7 семестр
Основы криптографии с открытыми ключами (ОКОК)
(для групп ИКТЗ)

Лекции – 20 часов,
Практические занятия (лабораторные работы)- 30 часов
Зачет

7 семестр

Криптопротоколы (КП)
(для групп ИКБ, ИКС)

Лекции – 20 часов,
Практические занятия
(лабораторные работы)- 30 часов
Зачет

Лекция
Криптосистемы на эллиптических кривых
Стандарты цифровой подписи на основе эллиптических кривых

1. **Криптографические системы на эллиптических кривых**

1.1 Математический базис КС на эллиптических кривых

-Понятия группы и поля

Изучено в прошлом семестре

- Модульная арифметика
- Алгоритм Евклида. Расширенный алгоритм Евклида (нахождение обратного элемента по модулю)
- Теоремы Эйлера и Ферма
- Методы быстрого возведения в степень
- Понятие односторонней функции
- Системы с открытыми ключами Эль-Гамаля и РША)

Понятие группы

Группой G называется множество элементов α,β,γ…обладающее,
1. Определена некоторая операция двух переменных,
$\alpha+\beta=\gamma$ (операция сложения) или $\alpha*\beta=\gamma$ (операция умножения).
2. Свойство замкнутости
В результате применения операции к двум элементам группы также получается элемент этой группы G;
3. Свойство ассоциативности (не имеет значения в каком порядке применяется операция группы)
$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$ или $(\alpha*\beta)*\gamma=\alpha*(\beta*\gamma)$;
3. В группе существует единичный (нейтральный) элемент, который обозначается как 0 для сложения и как 1 для умножения. То есть для любого элемента группы справедливо $0+\alpha=\alpha+0=\alpha$ или $1*\alpha=\alpha*1=\alpha$;
4. Каждый элемент группы обладает обратным элементом, который обозначается как $-\alpha$ для сложения, при этом $\alpha+(-\alpha)=0$, или как α^{-1} для умножения, при этом $\alpha*\alpha^{-1}=1$.

5. Если $\alpha+\beta=\beta+\alpha$ или $\alpha*\beta=\beta*\alpha$, то группа называется абелевой,

6. Число элементов в группе называется порядком группы.

Примеры группы

Аддитивная группа - группа с операцией сложения.

1. Множество целых чисел
2. Множество всех четных чисел
3. Множество рациональных чисел.

Мультипликативная группа.

1. Множество положительных действительных чисел

Элементы в группе могут быть числами, полиномами, матрицами и другими объектами; они могут быть также правилами, отображениями. функциями, действиями.

1.2 Элементы теории конечных полей

Определение. *Конечным полем* ($GF(q)$ - *полем Галуа*) называют конечное произвольное множество элементов с заданными между ними операциями сложения, умножения и деления. Эти операции обладают следующими свойствами:

1. $\forall a,b \in GF(q)$ $a+b \in GF(q)$;
2. $\forall a,b \in GF(q)$, $a \cdot b \in GF(q)$;
3. $a+b=b+a$;
4. $a \cdot b = b \cdot a$;
5. $(a+b)+c=(a+b)+c=a+b+c$;
6. $a \cdot (b+c) = a \cdot b + a \cdot c$;
7. $\exists$ элемент «*0*» $\in GF(q)$, $a+O=a$, $\forall a \in GF(q)$
8. $\exists$ элемент «-*a*» $\in GF(q)$, такой, что $a+(-a)=O$, $\forall a \in GF(q)$
9. $\exists$ элемент «*e*» $\in GF(q)$, $a \cdot e = a$, $\forall a \in GF(q)$
10. $\forall a \in GF(q)$, $a \neq 0$, $\exists a^{-1} : a \cdot a^{-1} = e$

Определение 2. *Характеристикой «p»* конечного поля $GF(q)$ называют наименьшее натуральное число, такое, что: $e \cdot p = \underbrace{e + e + e + \ldots + e}_{p} = 0$.

Характеристика любого конечного поля всегда будет простым числом.

Пусть $a, b \in GF(p^n)$, тогда $(a+b)^p = a^p + b^p$.

Утверждение 1. В любом конечном поле $GF(q)$ характеристики «*p*», существует *простое подполе* $GF(p)$, включенное в $GF(q)$.

Утверждение 2. *Всякое конечное поле может содержать число элементов равное только целой неотрицательной степени простого числа.*

Например, число элементов поля может быть: $q = 2, 3, 4, 5, 7, 8, 9, 11, 13, \ldots$ и не может быть: $q = 6, 10, 12, 15, \ldots$

Пример:

$p = 5$; $GF(5)$={ 0,1,2,3,4}; все операции выполняется по $\bmod 5$

Мы можем составить для поля *GF(5)* следующие таблицы сложения и умножения:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

а) сложение

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

б) умножение

Таблица 1. Действия в поле GF(5).

Построение конечного поля с элементами в виде двоичных последовательностей

Рассмотрим множество всех последовательностей длины n, каждая позиция которой принимает любое значение из множества $(0, \ldots, p-1)$. Тогда общее число последовательностей будет, очевидно, равно $q = p^n$.

Пример. Поле $GF(2^3)$. Тогда $n = 3$ и получаем следующие элементы поля $GF(2^3)$ в виде 8 двоичных последовательностей:

000, 001, 010=α, 011, 100, 101=β, 110, 111=γ

Определим сложение и вычитание на этом множестве последовательностей, как покомпонентное сложение по модулю p, то есть: $\alpha + \beta = 010 \oplus 101 = 111 = \gamma$.

Ноль в таком поле это нулевая последовательность - 000.

Однако для задания умножения и деления на множестве этих последовательностей нам потребуется дополнительное определение.

Далее будем отождествлять последовательности длины n с многочленами, коэффициенты которых соответствуют номерам позиций (значениям разрядов последовательностей):

$00000 \to 0$

$00\ldots1 \to 1$

$00\ldots10 \to x$

$11\ldots1 \to x^{n-1} + x^{n-2} + \ldots + 1$

Так для поля $GF\left(2^3\right)$ получаем:

0	000	0
1	001	1
2	010	x
3	011	$x+1$
4	100	x^2
5	101	x^2+1
6	110	x^2+x
7	111	x^2+x+1
последовательности		многочлены

Соответствие последовательностей и многочленов в поле GF(2^3)

Определим операции умножения между элементами поля $GF\left(p^n\right)$ как перемножение соответствующих этим элементам многочленов с приведением результатов по модулю любого неприводимого многочлена $f\left(x\right)$ степени n.

Приведенный по модулю $f(x)$ многочлен равен остатку от деления этого многочлена на *f(x)*.

Пример.

Рассмотрим поле $GF(2^3)$ и неприводимый многочлен $f(x) = x^3 + x + 1$ и перемножим элементы поля:

$\alpha = 110 \Rightarrow x^2 + x$

$\beta = 111 \Rightarrow x^2 + x + 1$

$\alpha \cdot \beta = x^4 + \cancel{x^3} + \cancel{x^3} + \cancel{x^2} + \cancel{x^2} + x = x^4 + x$

$$
\begin{array}{l|l}
x^4 + x & x^3 + x + 1 \\ \cline{2-2}
x^4 + x^2 + x & x \\ \hline
x^2 & \\ \hline
\alpha\beta = x^2 = 100 &
\end{array}
$$

Легко проверить, что такое определение сложения, вычитания и умножения между элементами поля соответствует всем аксиомам, которые предъявляются к конечным полям. Можно выполнить и деление на ненулевой элемент поля, что эквивалентно умножению на обратный элемент поля.

Основные свойства конечных полей

Определение 3. *Порядком* e элемента конечного поля $\alpha \in GF(q)$, называется наименьшее, целое, положительное число, такое, что $\alpha^e = 1$. Очевидно, что порядок любого элемента конечного поля всегда будет конечен.

В поле, $GF(q)$ порядок e любого элемента α делит $q-1$.

Определение 4. Элемент α, принадлежащий конечному полю $GF(q)$ называется *примитивным*, если его порядок равен $q-1$.

Ясно, что степени примитивного элемента $\alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^{q-1} = 1$ образуют все элементы поля, за исключение нуля.

Каждое конечное поле $GF(q)$ содержит хотя бы один примитивный элемент.

2. Криптосистемы на основе эллиптических кривых

Виды ЭК

- гладкие эллиптические кривые;
- сингулярные эллиптические кривые;
- суперсингулярные и несуперсингулярные эллиптические кривые.

2.1 Эллиптические кривые в вещественных числах

Эллиптические кривые в поле вещественных чисел используют специальный класс формы эллиптических кривых:

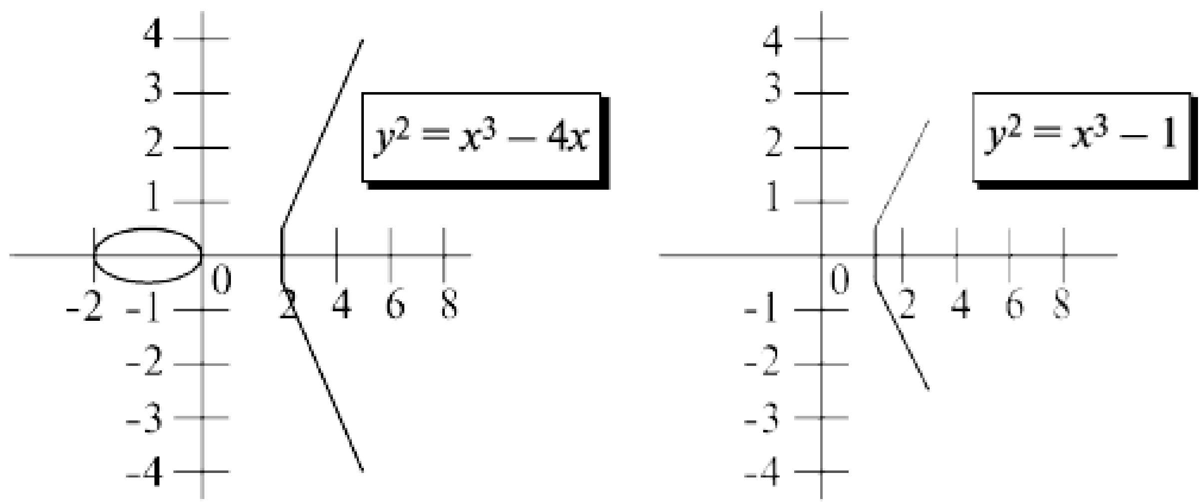
$$y^2 = x^3 + ax + b$$

В этом случае, если $4a^3 + 27b^2 \neq 0$, уравнение представляет несингулярную **эллиптическую кривую**; в противоположном случае оно описывает **сингулярную эллиптическую кривую**.

В уравнении, как мы можем видеть, левая сторона (y^2) имеет степень 2, в то время как правая сторона имеет степень 3 (x^3). Это означает, что горизонтальная линия может пересекать кривую в трех точках, если все корни вещественные. Однако вертикальная линия может пересечь кривую самое большее в двух точках.

ЭК обозначается E(a,b)

Рисунок показывает две эллиптические кривые с уравнениями $y^2 = x^3 - 4x$ и $y^2 = x^3 - 1$. Оба уравнения несингулярны. Однако первое имеет три вещественных корня ($x = -2$, $x = 0$, и $x = 2$), но второе — только один вещественный корень ($x = 1$) и два мнимых.



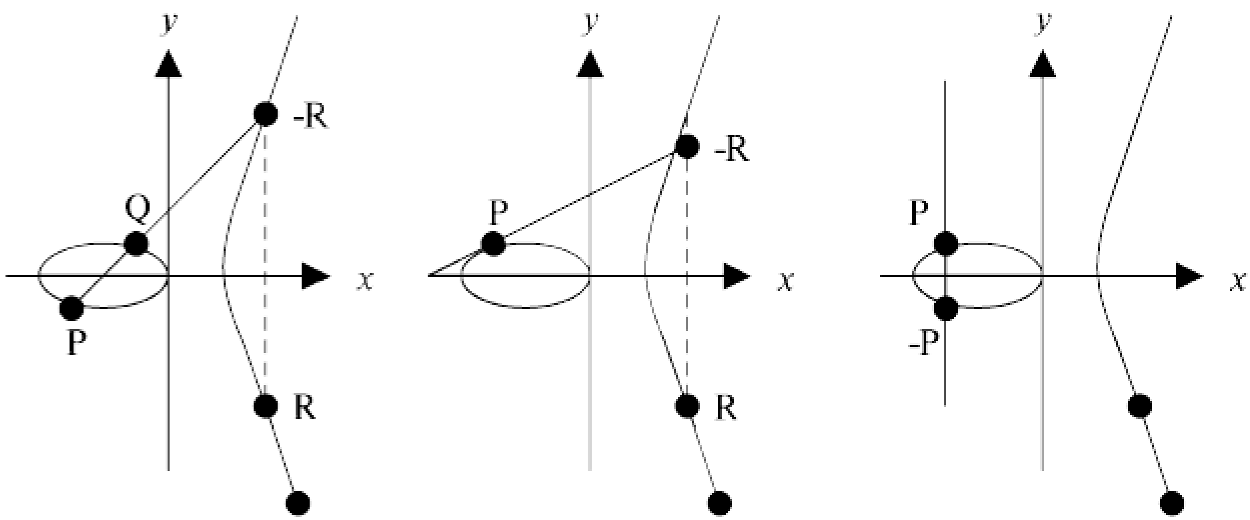
а. Три вещественных корня

b. Один вещественный корень и два мнимых корня

Операция сложения точек на кривой

Операция сложения двух точек на кривой проводится так, чтобы получить другую точку на кривой

R = P + Q, где P = (x1, y1), Q = (x2, y2), и R = (x3, y3)



a. (R = P +Q) b. (R = P + P) c. (O = P + (-P))

2.2 Эллиптические кривые в поле GF(p)

Эллиптическая кривая $E_p(a,b)$ задается уравнением

$$y^2 = x^3 + ax + b$$

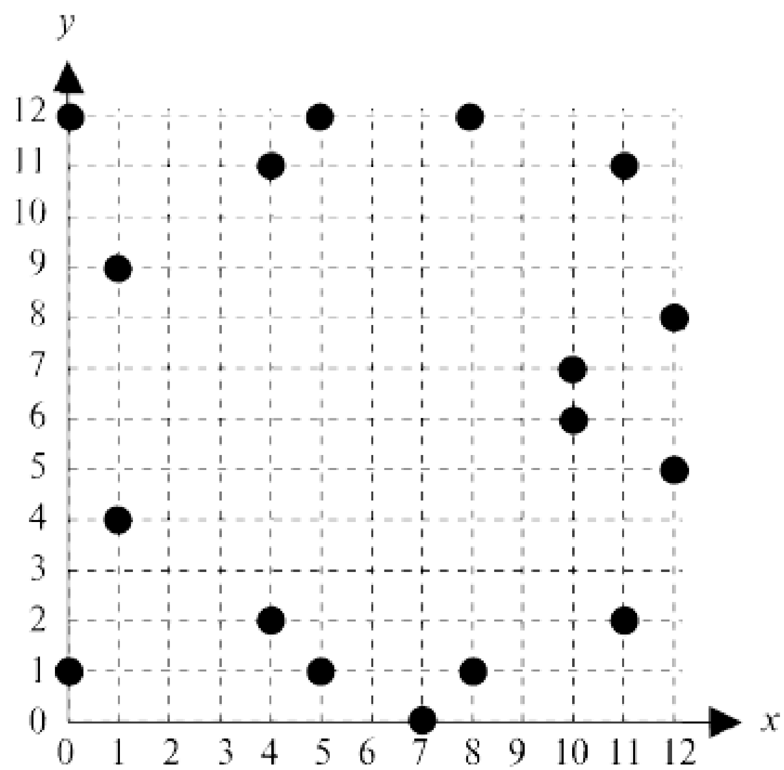
где a и b элемент поля GF(p). То есть операция сложения координат точек выполняется по модулю p.

Точки на кривой не представляют графа, как было в поле рациональных чисел.

Пример кривой $E_{13}(1,1)$ по уравнению $y^2 = x^3 + x + 1$

(0,1)	(0,12)
(1,4)	(1,9)
(4,2)	(4,11)
(5,1)	(5,12)
(7,0)	(7,0)
(8,1)	(8,12)
(10,6)	(10,7)
(11,2)	(11,11)

Точки



Граф

Замечания:

а. Некоторые значения y^2 не имеют квадратного корня по модулю 13. Они не являются точками на этой эллиптической кривой. Например, точки $x = 2$, $x = 3$, $x = 6$ и $x = 9$ не находятся на кривой.

б. Каждая точка, определенная на кривой, имеет инверсию. Инверсии перечислены как пары. Заметим, что (7, 0) — инверсия самой себя.

Правило сложения

Точки на эллиптической кривой образуют группу с операцией специфического сложения, определяемого следующими соотношениями

P = (x1, y1), Q = (x2, y2),

1-й случай $P \neq Q$

$$\lambda = (y_2 - y_1)/\,(x_2 - x_1)$$

$$x_3 = \lambda^2 - x_2 - x_1 \qquad y_3 = \lambda\,(x_1 - x_3) - y_1$$

2-й случай $P = Q$

$$\lambda = (3x_1^2 - a)\,/2\,y_1$$

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda\,(x_1 - x_3) - y_1$$

Все операции нужно выполнять по модулю *p* !

3-й случай. Точки P и Q инверсны друг другу:

$P=(x_1, y_1)$ $Q=(x_1,-y_1)$ тогда $P+Q=0$,

где 0- нулевая точка или точка в бесконечности.

Точка 0 является аддитивным нулевым элементом группы.

Примеры

Сложение двух точек

Мы используем группу эллиптической кривой, определенную ранее, но вычисления сделаны в GF (p). Вместо вычитания и деления мы применяем аддитивные и мультипликативные инверсии.

Сложим две точки , R = P + Q, где P = (4, 2) и Q = (10,6).

а. $\lambda = (6 - 2) \times (10 - 4)^{-1} \bmod 13 = 4 \times 6^{-1} \bmod 13 = 5 \bmod 13$.

б. $x = (5^2 - 4 - 10) \bmod 13 = 11 \bmod 13$.

в. $y = [5\,(4 - 11) - 2] \bmod 13 = 2 \bmod 13$.

г . R = (11, 2) является точкой на кривой

Умножение точки на константу

В арифметике умножение числа на константу *k* означает прибавление числа само к себе *k* раз. Здесь ситуация та же самая. Умножение точки P на эллиптической кривой *на* константу *k* означает прибавление точки P к себе *k* раз. Например, в $E_{13}(1, 1)$, если точка (1, 4) умножается на 4, результат есть точка (5, 1). Если точка (8,1) умножается на 3, результат — точка (10, 7).

- Умножение точки P на число k условно называют «возведением точки в k-ю степень» при этом понимают k кратное сложение точки с самой собой. $P + P + \cdots + P = P^k$,
- А обратную операцию: нахождение показателя степени k по известному значению точки P^k, условно называют логарифмированием точки на эллиптической кривой.
- Для возведения в степень можно использовать «быстрый алгоритм», подобный быстрому возведению в степень числа по модулю

ПРИМЕР. Найти Z=171P, где P$\in$E
Представим 171 в виде степеней числа 2: 171=128+32+8+2+1 или
Z=171P=128P+32P+8P+2P+P

- Для нахождения точек iP составим таблицу : 2P=P+P

  4P=2P+2P, 8P=4P+4P,

  16P=8P+8P, 32P=16P+16P^

  64P=32P+32P, 128P=64P+64P,

в которой каждая новая точка получается удвоением предыдущей.

Система шифрования Эль-Гамаля 1985г.

Пусть p -простое число; a - примитивный элемент.

Корреспондент A

Корреспондент B

Создание пары: закрытый-открытый ключи

A - генерирует число x_A, вычисляет ОНФ

$y_A = a^x \pmod p$.

(SK= x_A , PK= y_A).

y_A передается корр. B.

Шифрование сообщения

Пусть корр. B хочет послать корр.A сообщение $m<p$.

Генерирует случайное число $k<p$.

Формирует криптограмму $E=(c_1 c_2)$

$c_1 = a^k \bmod p$, $c_2 = m \cdot (y_A^{-1})^k \bmod p$.

Отправляет E корр. A.

Система шифрования Эль-Гамаля

Расшифрование сообщения.

Корр.А вычисляет $b=c_1^x \bmod p = a^{kx} \bmod p$,

Затем находит

$(c_2\, b) \bmod p= (m\cdot(y_A^{-1})^k\, a^{kx}) \bmod p= (m\cdot a^{-xk}\, a^{kx}) \bmod p=m$

Замечание.

Как найти y_A^{-1} ?

$y_A^{p-2} \bmod p= y_A^{p-1} \bmod p \cdot y_A^{-1} \bmod p= y_A^{-1} \bmod p$

Криптосистема Эль-Гамаля на эллиптической кривой

Генерирование ключей корр. В:

1. выбирает E (a,b) с эллиптической кривой в GF(p) или GF(2^n).
2. выбирает точку на кривой, e_1 (x_1, y_1).
3. выбирает целое число d.
4. вычисляет e_2 $(x_2, y_2) = d \times e_1$ (x_1, y_1). Обратите внимание: умножение здесь означает многократное сложение точек, которое было определено выше.
5. объявляет E (a,b), e_1 (x_1, y_1) и e_2 (x_2, y_2) как свой открытый ключ ; он сохраняет d как секретный ключ.

Шифрование

Кор.А выбирает P, точку на кривой, как исходный текст, P. Затем он вычисляет пару точек, направляет как зашифрованный текст:

$$C_1 = r \times e_1 \qquad C_2 = P + r \times e_2$$

Расшифрование

Кор.В после получения C_1 и C_2, вычисляет P, исходный текст, используя следующую формулу:

$P = C_2 - (d \times C_1)$ Знак «минус» здесь означает сложение с инверсией.

Доказательство обратимости, выполнения операции расшифрования

$$P + r \times e_2 - (d \times r \times e_1) = P + (r \times d \times e_1) - (r \times d \times e_1) = P + 0 = P$$

P, C_1, C_2 и e_2 — это точки на кривой. Обратите внимание, что результат сложения двух обратных точек на кривой — *нулевая точка*.

Пример построения системы Эль-Гамаля на эллиптической кривой

- 1.Кор. В выбирает ЭК $E_{67}(2,3)$ над GF(p).
- 2. Кор.В вычисляет e1=(2,22) и SK d=4.
- 3. Кор.В вычисляет e2=d*e1=(13,45).
- 4. Кор.В объявляет (E, e1, e2)-открытым ключем. d- закрытый ключ, его знает только В.
- 5. Кор.А хочет передать сообщение P=(24,26) кор.В. Он выбирает СЧ r=2.
- 6. кор.А находит точку C1=r*e1=(35,1).
- 7. Кор.А находит точку C2=P+C1=(21,44). Отправляет C1 и C2 кор. В.
- 8. Кор.В получает C1, C2, находит d*C1=(23,42).
- 9. Кор. В инвертирует (23,42), находит точку (23,42).
- 10. Кор.В складывает (23,42) с C2(21,44) получает первоначальное сообщение (24,26).

Выводы

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? (Сравните $y = a^x \bmod p$)

Эта задача называется задачей логарифмирования в группе точек эллиптической кривой. Эта задача во много тысяч раз более сложная чем задача логарифмирования в числовом поле.

3. Стандарт электронной цифровой подписи Р 34.10 -2012г.

Информационная технология.

Криптографическая защита информации.

Процессы выработки и проверки цифровой подписи.

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 34.10-94(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).

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. Процессы выработки и проверки цифровой подписи.
5. ГОСТ Р34.10-2012. Информационная технология. Криптографическая защита информации. Процессы выработки и проверки цифровой подписи.

Основные параметры ЦП ГОСТ Р.34.10-12

- длина подписываемого сообщения неограничена;
- использован стандарт функции хэширования

ГОСТ Р34.11-12 .

- длина подписи в новом стандарте 512 или 1024 бита.
- длина ключа подписи 256 бит или 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 $a,b \in GF(p)$, $4a^3+276b^2 \neq 0(\mathrm{mod}\,p)$;

- 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(/).

37

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, y), вычисляемой по правилу $\boldsymbol{Q = d\,P}$ **.**

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 чисел r и s,

39

Алгоритм проверки подписи

1. Вычисляется значение

$v = h\,(M\wedge)^{-1}\,(\mathrm{mod}\ q)$.

2. Вычисляются два числа:

$z_1 = s\wedge\cdot v\ (\mathrm{mod}\ q)$ и $z_2 = (q - r\wedge)\ v\ (\mathrm{mod}\ q)$.

3. Находится точка C 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

$$R = x_C\ (\mathrm{mod}\ q)$$

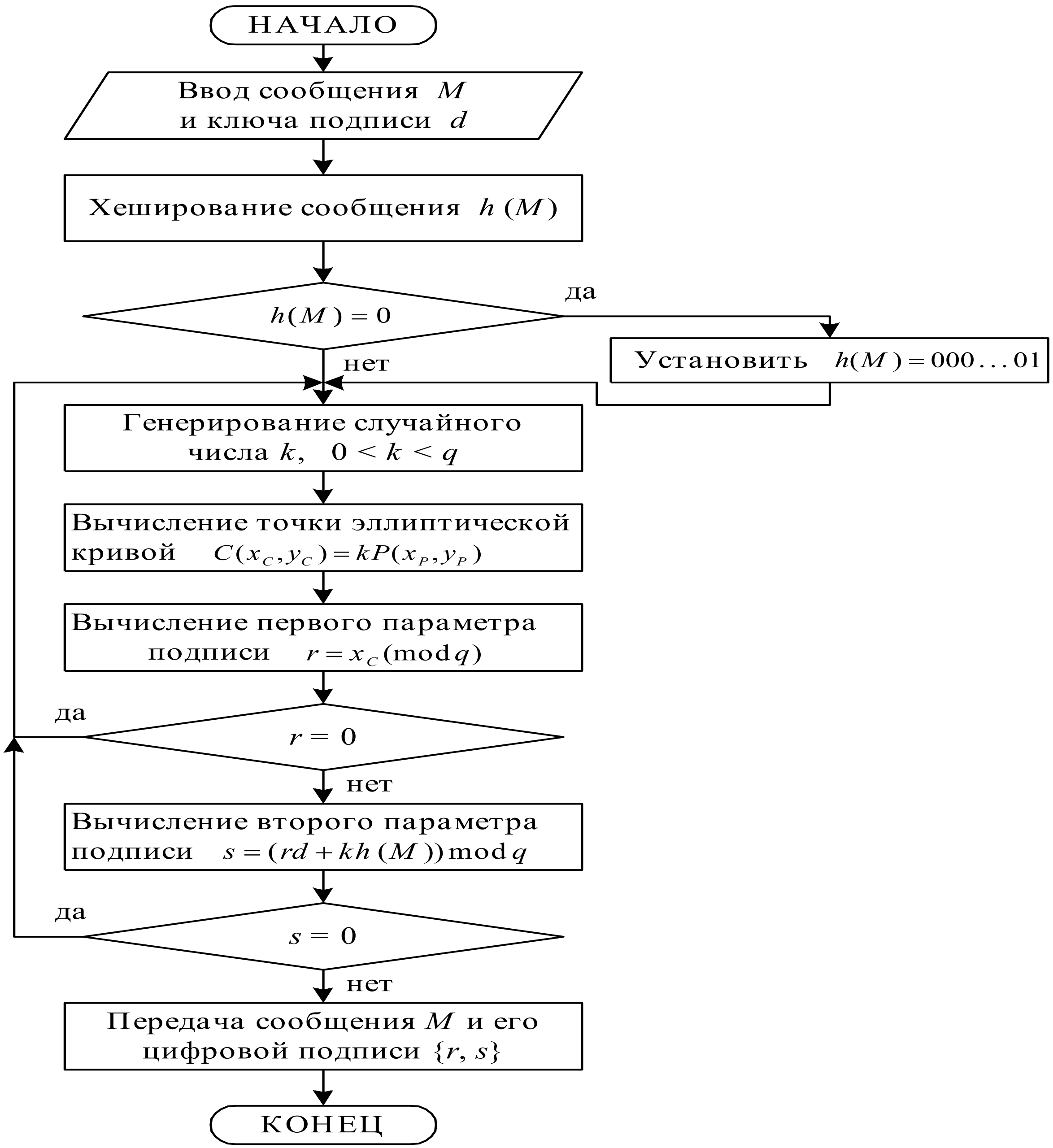
5. Проверяется выполнение равенства

$$R = \widehat{r}\ .$$

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

40

Формирование подписи в ГОСТ Р34.10-12



Проверка подписи в ГОСТ Р34.10-12