Лекция:

СТАНДАРТЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

1. ГОСТ 3410-94.
2. ГОСТ 3410-01

1. ГОСТ 3410-94.
2. ГОСТ 3410-01

Система ЭЦП Эль-Гамаля (1985г.)

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

Генерирование ключей

A - генерирует число x_A, $1< x_A <p-2$

вычисляет открытый ключ

$y_A=a^x \pmod p$.

(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

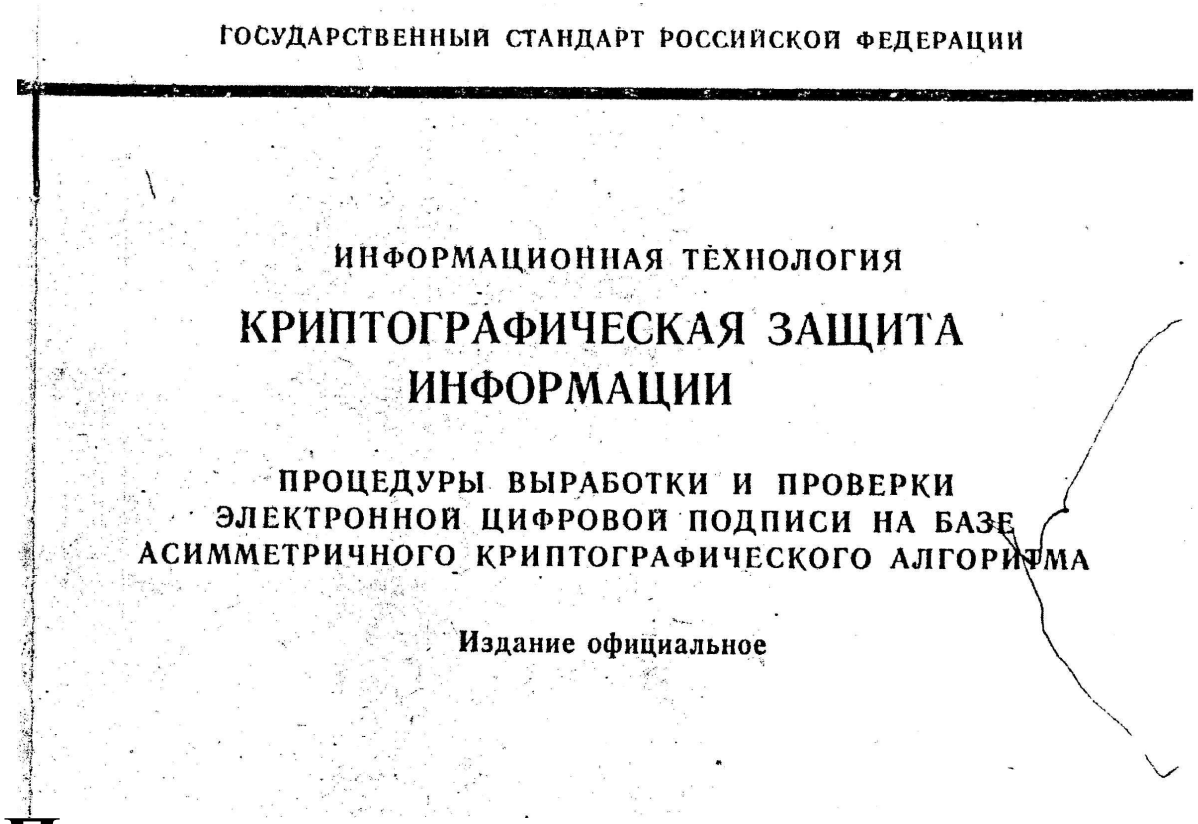
$y^r r^s (mod p) = a^{m'} (mod p)$

3. Если сравнение выполняется, то подпись верна.

Проверка обратимости преобразований

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

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 :

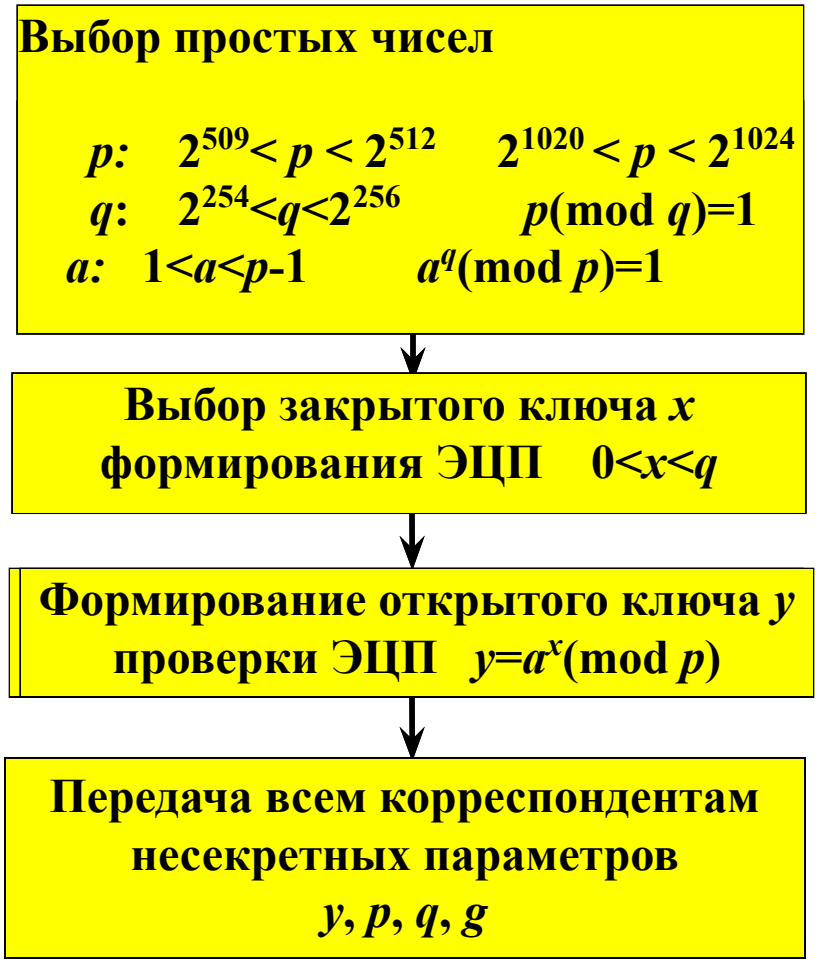
Длина подписываемого сообщения -неограничена;

Длина подписи 512 бит;

Длина закрытого ключа -256 бит;

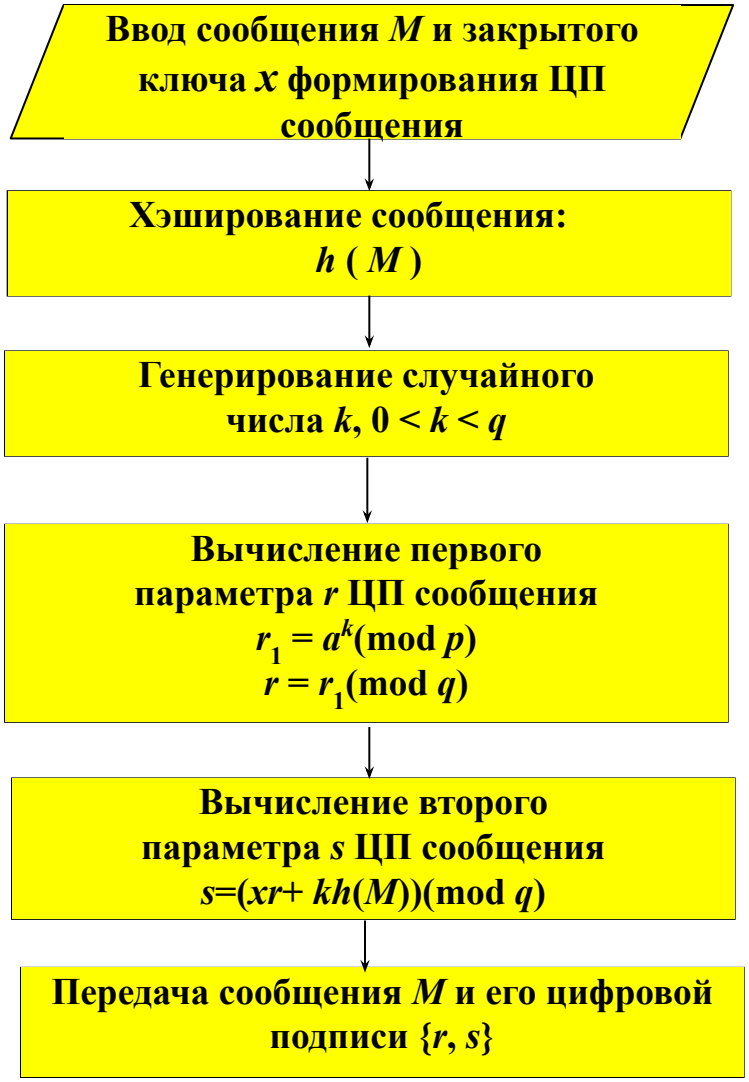
Длина открытого ключа - 512 (1024) бит

1.Генерирование ключевой информации.



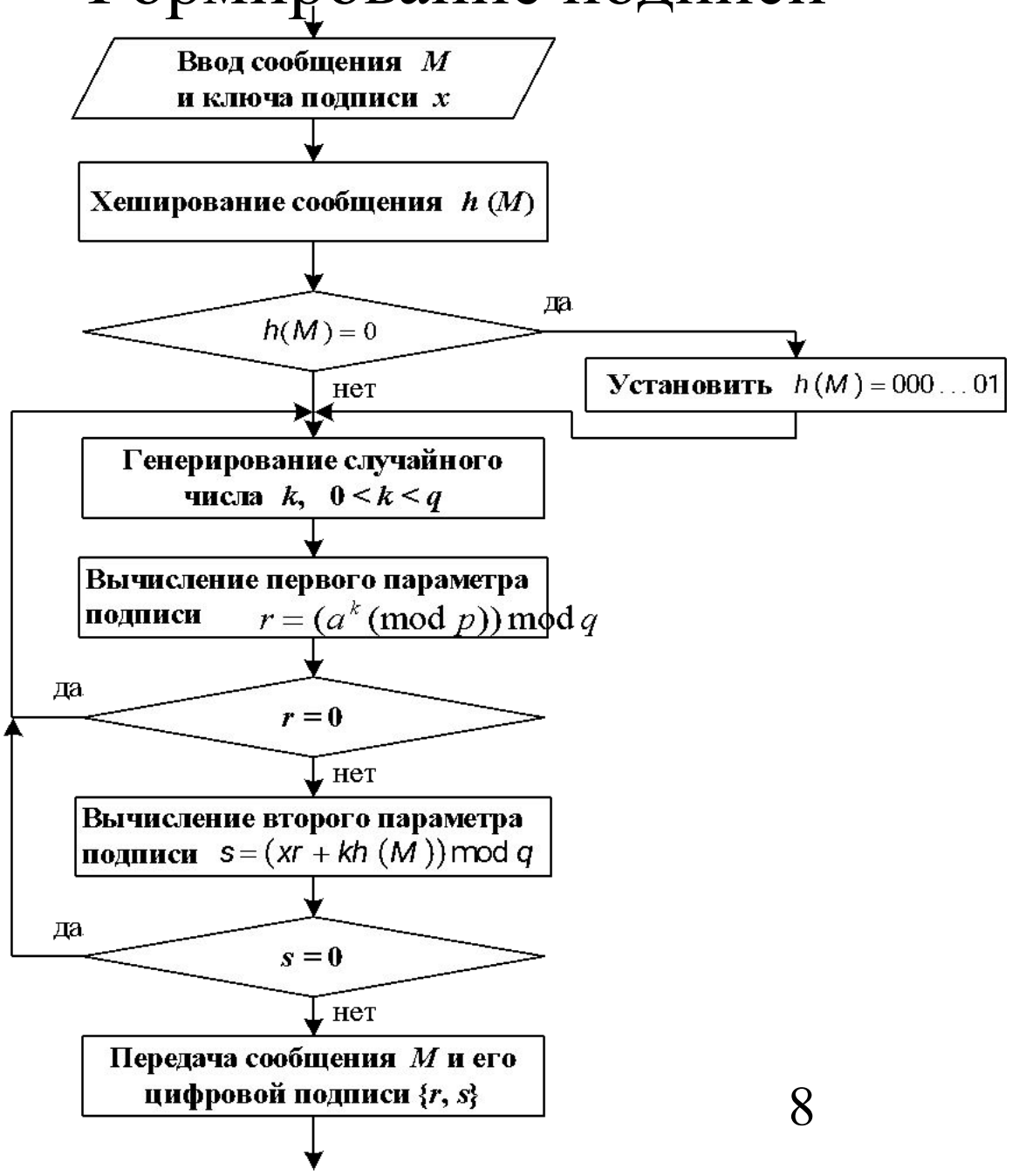
6

2.Формирование цифровой подписи сообщения.

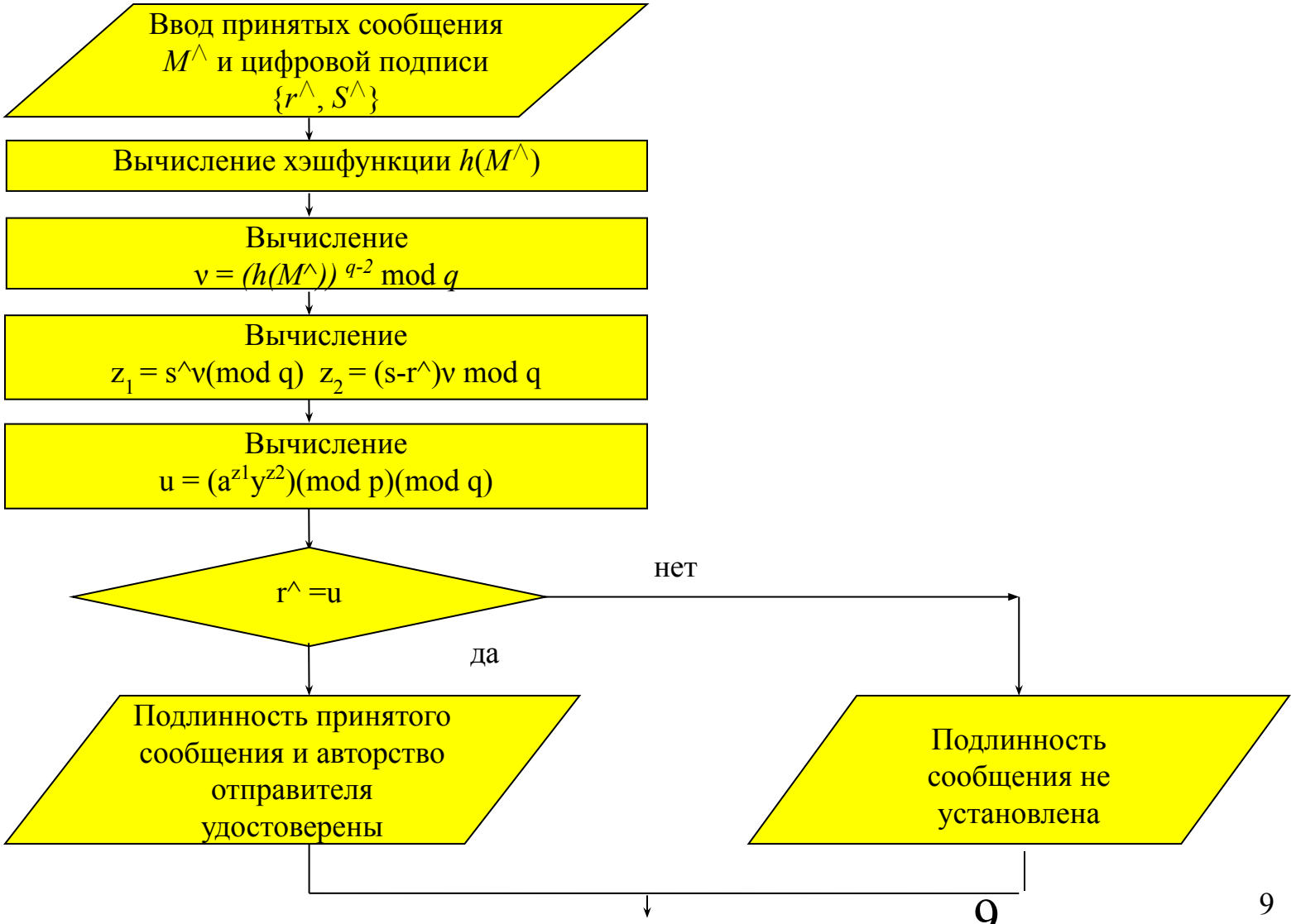


7

Формирование подписи



3. Проверка цифровой подписи сообщения.



9

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.

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);

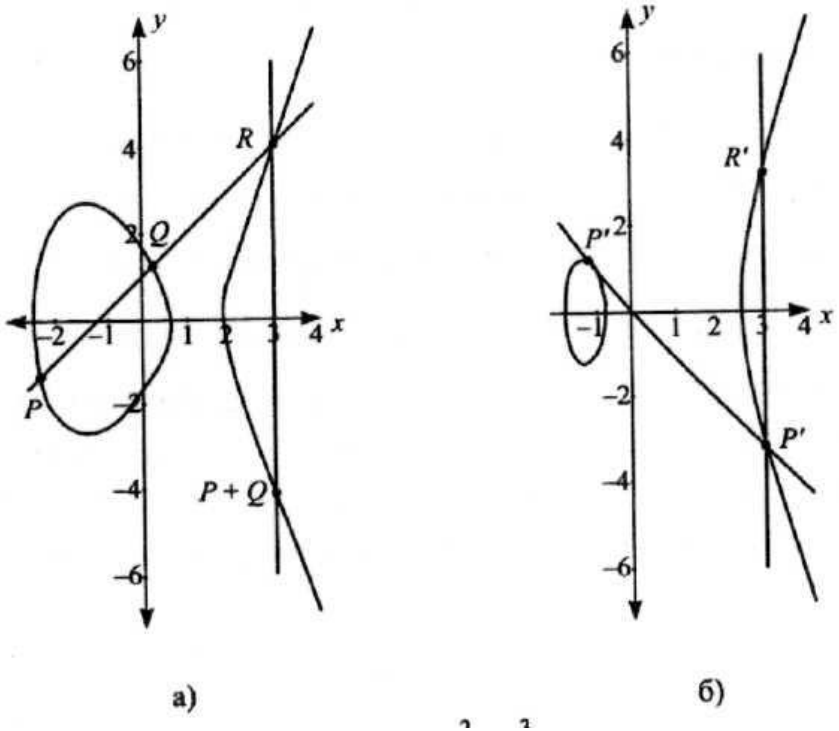
-(α+β)+ γ = α+(β+ γ) ИЛИ (α * β) * γ = α * (β * γ) ;

-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 О.

Операции сложения

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

$X_3=\lambda^2-X_1-X_2$ $Y_3=\lambda(X_1-X_3-Y_1)$

$\lambda=(Y_2-Y_1)/(X_2-X_1)$, если $P\neq Q$ $\lambda=3((X_1)^2+a)/2Y_1$, если $P=Q$

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.

Генерирование ключей

Выбираются общесистемные параметры:

-общий для всех корреспондентов модуль $p > 2^{255}$,

-эллиптическая кривая E, удовлетворяющая уравнению

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

-простое число q, $2^{254} < q < 2^{256}$,

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

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 Р34.10-01

1. Заверяемое сообщение сначала хэшируется с использованием
хэш-функции по ГОСТ Р34.11-94.
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
$s = (r\,d + k\,h\,(M)) \pmod q$.

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

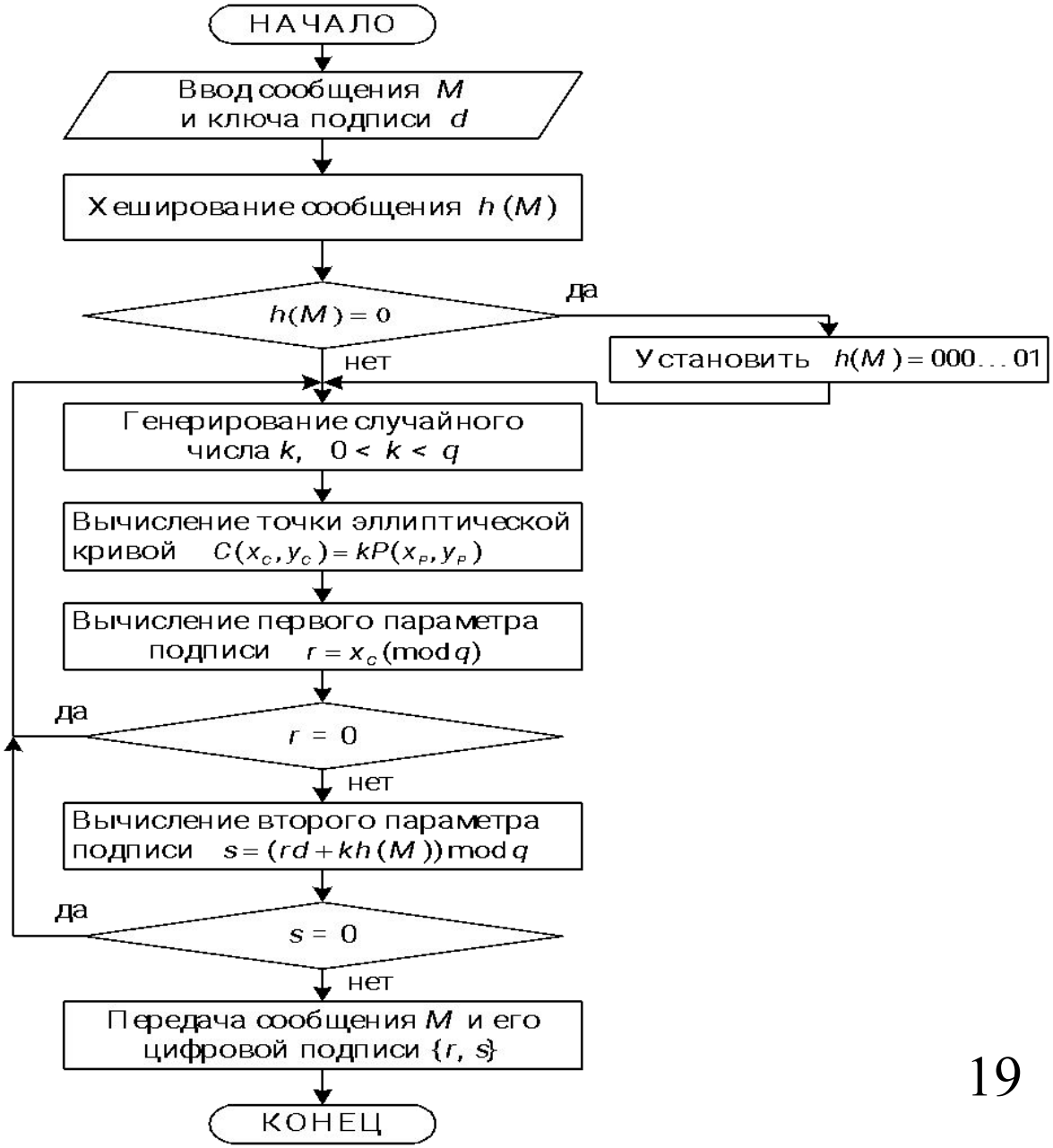
$$R = x_C \pmod q$$

5. Проверяется выполнение равенства

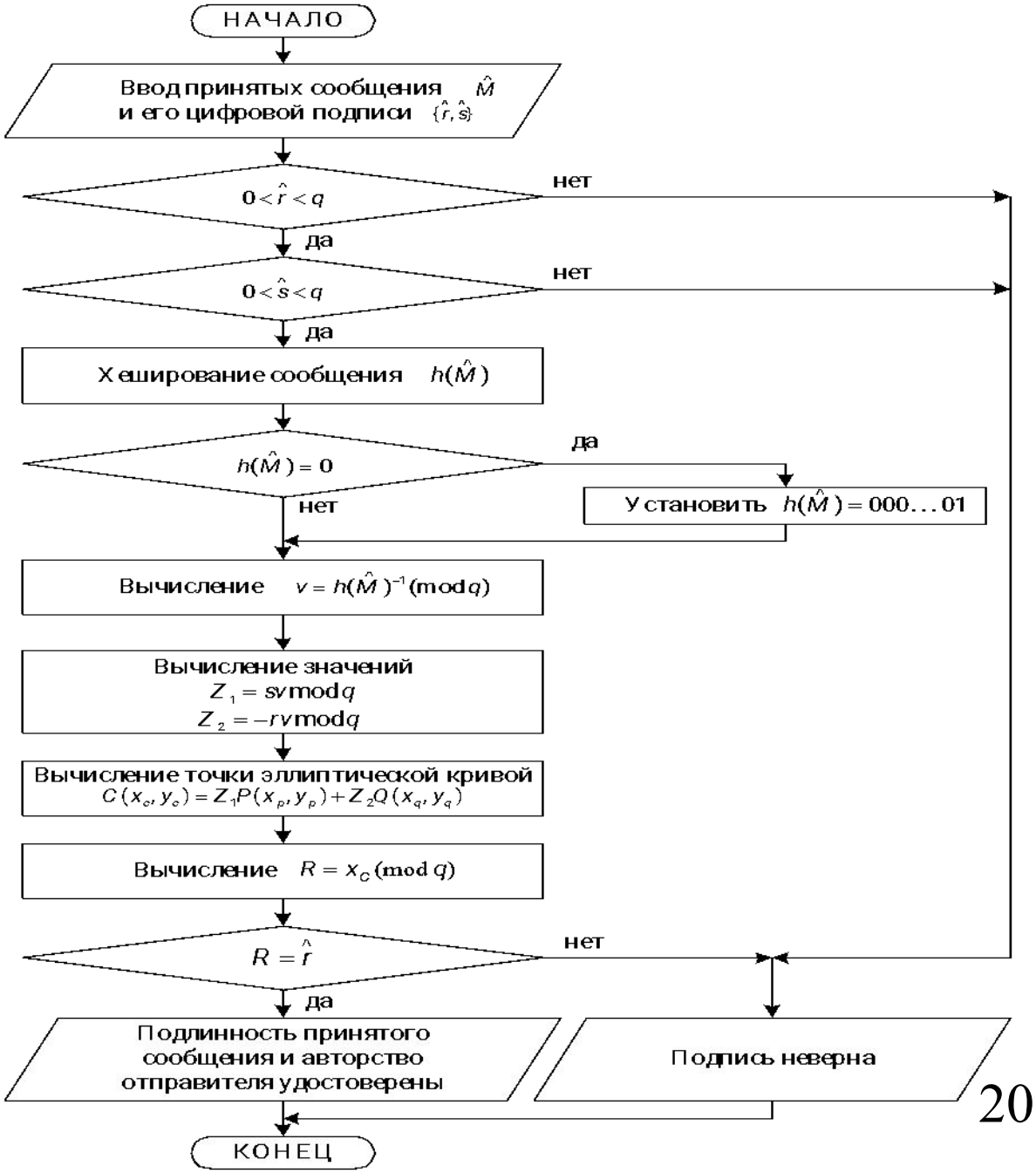
$$R = \hat{r}$$

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

Формирование подписи в ГОСТ Р34.10-01



Проверка подписи в ГОСТ Р34.10-01



Сравнение схем ЭЦП по Эль Гамалю и на ЭК

Схема подписи	ЭЦП Эль-Гамаля	ЭЦП на эллиптической кривой
Общесистемные параметры	p	p
	q	q
	a- образующий подгруппы $a^q=1(modp)$	P – базовая точка qP=O
Генерирование ключей	x – случайное число, закрытый ключ	d – случайное число, закрытый ключ
	$y=a^x(modp)$ – открытый ключ (число)	Q=dP - открытый ключ (точка ЭК)
Нахождение хэш-функции	m=h(M)	m=h(M)
Формированин подписи	Генерирование СЧ k $r1=a^k(modp)$, r=r1(modq)- первая часть подписи s=(xr+km)(modq)- вторая часть подписи	Генерирование СЧ k kP= $r=x_C(modq)$- первая часть подписи, s=(dr+km)(modq)- вторая часть подписи
Нахождение хэш-функции	m=h(M)	m=h(M)
Проверка подписи	u=r? $u=a^{z1}y^{z2}(modp)(modq)=$ z1=sv(modq), z2=(q-r)v(modq $v=m^{q-2}(modq)$	R=r? $R=x_C(modq)$, x_C – абсцисса точки ЭК $C(x_C,y_C)=z_1P+z_2Q$ z1=sv(modq), z2=(q-r)v(modq

Гибридные системы шифрования