414582124399060613 6\\
70722381859348159602526 71$_{10}$

v = 30D212A9E25D1A80A0F238532CADF3E64D7EF4E782B6AD140AAF8BBD9BB4729\\
84595EEC87B2F3448A1999D5F0A6DE0E14A55AD875721EC8CFD504000B3A840FF$_{16}$

Параметры $z_1 \equiv sv\ (\mathrm{mod}\, q)$ и $z_2 \equiv -rv\ (\mathrm{mod}\, q)$ принимают значения:

z_1 = 32064708273367686296869071018734752503433064480890303112144 84\\
38587274320504518034520882655290100349673294104978035779354194205 5\\

$$60008495619817370719790257 5_{10}$$

z_1 = 3D38E7262D69BB2AD24DD81EEA2F92E6348D619FA45007B175837CF13B026079\\
051A48A1A379188F37BA46CE12F7207F2A8345459FF960E1EBD5B4F2A34A6EEF$_{16}$

z_2 = 136677091183400310814297784802184759732045534753564127348 27\\
320820470283421680060312618142732308792036907264486312226797437575\\
616372669580568058596030082 03$_{10}$

z_2 = 1A18A31602E6EAC0A9888C01941082AEFE296F840453D2603414C2A16EB6FC529\\
D8D8372E50DC49D6C612CE1FF65BD58E1D2029F22690438CC36A76DDA444ACB$_{16}$

Точка $C = z_1P + z_2Q$ имеет координаты:

x_c = 248920447703134926507286464303214775366745131928213144402749 8637\\
357611092810221795101871412928823716805959828708330284243653453085 3\\
220044424425341517614 62$_{10}$

x_c = 2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$

y_c = 770173889928991836047844798780960441682062631876096137673946 8015\\
024422293532765176528442837832456936422662546513702148162933079517 0\\
8430050152108641508310$_{10}$

y_c = EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BDE80A91831DA27\\
C8100DAA876F9ADC0D28A82DD3826D4DC7F92E471DA23E55E0EBB3927C85BD6$_{16}$

Тогда параметр $R = x_c (\mathrm{mod}\, q)$ принимает значение:

R = 248920447703134926507286464303214775366745131928213144402749 86\\
373576110928102217951018714129288237168059598287083302842436534530 85\\
322004442442534151761462$_{10}$

R = 2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$

Поскольку выполнено равенство $R = r$, то цифровая подпись принимается.

Библиография [1]

[1] ИСО 2382-2:1976 Системы обработки информации.. Словарь. Часть 2. Арифметические и логические операции

[2] ИСО/МЭК 9796-2:2010 Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации

[3] ИСО/МЭК 9796-3:2006 Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 3. Механизмы на основе дискретного логарифма

[4] ИСО/МЭК 14888-1:2008 Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения

[5] ИСО/МЭК 14888-2:2008 Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 2. Механизмы, основанные на разложении на множители

[6] ИСО/МЭК 14888-3:2006 Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма

[7] ИСО/МЭК 14888-3:2006/Amd 1:2010 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

[8] ИСО/МЭК 10118-1:2000 Информационные технологии. Методы защиты информации. Хэш-функции. Часть 1. Общие положения

[9] ИСО/МЭК 10118-2:2010 Информационные технологии. Методы защиты информации. Хэш-функции. Часть 2. Хэш-функции с использованием алгоритма шифрования n-битными блоками

[10] ИСО/МЭК 10118-3:2004 Информационные технологии. Методы защиты информации. Хэш-функции. Часть 3. Выделенные хэш-функции

[11] ИСО/МЭК 10118-4:1998 Информационные технологии. Методы защиты информации. Хэш-функции. Часть 4. Хэш-функции с применением арифметики в остаточных классах

[1] Оригиналы международных стандартов ИСО/МЭК – в ФГУП «Стандартинформ» Федерального агентства по техническому регулированию и метрологии

УДК 681.3.06:006.354 **ОКС 35.040** **П 85** **ОКСТУ 5001**

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