МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №11 НА ТЕМУ:

Исследование криптографических алгоритмов на основе ЭК

Выполнил студент 3 курса 1 группы

Кашперко Василиса Сергеевна

2023 г.

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.

***Теоретические сведения***

*Эллиптические кривые над действительными*

*числами и конечными полями*

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

Частью ЭК является бесконечно удаленная точка (также известная как идеальная точка), которую мы обозначим 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 следующими свойствами:

• единичный элемент – это бесконечно удаленная точка О;

• обратная величина точки R – это точка, симметричная относительно оси Х;

сложение задается следующим правилом: сумма трех ненулевых точек P, Q и –R, лежащих на одной прямой, будет равна

P + Q + (–R) = О.

Законы сложения точек эллиптической кривой:

• прямая, проходящая через точки R и –R, является вертикальной прямой, которая не пересекает ЭК ни в какой третьей точке;

если R = (х, –у), то R + (х, у) = О. Точка (х, у) является отрицательным значением точки R и обозначается –R. Таким образом, по определению R + (–R) = О;

• P + Q = R: пусть P и Q – две различные точки ЭК (рис. 11.1),

и Р не равно Q; если проведем через P и Q прямую, то она пересечет ЭК еще только в одной точке, называемой –R; точка –R отображается относительно оси Х в точку R, равную сумме точек P и Q: P + Q = R.

Необходимо, чтобы вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом.

Конечное поле – это множество конечного числа элементов. Примером конечного поля является множество целых чисел по модулю p, где p – простое число.

Эллиптическая кривая над полем Fp задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю р (mod p): .

Если мы складываем два значения, кратных Р, то получаем значение, кратное Р (т. е. значения, кратные Р, замкнуты относительно операции сложения). Это означает, что множество кратных Р значений – это циклическая подгруппа группы, образованной эллиптической кривой.

Наименьшее значение числа q, для которого выполняется равенство qР = О, называется порядком точки Р.

Порядок группы точек эллиптической кривой равен числу различных точек ЭК, включая точку О.

Точка Р называется генератором или базовой точкой циклической подгруппы (такую точку во многих документах обозначают символом G).

Основная задача при разработке алгоритмов шифрования – получить one way function. Т.е. зная неизвестные (x) некоторые и набор известных параметров (a, b), мы можем получить значение, а обратно, зная это значение и все открытые значения, мы не можем получить неизвестное.

Ход работы

*Вариант 3*

В основе задания лежит эллиптическая кривая вида:

т. е. .

***Задание 1.1***

Мы должны найти точки на эллиптической кривой (ЭК) с заданными значениями x: x\_min = 71, x\_max = 105.

Для начала мы определяем ЭК, используя формульную запись E751 = (-1, 1).

Затем мы проверяем условие 4a^3 + 27b^2 != 0 mod p, чтобы убедиться, что ЭК является невырожденной.

Далее мы ограничиваем координаты точек, находящихся на кривой, в пределах квадрата определенных чисел по модулю 751. Это позволяет нам определить цикличность при вычислениях (рис. 1).

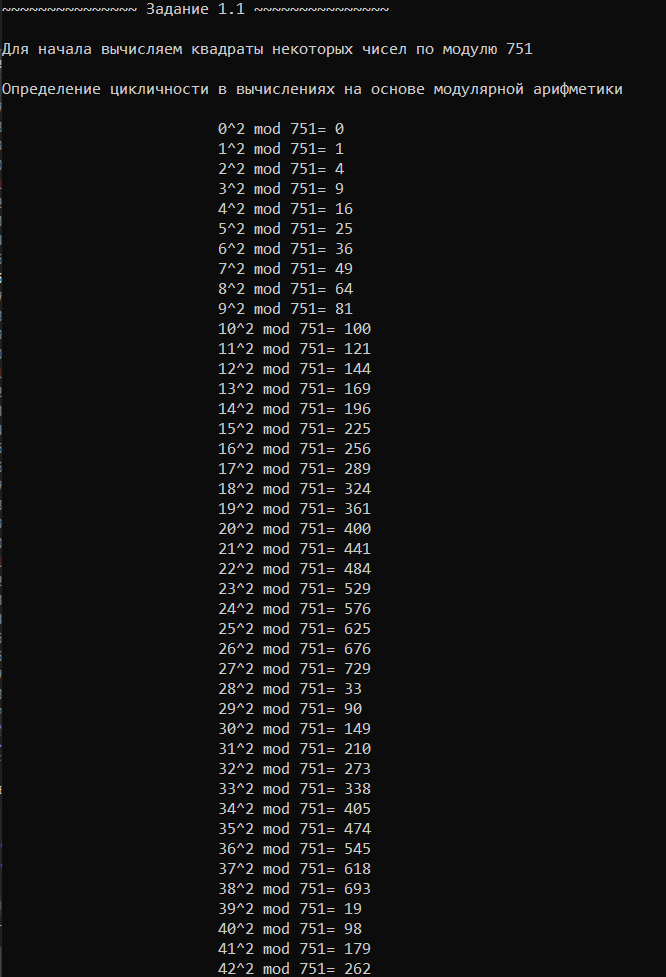


Рисунок 1 – Квадраты некоторых чисел по модулю 751

После вычисления квадратов, мы можем определить, какие числа после знака равенства являются квадратичными вычетами по модулю 751. Затем мы определяем целочисленные координаты.

Используя вычисленные квадраты чисел по модулю 751, мы рассматриваем различные сценарии для разных значений x, начиная с x\_min = 71 и заканчивая x\_max = 105 (рис. 2).

Для примера, рассчитаем значение y^2 при x = 71:

При помощи онлайн-калькулятора несложно быстро посчитать ответ:

На рисунке ниже показаны рассчитанные сценарии для разных значений x, используя данную формулу.

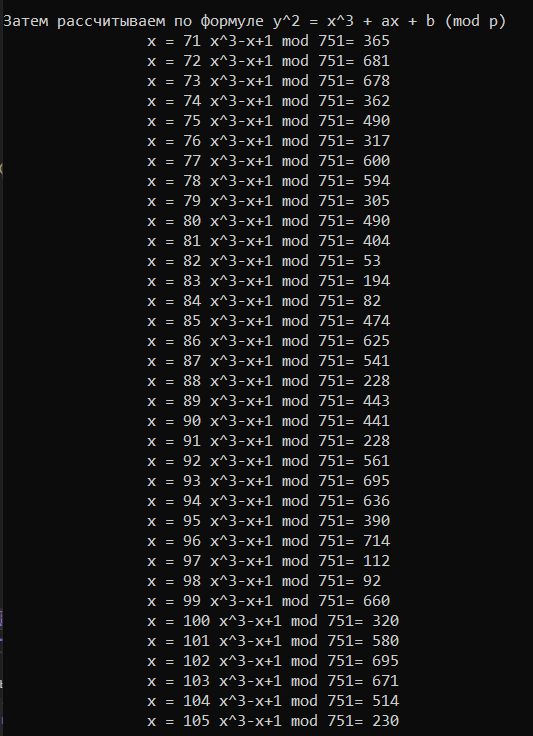


Рисунок 2 – Ситуации при разных x

Из данного выражения мы получаем, что y^2 равняется 365 для точки с x = 71. Мы проверяем это значение в ранее рассчитанных квадратичных вычетах.

Определяем, что точки на эллиптической кривой будут иметь координаты x и y, квадрат которых соответствует вычисленному квадратичному вычету.

В данном случае, полученное значение 365 не имеет соответствия с рассчитанными квадратичными вычетами. Это означает, что на рассматриваемой кривой нет точки с координатой x = 71.

Иногда бывает так, что для некоторых значений x не находятся соответствующие значения квадратичных вычетов. Это указывает на отсутствие точек с рассматриваемым значением x на данной кривой.

Затем мы продолжаем изучение точки, например, с x = 73.

По таблице квадратов некоторых чисел по модулю 751.

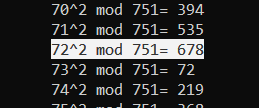


Рисунок 3 – Найденное значение квадрата

Соответственно точка будет (73, 72)

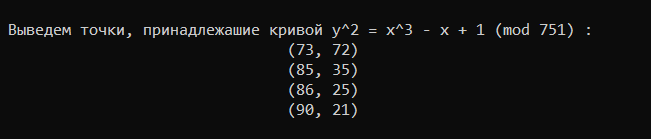


Рисунок 4 – Найденные точки ЭК для значений x

Таким образом алгоритм проделывается для каждого значения x.

***Задание 1.2***

Разработать приложение для выполнения операций над точками кривой:

а) kР;

б) Р + Q;

в) kР + lQ – R;

г) Р – Q + R.

Числовые значения коэффициентов для операций над точками: k = 7; l = 8.

при P != Q:

при P = Q:

Пусть Р = (62, 372) и Q = (70, 195).

Пусть Р + Q = ( , ), тогда при λ = (195 – 372) / (70 – 62) (mod 751) имеем, рассчитанные по формуле:

λ = (195 – 372) / (70 – 62) (mod 751) = 635

x3 = 635-62-70 mod 751 = 301,

y3 = 635\* (62-301)-372 mod 751 = 316.

Таким образом, Р + Q = (301, 316).

Затем следует выполнить проверку. Для этого мы используем разработанное консольное приложение.

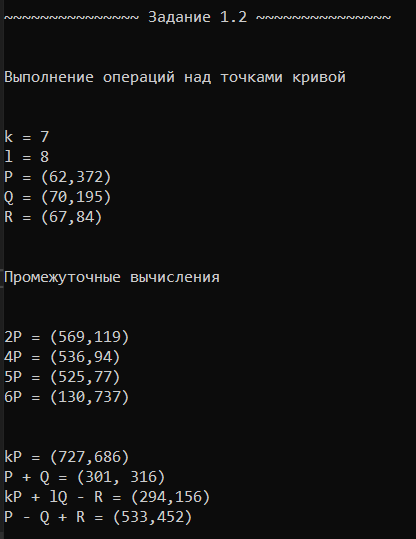


Рисунок 5 – Результат выполнения операций над точками ЭК

При поиске kP, где k=7, необходимо последовательно найти сначала 2P = P+P, 4P=2P+2P, 5P=4P+1P, 6P=5P+1P и, наконец, последним действием необходимо найти 7P=6P+1P.

Используя операцию с инверсией на эллиптической кривой (ЭК), знак "-" в операциях означает сложение с инвертированной точкой.

Инверсия точки (x, y) на ЭК осуществляется путем замены y на -y. Таким образом, инверсией точки (x, y) будет точка (x, -y) на ЭК.

***Задание 2***

Было создано оконное приложение для зашифрования/расшифрования собственного имени на основе ЭК, указанной в задании 1, для генерирующей точки G = (0, 1).

Опять же используем соотношения:

при P != Q:

при P = Q:

Не следует также забывать, что все вычисления производятся по mod 751.

Для зашифрования собственного имени "ВАСИЛИСА" на основе ЭК нам потребуется также уравнение: для генерирующей точки G = (0, 1) с использованием тайного ключа P = (62, 372), Q = (70, 195), R = (67, 84) и d = 25, в соответствии с вариантом, необходимо выполнить следующие шаги:

Выбираем случайное число d из промежутка [1, n-1], где n - порядок точки G на ЭК. По варианту оно равно 25.

Вычислить точку Q как результат умножения точки G на число d: Q = dG.

Каждый зашифрованный блок () сообщения состоит из двух чисел:

Блок шифртекста будет обозначаться .

= kG, где k=5, G = (0, 1).

= P + kQ вычислим по частям:

Сначала операцию умножения kQ, затем = P + kQ операцию сложения.

Приняв P, мы зашифровали первую букву имени «В», получив комбинацию .

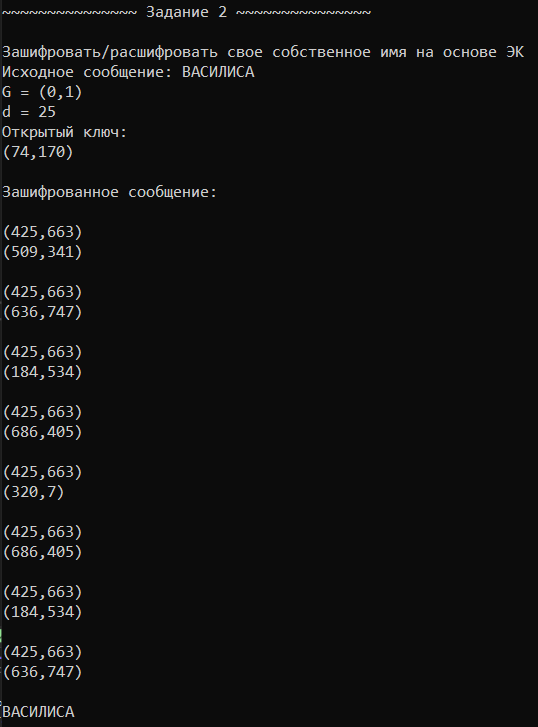


Рисунок 6 – Результат зашифрования собственного имени

В итоге, таким же образом зашифровывается каждая буква имени "ВАСИЛИСА".

Представляя в виде координат точки на ЭК из таблицы методического пособия, можно отобразить наше собственное имя так:

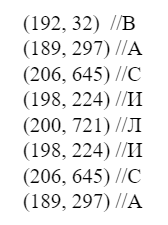


Рисунок 7 – Координаты точек на ЭК из таблицы

Расчет dС1: dС1 = 25 \* С1 = 25 \* (425, 663) = (10625, 16575)

Инвертирование точки dС1: (x1, y1) = (10625, -16575)

Используя операцию с инверсией на эллиптической кривой (ЭК), знак "-" в операциях означает сложение с инвертированной точкой.

Инверсия точки (x, y) на ЭК осуществляется путем замены y на -y. Таким образом, инверсией точки (x, y) будет точка (x, -y) на ЭК.

Вычисление P: P = С2 - dС1 = (509, 341) - (10625, -16575) = (-10116, 16916) = (192, 32) (после приведения по модулю 751)

Таким образом, мы получили, что P = (192, 32) соответствует исходной точке "В" - первой буквы собственного имени.

***Задание 3***

Созданное оконное приложение осуществляет генерацию/верификацию ЭЦП на основе алгоритма ЕСDSA: ЭК Е751(–1, 1) c генерирующей точкой G = (416, 55); порядок точки q = 13. Координаты точки ЭК, соответствующей символу алфавита: В - (192, 32). Численное значение тайного ключа - 7, в соответствии с вариантом.

*Генерация ЭЦП*

Для начала нужно выбрать число k, которое будет 1 < k < q, где q – порядок точки G.

k = 5

Затем нужно вычислить точку kG = (х, у) и вычислить r ≡ x mod q. Также надо проверить, чтобы r не было равно 0. Если r = 0, то нужно снова изменить k и повторить операцию на проверку.

Затем вычислить kG, отсюда r = 3, как значение x по модулю.

Далее вычисляется значение, которое будет равно

Вычислить s = (t (H(M) + dr)) mod q и при s = 0 изменить k и повторить весь алгоритм заново. Для этого нам понадобится хеш.

Хешем подписываемого сообщения (Н(М)) является модуль по основанию 13 (по условию лабораторной работы) координаты х точки ЭК, соответствующей первому символу собственного имени.

В моем случае Н(М) = 2 (рис. 7).

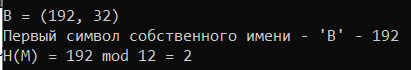


Рисунок 7 - Вычисление Н(М)

s = (8 \* (2 +7 \* 3)) mod 13 = 2

Стороне В отсылается сообщение М и ЭЦП (числа r = 3 и s = 2).



Рисунок 8 - Проверка расчетов программой

*Верификация ЭЦП*

Верификация электронной цифровой подписи (ЭЦП) - это процесс проверки подлинности и целостности электронного документа, защищенного ЭЦП. При верификации ЭЦП проверяется, была ли подпись создана правильным ключом и не была ли подпись изменена после создания.

Получатель знает алгоритм хеширования, который использовался отправителем (то, что мы выполняли ранее) и открытый ключ отправителя. Далее при помощи этих знаний он выполняет следующие операции над М и полученной ЭЦП.

Для начала проверяется выполнение условия: 1 < r, s < q. Если условие не выполняется, то легитимность подписи не подтверждается, а если условие успешно выполняется, то выполняются дальнейшие действия.

Затем вычисляем Н(М) и w ≡ s-1 mod q:

w ≡ 2-1 mod 13 = 1.

Далее вычисляются u1 ≡ w Н(М) (mod q) и u2 ≡ wr (mod q):

u1 ≡ 1\* 2(mod 13) = 2;

u2 ≡ 1\* 3(mod 13) = 3.

Финальным этапом вычислений считается вычисление Gu1 + Qu2 = (x', y') и v ≡ x' mod q:

v ≡ x' mod 13 = 3.

Для подтверждения легитимности и целостности полученного сообщения или пакетов, сравниваются v и r. Если равенство верно, получаем сообщение об успешной проверке легитимности (рис. 9).

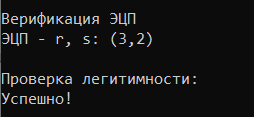


Рисунок 9 - Проверка легитимности

Таким образом, выполнение 3 задания выглядит таким образом, как изображено на рисунке 10.

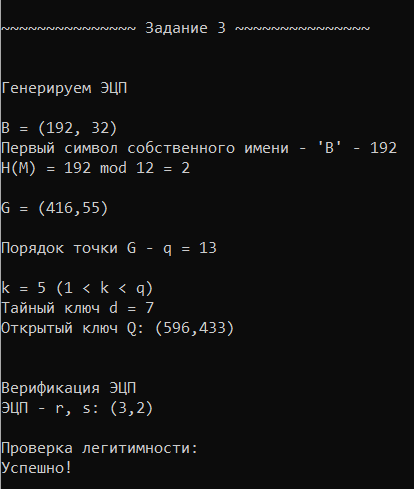


Рисунок 10 - Результат работы программы для задания 3

Вывод: в ходе выполнения лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.

**Контрольные вопросы**

*1. Дать определение эллиптической кривой.*

Эллиптическая кривая — это геометрический объект, представляющий собой набор точек на плоскости, удовлетворяющих определенному математическому уравнению. Это кривая в форме эллипса, но может иметь также и другие особенности.

*2. Записать уравнение ЭК над вещественными числами (ЭК в криптографии, ЕСС).*

Уравнение эллиптической кривой (ЭК) над вещественными числами в общем виде может быть записано как:

*y^2 = x^3 + ax + b,*

где x и y являются вещественными числами, а a и b — параметры, определяющие форму и свойства конкретной эллиптической кривой.

В криптографии и Эллиптической криптографии (EC) используются особые виды эллиптических кривых, называемые эллиптическими кривыми в форме Вейерштрасса. Эти кривые имеют дополнительную структуру и уравнение принимает следующий вид:

*y^2 = x^3 + ax + b (mod p),*

где x, y, a, b и p — целые числа, а (mod p) обозначает операцию взятия остатка от деления на p. Параметр p является простым числом, и такой вид уравнения позволяет работать с конечными полями (полем по модулю p), что имеет большое значение для реализации алгоритмов шифрования и подписи на эллиптических кривых.

*3. Объяснить и показать на примере правила выполнения основных операций над точками ЭК?*

Основные операции над точками на эллиптической кривой (ЭК) включают сложение точек, удвоение точек и умножение точек на целое число. Давайте рассмотрим каждую из этих операций на примере.

*Сложение точек на ЭК*

Пусть у нас есть две точки P и Q на ЭК. Для сложения точек P и Q, мы находим третью точку R, которая является результатом сложения P и Q на кривой. Правило сложения точек на ЭК называется "правилом треугольника" или "правилом прямой линии". Оно заключается в следующих шагах:

Проводим прямую линию через точки P и Q.

Находим пересечение этой линии с кривой и находим отражение этой точки относительно оси x.

Полученная точка R является результатом сложения P и Q на ЭК.

*Пример*

Пусть у нас есть эллиптическая кривая y^2 = x^3 + 2x + 2 и точки P(-1, 1) и Q(2, -5). Мы хотим найти сумму P + Q.

Проводим прямую линию через точки P и Q.

Получаем пересечение этой линии с кривой в точке R(3, -7).

Отражаем точку R относительно оси x и получаем сумму P + Q = (-1, 1) + (2, -5) = (3, 7).

Таким образом, сумма P + Q на данной ЭК равна (3, 7).

*Удвоение точки на ЭК*

Удвоение точки P на ЭК означает нахождение точки R, которая является результатом сложения P и P на кривой. Правило удвоения точки также основано на "правиле треугольника", но с прямой линией, проходящей через одну и ту же точку P. Шаги удвоения точки:

Проводим касательную к кривой в точке P.

Находим пересечение этой касательной с кривой и находим отражение этой точки относительно оси x.

Полученная точка R является результатом удвоения точки P на ЭК.

*Пример*

Пусть у нас есть та же эллиптическая кривая y^2 = x^3 + 2x + 2 и точка P(-1, 1). Мы хотим найти удвоение P.

Проводим касательную к кривой в точке P.

Получаем пересечение этой касательной с кривой в точке R(3, -7).

Отражаем точку R относительно оси x и получаем удвоение P: 2P = (-1, 1) + (-1, 1) = (3, 7).

Таким образом, удвоение точки P на данной ЭК равно (3, 7).

Умножение точки на целое число

Умножение точки P на целое число n на ЭК означает последовательное применение операций сложения и удвоения над точкой P n раз. То есть, мы складываем точку P саму с собой n раз.

Пример

Пусть у нас есть та же эллиптическая кривая y^2 = x^3 + 2x + 2 и точка P(-1, 1). Мы хотим найти результат умножения P на число 3.

Выполняем сложение точек P + P.

Выполняем удвоение полученной суммы (2P).

Выполняем сложение точек 2P + P.

Получаем конечный результат 3P = (3, 7).

Таким образом, результат умножения точки P на число 3 на данной ЭК равен (3, 7).

*4. Что такое «рациональная точка».*

Рациональная точка на эллиптической кривой (ЭК) — это точка, координаты которой являются рациональными числами.

Рациональные точки на эллиптической кривой играют важную роль в различных областях математики и криптографии, включая криптографию на эллиптических кривых (ЭК). Они используются, например, для реализации алгоритмов шифрования и протоколов обмена ключами, где операции над рациональными точками обеспечивают безопасность и эффективность криптографических вычислений.

Точки (1/2, 3/4) и (2, 5/3) являются рациональными точками, в то время как точка (pi) не является рациональной, так как ее координаты являются иррациональными числами.

Каждая точка на плоскости задается парой координат: х и у. Числа х и у являются рациональными, а точки P, Q, R и –R (как и любые точки ЭК) – рациональными точками.

*5. Как производится умножение точки ЭК?*

Умножение точки на эллиптической кривой (ЭК) производится путем последовательного применения операций сложения и удвоения точек. Этот процесс называется "умножением точки на целое число". Давайте рассмотрим шаги умножения точки на ЭК:

Задайте точку P на ЭК, которую вы хотите умножить.

Задайте целое число n, на которое вы хотите умножить точку P.

Инициализируйте результат R в качестве точки нейтрального элемента, обозначаемой как "бесконечность" (обычно обозначается как O или ∞).

Представьте целое число n в двоичной форме.

Начиная с самого левого бита двоичного представления числа n, выполняйте следующие шаги для каждого бита:

Если текущий бит равен 0, удвойте точку R на ЭК (выполните операцию удвоения).

Если текущий бит равен 1, сначала удвойте точку R на ЭК, а затем сложите с точкой P на ЭК (выполните операцию удвоения, а затем сложения).

После обработки всех битов двоичного представления числа n, результатом умножения будет точка R на ЭК.

*6. Как производится умножение точки Р на число k, если k принимает значение: 2, 5, 11, 20, 32, 100, 256, 751, 1024.*

При известном P нужно найти сначала 2P = P+P

5P = 2P+2P+P

Находим промежуточное: 10P = 5P+5P

11P = 10P+1P

20P = 10P+10P

32P = 11P+11P+10P

100P = 32P+32P+32P+4P

Промежуточное: 200P = 100P+100P

256P = 200P+20P+32P+4P

Промежуточное: 500P = 200P+200P+100P

751P = 500P+200P+20P+20P+11P

1024P = 500P+500P + 20P + 4P

*7. Составить алгоритм многократного сложения точки ЭК (умножения точки на число)?*

Вот алгоритм многократного сложения точки на эллиптической кривой (ЭК):

Вход: Точка P на эллиптической кривой, целое число k.

Инициализация:

Установите результат R в точку нейтрального элемента (обычно обозначается как O или ∞).

Представление числа k в двоичной форме:

Представьте число k в двоичной форме, сохраняя его биты в массиве или строке.

Цикл по битам числа k:

Для каждого бита b\_i (начиная с самого правого бита) в двоичном представлении числа k, выполняйте следующие шаги:

Удвоение:

Если b\_i равно 0, выполните операцию удвоения над точкой R: R = 2R.

Сложение:

Если b\_i равно 1, сначала выполните операцию удвоения над точкой R: R = 2R.

Затем выполните операцию сложения точки P с точкой R: R = R + P.

Возврат результата:

В конце цикла результатом умножения точки P на число k будет значение R.

Примечание: Во время выполнения операций сложения и удвоения точек на ЭК, следует использовать соответствующие правила, определенные уравнением кривой.

*8. Привести расчеты для точки Q при известных d и G из примера 7.*

Пусть у нас есть эллиптическая кривая y^2 = x^3 + 2x + 2 и точка P(-1, 1). Мы хотим умножить P на число 11.

Инициализируем R как точку O.

Представляем число 11 в двоичной форме: 1011.

Цикл по битам числа 11:

Первый бит: 1 (Младший бит)

Удваиваем точку R: R = 2R.

Складываем точку P с точкой R: R = R + P.

Второй бит: 1

Удваиваем точку R: R = 2R.

Складываем точку P с точкой R: R = R + P.

Третий бит: 0

Удваиваем точку R: R = 2R.

Четвертый бит: 1 (Старший бит)

Удваиваем точку R: R = 2R.

Складываем точку P с точкой R: R = R + P.

Результат умножения точки P на число 11: R = (-1, -1).

*9. Есть ли отличия в применении операций над точками ЭК над конечными полями и над действительными числами.*

Да, есть отличия в применении операций над точками эллиптической кривой (ЭК) над конечными полями и над действительными числами.

*Определение точек*

В случае конечного поля, уравнение эллиптической кривой обычно записывается в форме y^2 = x^3 + ax + b, где a и b являются элементами конечного поля.

В случае действительных чисел, уравнение эллиптической кривой может быть записано в форме y^2 = x^3 + ax + b, где a и b являются действительными числами.

*Операции сложения и удвоения*

В обоих случаях операции сложения и удвоения точек на ЭК выполняются с использованием определенных правил, которые определяются уравнением кривой.

Однако в случае конечного поля, эти операции осуществляются с использованием арифметики в этом конечном поле, где все операции и вычисления происходят по модулю числа элементов в поле (порядка поля).

В случае действительных чисел операции сложения и удвоения выполняются с использованием обычной арифметики действительных чисел.

*Представление точек*

В случае конечного поля, координаты точек на ЭК являются элементами конечного поля.

В случае действительных чисел, координаты точек могут быть рациональными числами или действительными числами.

*Эффективность вычислений*

Вычисления над конечными полями могут быть более эффективными, чем вычисления над действительными числами. Это связано с особыми свойствами конечных полей, такими как возможность использования быстрого алгоритма умножения (например, алгоритм Карацубы или алгоритм Штрассена).

*10. Записать уравнение ЭК при формальном ее представлении в следующем виде: (а, b).*

Уравнение эллиптической кривой (ЭК) при формальном представлении в виде Ep(a, b) записывается следующим образом:

Ep(a, b): y^2 + xy = x^3 + ax^2 + b

где a и b - параметры, определяющие конкретную кривую Ep(a, b).

Обратите внимание, что в формальном представлении коэффициент перед x^3 всегда равен 1, поэтому его можно опустить в уравнении.

*11. Из какого числа точек состоит ЭК (6, –9)? Дать их координаты.*

Для определения количества точек на эллиптической кривой (ЭК) E11(6, -9) и их координат, можно использовать теорему Хасе-Нульлмана. Она утверждает, что количество рациональных точек на кривой, включая точку в бесконечности, можно найти с помощью формулы:

N = p + 1 - t

где N - количество точек на кривой, p - характеристика поля (в данном случае 11), а t - след Фробениуса.

Для вычисления значения t, мы можем возвести характеристику поля в степень 2 и вычесть значение двойного коэффициента a (6 в данном случае).

t = p^2 - 2a = 11^2 - 2\*6 = 121 - 12 = 109.

Теперь мы можем вычислить количество точек:

N = 11 + 1 - 109 = 3 - 109 = -105.

Значение N -105 означает, что на кривой E11(6, -9) нет рациональных точек (кроме точки в бесконечности). Таким образом, количество точек на этой кривой равно 1, и единственной точкой на ЭК E11(6, -9) является точка в бесконечности.

*12. Найти все точки ЭК (1, 2).*

Для нахождения всех точек на эллиптической кривой (ЭК) E11(1, 2), мы можем использовать следующий алгоритм:

Подставим значения x в уравнение ЭК и найдем соответствующие значения y:

Выберем значение x из полей Галуа GF(11), начиная с 0 и до 10.

Подставим каждое значение x в уравнение ЭК: y^2 = x^3 + x + 2.

Найдем квадраты чисел в поле Галуа GF(11) и сравним их с результатом правой стороны уравнения.

Запишем пары (x, y), которые удовлетворяют уравнению.

Добавим точку в бесконечности:

Добавим точку в бесконечности (0, 1, 0), которая является нейтральным элементом на ЭК.

Получим все точки на ЭК E11(1, 2):

Соберем все найденные пары (x, y) из шага 1 и точку в бесконечности.

Эти точки будут представлять все точки на ЭК E11(1, 2).

Решая уравнение y^2 = x^3 + x + 2 для каждого значения x из поля Галуа GF(11), получим следующие точки:

(0, 1, 0) - точка в бесконечности.

(0, 10) и (0, 1) - точки, удовлетворяющие уравнению.

(1, 0) и (1, 0) - точки, удовлетворяющие уравнению.

(3, 2) и (3, 9) - точки, удовлетворяющие уравнению.

(4, 2) и (4, 9) - точки, удовлетворяющие уравнению.

(5, 0) и (5, 0) - точки, удовлетворяющие уравнению.

(9, 4) и (9, 7) - точки, удовлетворяющие уравнению.

(10, 6) и (10, 5) - точки, удовлетворяющие уравнению.

Таким образом, все точки на ЭК E11(1, 2) состоят из следующих координат:

(0, 1, 0)

(0, 10)

(1, 0)

(3, 2)

(3, 9)

(4, 2)

(4, 9)

(5, 0)

(9, 4)

(9, 7)

(10, 6)

(10, 5)

Их координаты представлены в формате (x, y, z), где z = 0 указывает на точку в бесконечности.

*13. На чем основа криптостойкость систем на основе ЭК? Области применения ЭК в криптографии.*

Основой криптостойкости систем на основе эллиптических кривых (ЭК) является вычислительная сложность задачи дискретного логарифмирования на эллиптических кривых. Эта задача заключается в поиске значения x в уравнении P = kG, где P - точка на эллиптической кривой, G - базовая точка (генератор группы точек) и k - случайное число. Вычисление дискретного логарифма на ЭК считается вычислительно сложной задачей, особенно при использовании достаточно больших параметров ЭК.

Области применения эллиптических кривых в криптографии включают в себя:

Эллиптическое криптографическое шифрование (Elliptic Curve Cryptography, ECC): ЭК используются для шифрования и дешифрования данных, а также для генерации и проверки электронной подписи. При этом используются алгоритмы, такие как ECDSA (Эллиптический Цифровой Алгоритм Подписи) и ECDH (Эллиптический Диффи-Хеллманов Обмен Ключами).

Эллиптическое криптографическое распределение ключей (Elliptic Curve Key Agreement, ECKA): ЭК применяются для согласования общего секретного ключа между двумя или более участниками коммуникации. Примером является протокол Диффи-Хеллмана на основе эллиптических кривых (ECDH).

Эллиптические цифровые подписи (Elliptic Curve Digital Signatures, ECDS): ЭК используются для создания и проверки цифровых подписей, обеспечивая аутентификацию, целостность и невозможность отказа от сообщения. Наиболее распространенным алгоритмом является ECDSA.

Криптографические протоколы: ЭК применяются в различных криптографических протоколах, таких как SSL/TLS, SSH, IPSec и другие, для обеспечения защищенного обмена информацией и установки сессионных ключей.

Эллиптические кривые в криптографии предлагают высокий уровень безопасности при более компактных ключах и операциях. Они широко применяются в различных системах и протоколах, где важны эффективность, безопасность и малый размер ключа.

*14. Что такое «порядок точки» ЭК? Показать на примере. Какую роль этот параметр играет в криптографии на основе ЭК.*

Порядок точки на эллиптической кривой (ЭК) определяет количество точек, которые могут быть порождены путем многократного сложения базовой точки на данной кривой. Порядок точки обозначается как n и является целым положительным числом.

Формально, порядок точки P на ЭК определяется как наименьшее положительное целое число n, такое что nP = O, где O - точка в бесконечности (нулевая точка на ЭК).

Для примера, рассмотрим эллиптическую кривую E7(-2, 4) над полем GF(7). Предположим, что базовая точка G имеет координаты (0, 2) на этой кривой. Если мы будем многократно складывать G с самим собой, мы получим следующие точки:

G = (0, 2)

2G = (3, 2)

3G = (5, 4)

4G = (1, 0)

5G = (3, 5)

6G = (0, 5)

7G = O (точка в бесконечности)

Здесь мы видим, что при достижении 7G мы получаем точку в бесконечности O, и порядок точки G на этой кривой составляет 7. То есть точка G порождает группу точек, содержащую 7 различных точек, включая O.

Роль порядка точки в криптографии на основе эллиптических кривых заключается в его связи с проблемой дискретного логарифмирования. Если порядок точки P является большим простым числом, то нахождение дискретного логарифма для P становится вычислительно сложной задачей. Это обеспечивает криптостойкость протоколов на основе ЭК, таких как эллиптическое криптографическое шифрование (ECC) и эллиптические цифровые подписи (ECDS). Большой порядок точки также обеспечивает устойчивость к атакам методом подбора и перебора всех возможных значений дискретного логарифма.

*15. Что такое «базовая точка» ЭК? Какую роль этот параметр играет в криптографии на основе ЭК.*

Базовая точка (или также называемая генератором) на эллиптической кривой (ЭК) представляет собой фиксированную точку на кривой, которая используется для генерации всех других точек на этой кривой.

Формально, базовая точка G на ЭК - это точка, которая имеет порядок, не являющийся делителем порядка всей группы точек на кривой. Порядок базовой точки обычно большой простой числовой величины.

Генерация ключей: Базовая точка G используется в алгоритмах на основе эллиптических кривых для генерации ключевой пары (приватный ключ и публичный ключ). Приватный ключ представляет собой случайное число, а публичный ключ представляет точку, полученную путем умножения базовой точки на приватный ключ.

Многократное сложение точек: Базовая точка G используется для многократного сложения с самой собой, что позволяет генерировать другие точки на кривой. Это позволяет строить группу точек, которая обладает определенными математическими свойствами, используемыми в криптографии.

Криптографические операции: Базовая точка G используется в различных криптографических операциях на основе эллиптических кривых, таких как шифрование, создание и проверка электронной подписи, согласование ключей и другие. Она обеспечивает основу для выполнения этих операций на кривой.

*16. Объяснить порядок формирования ключевой информации на основе ЭК.*

Порядок формирования ключевой информации на основе эллиптических кривых (ЭК) может быть разделен на несколько этапов:

Генерация приватного ключа: На этом этапе случайным образом выбирается приватный ключ, который представляет собой случайное число из определенного диапазона. Приватный ключ обычно является секретной информацией и должен быть сохранен в тайне.

Вычисление публичного ключа: Используя базовую точку на ЭК и приватный ключ, публичный ключ вычисляется путем умножения базовой точки на приватный ключ. Это делается с помощью операции умножения точки на число на ЭК. Результатом является точка на кривой, которая становится публичным ключом.

Формирование общего секретного ключа: Общий секретный ключ формируется путем использования приватного ключа одной стороны и публичного ключа другой стороны. Это осуществляется путем умножения публичного ключа одной стороны на приватный ключ другой стороны (или наоборот). Результатом будет точка на кривой, которая может быть преобразована в общий секретный ключ.

*17. Сгенерировать ключевую информацию на основе кривой (1, 2).*

Для генерации ключевой информации на основе эллиптической кривой E11(1, 2) следуйте этим шагам:

Выберите случайное число в качестве приватного ключа (например, 5).

Используя базовую точку на кривой (например, G = (0, 2)), выполните операцию умножения точки на число, чтобы получить публичный ключ. Выполните следующее умножение: P = 5G.

Процесс умножения точки на число может быть выполнен следующим образом:

Инициализируйте переменную S как нулевую точку на кривой: S = O.

Преобразуйте приватный ключ в двоичную форму (5 в двоичной форме равно 101).

Начиная с самого левого бита двоичной формы, двигайтесь слева направо.

При обработке каждого бита, удвойте текущую точку S на кривой (S = 2S).

Если текущий бит равен 1, добавьте базовую точку G к текущей точке S (S = S + G).

После обработки всех битов приватного ключа, финальная точка S будет являться публичным ключом.

Результатом будет публичный ключ P, который будет представлять собой точку на кривой E11(1, 2).