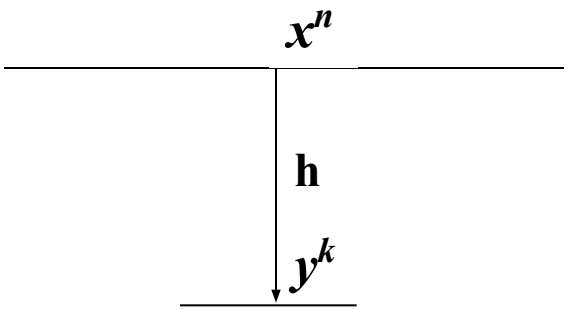
Лекция 8
Электронная подпись сообщения

Учебные вопросы

1. Понятие и классы хэш-функций.
2. Определение, классификация, основные свойства ЭЦП.
3. Стандарты ЭЦП

1. Понятие о хэширующей-функции

Определение . *Хеш-функцией* $y = h(x)$ называется преобразование, отображающее множество всех двоичных последовательностей *X* длины *n* во множество двоичных последовательностей *Y* длины *b*, где b<n.



y=h(x)

Hash –мешанина, крошево. рубить, крошить

$x \in X$, $y \in Y$, $h \in H$, X,Y - дискретные множества, $|X|=2^n$, $|Y|=2^k$

Хеш-функции бывают *ключевыми* и *бесключевыми* (т. е. зависящими или не зависящими от ключа). Если хеш-функция является ключевой, то можно говорить о классе хеш-функций, где каждая функция из класса соответствует выбору определенного ключа.

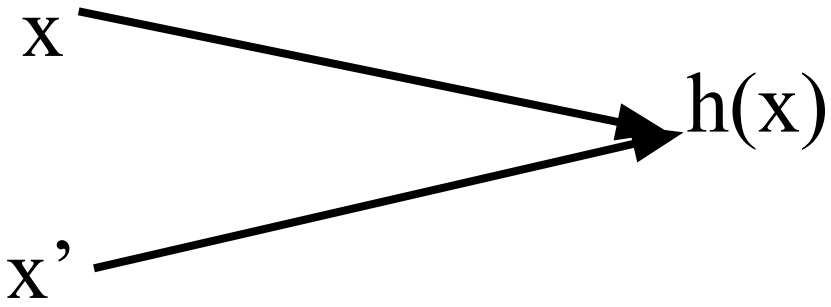
Требования к криптографическим ХФ (стр. 209)

1.*Однонаправленность*, когда при известном хеше h вычислительно неосуществимо (то есть требует нереализуемо большого числа операций) нахождение хотя бы одного значения x , для которого , $h(x) = h$ то есть h(x) оказывается *однонаправленной функцией (ОНФ*).

2.*Слабая коллизионная стойкость,* когда для заданных x, h(x)=h вычислительно неосуществимо найти такое другое x’ значение , которое удовлетворяет уравнению h(x’)=h.

3.*Сильная коллизионная стойкость*, когда вычислительно неосуществимо найти такую пару аргументов x, x’ , для которых выполняется соотношение h(x)=h(x’).

.

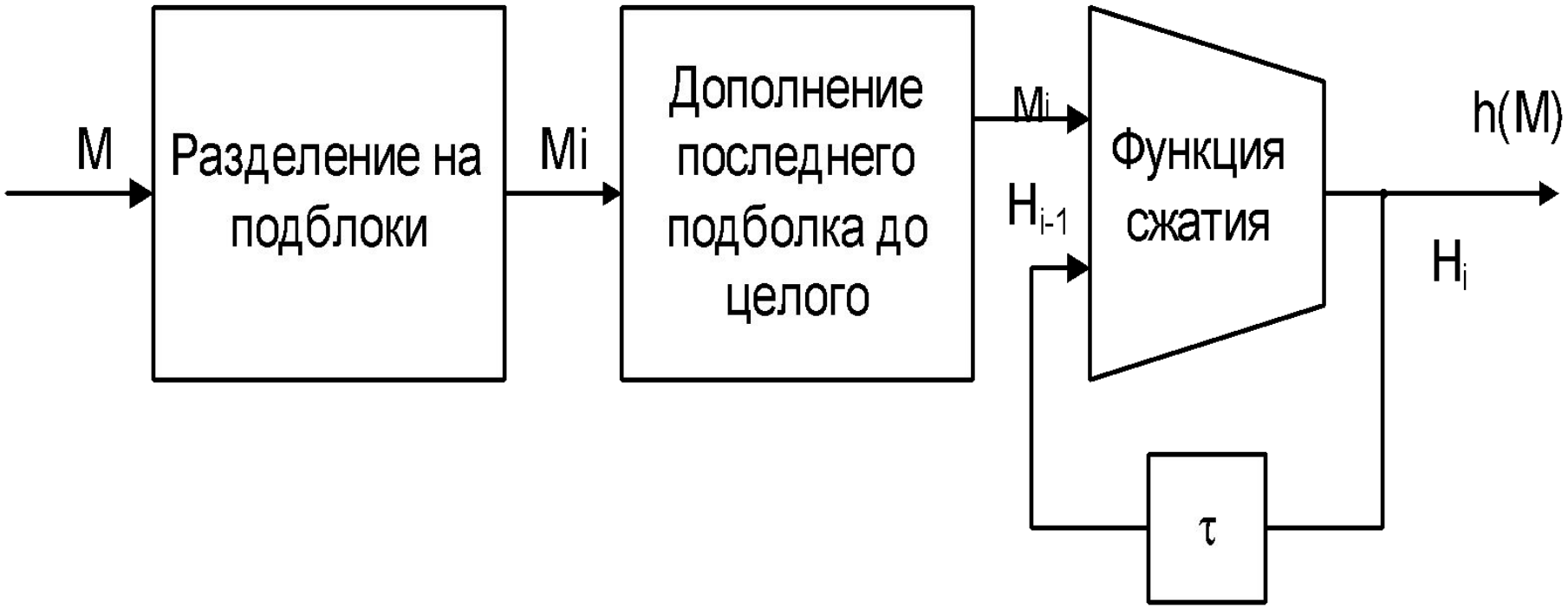

x
h(x)
x’

- Хорошая криптографическая ХФ должна обладать тем свойством, что при любом случайном и равномерно распределённом выборе аргумента x , вероятность преобразования его ХФ в фиксированный хеш h=h(x) будет близка к величине 2^{-m}, где m - длина двоичной цепочки хеша. Тогда при случайном выборе L различных аргументов ХФ x1,x2,…,xL вероятность того, что, хотя бы для одного из них хеш совпадет с заранее заданным значением, будет равна .

$$1-(1-2^{-m})^{L} \cong L2^{-m}$$

Поэтому число попыток, необходимых для обращения ХФ будет с вероятностью P равно $P2^{m}$

Принцип построения итеративной, бесключевой хэшфункции



Принцип хэширования на основе сжимающей функции

$H_0 = v$

$H_i \leftarrow h(M_i, H_{i-1}),\ i = 1,2,\ldots N$

$h(M^n) = H_N$

v- начальный (стартовый) вектор

2. Определение, классификация, основные свойства ЭЦП

Подпись – собственноручно написанная фамилия.

Толковый словарь русского языка.

С.И. Ожегов, Н.Ю. Шведова

Свойства подписи на бумаге

1. Сформировать подпись может только ее автор. (подпись уникальна)
2. Проверить подпись может каждый, имеющий образец подписи.
3. Подпись трудно подделать.
4. Подпись неоспорима, автор не может отказаться от подписи.
5. Документ с подписью неизменяем.
6. Подпись неотделима от документа.

Основные понятия электронной подписи

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписавшего информацию.

ключ ЭП – уникальная последовательность символов предназначенная для создания электронной цифровой подписи.

ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключем ЭП и предназначенная для проверки подлинности электронной подписи.

Закон РФ от 6 апреля 2011г. N 63-ФЗ. Об электронной подписи

Свойства электронной подписи

1. Сформировать подпись может только обладатель закрытого ключа.
2. Проверить подпись может любой пользователь, имеющий открытый ключ.
3. Вероятность подделки подписи пренебрежительно мала.
4. Подпись неоспорима, пользователь не может отказаться от подписи.
5. Электронный документ неизменяем.
6. Подпись и подписанное сообщение могут передаваться и храниться отдельно.

Свойства электронной цифровой подписи (ЭЦП)

Свойства подписи на бумаге

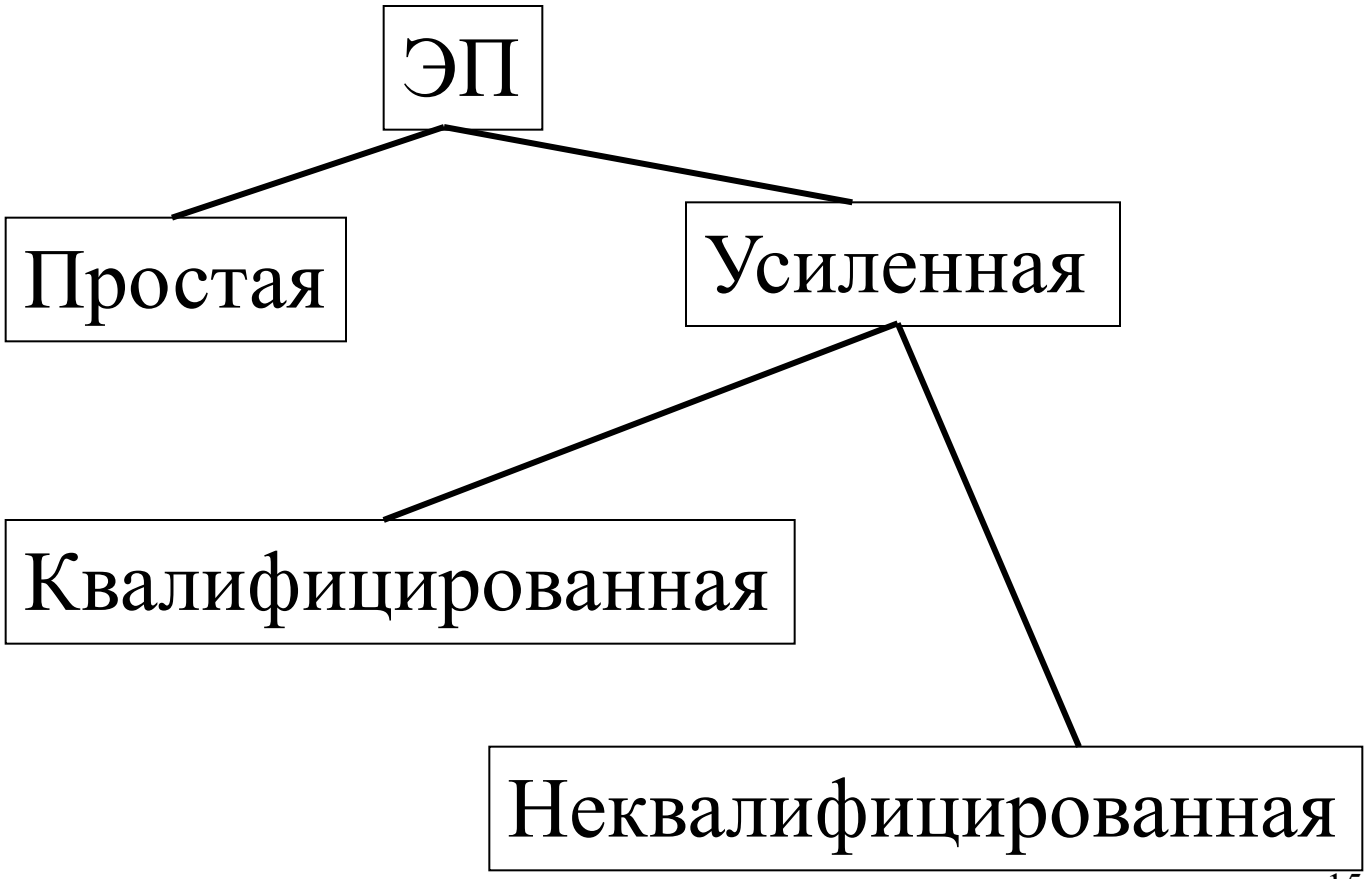
1. Сформировать подпись может только ее автор.
2. Проверить подпись может каждый , имеющий образец подписи.
3. Подпись трудно подделать.
4. Подпись неоспорима, автор не может отказаться от подписи.
5. Документ с подписью неизменяем.
6. Подпись неотделима от документа.

Свойства ЭЦП

1. Сформировать подпись может только обладатель закрытого ключа.
2. Проверить подпись может любой пользователь, имеющий открытый ключ.
3. Вероятность подделки подписи пренебрежительно мала.
4. Подпись неоспорима, пользователь не может отказаться от подписи.
5. Электронный документ неизменяем.
6. Подпись и подписанное сообщение могут передаваться

Виды электронных подписей

(Согласно Закону РФ от 6 апреля 2011г. N 63-ФЗ. Об электронной подписи)



- Простая ЭП – подпись, которая путем использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом.

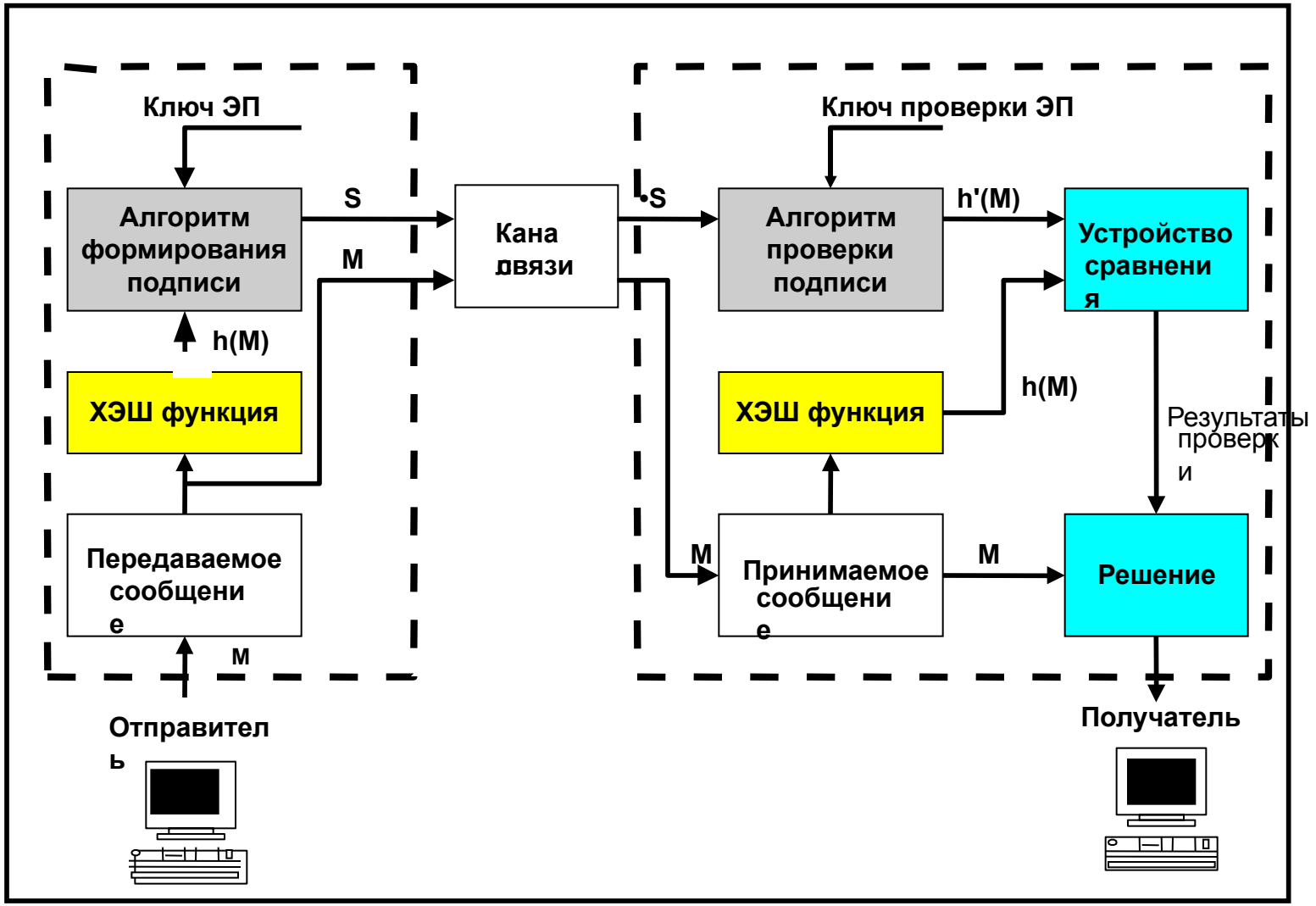
Неквалифицированная ЭП

- Получена в результате криптографического преобразования информации с использованием ключа ЭП;
- Позволяет определить лицо, подписавшее документ;
- Позволяет обнаружить факт внесения изменений в ЭД;
- Создается с использованием средств ЭП;

Квалифицированная ЭП

- 1. Соответствует всем признакам неквалифицированной ЭП;
- 2. Ключ проверки ЭП указан в квалифицированном сертификате.
- 3. Для создания и проверки ЭП используются средства ЭП, получившие подтверждение соответствия в соответствии с законом об ЭП.

Модель ЭЦП


Ключ ЭП
Алгоритм формирования подписи
S
M
Кана
двязи
S
Ключ проверки ЭП
Алгоритм проверки подписи
h'(M)
Устройство сравнени я
h(M)
ХЭШ функция
ХЭШ функция
h(M)
Результаты проверк и
Передаваемое сообщени е
M
M
Принимаемое сообщени е
M
Решение
Отправител ь
Получатель

Хронология развития систем ЭЦП

- **1976 г. – открытие М. Хэлменом и У. Диффи асимметричных криптографических систем;**
- **1978 г. – Р. Райвест, А. Шамир, Л. Адельман – предложили первую систему ЭЦП, основанную на задаче факторизации большого числа;**
- **1985 г. – Эль Гамаль предложил систему ЭЦП, основанную на задаче логарифмирования в поле чисел из *p* элементов;**
- **1991 г.- Международный стандарт ЭЦП ISO/IEC 9796 (вариант РША);**
- **1994 г. – Стандарт США FIPS 186 (вариант подписи Эль Гамаля);**
- **1994 г. – ГОСТ Р 34.10-95 (вариант подписи Эль Гамаля);**
- **2000 г. – Стандарт США FIPS 186 – 2;**
- **2001 г. – ГОСТ Р 34.10-01 (ЭЦП на основе математического аппарата эллиптических кривых).**

Разновидности ЭЦП (теоретические разработки)

1. Неоспоримая ЭЦП (для проверки ЦП необходимо участие подписавшего лица).

2. Групповая ЭЦП (владелец подписи является анонимным членом группы).

3. Слепая подпись (подпись электронного документа без ознакомления с его содержанием).

4. Одновременный обмен секретами (пользователь передает другому пользователю свой секрет при одновременном получении от него его секрета)

5. Коллективная подпись. В подписании документа участвуют несколько лиц. Проверка подписи- одно лицо.

Система ЭЦП Эль-Гамаля (1985г.)

Пусть p -простое число; a - примитивный элемент GF(p).

Генерирование ключей

A - генерирует число x_A, $1< x_A <p-2$ (ключ подписи),
вычисляет открытый ключ $y_A=a^x \pmod p$. (ключ проверки подписи)
($SK= x_A$, $PK= y_A$). y_A передается корр. B.

Подписание сообщения

Пусть корр. A хочет послать корр.B подписанное сообщение M.

1.Корр. A осуществляет хэширование M m=h(M), m<p.

2. Генерирует случайное число 1<k<p-2.

3. Формирует первую часть подписи
$r=a^k \pmod p$,

4. Находит вторую часть подписи

$s=k^{-1} \cdot (m-xr) \pmod{p-1}$, $kk^{-1}=1 \pmod{(p-1)}$

5, Отправляет корр. B (M,(r,s)).

Система ЭЦП Эль-Гамаля (1985г.)

Проверка подписи

1.Корр. В осуществляет хэширование принятого сообщения M’ m’=h(M’)

2. Проверяет выполнение сравнения

$y^r r^s (mod p) = a^{m'} (mod p)$

3. Если сравнение выполняется, то подпись верна.

Проверка обратимости преобразований

$a^{xr}\, a^{ks} (mod p) = a^{xr+ks} (mod p) =$ $a^{xr+kk^{-1}(m-xr)} (\mathrm{mod}\ p) = a^m (\mathrm{mod}\ p)$

$$s=k^{-1} \cdot (m-xr)(modp-1),$$

Пример ЭЦП

Общесистемные параметры: p=11, a=2

Генерирование ключей: случайно генерируем x=3 – закрытый ключ;
Находим $y=a^x(\mathrm{mod}p)= 2^3(\mathrm{mod}11)= 8$, y=8 – открытый ключ

Формирование подписи:
Пусть хэшированное сообщение m=4.
Случайно генерируем число k=7.
Находим первую часть подписи $r=a^{k(}\mathrm{mod}p)=2^7(\mathrm{mod}11)=7$, $k^{-1}=3$,т.к
$k\,k^{-1}=1(\mathrm{mod}10)$
Находим вторую часть подписи $s=k^{-1}(m -xr)(\mathrm{mod}p-1)$
$=3(4-3*7)(\mathrm{mod}10)=9$
Подпись (r=7,s=9).

Проверка подписи.
Проверяем выполнение сравнения
$y^r r^s(\mathrm{mod}p)=a^{m'}(\mathrm{mod}p)$. $y^r r^s(\mathrm{mod}p)=8^7 7^9(\mathrm{mod}11)=2*8(\mathrm{mod}11)=5$
$a^{m'}(\mathrm{mod}p)=2^4=16(\mathrm{mod}11)=5$
Подпись верна.

Быстрое возведение в степень методом Д. Кнута

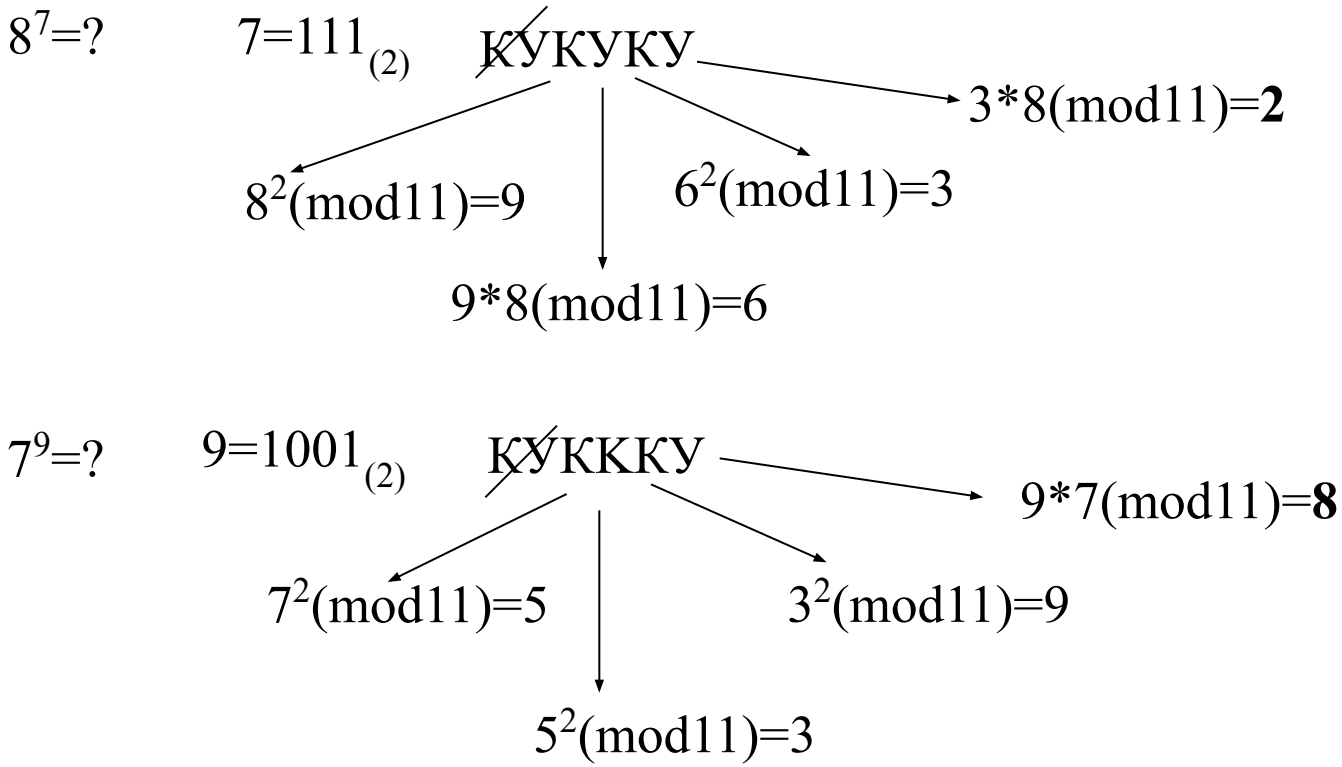


Схема ЭЦП РША

Генерирование ключей.

Случайно выбираются два простых числа p и q

Находится модуль N=pq. Находится функция Эйлера $\phi(N)= (p-1)(q-1)$

Выбираем число e такое, что НОД(e, $\phi(N)$)=1. Находим d, как обратный элемент к e $de=1(\mathrm{mod}\ \phi(N))$.

Объявляем d=SK, (e,N)=PK. PK сообщается всем корреспондентам.

Формирование подписи.

Корр. А хэширует сообщение M m=h(M).

Используя свой закрытый ключ d подписывает m $s=m^d(\mathrm{mod}N)$.

Передает корр. B (M,s)

Проверка подписи.

Корр. B хэширует сообщение M m'=h(M)

Используя открытый ключ, корр.A осуществляет проверку подписи, вычисляя $m=s^e(\mathrm{mod}N)$.

Сравнивая m и m' принимает решение о верности подписи.

3. СТАНДАРТЫ ХЭШ-ФУНКЦИИ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

ПРАВОВЫЕ ДОКУМЕНТЫ ОБ ЭЛЕКТРОННОЙ ПОДПИСИ

1. Закон РФ от 6 апреля 2011г. N 63-ФЗ. Об электронной подписи.
2. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.
2. ГОСТ Р34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
3. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки цифровой подписи на базе асимметричного криптографического алгоритма.
4. ГОСТ Р34.10-01. Информационная технология. Криптографическая защита информации. Информационная технология. Процессы выработки и проверки цифровой подписи.
5. ГОСТ Р34.10-2012. Информационная технология. Криптографическая защита информации. Информационная технология. Процессы выработки и проверки цифровой подписи.

ГОСТ Р34.11-1994
Информационная технология. Криптографическая защита информации. Функция хэширования

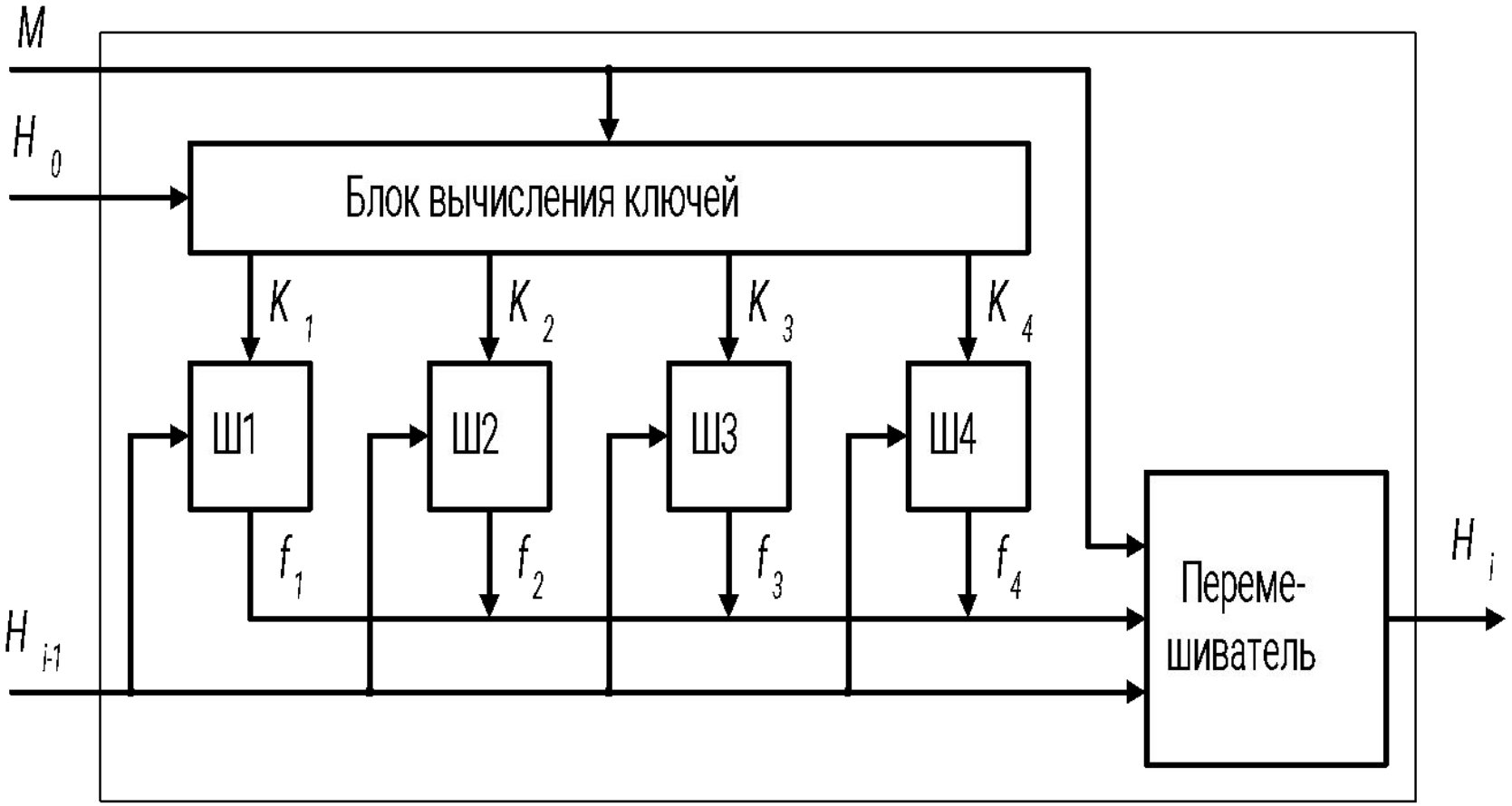
ГОСТ Р34.11-2012
Информационная технология. Криптографическая защита информации. Функция хэширования

Длина хэш-кода

ГОСТ Р34.11-1994 256 бит

ГОСТ Р34.11-2012 256 или 512 бит

Функция сжатия по ГОСТ Р34.11-94г.



Алгоритм вычисления функции сжатия

1-й этап.

Генерация четырех 256 битных ключей K_1, K_2, K_3, K_4

$K_j = A_j M + C_j$, $j=1,2,3,4$.

A_j - блочная матрица, C_j – вектор (константа).

2-й этап.

Зашифрование четырех 64-битных слов на этих ключах:

$f_j = E(h_j, K_j)$, $j=1,2,3,4$, где h_j – 64-битный подблок 256 –битного блока хэш-функции, вычисленного на предыдущем шаге.

Формирование 256- блока криптограммы $f = f_1 | f_2 | f_3 | f_4$

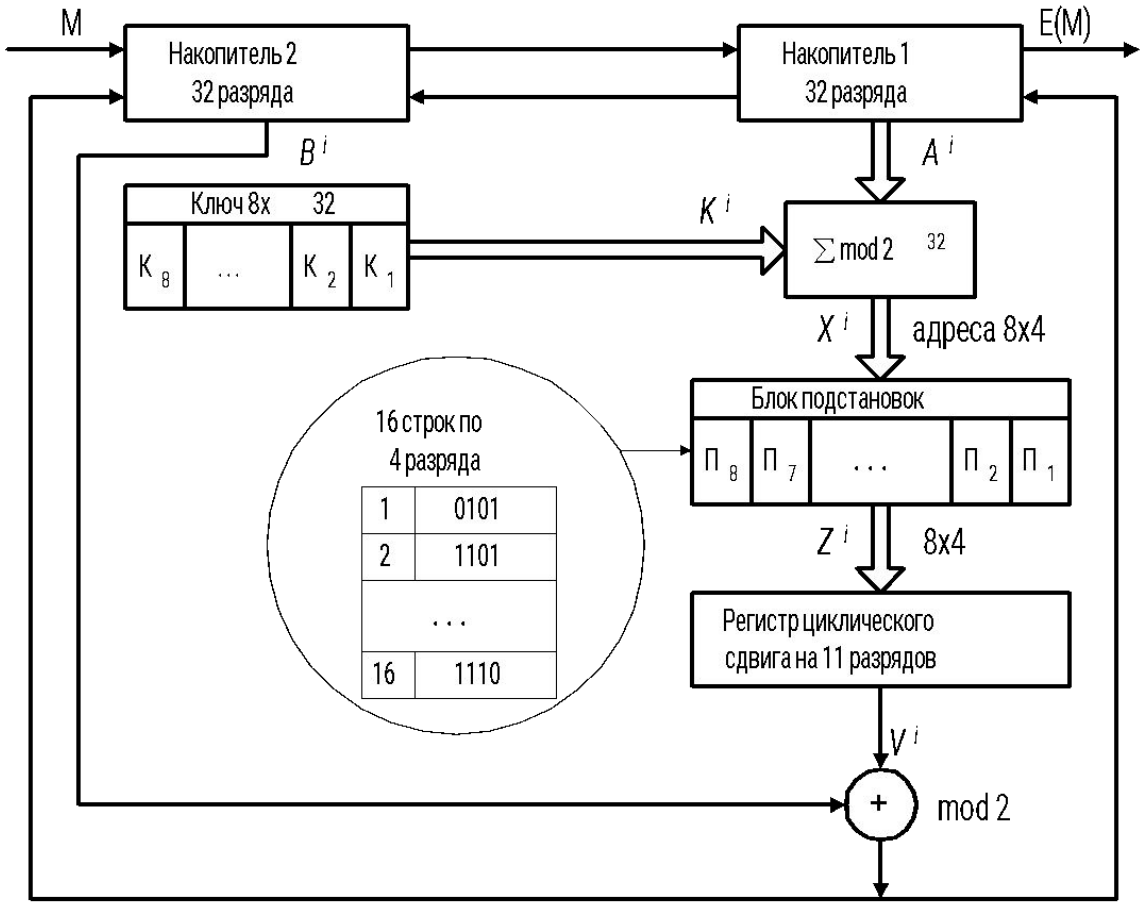
3-й этап. Перемешивание блока сообщения, результата шифрования и предыдущего значения хэш-кода.

$$H_i = \Psi^{61}(H_{i-1} \oplus \Psi(M_i \oplus \Psi^{12}(f_i))),$$

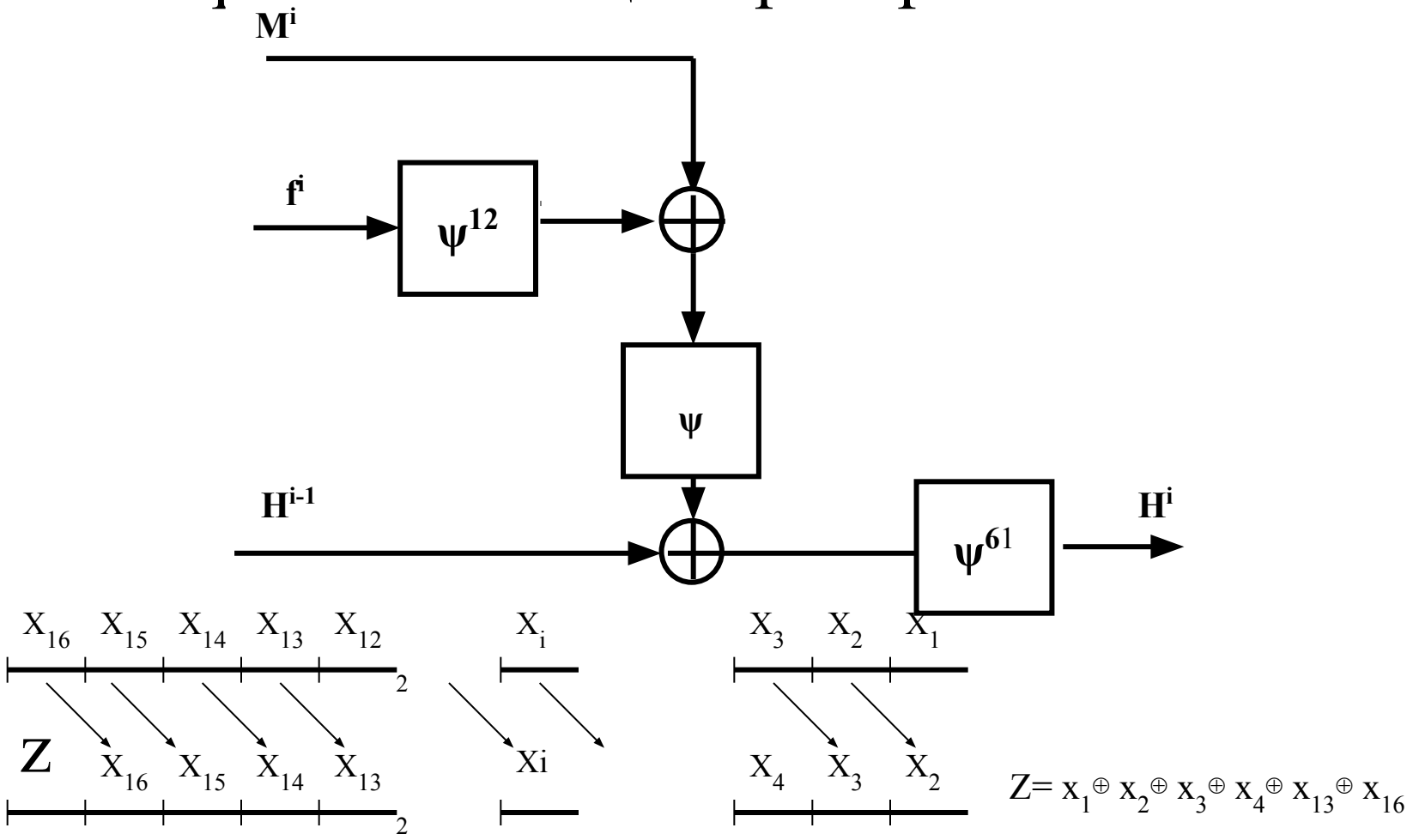
где Ψ^r – обозначает r -кратное применение перемешивающего преобразования Ψ.

$\Psi: \{0,1\}^{256} \rightarrow \{0,1\}^{256}$

Алгоритм шифрования согласно ГОСТ 28147-89

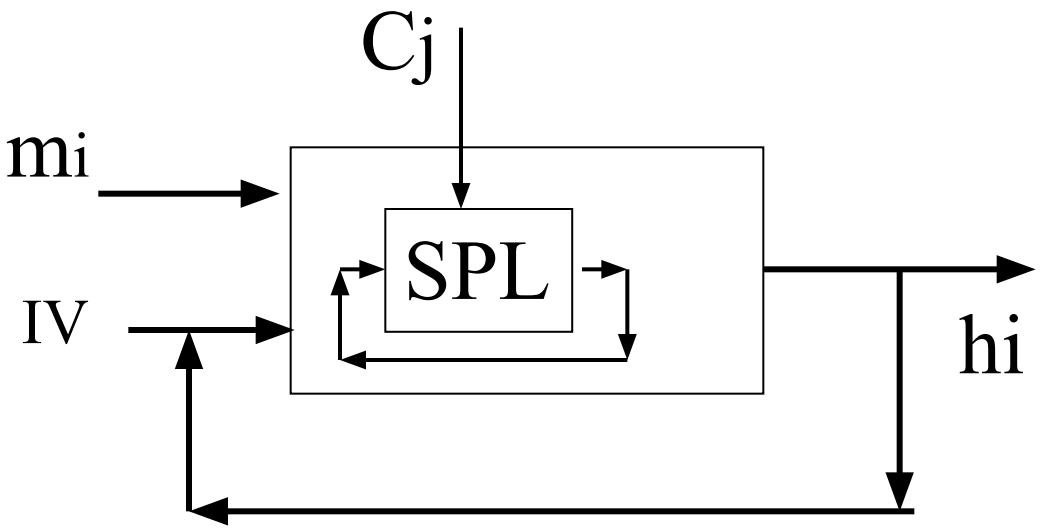


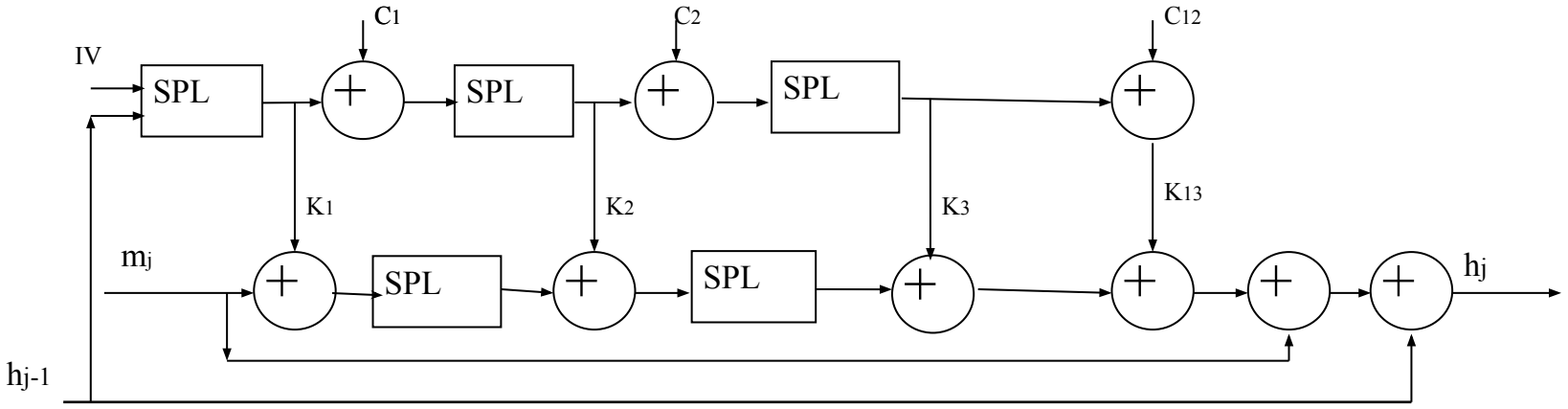
Перемешивающее преобразование



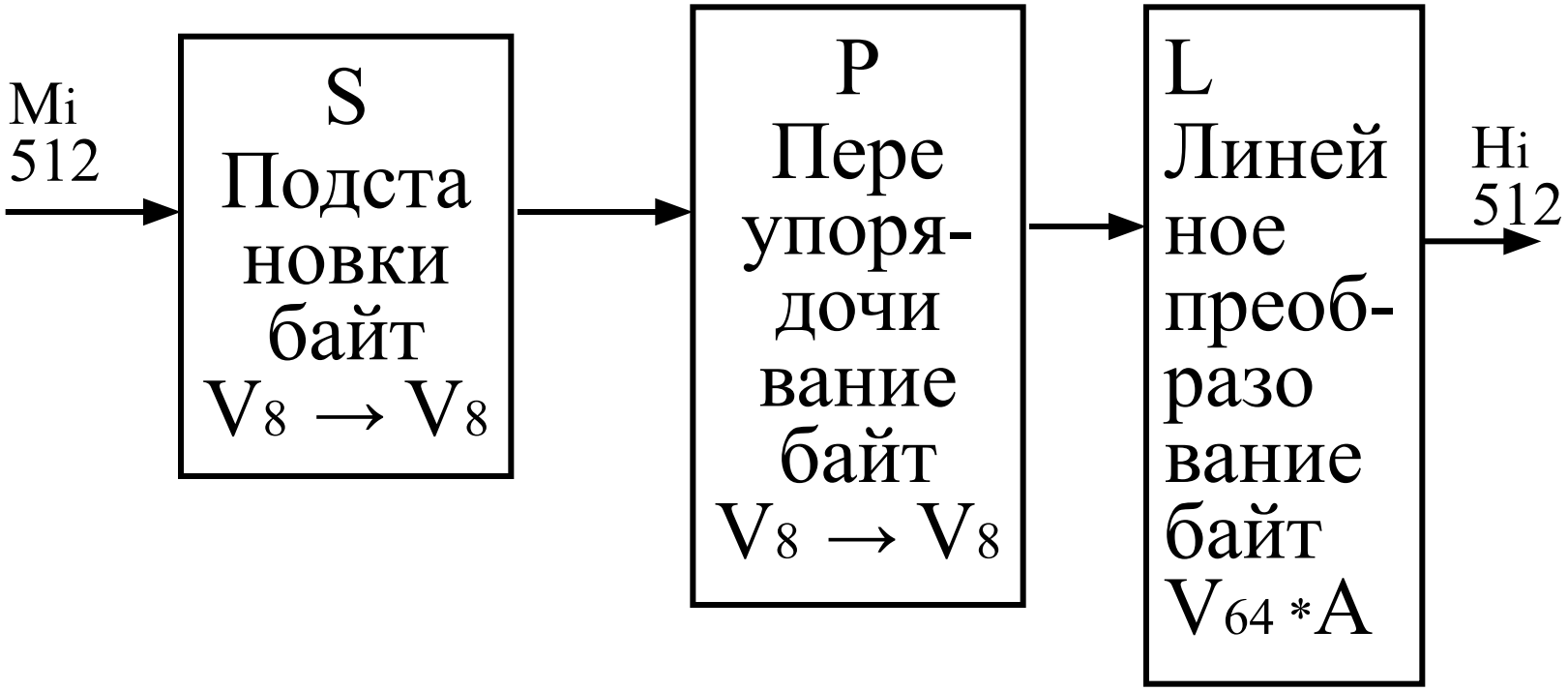
Пусть $X = x_{16} \mid x_{15} \mid x_{14} \mid \ldots \mid x_2 \mid x_1 \mid$, где x_i –16-битные блоки.
Тогда
$\Psi(X) = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_{13} \oplus x_{16} \mid x_{16} \mid x_{15} \mid x_{14} \mid \ldots \mid x_2 \mid$

Функция сжатия по ГОСТ Р34.11-2012





SPL преобразование.



Преобразование *SPL*, составляет основу функции сжатия и включает три последовательно проводимых преобразования: *S, P* и *L.*

S – замена байт. 512 бит аргумента представляются как 64 байтный массив и каждый байт заменяется по заданной таблице.

P - переупорядочивание байт - байты аргумента меняются местами по определенному стандартом порядку.

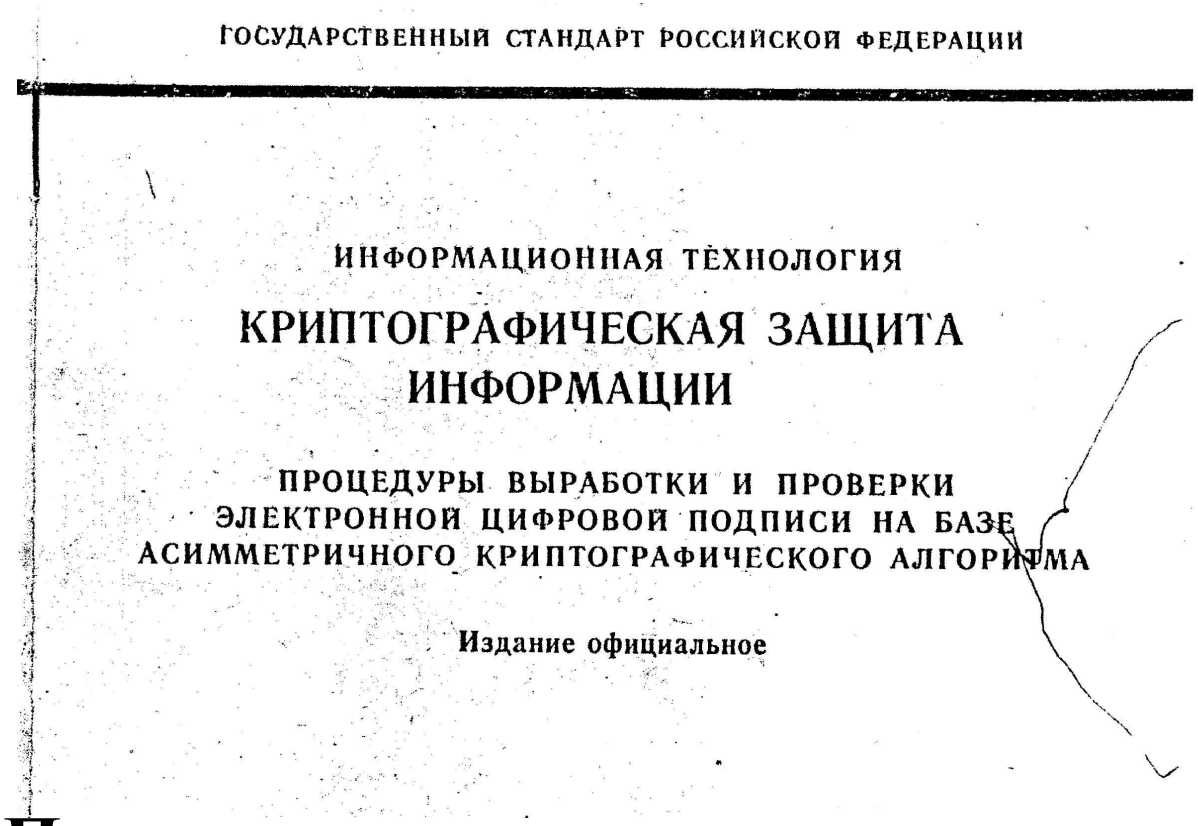
L - линейное преобразование. Аргумент рассматривается как восемь 64 битных векторов, каждый из которых заменяется результатом умножения вектора на определенную стандартом матрицу A_{64X64} над GF(2).

Реализация стандарта на цифровом процессоре архитектуры x86.64 обеспечивает скорость работы 94 МБ/с и требует 87 тактов на байт [ ].

Хронология развития систем ЭЦП

- **1976 г. – открытие М. Хэлменом и У. Диффи асимметричных криптографических систем;**
- **1978 г. – Р. Райвест, А. Шамир, Л. Адельман – предложили первую систему ЭЦП, основанную на задаче факторизации большого числа;**
- **1985 г. – Эль Гамаль предложил систему ЭЦП, основанную на задаче логарифмирования в поле чисел из *p* элементов;**
- **1991 г.- Международный стандарт ЭЦП ISO/IEC 9796 (вариант РША);**
- **1994 г. – Стандарт США FIPS 186 (вариант подписи Эль Гамаля);**
- **1994 г. – ГОСТ Р 34.10-95 (вариант подписи Эль Гамаля);**
- **2000 г. – Стандарт США FIPS 186 – 2;**
- **2001 г. 2012 г – ГОСТ Р 34.10-01 (12) (ЭЦП на основе математического аппарата эллиптических кривых).**

1. ГОСТ Р 3410 -94



ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРОЦЕДУРЫ ВЫРАБОТКИ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ АСИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

Издание официальное

Параметры :

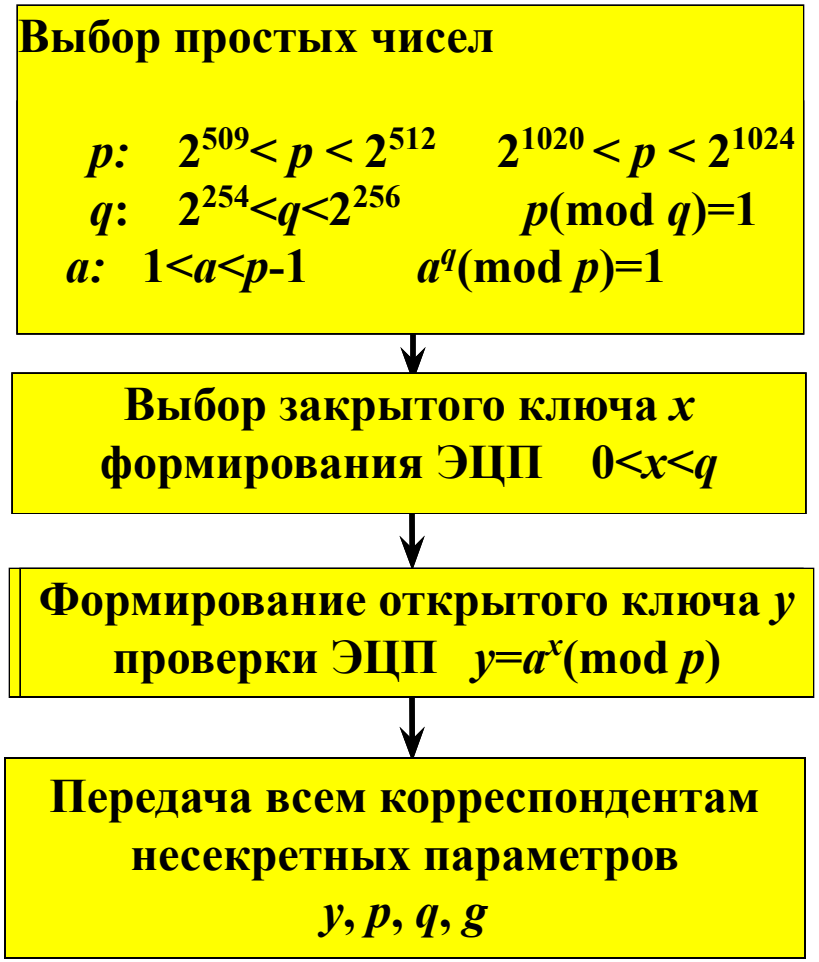
Длина подписываемого сообщения -неограничена;

Длина подписи 512 бит;

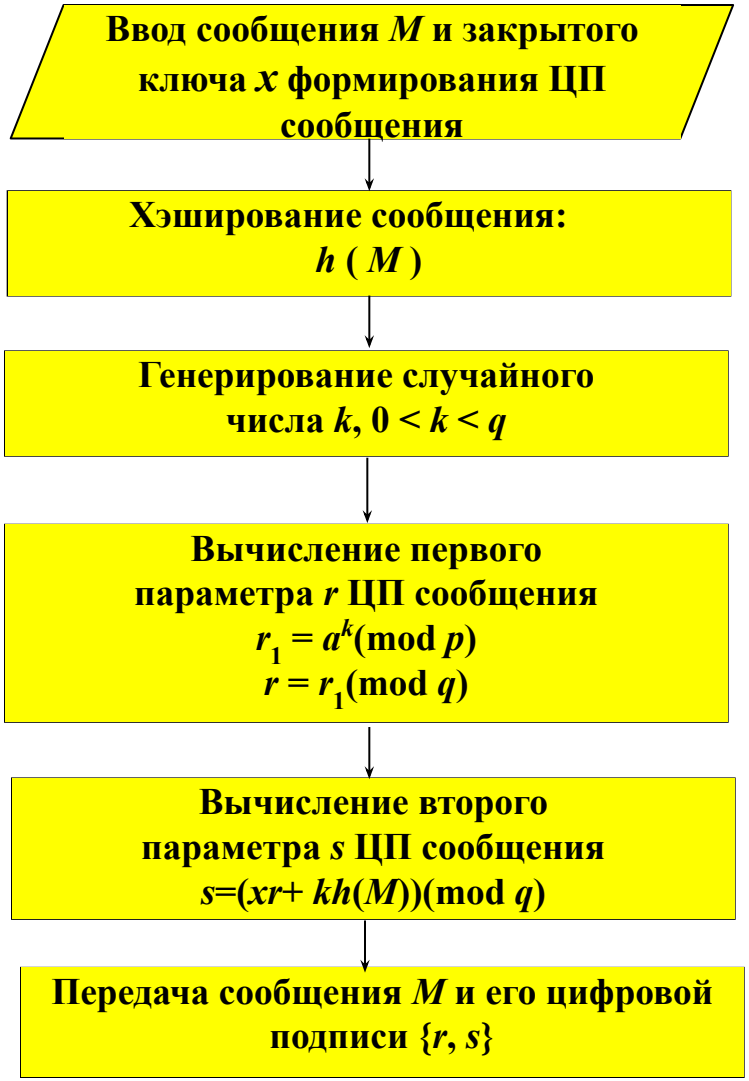
Длина закрытого ключа -256 бит;

Длина открытого ключа - 512 (1024) бит

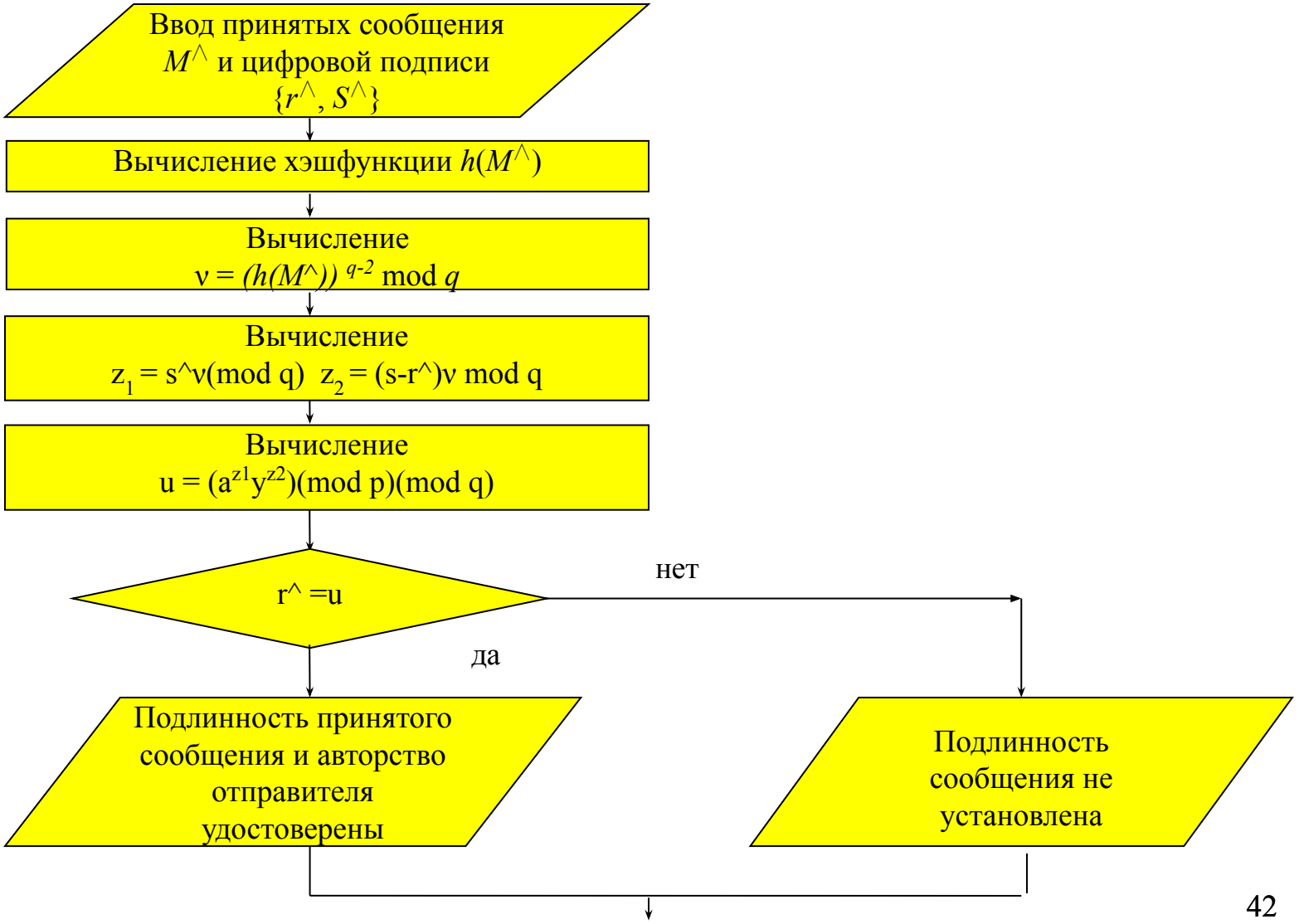
1.Генерирование ключевой информации.



2.Формирование цифровой подписи сообщения.



3. Проверка цифровой подписи сообщения.



Пример ЭЦП

Общесистемные параметры: p=11, q=5, a=4, проверим a^q(modp)= 4^5(mod11)=1024(mod11)=1

Генерирование ключей: случайно генерируем x=3 – закрытый ключ;
Находим y=a^x(modp)= 4^3(mod11)= 9, y=9 –

Формирование подписи:
Пусть хэшированное сообщение m=4.
Случайно генерируем число k=3.
Находим первую часть подписи r_1=a^k(modp)=4^3(mod11)=9,
r=r_1(modq)=9(mod5)=4.
Находим вторую часть подписи s=(xr+km)(modq)=(3*4+3*4)(mod5)=
24(mod5)=4
Подпись (r=4,s=4).

Проверка подписи
Находим обратный элемент к m. v=m^{q-2}(modq)= 4^3(mod5)=4
z_1=sv(modq)=4*4(mod5)=1, z_2=(q-r)v(modq)=(5-4)*4(mod5)=4
Проверка сравнения u=r? u=$a^{z1}y^{z2}$(modp)(modq)= 4^1 *9^4 (mod11)(mod5)=
=4*81*81=4*4*4(mod11)(mod5) =20(mod11)(mod5)=4
u=4, r=4 - Подпись верна.

3. ГОСТ Р.34.10-01

Стандарт определяет процедуры (алгоритмы) формирования и проверки цифровой подписи на основе математического аппарата эллиптических кривых.

Особенности нового стандарта ЦП.

1. Максимальная преемственность по отношению к стандарту Р34.10-94.

-использован действующий стандарт функции хэширования.

- длина подписи в новом стандарте остается без изменений -

2. Стойкость подписи к подделке в новом стандарте в десятки тысяч раз выше по сравнению с Р34.10-94. В основе стандарта - вариант подписи Эль-Гамаля, в котором вместо операций умножения и возведения в степень в числовом поле из *p* элементов операции выполняются на эллиптической кривой, определенной над этим полем.

3. Возможность высокоскоростной реализации процедур формирования и проверки подписи на различных вычислительных платформах и средствах.

ГОСТ Р.34.10-12

Отличия от стандарта Р34.10-01:

-использован новый стандарт функции хэширования ГОСТ Р34.11-12

- длина подписи в новом стандарте 512 иили 1024 бита

Понятие об эллиптической кривой

Пусть $GF(q)$, $q = p^n$ **некоторое конечное поле причем** $p \neq 2$. **Тогда** ***эллиптической кривой*** E **над полем** $GF(q)$ **называется множество пар элементов** (x, y), $x, y \in GF(q)$, **которые удовлетворяют уравнению:**

$$y^2 = x^3 + ax^2 + bx + c \qquad (1)$$

где, $a, b, c \in GF(q)$

Множество точек на эллиптической кривой образуют так называемую *группу* относительно операций специфического сложения, заданной на эллиптической кривой.

Вспомогательные определения

Группой G называется множество элементов α,β,γ…обладающее, следующими свойствами:

1. определена некоторая операция двух переменных,
α+β= γ (операция сложения) ИЛИ α*β= γ (операция умножения).

2. На множестве G выполняются законы:

-В результате применения операции к двум элементам группы также получается элемент этой группы (свойство замкнутости);

-(α+β)+ γ = α+(β+ γ) ИЛИ (α * β) * γ = α * (β * γ) ;

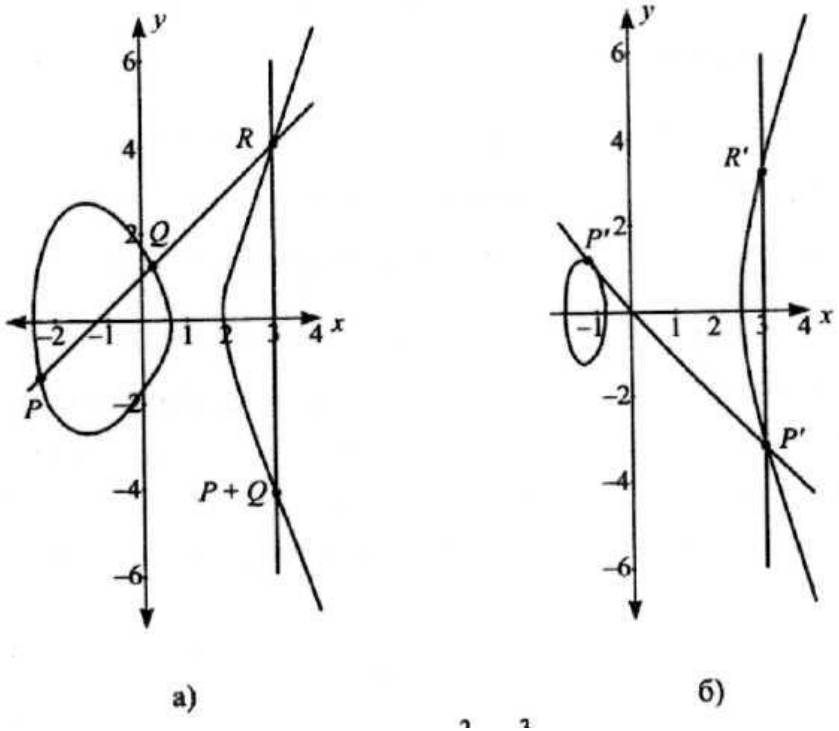
-В группе существует единичный элемент, который обозначается как 0 для сложения и как 1 для умножения, при этом для любого элемента группы справедливо 0+α= α+0 ИЛИ 1*α= α*1;

-Каждый элемент группы обладает обратным элементом, который обозначается как -α для сложения, при этом α+(- α)=0, ИЛИ α^{-1} для умножения, при этом α * α^{-1} =1.

Если **α+β= β+α ИЛИ α *β= β *α, то группа называется абелевой,**

Число элементов в группе называется порядком группы.

Пример ЭК на полем вещественных чисел



$y^2=x^3-5x+3$

Если взять две различные точки, *P* и *Q*, на кривой, то соединяющая их хорда пересечет кривую в третьей точке. Зеркально отразив точку пересечения относительно оси абсцисс, получим точку, являющуюся суммой *P* + *Q*. На эллиптической кривой определена также операция умножения точки на число. Сложение двух точек с координатами $x_P = x_Q$ и $y_P = -y_Q$ дает нулевую точку O.

Операции сложения

$P=(X_1,Y_1)$ $Q=(X_2,Y_2)$ $P+Q=(X_3,Y_3)$

Если $P\neq Q$ $X_3=\lambda^2-X_1-X_2 \pmod p$ $Y_3=\lambda(X_1-X_3)-Y_1) \pmod p$

$\lambda=(Y_2-Y_1)/(X_2-X_1) \pmod p$

Если $P=Q$ $X_3=\lambda^2-X_1-X_2 \pmod p$ $Y_3=\lambda(X_1-X_3)-Y_1) \pmod p$

$\lambda=(3X_1^2+a)/2Y_1 \pmod p$

Возведение в k-ую степень "точки P на эллиптической кривой понимается как k-кратное сложение этой точки с самой собой на этой кривой: $P^k = P + P + \ldots + P$.

Число q, при котором qP=O, называется порядком точки P.

Использование ЭК в криптосистемах основывается на сложности для нарушителя решения следующей задачи:

Даны точки ЭК P и Q, найти число x такое, что P=xQ?

Параметры
ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012

Длина подписываемого сообщения неограничена;

Длина подписи - 512 бит; (1024 бит)

Длина ключа подписи -256 бит; (512 бит)

Длина ключа проверки подписи- определяется числом p, $p > 2^{255}$

Параметры ЭЦП

Выбираются общесистемные параметры:

-p- модуль эллиптической кривой, простое число $p>2^{255}$;

-эллиптическая кривая E, удовлетворяющая уравнению

$y^2=x^3+ax+b$, где $a,b \in GF(p)$, $4a^3+276b^2 \neq 0 (mod p)$;

- целое число m – порядок группы точек эллиптическорй кривой

-простое число q – порядок подгруппы группы точек эллиптической кривой E,для которой выполнены следующие условия

$m = nq, n \in Z, n \geq 1$

$2^{254} < q < 2^{256}$, или $2^{508} < q < 2^{512}$

-ненулевая точка кривой P с координатами (x_p, y_p), удовлетворяющая равенству $q P = O$. (Базовая точка)

-хэширующая функция h(/)_

Генерирование ключей

- **Ключом подписи** является равновероятное целое число d ($0 < d < q$),
- **Ключ проверки подписи** формируется в виде точки Q эллиптической кривой с координатами (x_q, y_q), вычисляемой по правилу $\boldsymbol{d\,P = Q}$.

Алгоритм формирования подписи на эллиптической кривой по ГОСТ Р34.10-12

1. Заверяемое сообщение сначала хэшируется с использованием хэш-функции по ГОСТ Р34.11-12
2. Генерируется случайное число k ,
3. Вычисляется точка C эллиптической кривой умножением точки P на число k: $C(x_C, y_C) = k\,P(x_P, y_P)$,
4. Определяется первый параметр подписи r из координаты по оси абсцисс вычисленной точки $r = x_C \pmod q$.
5. Вычисляется второй параметр подписи по правилу
$s = (r\,d + k\,h\,(M)) \pmod q$.
6, Определить ЭЦП, как конкатенацию r и s,

Алгоритм проверки подписи

1. Вычисляется значение

$v = h\,(M\hat{}\,)^{-1} \pmod q$.

2. Вычисляются два числа:

$z_1 = s\hat{}\cdot v \pmod q$ и $z_2 = (q - r\hat{}\,)\, v \pmod q$.

3. Находится точка С эллиптической кривой

$C(x_C, y_C) = z_1 P(x_P, y_P) + z_2 Q(x_q, y_q)$.

4. Из координаты по оси абсцисс этой точки определяется значение

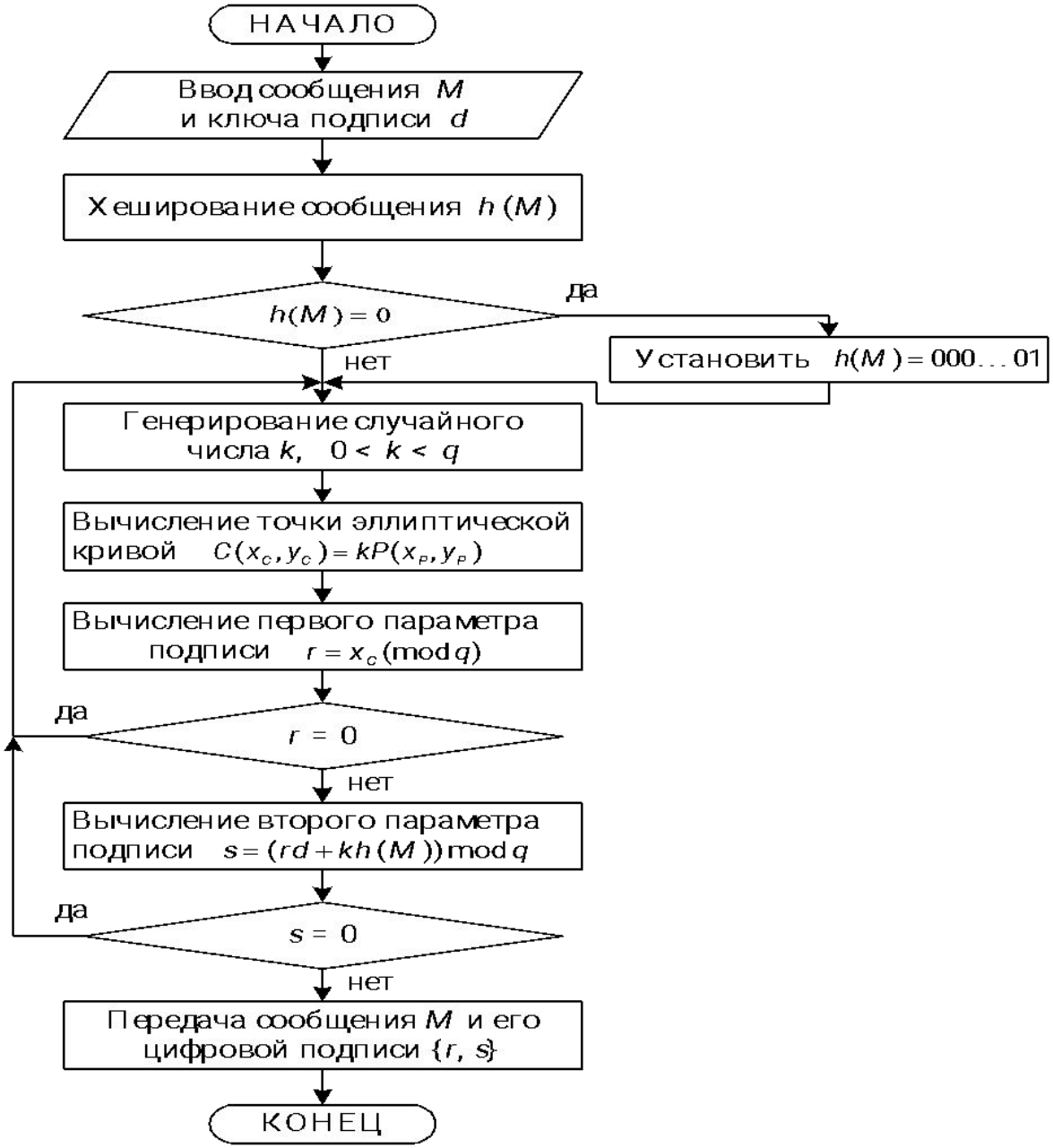
$$R = x_C \pmod q$$

5. Проверяется выполнение равенства

$$R = r$$

6. При выполнении равенства подлинность полученного сообщения и авторство удостоверены,

Формирование подписи в ГОСТ Р34.10-01, ГОСТ Р34.10-12



Проверка подписи в ГОСТ Р34.10-01, ГОСТ Р34.10-01