O‘z DSt 1826 : 2014

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи на базе эллиптических кривых

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

O‘z DSt 3826:2014

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований «UNICON.UZ» (ГУП «UNICON.UZ»)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи, информатизации и телекоммуникационных технологий № 7

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 30.05.2014 № 05-546

4 ВВЕДЕН ВПЕРВЫЕ

5 В настоящем стандарте реализованы нормы законов Республики Узбекистан «Об электронной цифровой подписи» и «Об электронном документообороте»

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

O'ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Содержание

1 Область применения 1

2 Нормативные ссылки 1

3 Термины, определения и обозначения 2

3.1 Термины и определения 2

3.2 Обозначения 3

4 Общие положения 3

5 Математические соглашения 4

5.1 Математические определения 4

5.2 Параметры алгоритма электронной цифровой подписи 7

6 Алгоритм. Основные процессы 8

6.1 Вводные замечания 8

6.2 Формирование электронной цифровой подписи 8

6.3 Подтверждение подлинности электронной цифровой подписи 9

Приложение А (справочное) Контрольный пример. Процессы формирования и подтверждения подлинности электронной цифровой подписи по алгоритму 10

O‘ZBEKISTON DAVLAT STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
АХБОРОТНИНГ КРИПТОГРАФИК МУҲОФАЗАСИ
Эллиптик эгри чизиқларга асосланган электрон рақамли имзони шакллантириш ва текшириш жараёнлари

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Процессы формирования и проверки электронной цифровой подписи на базе эллиптических кривых

Information technology
Cryptographic data security
The processes of generation and verification of digital (electronic) signature based on elliptic curves

Дата введения 03.06.2014

1 Область применения

Настоящий стандарт устанавливает процессы формирования электронной цифровой подписи и подтверждения ее подлинности на базе эллиптических кривых под заданным сообщением (электронным документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования.

Стандарт предназначен для использования в системах обработки информации различного назначения при формировании и подтверждении подлинности электронной цифровой подписи.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt 1092:2009 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

O‘z DSt 1106:2009 Информационная технология. Криптографическая защита информации. Функция хэширования

O‘z DSt 1109:2013 Информационная технология. Криптографическая защита информации. Термины и определения

Издание официальное

O'ZSTANDART AGENTLIGI
4391 son bilan
«30» 05 2014 yilda
Davlat ro'yxatiga olindi

O‘z DSt 1204:2009 Информационная технология. Криптографическая защита информации. Требования безопасности к криптографическим модулям

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов на территории Узбекистана по соответствующему указателю стандартов, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и обозначения

3.1 Термины и определения

В настоящем стандарте применены термины по O‘z DSt 1109, а также следующие термины с соответствующими определениями:

3.1.1 **аппаратный модуль** (hardware module): Модуль, составленный, прежде всего, из аппаратных средств, которые могут также содержать некоторое программное обеспечение. Аппаратный модуль включает средства генерации личного ключа владельца и снабжен механизмами защиты от извлечения информации о личном ключе владельца.

3.1.2 **криптографический модуль** (cryptographic module): Набор аппаратных, программных или аппаратно-программных компонентов, заключенных в пределах явно определенного непрерывного периметра, реализующих утвержденные функции безопасности, включая криптографические алгоритмы, генерацию и распределение криптографических ключей, аутентификацию.

3.1.3 **особый аппаратный модуль** (specific hardware module): Модуль, состоящий, в основном, из аппаратной части, которая содержит секретный блок с встроенным особым личным ключом уполномоченного субъекта.

3.1.4 **особый личный ключ** (specific private key): Криптографический ключ, однозначно связанный с уполномоченным субъектом и не являющийся открытым, используемый в асимметричных и симметричных криптографических алгоритмах (например, тройка параметров (R, g, κ_h), где: R – параметр степени, g – основание, κ_h – ключ хэширования).

3.1.5 **программный модуль** (software module): Модуль, который состоит исключительно из программного обеспечения.

O'ZBEKISTON ARENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

3.2 Обозначения

В настоящем стандарте использованы следующие обозначения:

M – сообщение пользователя, представленное двоичным кодом, произвольной конечной длины

p – простое число (характеристика эллиптической кривой)

R – натуральное число - параметр

F_p –ко нечное простое поле, представляемое как множество из p целых чисел $\{0,1,..., p-1\}$

$b \pmod p$ – минимальное неотрицательное число, сравнимое с b по модулю p

a, b – коэффициенты эллиптической кривой

B – коэффициент эллиптической кривой с параметром

w – порядок группы точек эллиптической кривой с параметром

q – порядок подгруппы группы точек эллиптической кривой с параметром

0_E – нулевая точка эллиптической кривой с параметром

G – точка эллиптической кривой с параметром порядка q

d – целое число, закрытый ключ электронной цифровой подписи (ЭЦП)

Y – точка эллиптической кривой с параметром, открытый ключ ЭЦП

S – начальное значение, которое включает в состав системных параметров тогда, когда эллиптическая кривая с параметром генерируется по стратегии «случайного выбора»

H – хэш-функция

h – значение хэш–функции, где $h = H(.)$

l – целое число, кофактор

D – домен (системные параметры), который генерируется и верифицируется пользователем (p, эллиптическая кривая с параметром, $a, b, G, q, l, H(.), S$).

(r, s) – пара целых чисел – ЭЦП под сообщением M

$\circledR$ – символ операции умножения чисел с параметром R по модулю

$^{-1}$ – символ операции обращения с параметром по модулю

$^{-1}$ – символ операции обращения по модулю

$+$ – символ операции сложения в группе точек эллиптической кривой с параметром

$[k]\cdot$ – символ k-кратного выполнения операции сложения в группе точек эллиптической кривой с параметром

4 Общие положения

4.1 Общепризнанная схема (модель) ЭЦП охватывает три процесса:

- генерация ключей ЭЦП;
- формирование ЭЦП;

O‘ZBEKISTON STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

- проверка (подтверждение подлинности) ЭЦП.

4.2 При получении сообщения получатель может осуществить проверку целостности передачи и подлинность отправителя средствами в рамках алгоритма электронной цифровой подписи (АЭЦП).

4.3 ЭЦП является электронным аналогом письменной подписи и поэтому ЭЦП может использоваться получателем или третьей стороной для удостоверения, что сообщение было действительно подписано отправителем. ЭЦП может также формироваться для сохранения данных и программ, чтобы в любое время можно было проверить целостность данных и программ.

4.4 Настоящий стандарт описывает алгоритм для формирования и подтверждения подлинности ЭЦП, который реализуется на особом аппаратном криптографическом модуле.

4.5 Установленный в настоящем стандарте алгоритм должен быть реализован с использованием операций группы точек неявной эллиптической кривой, определенной над конечным простым полем, а также с применением хэш-функции по O‘z DSt 1106.

4.6 Криптографическая стойкость алгоритма ЭЦП основывается на сложности решения проблемы параметра неявной эллиптической кривой применительно к особым криптографическим модулям, а также на стойкости используемой хэш-функции по O‘z DSt 1106.

4.7 При изложении алгоритма не определены процессы генерации параметров АЭЦП. Конкретный алгоритм (способ) реализации данного процесса определяется субъектами схемы ЭЦП, исходя из требований к аппаратным и аппаратно-программным средствам по O‘z DSt 1204.

5 Математические соглашения

5.1 Математические определения

5.1.1 Для определения алгоритмов ЭЦП необходимо описать базовые математические объекты, используемые в процессе формирования и подтверждения подлинности ЭЦП. В данном разделе установлены основные математические определения и требования, накладываемые на объекты алгоритмов ЭЦП.

5.1.2 Пусть задано простое число $p > 3$. Тогда эллиптической кривой E, определенной над конечным простым полем F_p, называется множество пар чисел (x_0, y_0), $x_0, y_0 \in F_p$, удовлетворяющих тождеству:

$$y_0^2 \equiv x_0^3 + ax_0 + b \pmod{p}, \qquad (1)$$

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

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

На основе введения параметра R, замены переменных и коэффициентов (1) приводится к следующей модулярной форме:

$$y^{\backslash 2} \equiv x^{\backslash 3} + ax + B \ (mod\ p), \tag{2}$$

где: $B \equiv (a+b)\ R^{-1} (mod\ p)$;
$y^{\backslash 2} \equiv (y_0^2 - 1)\ R^{-1} (mod\ p)$;
$y \equiv (y_0 - 1)\ R^{-1} (mod\ p)$;
$y \equiv (x^{\backslash 3} + ax + B)^{\backslash 0.5} (mod\ p)$;
$y^{-} \equiv -(y + 2\ R^{-1})\ (mod\ p)$;
$x^{\backslash 3} \equiv (x_0^3 - 1)\ R^{-1} (mod\ p)$;
$x \equiv (x_0 - 1)\ R^{-1}\ (mod\ p)$;
y_0, x_0, y, y^{-}, x – переменные;
a, B – целочисленные коэффициенты;
R – параметр, $0 < R < p$, удовлетворяющий условию $(R; p) = 1$.

Введение дополнительного секрета R в уравнение (1) эллиптической кривой в явной форме преобразует его в уравнение эллиптической кривой в неявной форме (2).

5.1.3 Если $PE(F_p)$ = {множество всех точек эллиптической кривой с параметром} U 0_E, R параметр, где $0 < R \in F_p$, $+^{\backslash}$ – операции сложения с параметром над $PE(F_p)$, тогда пара $(PE(F_p);\ +^{\backslash})$ называется конечной коммутативной группой точек эллиптической кривой с параметром.

Инвариантом эллиптической кривой с параметром называется величина $J(PE)$, удовлетворяющая тождеству:

$$J(PE) = 1728 \frac{4a^3}{4a^3 + 27(BR - a)^2} (\mathrm{mod}\, p), \tag{3}$$

где: a, $B \in PE(F_p)$ и удовлетворяет условию $4a^3 + 27(BR - a)^2 \neq 0 \bmod p$.

Коэффициенты: a, B эллиптической кривой с параметром PE по инварианту $J(PE)$ определяется следующим образом

$$\begin{cases} a \equiv 3 \cdot k (\mathrm{mod}\, p), \\ B \equiv 5 \cdot k \cdot R^{-1} (\mathrm{mod}\, p), \end{cases} \tag{4}$$

где $k \equiv \dfrac{J(PE)}{1728 - J(PE)} (\mathrm{mod}\, p)$, $J(PE) \neq 0$ или 1728.

Пары (x, y), удовлетворяющие тождеству (2), называются точками эллиптической кривой с параметром PE, x и y – соответственно являются x- и y- координатами точки.

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

O'zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

На множестве всех точек эллиптической кривой PE введем операцию сложения, которую будем обозначать знаком «+\». Для двух произвольных точек $T_1\ (x_1,\ y_1)$ и $T_2\ (x_2,\ y_2)$ эллиптической кривой PE рассмотрим несколько вариантов.

Пусть координаты точек T_1 и T_2 удовлетворяют условию $x_1 \neq x_2$. В этом случае их суммой будем называть точку $T_3\ (x_3,\ y_3)$, координаты которой определяются сравнениями:

$$\begin{cases} x_3 \equiv (L^2 - 3)R^{-1} - x_1 - x_2 (\mathrm{mod}\, p), \\ y_3 \equiv L(x_1 - x_3) + y_1^- (\mathrm{mod}\, p), \end{cases} \tag{5}$$

где: $L \equiv (y_2 - y_1)\ (x_2 - x_1)^{-1}\ (mod\, p)$.

Если выполнены равенства $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то определяются координаты точки T_3 следующим образом:

$$\begin{cases} x_3 \equiv (L^2 - 3)R^{-1} - 2x_1 (\mathrm{mod}\, p), \\ y_3 \equiv L(x_1 - x_3) + y_1^- (\mathrm{mod}\, p), \end{cases} \tag{6}$$

где: $L \equiv (3(R\, x_1^{\backslash 2} + 1) + a)(2(R\, y_1 + 1))^{-1}\ (mod\, p)$.

В случае, когда выполнено условие $x_1 = x_2$ и $y_1 = -y_2\ (\mathrm{mod}\, p)$, сумму точек T_1 и T_2 будем называть нулевой точкой 0_E, не определяя ее x- и y-координаты. В этом случае точка T_2 называется отрицанием точки T_1. Для нулевой точки 0_E выполнены равенства:

$$T +^{\backslash} 0_E = 0_E +^{\backslash} T = T, \tag{7}$$

где: T – произвольная точка эллиптической кривой с параметром PE.

Относительно введенной операции сложения множество всех точек эллиптической кривой с параметром PE, вместе с нулевой точкой, образуют конечную абелевую (коммутативную) группу порядка w, для которой выполнено неравенство:

$$p + 1 - 2\sqrt{p} \leq w \leq p + 1 + 2\sqrt{p}\ . \tag{8}$$

Точка T называется точкой кратности k, или просто кратной точкой эллиптической кривой с параметром PE, если для некоторой точки N выполнено равенство:

O'ZBEKISTON STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

$$T = \underbrace{N +^{\backslash} \ldots +^{\backslash} N}_{k} = [k] \cdot^{\backslash} N . \qquad (9)$$

5.1.4 Алгоритм ЭЦП основан на сложности проблемы параметра неявной эллиптической кривой применительно к особым криптографическим модулям. Если в группе $(PE(F_p);\ +^{\backslash})$ точек неявной эллиптической кривой (с закрытой тройкой параметров (R, a, B)) заданы порядок подгруппы группы точек q, базовая точка $G=(x_1, y_1)$ и открытый ключ $Y=(x_2,y_2)$ (или x координата x_2), удовлетворяющего равенству $Y=[d]\cdot^{\backslash}G$, тогда найти d и тройку параметров (R, a, B), где уравнение эллиптической кривой с параметром имеет вид $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \ (mod\ p)$.

5.2 Параметры алгоритма электронной цифровой подписи

5.2.1 Алгоритм ЭЦП использует следующие параметры:

a) p – простое число, удовлетворяющее условию $p>2^{255}$. Верхние границы данного числа должны определяться при конкретной реализации ЭЦП;

b) эллиптическая кривая PE задается своим инвариантом $J(PE)$ или коэффициентами $a,B \in PE(F_p)$, удовлетворяет условию:

$4a^3+27(B\cdot R-a)^2 (mod\ p) \neq 0$;

c) R – параметр эллиптической кривой PE с параметром, удовлетворяющий условию $2^{160} < R < 2^{255}$;

d) целое число $w=\#\,PE(F_p)$ - порядок группы точек эллиптической кривой с параметром PE;

e) простое число q - порядок циклической подгруппы группы точек эллиптической кривой с параметром PE, для которого выполнены следующие условия:

$$\begin{cases} w = lq, \quad l \in Z, \quad 1 \le l \le 4 \\ 2^{254} < q < 2^{256} \end{cases}, \qquad (10)$$

где: l – кофактор, $l=\#PE(F_p)/q$;

f) $G=(x_3, y_3)$ – базовая точка эллиптических кривых PE с параметром R, удовлетворяющая условию $[q]\cdot^{\backslash}G=0_E$, где 0_E - нулевая точка эллиптической кривой с параметром, $\cdot^{\backslash}$ – символ операции умножения с параметром R;

g) H – хэш-функция;

h) S – начальное значение, которое включается в состав системных параметров только тогда, когда эллиптические кривые с параметром генерируется по стратегии «случайного выбора».

На приведенные выше параметры ЭЦП накладываются следующие требования:

O‘ZBEKISTON AXBOROT
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

– должно быть выполнено условие $p^t \neq 1(\mathrm{mod} q)$, для всех $t = 1,2,...,C$, где C удовлетворяет неравенству $C \geq 31$;

– должно быть выполнено неравенство $w \neq p$;

– инвариант кривой должен удовлетворять условию $J(PE) \neq 0$ или 1728.

Примечание - Выбор параметров, перечисленных в а), е) может осуществляться в соответствии с прототипом O‘z DSt 1092 (2- алгоритм).

5.2.2 Каждый пользователь алгоритма ЭЦП должен обладать личными ключами:

а) d_i – закрытый ключ ЭЦП i-пользователя, здесь $2^{160} \leq d_i < q-2^{160}$;

b) $Y_i = (x, y)$ - открытый ключ ЭЦП i-пользователя.

6 Алгоритм. Основные процессы

6.1 Вводные замечания

В данном разделе определены процессы формирования и подтверждение подлинности ЭЦП под сообщением пользователя.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры АЭЦП, перечисленные в 5.2.1.

Кроме того, каждый i-пользователь должен иметь закрытый ключ ЭЦП d_i и открытый ключ ЭЦП Y_i, которые также должны соответствовать требованиям 5.2.2.

6.2 Формирование электронной цифровой подписи

Для создания ЭЦП под сообщением M необходимо выполнить следующие действия (шаги) по **алгоритму**:

Шаг 1: вычисляется хэш-значение $h=H(M||R||a||B)$ от конкатенации M, тройки параметров R, a и B;

Шаг 2: вычисляется $e \equiv h(\mathrm{mod}\ q)$. Если $e=0$, тогда принимается $e=1$;

Шаг 3: генерируется случайное число k_i, удовлетворяющее неравенству $2^{160} < k_i < q-2^{160}$;

Шаг 4: по случайному числу k_A вычисляется точка $[k_i]\cdot G = (x_1, y_1)$ на эллиптической кривой с параметром;

Шаг 5: вычисляется $r_i \equiv x_1 (\mathrm{mod}\ q)$, если $r=0$, тогда осуществляется возврат к шагу 3;

Шаг 6: вычисляется $s_i \equiv (r_i d_i + k_i e)(\mathrm{mod}\ q)$, если $s=0$, тогда осуществляется возврат к шагу 3;

Шаг 7: на выходе программного криптографического модуля формируется $ЭЦП\ (r_i, s_i)$.

Исходными данными этого процесса являются d_i – закрытый ключ и подписываемое сообщение, а выходным результатом –ЭЦП (r_i, s_i).

...VLASHTIRISH, DAVLAT
...LASHTIRISH VA
...OLOGIYALARINI
...TIRISH XIZMATI

6.3 Подтверждение подлинности электронной цифровой подписи

Для подтверждения подлинности ЭЦП под полученным сообщением M необходимо выполнить следующие действия (шаги) по **алгоритму** :

Шаг 1: проверяется выполнение условий $0< r_i, s_i<q$, если условие удовлетворяется, тогда осуществляется переход к следующему шагу, в противном случае на выходе программного криптографического модуля появляется сообщение «ЭЦП неподлинна»;

Шаг 2: вычисляется хэш-значение $h=H(M||R||a||B)$ от конкатенации M, тройки параметров R, a и B;

Шаг 3: вычисляется $e\equiv h(mod\ q)$. Если $e=0$, тогда принимается $e=1$;

Шаг 4: вычисляется $v \equiv e^{-1}(mod\ q)$;

Шаг 5: вычисляются $z_1 \equiv s_i\ v(mod\ q)$ и $z_2 \equiv -r_i\ v(mod\ q)$;

Шаг 6: если открытый ключ введен в виде x, то по x_i вычисляются $y_i^{\backslash 2}\equiv x_i^{\backslash 3}+ax_i+B(mod\ p)$ и $y_i\equiv(x_i^{\backslash 3}+ax_i+B)^{\backslash 0.5}(mod\ p)$, формируется точка $Y_i=(x_i, y_i)$ на эллиптической кривой с параметром;

Шаг 7: вычисляется точка $C=[z_1]\cdot^{\backslash}G+^{\backslash}[z_2]\cdot^{\backslash}Y_i$ на эллиптической кривой с параметром и принимается $X \equiv x_c\ (mod\ q)$, где x_c – x координата точки C;

Шаг 8: проверяется равенство $X=r_i$, если равенство удовлетворяется, тогда на выходе появляется сообщение «ЭЦП подлинна», в противном случае - «ЭЦП неподлинна».

В приложении А приведен контрольный пример для процессов формирования и проверки ЭЦП по алгоритму.

O'ZBEKISTON STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Приложение А
(справочное)

Контрольный пример. Процессы формирования и подтверждения подлинности электронной цифровой подписи по алгоритму

Приводимые ниже значения параметров p, a, b, w, q, G, а также значения закрытого ключа ЭЦП d_i и открытого ключа Y_i рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритма, описанного в разделе 6 данного стандарта.

Все числовые значения приведены в шестнадцатеричной системе счисления.

Параметры электронной цифровой подписи

Модуль эллиптической кривой

Параметру p присвоено следующее значение:

$p =$
F656DE439CED972226B7229D182FEDC9D1ABE82D8AEDF7CB89A841907994E517

Коэффициенты эллиптической кривой

Параметры a и b принимают следующие значения:

$a =$ B97D1B7E9695FE6B889D7FECEF835896EB5426FFBB7916723D

$b =$
52205870015F14CA39210F8964A3EA95905A1C77150D964479474861826451A9

$B =$
55DBBFD580AB9229A3C615C1EA6EE8068E435C3AD62117AEA16B659C77A3BAB1

Параметр R эллиптической кривой

$R =$
8199FA45799C9F14840753E2F309D253644CDF30544E19B95F9C466E64B696CE

Порядок группы точек эллиптической кривой

Параметр w принимает следующее значение:

$w =$
F656DE439CED972226B7229D182FEDCAD7526FB15C17E97BEA43A66FEF1988DF

Порядок циклической подгруппы группы точек эллиптической кривой

Параметр q принимает следующее значение:

$q =$
F656DE439CED972226B7229D182FEDCAD7526FB15C17E97BEA43A66FEF1988DF

Базовая точка G эллиптической кривой с параметром

O'zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

$x =$
8557FAB9673CDE27B463FBC2959B9211AC0EC804E4E8A9805FD843E8D69B8970

$y =$
F4E31EDE15C9CBC588A3E6370B185A059B17F47398FC615B91D33330E11A5D2A

Личные ключи пользователей ЭЦП

Каждый из *i*-пользователей на своем особом аппаратном криптографическом модуле генерирует свой закрытый ключ d_i как случайное число и вычисляет свой открытый ключ Y_i на основе выражения:

$$Y_i = [d_i] \cdot G = (x_i, y_i).$$

В данном случае

$d_i =$
74795AEBCC2E70BEC4514F3D26A93C0A5184832A7BDC67F833D97BD481490A55

Открытый ключ ЭЦП

$x_i =$
E58BB9459D0B526A83137239C25ECE4D4D55A1C21CE7E1190E24D657FC09666E

$y_i =$
202428C8340A30477093F84F5C7BB909596920AD63538DCC2A24C9A047B0307E

Процесс формирования электронной цифровой подписи

$h =$
E37ED04A5D39CC09C0185B3D205F42E09E9E530DB88CBAFFE67232CDDB312E73

$e =$
E37ED04A5D39CC09C0185B3D205F42E09E9E530DB88CBAFFE67232CDDB312E73

$k =$
1AE5E8BD1E8F5C8E4B8B4986033769625EDF300F1723260688235B7882221E82

При этом $[k] \cdot G = (x_1, y_1)$ имеет координаты:

$x_1 =$
761A94111484AD9036C9835768D0248012B9AAE93B13FC682759D3E9D627CC61

$y_1 =$
284559E544FE2FA2FDA0A81FB8E100802C35E95A940DF02E5ACC243A126CB906

Параметр $r \equiv x_1 \ (mod\ q)$ принимает значение:

O‘ZBEKISTON AGENTLIGI STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

$r =$

ECC312FC7EF14896C91A6D0E9E50347046092AFA063CBACA3940CD6B9C85CB18

Параметр $s \equiv (rd_i + ke) \pmod q$ принимает значение:

$s =$

BA3386BE63F9B72A5C1406DB744D59420444B7677E6D9641474E5572F73E3633

Процесс подтверждения подлинности электронной цифровой подписи

На особом аппаратном криптографическом модуле проверяется выполнение условия $0<r,\ s<q$, есл и условие удовлетворяется, тогда осуществляется переход к следующему шагу, в противном случае на выходе особого аппаратного криптографического модуля появляется сообщение «ЭЦП неподлинна»

$h =$

E37ED04A5D39CC09C0185B3D205F42E09E9E530DB88CBAFFE67232CDDB312E73

$e =$

E37ED04A5D39CC09C0185B3D205F42E09E9E530DB88CBAFFE67232CDDB312E73

$v =$

87C5711BF5939F2F464A697490DD357A561B7FFCDDFF57E3B1EBEDF0419AAAC8

$z_1 =$

EA2DA0DA80CDCB723EDE3A4E38E65C6EE9AB06DAF30CDC6AD0EEFD0E8DE29E28

$z_2 =$

A589C9A9574B5D5D36303DA17BDD9EC06B75E6BE5285C556AB47A4D18416F1AD

По x_i вычисляются $y_i^{\backslash 2} \equiv x_i^{\backslash 3} + ax_i + B \pmod p$ и $y_i \equiv (x_i^{\backslash 3} + ax_i + B)^{\backslash 0.5} \pmod p$, формируется точка $Y_i = (x_i, y_i)$ на эллиптических кривых с параметром

$x_i =$

BDE838FAB56CA14313B9E079DEB3632022F0FDFD257C9B74334F3FB17923313A

$y_i =$

C735651B108272AC62C1110957B3B46510559CBE780696051 4A01E6BEE226BFF

Вычисляются точки $C = [z_1] \cdot {}^{\backslash}G + {}^{\backslash}[z_2] \cdot {}^{\backslash}Y_i$ на эллиптических кривых с параметром:

$x_c =$

761A94111484AD9036C9835768D0248012B9AAE93B13FC682759D3E9D627CC61

O‘zbekiston Respublikasi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

$y_c =$

284559E544FE2FA2FDA0A81FB8E100802C35E95A940DF02E5ACC243A126CB906

предполагается, что $X \equiv x_c \ (mod\ q)$ принимает значение:

$X =$

ECC312FC7EF14896C91A6D0E9E50347046092AFA063CBACA3940CD6B9C85CB18

$X=r$, равенство удовлетвряется, «ЭЦП подлинна».

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

УДК 621.391 ОКС 35.040 П 85

Ключевые слова: электронный документ, электронная цифровая подпись, подписанное сообщение, эллиптическая кривая, открытый ключ, закрытый ключ, обработка данных, криптографический алгоритм

O‘zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

O'z DSt 826 : 2014

Вр.и.о. директора
ГУП «UNICON.UZ» Х. Хасанов

Начальник
научно-исследовательского
отдела криптографии, к.т.н. О. Ахмедова

Ведущий научный сотрудник
научно-исследовательского
отдела криптографии, к.ф.- м.н. М. Назарова

Ведущий инженер
научно-исследовательского
отдела криптографии О. Нуриддинов

Нормоконтроль Л. Шаймарданова
21.05.2014

СОГЛАСОВАНО

Начальник отдела информационной
безопасности Государственного
комитета связи, информатизации
и телекоммуникационных
технологий Республики Узбекистан

А. Гафуров
письмо от 18.02.2014
№ 14-8/960

СОГЛАСОВАНО

Начальник Управления СНБ

Б. Пономарёв
письмо от 04.03.2014
№ 33/746

O'ZBEKISTON AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI