# Лабораторная 13

на чем основывается криптостойкость

какие операции над точками

***Эллиптические кривые*** - математический объект, который может быть определен над любым полем.

***Эллиптическая кривая*** над вещественными числами - это множество точек, описываемых уравнением **y^2 = x^3 + ax + b** при этом константы (a и b - вещественные числа) должны удовлетворять условию **4a^2 + 27b^2 !=0**

Частью ЭК является бесконечно удаленная точка которую обозначают символом О

Группа - непустое множество с определённой на нём бинарной операцией, называемой сложением и удовлетворяющей нескольким аксиомам

Группа для ЭК есть непустое множество, элементы которого являются точками ЭК, обладающими ***свойствами***:

* единичный элемент - это бесконечно удаленная точка О
* обратная величина точки R - это точка, симметричная относительно оси x
* сложение - сумма трех ненулевых точек P, Q, -R, лежащих на одной прямой, будет равна P+Q+(-R) = O
* прямая проходящая через точки R и -R явл вертикальной прямой, которая не пересекает ЭК ни в какой третьей точке
* P+Q=R - пусть P и Q - две различные точки ЭК, P не равна Q. Если провести через P и Q прямую, то она пересечет ЭК еще только в одной точке, называемой -R - отображается относительно оси x в точку R, равную сумме точек P и Q: P + Q = R

**Удвоение точки** - если P=Q то P+P=2P

**Принцип умножения точки** P на целое число n это сумма n точек P: nP=P+P+...+P

**Скалярное умножение** осуществляется - комбинацией сложения и удвоения точек ЭК 25P - 2(2(2(2P))) + 2(2(2P)) + P

Каждая точка задается парой координат x и y

Числа x и y - явл рациональными, а точки P, Q, R и -R - рациональные точки

Если Р = (х1, у1) и Q = (х2, у2), то P+Q = (x3,y3)

x3 = λ^2 - x1 - x2

y3 = λ(x1-x3) - y1

λ - угловой коэффициент секущей проведенной через точки P и Q, и касательной при P=Q

λ = (y2-y1)/(x2-x1) - если P!=Q

λ = (3(x1)^2 + a)/2y1 - если P=Q

**Конечное поле** - это множество конечного числа элементов. Примером конечного поля явл множество целых чисел по модулю p, где p - простое число. Операции сложения и умножения работают как в модулярной арифметике

**Эллиптическая кривая над полем Fp** - задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю p : y^2 = x^3 + ax +b (modp)

для упрощения используем знак простого неравенства: 4a^3 + 27b^2 != 0 mod(p)

Если складываем два значения кратных Р, то получим значение кратное Р. Это означает, что множество кратных Р значений - это **циклическая подгруппа**

Наименьшее значение числа q, для которого выполняется равенство qP = O, называется **порядком точки Р**

**Порядок группы точек ЭК** равен числу различных точек ЭК, включая точку О

Точка Р называется **генератором или базовой точкой** циклической подгруппы(такую точку во многих док обозначают G)

Порядок точки Р связан с порядком m ЭК **Теорема Лагранжа,** согласно которой порядок подгруппы - это делитель порядка исходной группы. Иными словами, если ЭК содержит m точек, а одна из подгруппы содержит q, то q является делителем m

## Задача дискретного логарифмирования

Важным явл вычисление некоторого числа d, если мы знаем P и Q для Q=dP

Тайный ключ это случайное число d, выбранное из множества {1, 2, …, q-1}, где q - порядок подгруппы; открытый ключ - это точка Q, такая что Q=dG, g - базовая точка подгруппы

### Генерация ключевой информации на основе ЭК

#### Первый этап: выбор ЭК

1. входные параметры: число l, число p - удовлетворяющее условию 2^2l-1 < p < 2^2l, p=3mod4, 0<a<p
2. выбирается число b такое что 0 < b < p
3. выбирается порядок q и генерирующая точка G, которая задается двумя координатами

#### Второй этап: генерация ключевой информации

1. Входные параметры: p, a, b, q и G
2. Генерируется тайный ключ - число d, выбранное из множества {1, 2, …, q-1}
3. Вычисляется открытый ключ - точка Q: Q=dG (к открытому ключу также относятся p, a, b, q)

### Использование ЭК в криптографии

* алгоритмы согласования (Диффи-Хелмана)
* алгоритмы симметричного шифрования
* алгоритмы генерации/верификации ЭЦП

#### Алгоритм ДХ

Ep - это ЭК на Fp

Q - заранее определенная и согласованная сторонами А и В точка E

* Отправитель - выбирает тайное случайное число kA, вычисляет точку PA=kAQ - и отправляет ее получателю В
* В - действует аналогично: случайным образом выбирает kB, вычисляет PB=kBQ - и отправляет результат А
* Общий ключ P = kAkBQ

#### Зашифрование/расшифрование на основе ЭК

Используем ключи получателя

Сообщение - это точка P ЭК с известной точкой G и известным Q.

Шифртекст - это две точки на той же ЭК: C1 и С2

С1 = kG C2 = P+kQ

Расшифрование P=C2-dC1

#### Реализация ЭЦП на основе ЭК

ИСпользуем ключи отправителя

##### Генерация ЭЦП

1. выбрать число k (1<k<q, q - порядок точки G)
2. вычислить точку kG =(x, y), вычислить r = x mod q, при r = 0, изменить k и выполнить 2 еще раз
3. вычислить t = k^(-1) mod q
4. вычислить s = (t(H(M) + dr)) mod q$ при s = 0 изменить k и повторить алгоритм
5. В отсылается сообщение M и ЭЦП(числа r и s)

##### Верификация ЭЦП

Получатель знает алгоритм хеширования и открытый ключ

1. проверить выполнение условия: 1< r, s< q- если не выполняется легитимность подписи не подтверждается
2. вычисляется H(M) и w=s^(-1) mod q
3. вычисляются u1=wH(M) mod q u2 = wr mod q
4. вычисляется Gu1 + Gu2 = (x’, y’) v = x’ mod q
5. сравнить v и r - если равны подтверждается легитимность подписи и целостность сообщения

# Лабораторная 14

**Стеганографическая система** - совокупность средств и методов, которые используются для формирования скрытого канала передачи(или хранения информации)

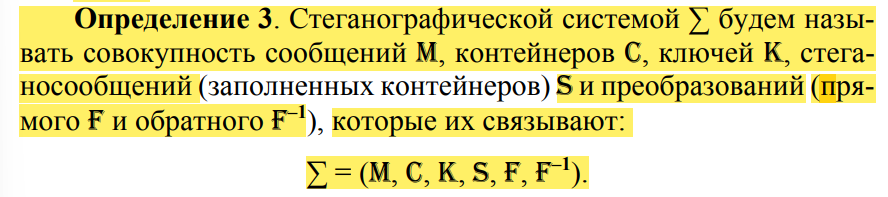
Абстрактно **стеганографическая система** обычно определяется как некоторое множество отображений одного пространства(множество сообщений) в другое пространство(множество стеганосообщений)

## Основные компоненты:

* контейнер С(файл-контейнер) - размещается тайное сообщение
* тайное сообщение - осаждаемое в контейнер для передачи или хранения
* ключи - выполняют ту же функцию что и в криптографии
* контейнер с встроенным сообщением(стеганоконтейнер) - передается по открытому каналу
* субъекты системы: отправитель и получатель

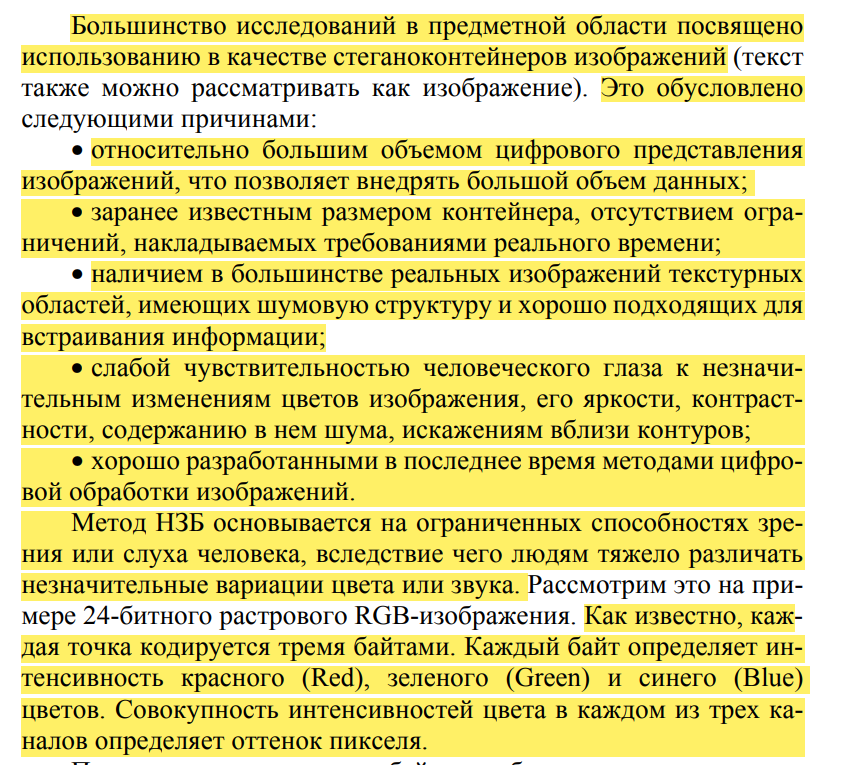
В зависимости ***от формата документа-контейнера*** стеганогравия делится на:

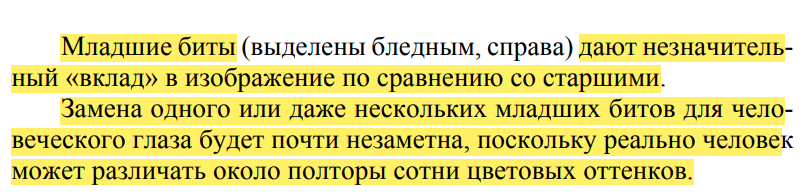
* аудио-
* видео-
* графичкская-
* текстова стеганография и др.



Сущностью системы является тайное хранение или передача одной информации в другой

## Метод НЗБ





##### ВОТ ЭТО УЖЕ НЕ ОСОБО ВАЖНО

