# Алгоритмы электронной подписи.
# Схема Эль-Гамаля
# ГОСТ 34.10-2018

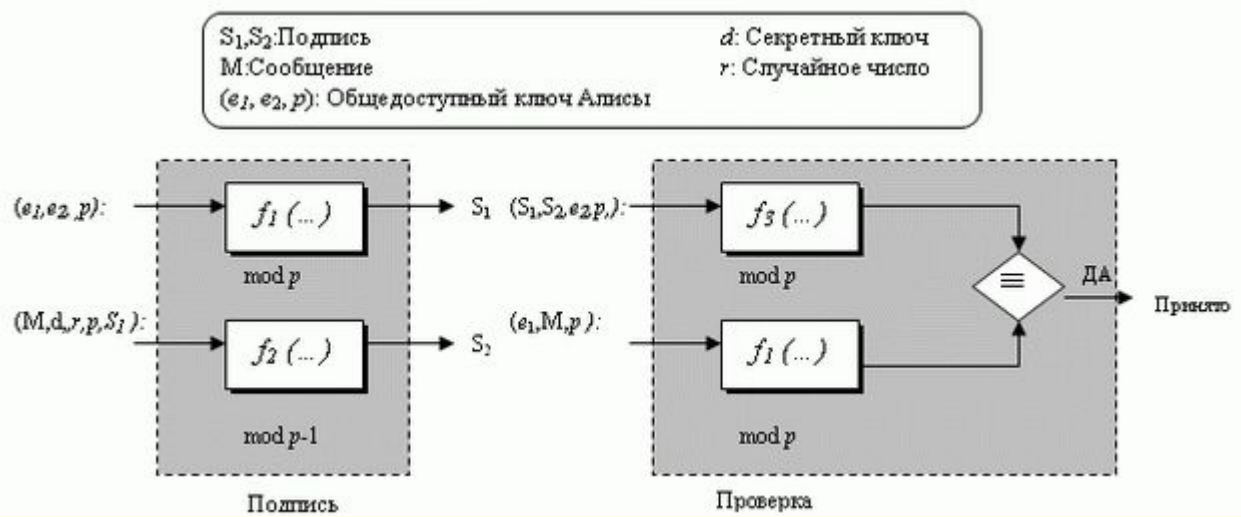
# Схема Эль-Гамаля

- Алгоритм Эль-Гамаля базируется на трудности вычисления дискретного логарифма;

Алгоритм состоит из двух основных этапов:

- формирование цифровой подписи;
- ее проверка на подлинность.

# Схема Эль-Гамаля




В процессе подписания две функции создают две подписи. На стороне подтверждения обрабатывают выходы двух функций и сравнивают между собой для проверки. Одна и та же функция применяется и для подписания, и для проверки, но использует различные входы. Рисунок показывает входы каждой функции. Сообщение - часть входа, для обеспечения функционирования при подписании; оно же - часть входа к функции 1 при подтверждении. Вычисления в функциях 1 и 3 проводятся по модулю p, а функции 2 - по модулю p - 1.

# Генерация ключей

- Выберем достаточно большое простое число p $(\sim 10^{308}$ *или* $\sim 2^{1024})$
- Пусть $e_1$ - простой элемент в $Z_{p^*}$(мультипликативная группа по модулю p).
- Алиса выбирает свой секретный ключ d, чтобы он был меньше, чем p - 1.
- Она вычисляет $e_2 = e_1^d$.

**В *схеме цифровой подписи Эль-Гамаля***

**(e1, e2, p) - открытый ключ Алисы;**

d **-секретный ключ Алисы**.

# Подписание дайджеста

- Алиса выбирает секретное случайное число r (открытые и секретные ключи могут использоваться неоднократно, но для каждого нового сообщения Алиса выбирает новое r);
- Алиса вычисляет первую подпись $S_1 = e1^r \bmod p$.
- Алиса вычисляет вторую подпись $S_2 = (M - d \times S_1) \times r^{-1} \bmod (p - 1)$,где r - мультипликативная инверсия r по модулю p - 1.
- Алиса передает M, $S_1$ и $S_2$ Бобу.

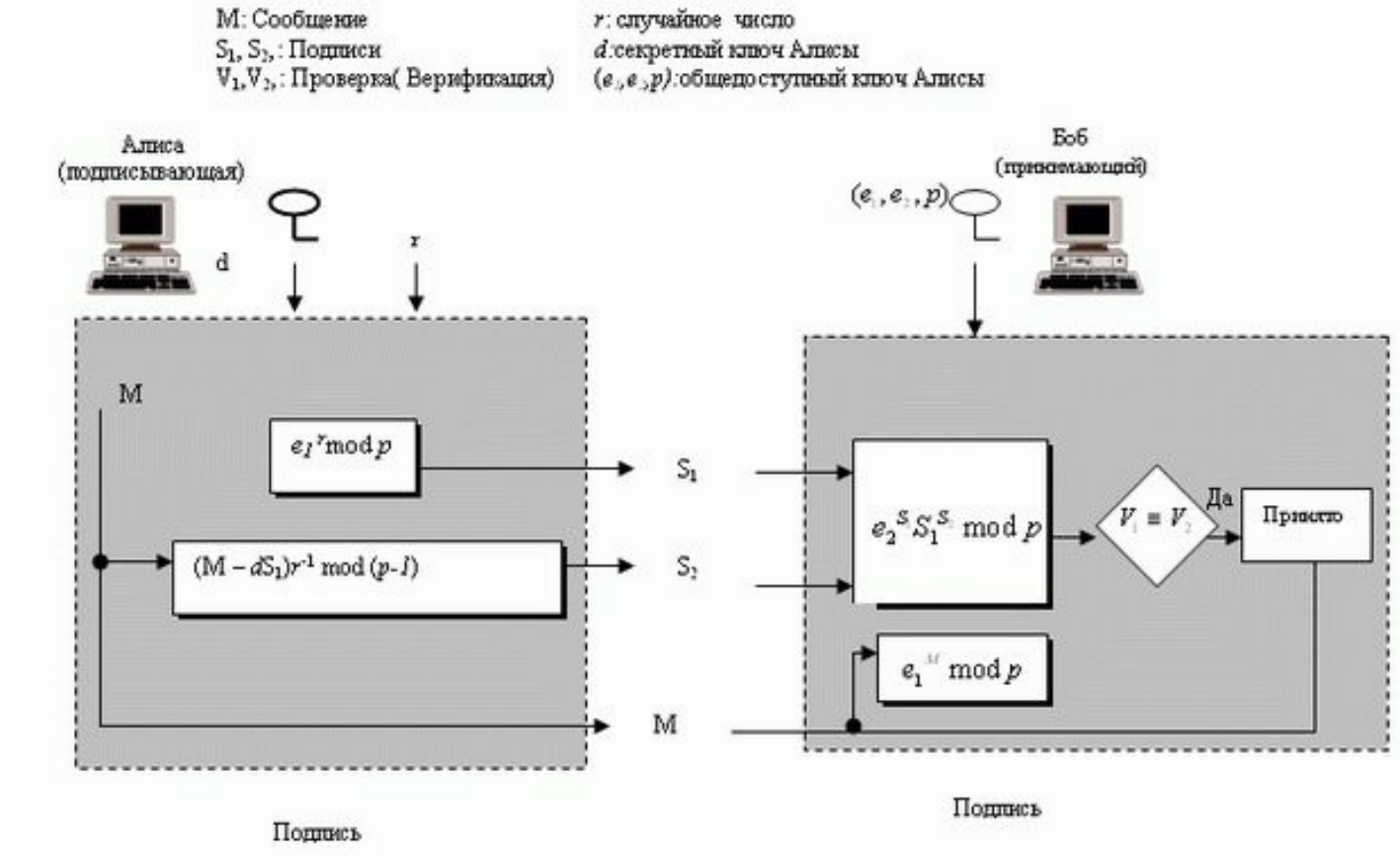
# Проверка

Объект, например Боб, получает M, $S_1$ и $S_2$ и может проверить их следующим образом.

- Боб проверяет, что $0 < S_1 < p$.
- Боб проверяет, что $0 < S_2 < p - 1$.
- Боб вычисляет $V_1 = e_1^M \bmod p$.
- Боб вычисляет $V_2 = e_2^{S1} \times S_1^{S2} \bmod p$.

**Если $V_1$ является конгруэнтным $V_2$, сообщение принято; иначе оно будет отклонено.**

# Схема цифровой подписи Эль-Гамаля



# Пример подписание

- Алиса выбрала p = 3119, $e_1$ = 2, d = 127 и вычислила $e_2 = 2^{127} \bmod 3119 = 1702$. Она выбрала r равным 307. Она объявила $e_1$, $e_2$ и p ; она сохранила в тайне d.
- M = 320
- $S_1 = e_1^r = 2^{307} \bmod 3119 = 2083$
- $S_2 = (M - d \times S_1) \times r^{-1} = (320 - 127 \times 2083) \times 307^{-1} = 2105 \bmod 3118$

# Пример проверка

Алиса передает M, $S_1$ и $S_2$ Бобу. Боб использует открытый ключ, чтобы вычислить, что сообщение подписано Алисой, потому что никто, кроме Алисы, не имеет секретного ключа d.

- $V_1 = e_1^{M} = 2^{320} = 3006 \bmod 3119$;
- $V_2 = d^{S1} \times S_1^{S2} = 1702^{2083} \times 2083^{2105} = 3006 \bmod 3119$.

Поскольку $V_1$ и $V_2$ являются конгруэнтными, Боб принимает сообщение, и он предполагает, что сообщение было подписано Алисой, потому что никто, кроме нее, не имеет секретного ключа Алисы d.

# ГОСТ 34.10-2018

(http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=224247) **ссылка на документ**

- *ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи —*
действующий межгосударственный криптографический ст андарт, описывающий алгоритмы формирования и проверки электронной подписи реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.
- Стандарт разработан на основе национального стандарта Российской Федерации **ГОСТ Р 34.10-2012** и введен в действие с 1 июня 2019
года приказом Росстандарта № 1059-ст от 4 декабря 2018 года.

# ГОСТ 34.10-2018

Механизм цифровой подписи определяется посредством реализации двух основных процессов:

- формирование подписи;
- проверка подписи.

(В настоящем стандарте процесс генерации ключей не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами, которые устанавливают соответствующие параметры по взаимному согласованию.)

# ГОСТ 34.10-2018

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции.

Алгоритмы вычисления хэш-функции установлены в ГОСТ 34.11.

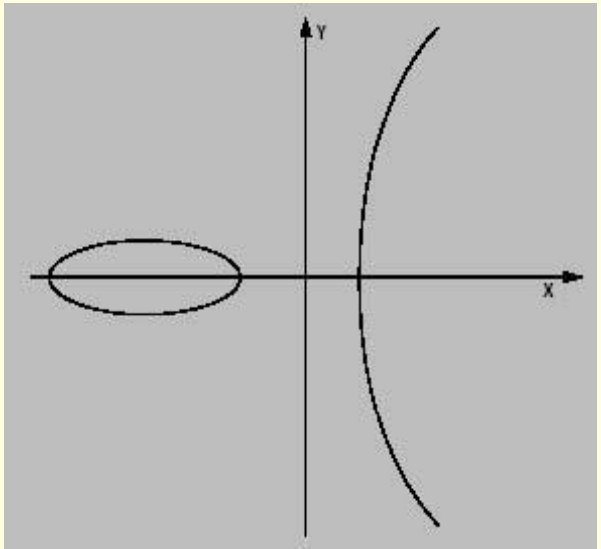
Цифровая подпись, представленная в виде двоичного вектора длиной 512 или 1024 бита

# Криптография на эллиптических кривых

Эллиптической кривой называют множество пар точек (X,Y), удовлетворяющих уравнению:

$y^2 = ax^3 + bx + c$

Можно наложить ограничения на множество значений переменных x, y, и коэффициентов a, b, c. Ограничивая область определения уравнения значимым для приложений числовым множеством (полем) мы получим эллиптическую кривую, заданную над рассматриваемым полем. На рисунке изображен общий вид эллиптической кривой, определенной на множестве действительных чисел.

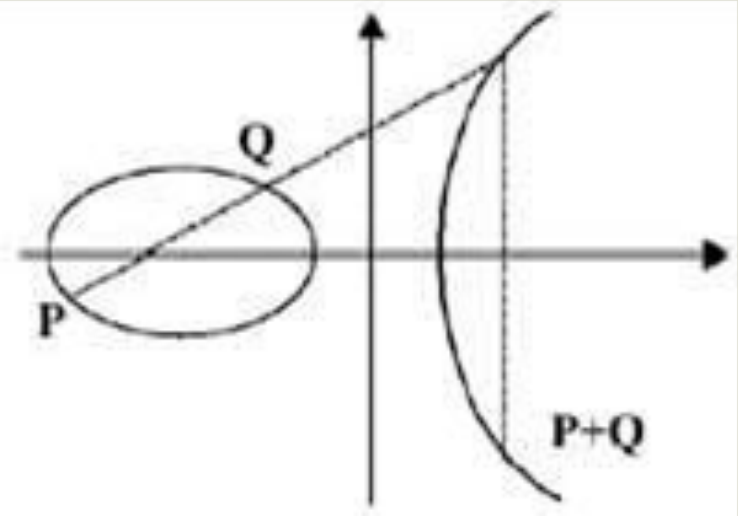


# Криптография на эллиптических кривых

В приложении к криптографии (и в новом стандарте на цифровую подпись) эллиптическая кривая над конечным простым полем GF(p) определяется как множество пар (x,y), таких что x,y ≡ GF(p), удовлетворяющих уравнению:

$y^2 = x^3 + ax + b \bmod p,\ a, b \equiv GF(p)$

Пары (x,y) будем называть точками. Точки эллиптической кривой можно складывать. Сумма двух точек, в свою очередь, тоже лежит на эллиптической кривой.



# Криптография на эллиптических кривых

Математическое свойство, которое делает эллиптические кривые полезными для криптографии, состоит в том, что если взять две различных точки на кривой, то соединяющая их хорда пересечет кривую в третьей точке (так как мы имеем кубическую кривую). Зеркально отразив эту точку по оси X, мы получим еще одну точку на кривой (так как кривая симметрична относительно оси X). Если мы обозначим две первоначальных точки как P и Q, то получим последнюю – отраженную – точку P+Q. Это «сложение» удовлетворяет всем известным алгебраическим правилам для целых чисел.

Кроме точек, лежащих на эллиптической кривой, рассматривается также нулевая точка. Считается, что сумма двух точек – A с координатами $(X_A, Y_A)$ и B с координатами $(X_B, Y_B)$ – равна 0, если $X_A = X_B$, $Y_A = -Y_B \pmod p$. Нулевая точка не лежит на эллиптической кривой, но, тем не менее, участвует в вычислениях. Ее можно рассматривать как бесконечно удаленную точку.

# Криптография на эллиптических кривых

Можем определить конечную абелеву группу на точках кривой, где нулем будет являться бесконечно удаленная точка. В частности если точки P и Q совпадут, то можно вычислить P+P, т.е. 2P. Развивая эту идею, можно определить kP для любого целого числа k, и следовательно, определить значение P и значение наименьшего целого числа k, такого, что kP = F, где F – бесконечно удаленная точка.

Кратные точки эллиптической кривой являются аналогом степеней чисел в простом поле. Задача вычисления кратности точки эквивалентна задаче вычисления дискретного логарифма. На сложности вычисления кратности точки эллиптической кривой и основана надежность цифровой подписи.

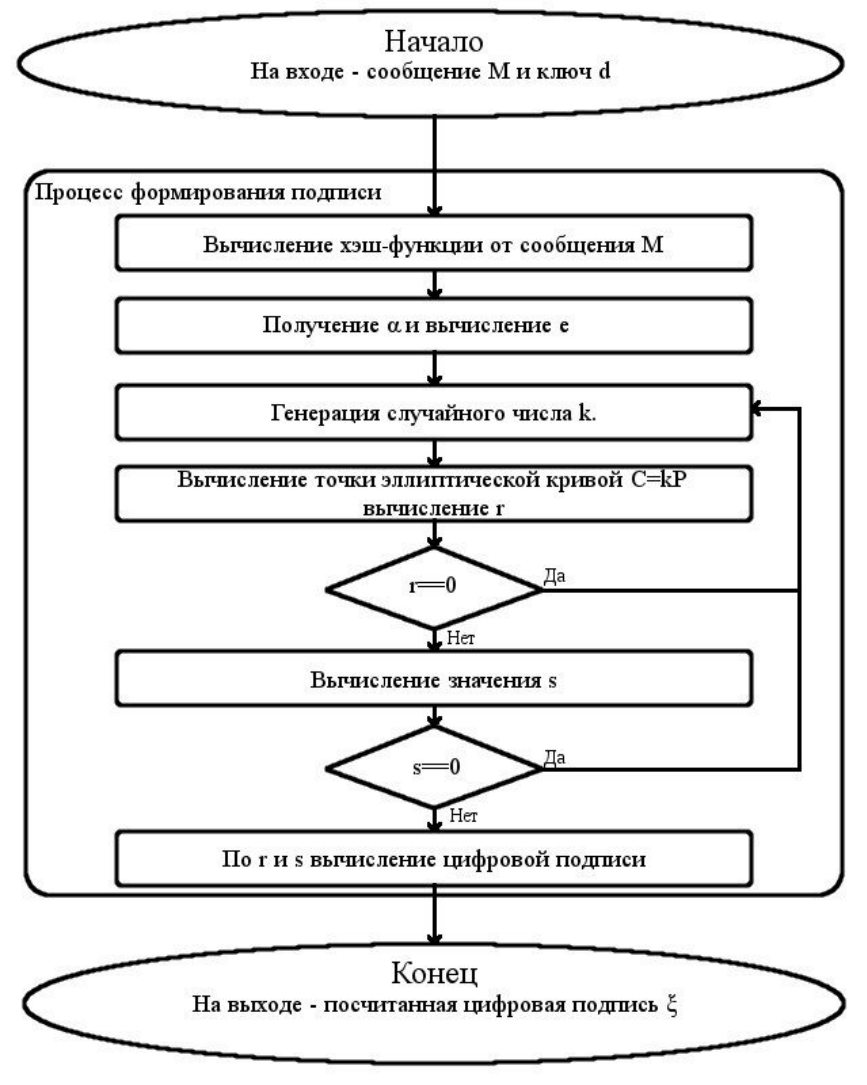
Секретным ключом является некоторое случайное число x. Открытым ключом будем считать координаты точки на эллиптической кривой P, определяемую как P = xQ, где Q — специальным образом выбранная точка эллиптической кривой («базовая точка»). Координаты точки Q вместе с коэффициентами уравнения, задающего кривую, являются параметрами схемы подписи и должны быть известны всем участникам обмена сообщениями.

# Формирование подписи ГОСТ 34.10-2018

Основные шаги:

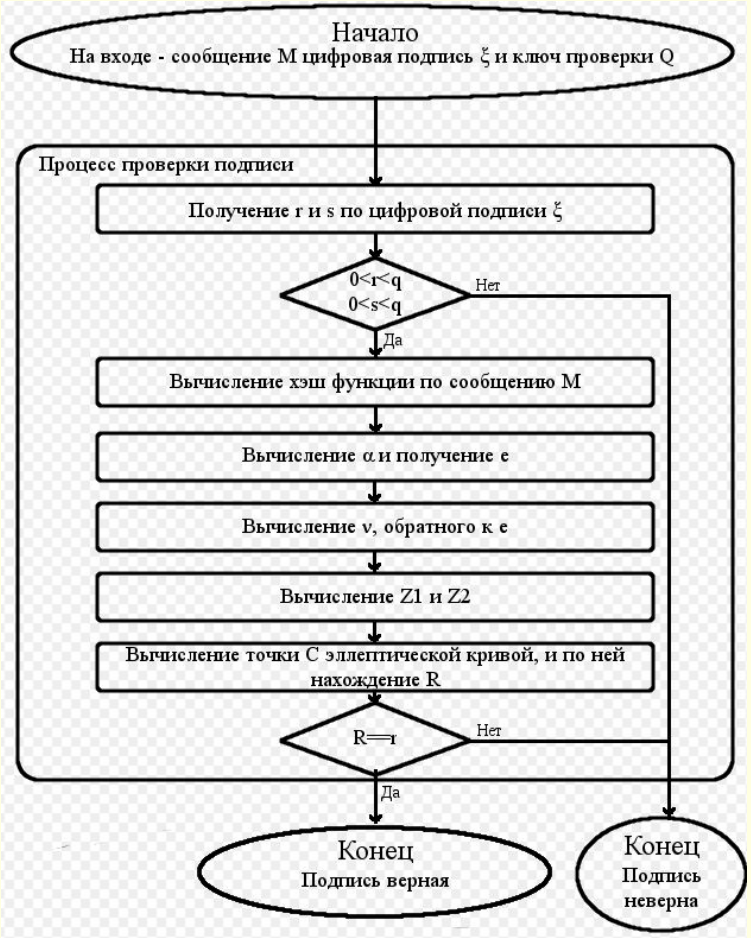
1. Вычисление хэш-функции от сообщения;
2. Генерация случайного числа k (элемента секретного ключа) и вычисление точки эллиптической кривой;
3. Вычисление (на основе полученных данных) двух векторов, их конкатенация и формирование ЭП

# Формирование подписи **ГОСТ 34.10-2018**



# Проверка подписи **ГОСТ 34.10-2018**

Исходными данными этого процесса являются подписанное сообщение, цифровая подпись и ключ проверки подписи (точка эллиптической кривой).



# Задание к лекции

Ознакомиться со стандартами разных лет на ЭП, провести сравнительный анализ, отметить основные отличия и записать в таблицу:

| | ГОСТ Р 34.10-94 | ГОСТ Р 34.10-2001 | ГОСТ Р 34.10-2012 | ГОСТ 34.10-2018 |
|---|---|---|---|---|
| Длина простого числа p (по модулю которого производятся вычисления) | | | | |
| Открытый ключ | | | | |
| Закрытый ключ | | | | |
| Алгоритм формирования | | | | |
| Алгоритм проверки | | | | |
| Криптостойкость | | | | |