Электронная цифровая подпись (ЭЦП)

Угрозы в фокусе темы

Модель протокола формирования и проверки ЭЦП

Сравнение рукописных и цифровых подписей

- Основные операции над подписью. Формирование подписи(подписание) и проверка подписи (верификация)
- Способ формирования. В случае рукописной подписи считается, что каждый документ подписывается одинаковым образом (отношение "один ко многим" между подписью и документами). В случае цифровой подписи разным документам (сообщениям) соответствуют существенно различные значения подписи (отношения «многие ко многим")
- Способ проверки: В случае обычной подписи получатель сравнивает подпись на документе с эталоном. При цифровой подписи получателю предоставляется сообщение, алгоритм и ключ проверки, но копия эталона подписи нигде не хранится

Цифровая подпись против угроз

- Защита от модификации сообщения - целостность сообщения может контролироваться, поскольку криптопреобразованию подвергается все сообщение, поэтому нельзя получить ту же самую подпись, если сообщение изменено.
- Защита от имитации источника сообщения – установление подлинности цифровой подписи потенциально возможно, поскольку цифровая подпись создается с помощью персонального (закрытого ключа) отправителя
- Защита от отказа от авторства – потенциально возможна с привлечение доверенной стороны, заверяющей документы свой цифровой подписью

Виды подделок цифровой подписи

Экзистенциальная
(existential forgery)

- Противник, НЕ владеющий закрытым ключом, создает пару (сообщение, подпись), которая будет принята алгоритмом проверки цифровой подписи
- Противник никак не контролирует выбор того сообщения, для которого в итоге будет подделана подпись – очень вероятно, это сообщение будет бессмысленным

Селективная
(*selective forgery*)

- Противник, НЕ владеющий закрытым ключом, выбирает осмысленное сообщение (отсюда название угрозы)
- Далее, получив открытый ключ, пытается подделать цифровую подпись для этого выбранного сообщения.

Цифровая подпись RSA

RSA генерация ключей

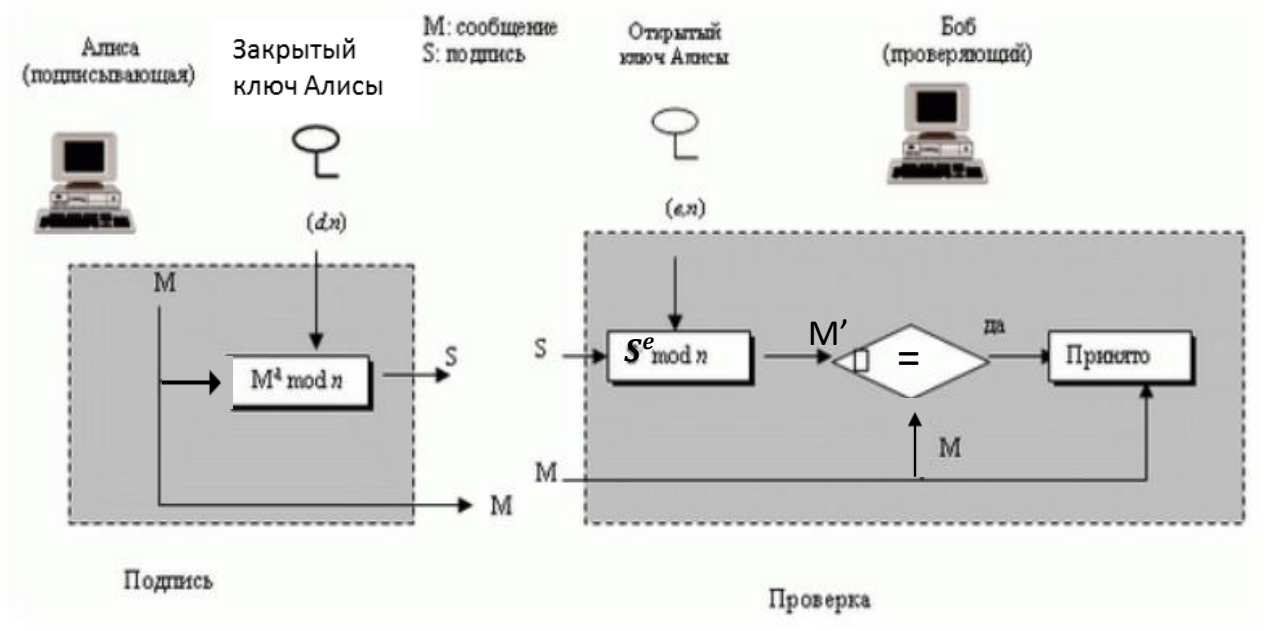
- Выбираются два больших простых числа *p* и *q*
- Вычисляется *n=p*q*
- Выбирается произвольное число *e (e<n)*, взаимно простое с *(p-1)*(q-1)*
- Вычисляется закрытый ключ (расширенный алгоритм Евклида) :

$$e \times \boldsymbol{d} \equiv 1\ mod\big((p-1)*(q-1)\big) \equiv 1\ mod\ (p-1)*(q-1)$$

Пара чисел *(e, n)* объявляются открытым ключом, *d* выбирается закрытым ключом

- *p* и *q* нужно уничтожить

RSA подписание и проверка



- Формирование подписи отправителем:
  - Ключ подписания (закрытый ключ) – пара чисел *(d, n)*
  - $S=(M^d) mod\ n$
- Проверка подписи получателем:
  - Ключ проверки (открытый ключ) – пара чисел *(e, n)*
  - $M' = (S^e) mod\ n$
  - Если $M' \equiv M\ mod\ n$ подпись верна

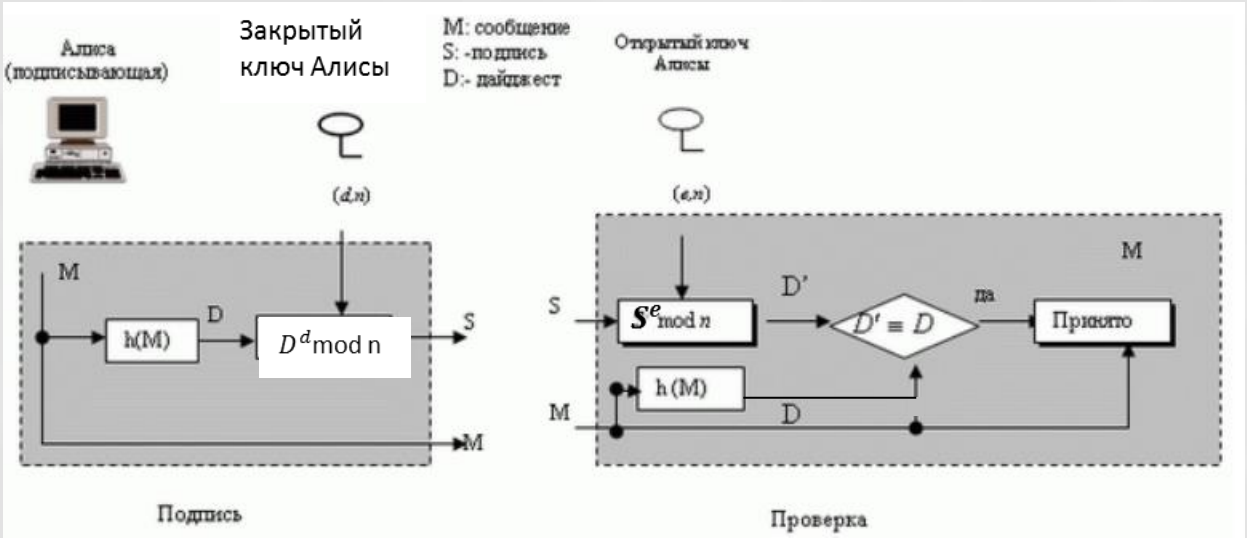
Примечание

- Подписи, созданные с применением алгоритма RSA, называются *детерминированными,* так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будет создаваться одна и та же подпись

Подделка цифровой подписи RSA

- Экзистенциальная подделка. Перехватываются две пары (M_1, S_1), (M_2, S_2).Подписи созданы с помощью одного ключа d. Создается новое сообщение $M = M_1 \times M_2$ и соответствующая подпись $S = S_1 \times S_2 = M_1^d \times M_2^d = (M_1 \times M_2)^d = M^d$
- Селективная подделка. Целенаправленно создается $M = M_1 \times M_2$ и с помощью обмана отправителя противник получает подписи S_1 и S_2, что позволяет ему сформировать $S = S_1 \times S_2$ (если использовался один и тот же ключ).

RSA подпись на дайджесте сообщения



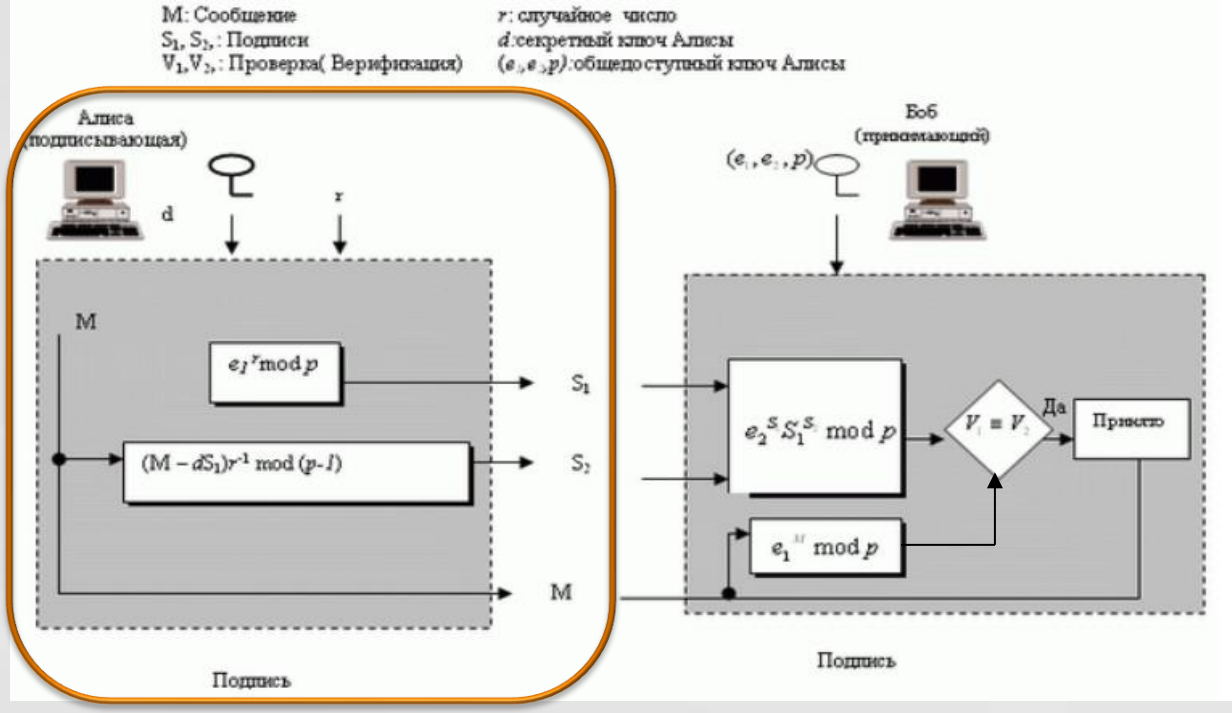
- Экзистенциальная подделка. Перехватываются две пары $(M_1, S_1), (M_2, S_2)$. Подписи созданы с помощью одного ключа. Создается подпись $S = S_1 \times S_2$. Атака будет успешной, если найдется сообщение M, такое, что $h(M) = h(M_1) \times h(M_2)$ (зависит от устойчивости хэш-функции к прообразу)
- Селективная подделка. Целенаправленно создается $M = M_1 \times M_2$ и с помощью обмана отправителя противник получает подписи S_1 и S_2, что позволяет ему сформировать $S = S_1 \times S_2$ (если использовался один и тот же ключ). Атака будет успешной, если найдется осмысленное сообщение M' близкое по смыслу к М, такое, что $h(M') = S^e mod\ n$ (зависит от устойчивости хэш-функции к прообразу)

Цифровая подпись Эль-Гамаля

Elgamal генерация ключей

- Генерируется случайное простое число p
- Выбирается целое число e_1 такое, что $1 < e_1 < p$, и e_1-первообразный корень p
- Выбирается случайное целое число d такое, что $1 < d < p$
- Вычисляется $e_2 = e_1{}^d mod\ p$
- Открытым ключом объявляется тройка (e_1, e_2, p)
- Закрытым ключом назначается число d

Elgamal подписание

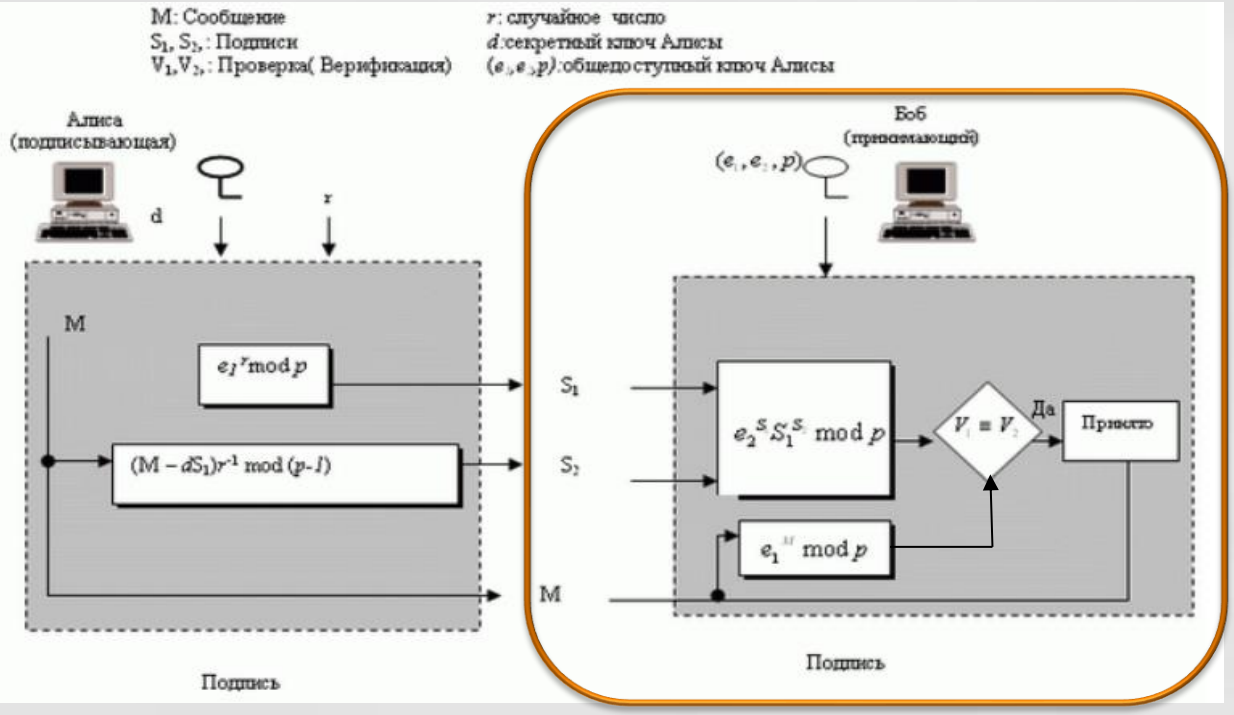


- Выбирается секретное случайное число r
- Вычисляется (f_1) первая часть подписи $S_1 = {e_1}^r mod\ p$
- Вычисляется (f_2) вторая часть подписи

$$S_2 = (M - d \times S_1) \times r^{-1} mod(p-1),$$

где r^{-1} - мультипликативная инверсия r по модулю $(p-1)$

Elgamal проверка



- Проверяем :
  - $0 < S_2 < p$
  - $0 < S_1 < p - 1$
- Вычисляем (f_1):
  - $V_1 = {e_1}^M mod\ p$
- Вычисляем (f_3):
  - $V_2 = {e_2}^{S_1} \times {S_1}^{S_2}\ mod\ p$
- Если $V_1 \equiv V_2 mod\ p$ подпись действительна

Обоснование критерия проверки

- Ранее принято:

$$e_2 = {e_1}^d mod\ p, S_1 = {e_1}^r mod\ p, V_1 = {e_1}^M mod\ p,\ V_2 = {e_2}^{S_1} \times {S_1}^{S_2}\ mod\ p$$

- Заменим критерий $V_1 \equiv V_2 mod\ p$ на эквивалентный (подстановками)
- $${e_1}^M \equiv {e_2}^{S_1} \times {S_1}^{S_2}\ mod\ p \equiv ({e_1}^d)^{S_1} \times ({e_1}^r)^{S_2} mod\ p \equiv {e_1}^{dS_1 + rS_2} mod\ p$$

- Поскольку e_1 - первообразный корень, то можно доказать, что полученное сравнение справедливо тогда и только тогда, когда

$$\mathrm{M} \equiv (dS_1 + rS_2) mod\ (p-1)\ ,\ \text{поэтому}$$

$$S_2 \equiv \left((M - d \times S_1) \times r^{-1}\right) mod (p-1)$$

- Получен тот же результат, с которого начато подписание

Примечание

- Подписи, созданные с использованием алгоритма Elgamal называются *рандомизированными*, так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будут создаваться разные части подписи (S_1, S_2), поскольку будет использоваться новое значение r

Подделка цифровой подписи Elgamal

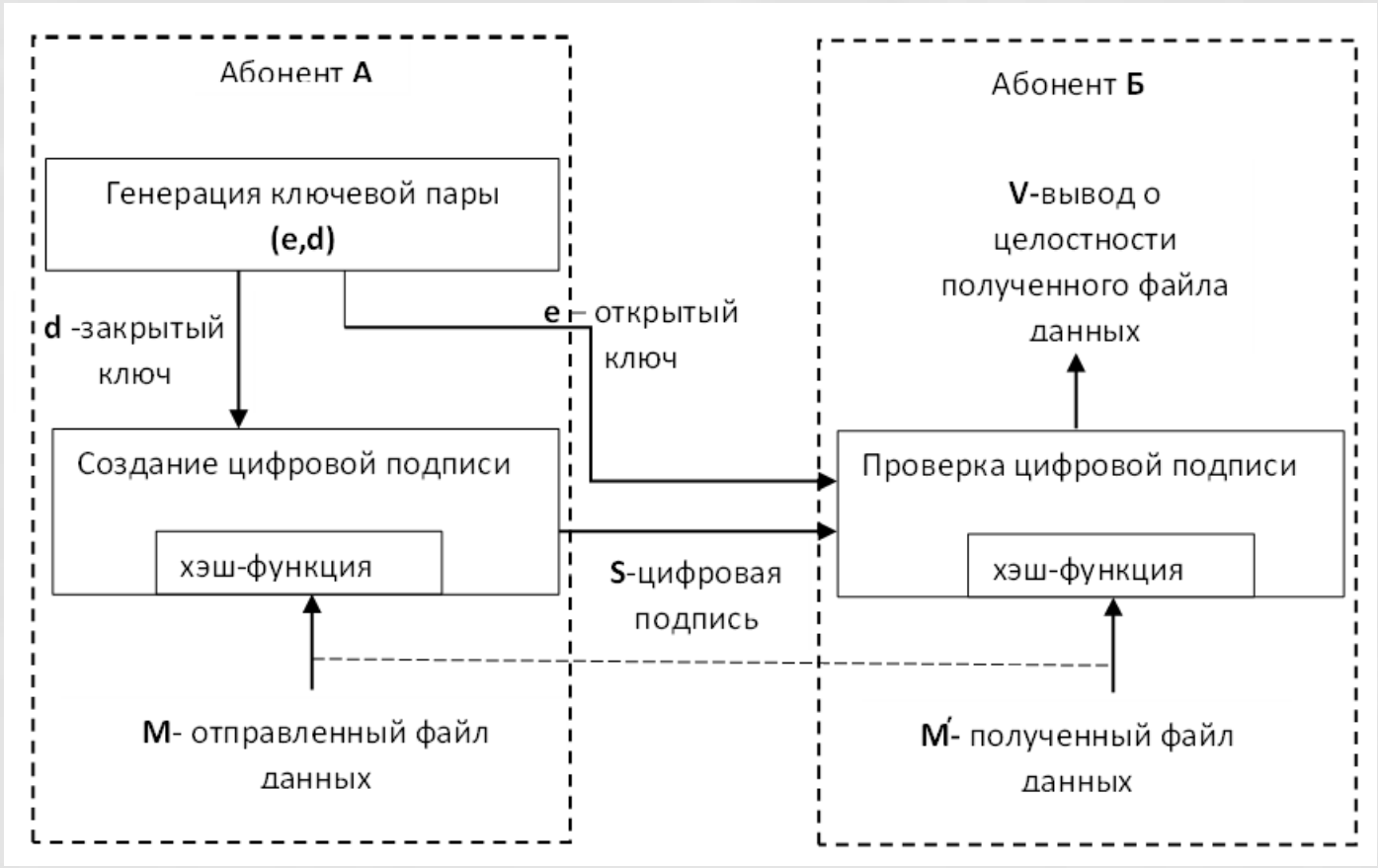
- Экзистенциальная подделка. Перехвачена цифровая подпись S_1 и S_2 и подбирается M', a, b удовлетворяющие сравнению

$$M' \equiv (\mathrm{a} \times S_1 + b \times S_2) mod\ (p-1)$$

- Селективная подделка. Имеется заданное сообщение M и требуется подобрать две части подписи S_1 и S_2 . Выбираем S_1 и пытаемся вычислить S_2 из ${e_2}^{S_1} \times {S_1}^{S_2} \equiv {e_1}^{M} mod\ p$. Это вычислительно трудная задача дискретного логарифмирования

$$S_2 \equiv log_{S_1}\ {e_2}^{-S_1} \times {e_1}^{M} mod\ p$$

Детализация модели протокола ЭЦП



Цифровая подпись ECDSA
(Elliptic Curve Digital Signature Algorithm)

Стандарт цифровой подписи (ECDSS) принят ANSI в 1999 и NIST в 2000 г.

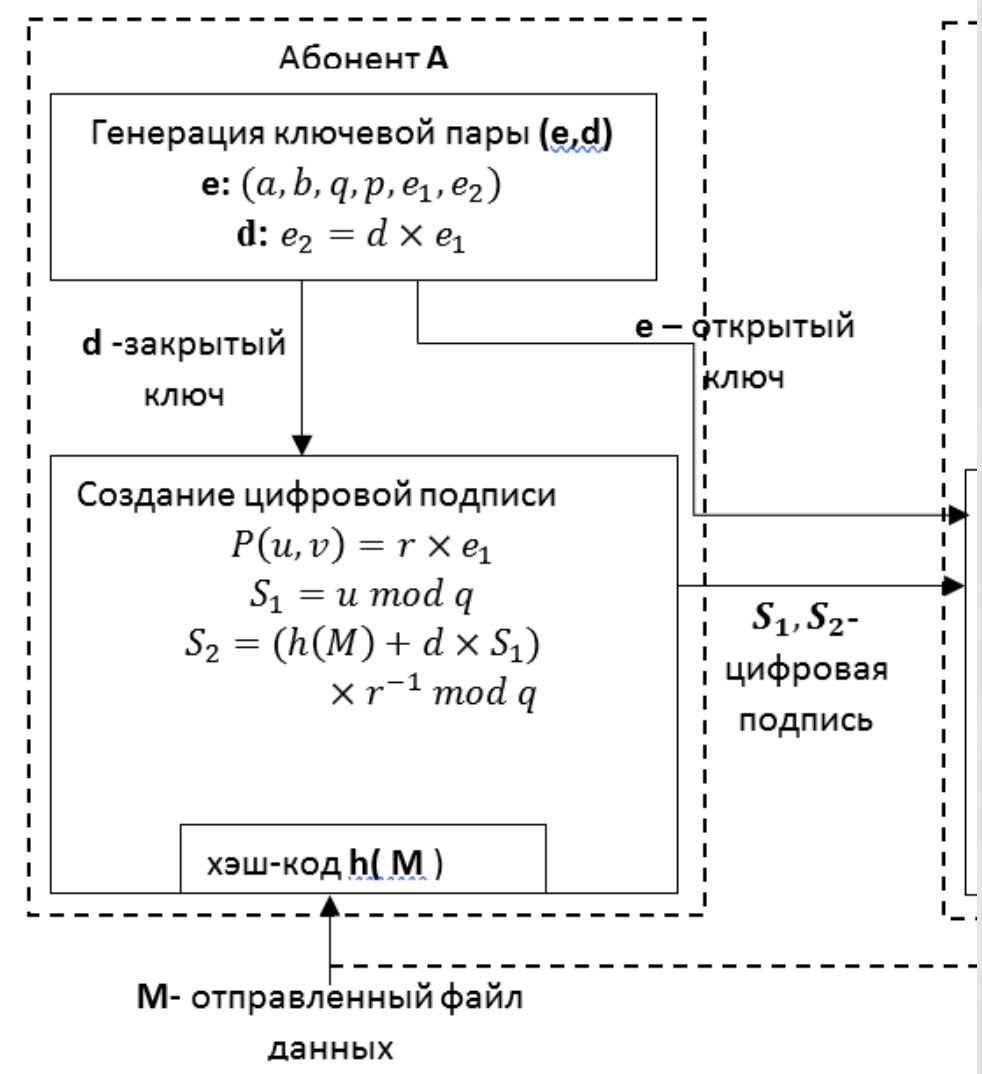
Основа стандарта

- Безопасность подписей RSA и Elgamal обеспечивается ценой использования больших ключей
- Альтернативой является метод на основе эллиптических кривых (*Elliptic Curve Cryptography — ECC*), который дает тот же самый уровень безопасности, но с меньшими размерами ключей

Генерация ключей ECDSA

- Выбирается эллиптическая кривая $E_p(a,b)$, p — простое
- Выбирается базовая точка на кривой $\boldsymbol{e_1}$= (x_1,y_1)
- Для дальнейших вычислений выбирается другое простое число q - порядок циклической подгруппы группы точек эллиптической кривой : $q \times (x_1,y_1)$=O
- Выбирается целое число d , $1 < d < q - 1$ и назначается закрытым ключом
- Вычисляется другая точку на кривой $\boldsymbol{e_2} = d \times \boldsymbol{e_1}$
- Объявляется открытый ключ $(a, b, p, q, \boldsymbol{e_1}, \boldsymbol{e_2})$

ECDSA подписание



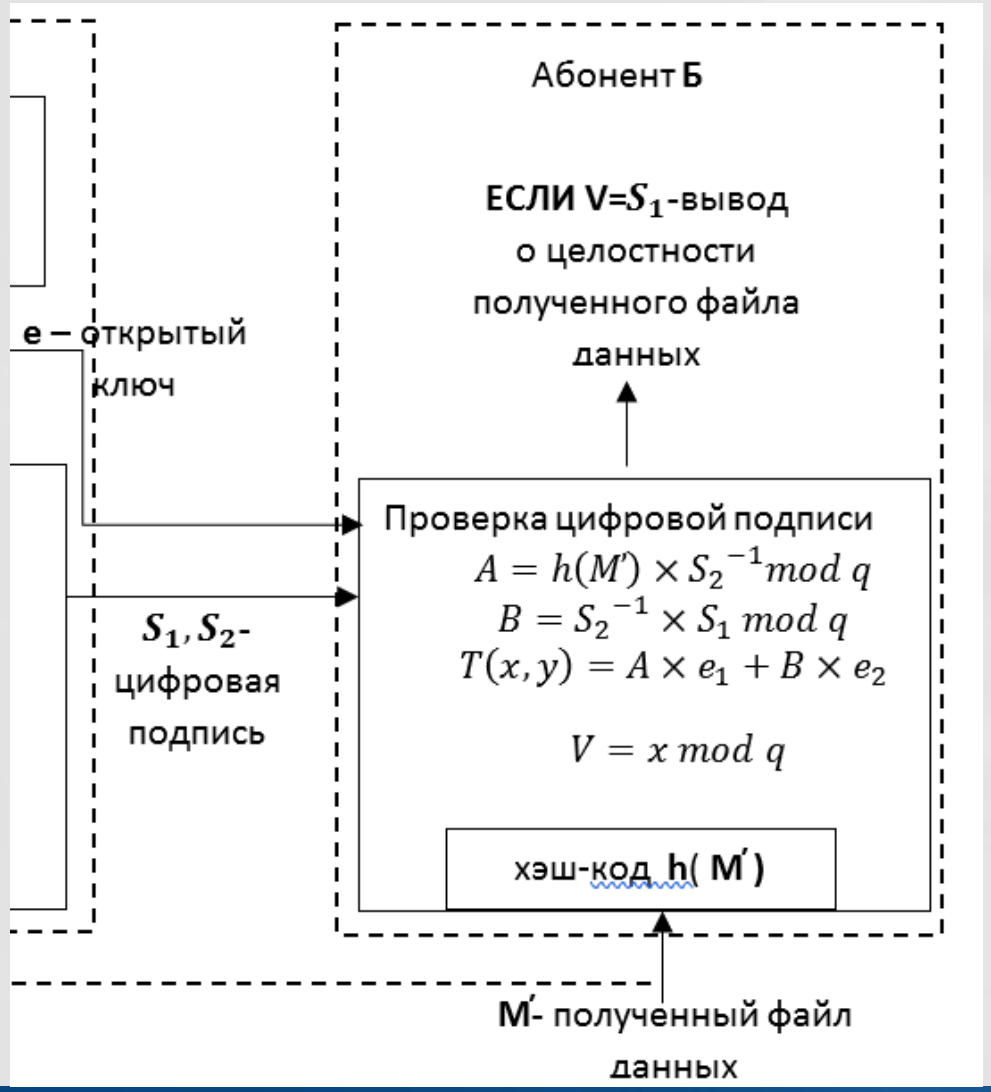
- Выбирается секретное случайное число, $r,\ 1 < r < q - 1$
- Выбирается третья точка на кривой, $\boldsymbol{P}(u, v) = r \times \boldsymbol{e_1}$
- Используем абсциссу u , чтобы вычислить первую часть подписи

$$S_1 = u \bmod q$$

- Используем дайджест сообщения $h(M)$, закрытый ключ d, секретное случайное число r и S_1, чтобы вычислить вторую часть подписи

$$S_2 = (h(M) + d \times S_1) \times r^{-1} \bmod q$$

ECDSA проверка



- Используем M, S_1, S_2 для получения промежуточных результатов A и B:

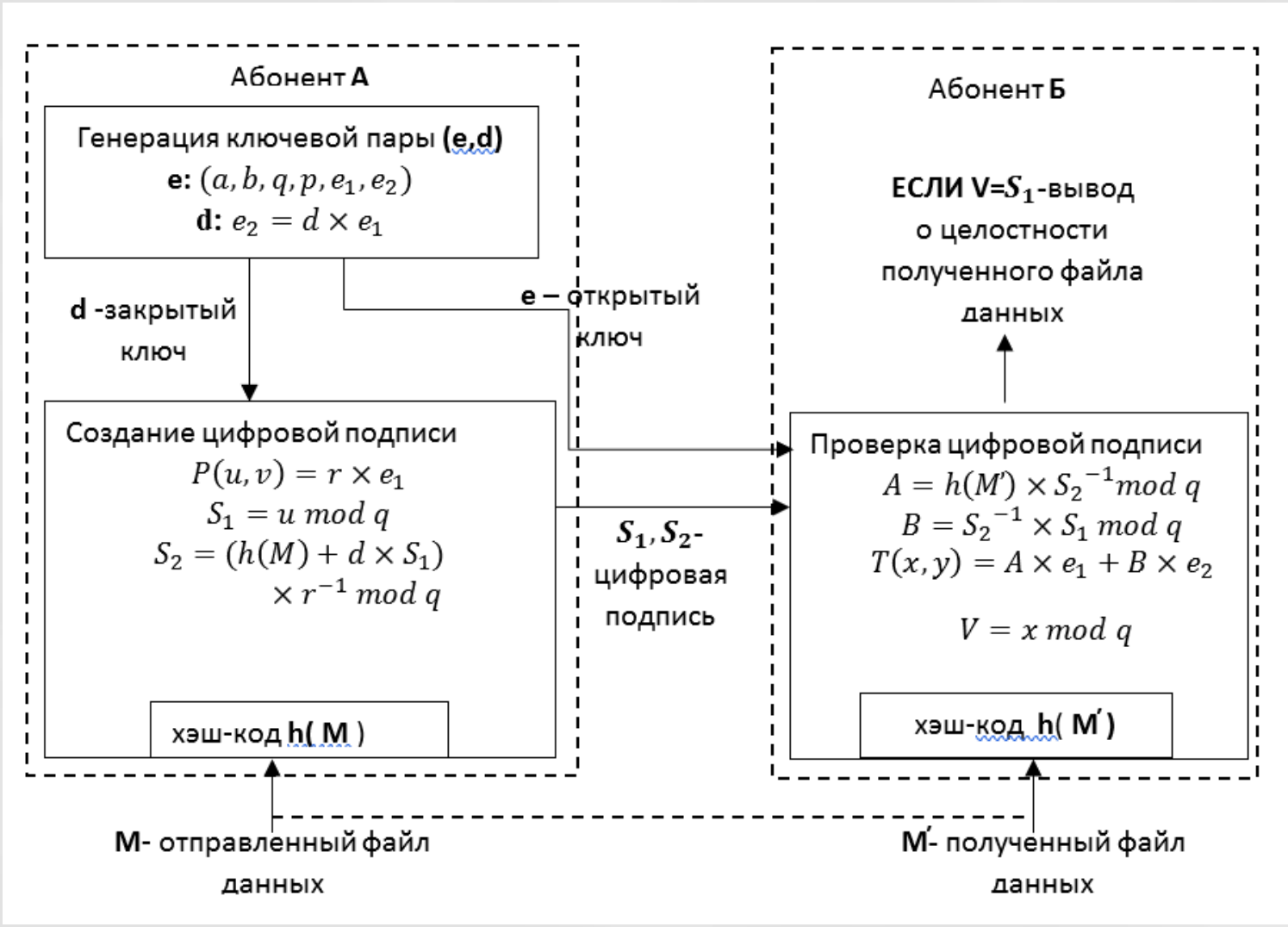
$$A = h(M) \times S_2{}^{-1} mod\ q$$
$$B = S_2{}^{-1} \times S_1 mod\ q$$

- Затем восстанавливаем третью точку

$$\boldsymbol{T(x,y) = A \times e_1 + B \times e_2}$$

- Верификатор $V = x\ mod\ q$ сравниваем с S_1

Схема протокола ECDSA



Цифровая подпись ГОСТ Р 34.10–2012

Российский стандарт, введен в действие 01.01.2013

Общие сведения о стандарте

- Определяет алгоритм, аналогичный алгоритму ECDSA
- Разработан Центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»)
- Использует хэш-функцию стандарта ГОСТ Р 34.11–2012, которая создает хэш-код длиной 256 и 512 бит
- Процесс генерации ключей (для подписи и проверки подписи) не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами, которые устанавливают соответствующие параметры по взаимному согласованию
- 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

Генерация ключей ГОСТ

- Выбирается эллиптическая кривая $E_p(a,b)$: $y^2 \equiv x^3 + ax + b \; mod \; p, p > 3 -$ простое
- Выбирается простое число q (порядок циклической подгруппы точек):
  - $2^{254} < q < 2^{256}$, если длина хэш-кода 256
  - $2^{508} < q < 2^{512}$, если длина хэш-кода 512
- Выбирается базовая точка на кривой $\boldsymbol{e_1} = (x_1, y_1)$, q$\times \boldsymbol{e_1}$=0
- Выбирается целое число $d, (0 < d < q)$ и назначается закрытым ключом
- Вычисляется другая точку на кривой $\boldsymbol{e_2} = d \times \boldsymbol{e_1}$
- Объявляется открытый ключ $(a, b, p, q, \boldsymbol{e_1}, \boldsymbol{e_2})$

ГОСТ подписание

- Выбирается секретное случайное число, $r,\ 1 < r < q$
- Выбирается третья точка на кривой, $\boldsymbol{P}(u, v) = r \times \boldsymbol{e_1}$
- Используем абсциссу u , чтобы вычислить первую часть подписи

  $$S_1 = u\ mod\ q$$

- Используем дайджест сообщения $h(M),$ закрытый ключ $d,$ секретное случайное число r и S_1, чтобы вычислить вторую часть подписи

  $$S_2 = (r \times h(M) + d \times S_1)\ mod\ q$$

- S_1 и S_2 - две составляющие цифровой подписи

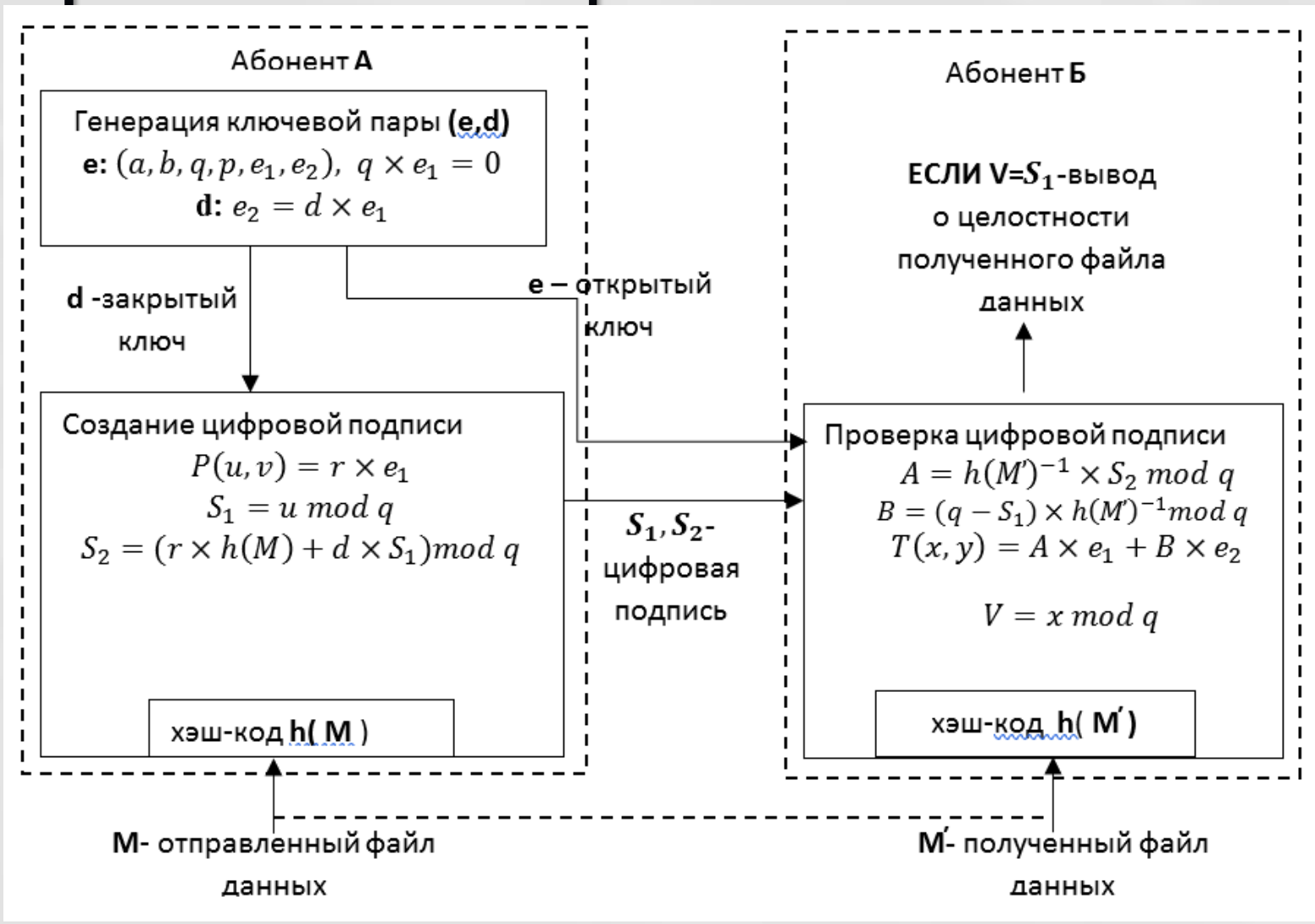
ГОСТ проверка

- Используем M, S_1, S_2 для получения промежуточных результатов A и B:
  - $A = h(M)^{-1} \times S_2 \, mod \, q$
  - $B = (q - S_1) \times h(M)^{-1} mod \, q$
- Затем восстанавливаем третью точку

$$\boldsymbol{T}(x, y) = A \times \boldsymbol{e_1} + B \times \boldsymbol{e_2}$$

- Верификатор $V = x \, mod \, q$ сравниваем с S_1

Схема протокола ЭЦП ГОСТ



ГОСТ примечание

- Криптостойкость цифровой подписи опирается на две компоненты — на стойкость хэш-функции и на стойкость самого алгоритма шифрования
- Вероятность взлома хэш-функции составляет 1.73×10^{-77} при подборе коллизии на фиксированное сообщение и 2.94×10^{-39} при подборе любой коллизии.
- Стойкость алгоритма шифрования основывается на проблеме дискретного логарифмирования в группе точек эллиптической кривой. На данный момент нет метода решения данной проблемы лучше, чем $O\left(\sqrt{q}\right)$ битовых операций. Таким образом при использовании 256-разрядное q, обеспечивается криптостойкость 10^{38} операций

Рекомендации по стандартизации 2019

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.024— 2019

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Параметры эллиптических кривых для криптографических алгоритмов и протоколов

Издание официальное

Москва
Стандартинформ
2019

Область применения рекомендаций

- Параметры эллиптических кривых для использования совместно с алгоритмами формирования и проверки электронной цифровой подписи в соответствии с ГОСТ Р 34.10
- Параметры эллиптических кривых для использования совместно с алгоритмами согласования ключей при защите информации, не содержащей сведений, составляющих государственную тайну.

Параметры эллиптической кривой

$y^2 = x^3 + ax + b \pmod p$

- p — модуль эллиптической кривой;
- a, b — коэффициенты уравнения эллиптической кривой в канонической форме;
- m — порядок группы точек эллиптической кривой;
- q— порядок циклической подгруппы группы точек эллиптической кривой;
- (x, y) — координаты точки P (порождающего элемента подгруппы порядка q) на эллиптической кривой (qxP=0)

Набор параметров id-tc26-gost-3410-12-512-paramSetA

- p
- a
- b
- m
- q
- x
- y

```
INTEGER
00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
C7
INTEGER
00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
C4
INTEGER
00 E8 C2 50 5D ED FC 86 DD C1 BD 0B 2B 66 67 F1
DA 34 B8 25 74 76 1C B0 E8 79 BD 08 1C FD 0B 62
65 EE 3C B0 90 F3 0D 27 61 4C B4 57 40 10 DA 90
DD 86 2E F9 D4 EB EE 47 61 50 31 90 78 5A 71 C7
60
NTEGER
00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF 27 E6 95 32 F4 8D 89 11 6F F2 2B 8D 4E 05 60
60 9B 4B 38 AB FA D2 B8 5D CA CD B1 41 1F 10 B2
75
INTEGER
00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF 27 E6 95 32 F4 8D 89 11 6F F2 2B 8D 4E 05 60
60 9B 4B 38 AB FA D2 B8 5D CA CD B1 41 1F 10 B2
75
INTEGER
03
INTEGER
75 03 CF E8 7A 83 6A E3 A6 1B 88 16 E2 54 50 E6
CE 5E 1C 93 AC F1 AB C1 77 80 64 FD CB EF A9 21
DF 16 26 BE 4F D0 36 E9 3D 75 E6 A5 0E 3A 41 E9
80 28 FE 5F C2 35 F5 B8 89 A5 89 CB 52 15 F2 A4
```

Набор параметров id-tc26-gost-3410-12-512-paramSetB

- p
- a
- b
- m
- q
- x
- y

```
INTEGER
00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F
INTEGER
00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6C
INTEGER
68 7D 1B 45 9D C8 41 45 7E 3E 06 CF 6F 5E 25 17
B9 7C 7D 61 4A F1 38 BC BF 85 DC 80 6C 4B 28 9F
3E 96 5D 2D B1 41 6D 21 7F 8B 27 6F AD 1A B6 9C
50 F7 8B EE 1F A3 10 6E FB 8C CB C7 C5 14 01 16
INTEGER
00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01 49 A1 EC 14 25 65 A5 45 AC FD B7 7B D9 D4 0C
FA 8B 99 67 12 10 1B EA 0E C6 34 6C 54 37 4F 25
BD
INTEGER
00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01 49 A1 EC 14 25 65 A5 45 AC FD B7 7B D9 D4 0C
FA 8B 99 67 12 10 1B EA 0E C6 34 6C 54 37 4F 25
BD
INTEGER
02
INTEGER
1A 8F 7E DA 38 9B 09 4C 2C 07 1E 36 47 A8 94 0F
3C 12 3B 69 75 78 C2 13 BE 6D D9 E6 C8 EC 73 35
DC B2 28 FD 1E DF 4A 39 15 2C BC AA F8 C0 39 88
28 04 10 55 F9 4C EE EC 7E 21 34 07 80 FE 41 BD
```

Набор параметров id-tc26-gost-3410-2012-256-paramSetB

- p
- a
- b
- m
- q
- x
- y

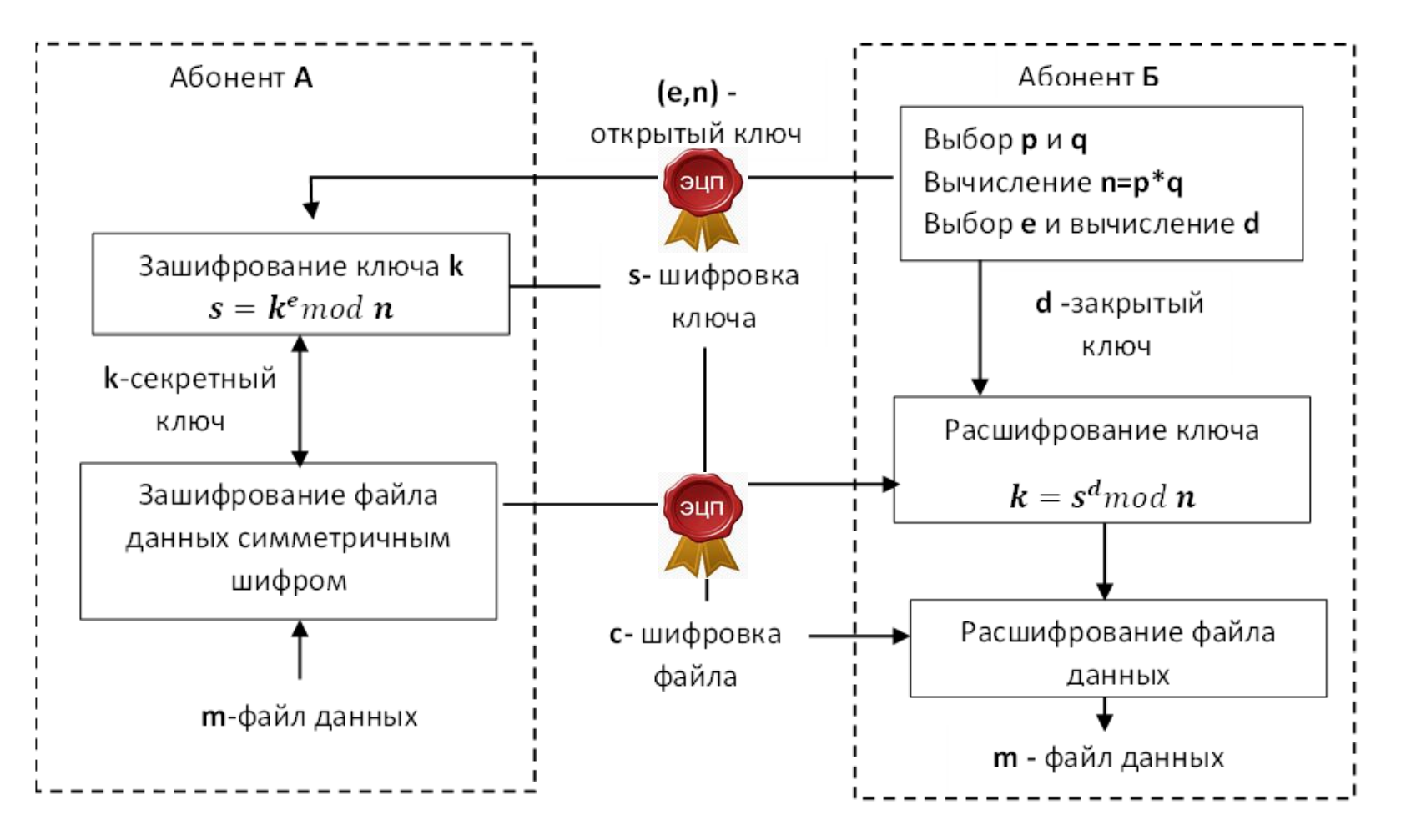
```
INTEGER
00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
97
INTEGER
00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
94
INTEGER
A6
INTEGER
00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF 6C 61 10 70 99 5A D1 00 45 84 1B 09 B7 61 B8
93
INTEGER
00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF 6C 61 10 70 99 5A D1 00 45 84 1B 09 B7 61 B8
93
INTEGER
01
INTEGER
00 8D 91 E4 71 E0 98 9C DA 27 DF 50 5A 45 3F 2B
76 35 29 4F 2D DF 23 E3 B1 22 AC C9 9C 9E 9F 1E
14
```

Набор параметров id-tc26-gost-3410-2012-256-paramSetC

- p
- a
- b
- m
- q
- x
- y

```
INTEGER
00 9B 9F 60 5F 5A 85 81 07 AB 1E C8 5E 6B 41 C8
AA CF 84 6E 86 78 90 51 D3 79 98 F7 B9 02 2D 75
9B
INTEGER
00 9B 9F 60 5F 5A 85 81 07 AB 1E C8 5E 6B 41 C8
AA CF 84 6E 86 78 90 51 D3 79 98 F7 B9 02 2D 75
98
INTEGER
80 5A
NTEGER
00 9B 9F 60 5F 5A 85 81 07 AB 1E C8 5E 6B 41 C8
AA 58 2C A3 51 1E DD FB 74 F0 2F 3A 65 98 98 0B
B9
NTEGER
00 9B 9F 60 5F 5A 85 81 07 AB 1E C8 5E 6B 41 C8
AA 58 2C A3 51 1E DD FB 74 F0 2F 3A 65 98 98 0B
B9
INTEGER
00
INTEGER
41 EC E5 57 43 71 1A 8C 3C BF 37 83 CD 08 C0 EE
4D 4D C4 40 D4 64 1A 8F 36 6E 55 0D FD B3 BB 67
```

Защищенный гибридный (RSA) протокол шифрования



Спасибо за внимание !