МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №13 НА ТЕМУ:**

**Исследование криптографических алгоритмов на основе эллиптических кривых**

Выполнила студентка 3 курса 4 группы

Коржова Валерия Сергеевна

Минск 2023

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

**Теоретические сведения**

Эллиптическая кривая – математический объект, который может быть определен над любым полем. Представляет собой множество точек, описываемых уравнением Вейерштрасса:

При этом константы *a* и *b* должны удовлетворять условию:

**Группа** – непустое множество с определенной на нем бинарной операцией, называемой сложением и удовлетворяющей нескольким аксиомам.

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

1. Единичный элемент – это бесконечно удаленная точка *О*;
2. Обратная величина точки *R* – это точка, симметричная относительно оси *Х*;
3. Сложение задается следующим правилом: сумма трех ненулевых точек *P*, *Q* и *–R*, лежащих на одной прямой, будет равна *O.*

**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** задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю *р*.

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

**Практическая часть**

В основе задания – ЭК вида *у2 = х3 – х +* 1 (mod 751): *а* = –1, *b* = 1, *р* = 751.

**Задание 1.1**. Найти точки ЭК для значений х, указанных в таблице.

Так как в задании задана эллиптическая кривая над полем, принадлежать кривой будут точки с таким значением *x*, при которых *y* будет целым числом. Результаты вычислений представлены на рисунке 1.1. Как видно на рисунке, ни одна точка с аргументом из предоставленного диапазона значений не принадлежит кривой, так как ни одно из вычисленных по вышеприведённой формуле значений *y* не является целочисленным.

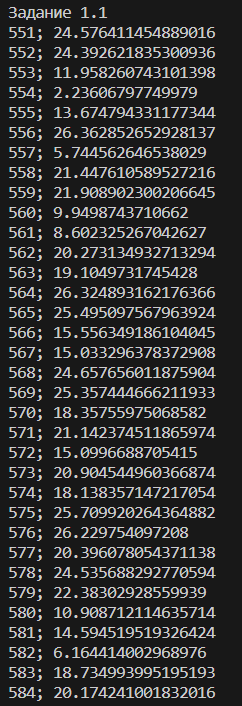


Рисунок 1.1 – Результаты вычислений значений *y*

**Задание 1.2.** Разработать приложение для выполнения операций над точками кривой, принять *k* = 11; *l* = 14.

Для начала необходимо рассмотреть правила сложения точек ЭК над полем. Результатом сложения двух и более точек, принадлежащих ЭК, является другая точка, принадлежащая этой же ЭК. При сложении двух точек, обозначаемых *P* (*x1, y1*) и *Q* (*x2, y2*), вычисляется параметр λ, который равен:

Где *field* – поле, над которым строится ЭК.

Далее координаты новой точки вычисляются по формулам:

Пусть *P* = (210, 31), *Q* = (106, 24). Тогда параметр *λ* равен:

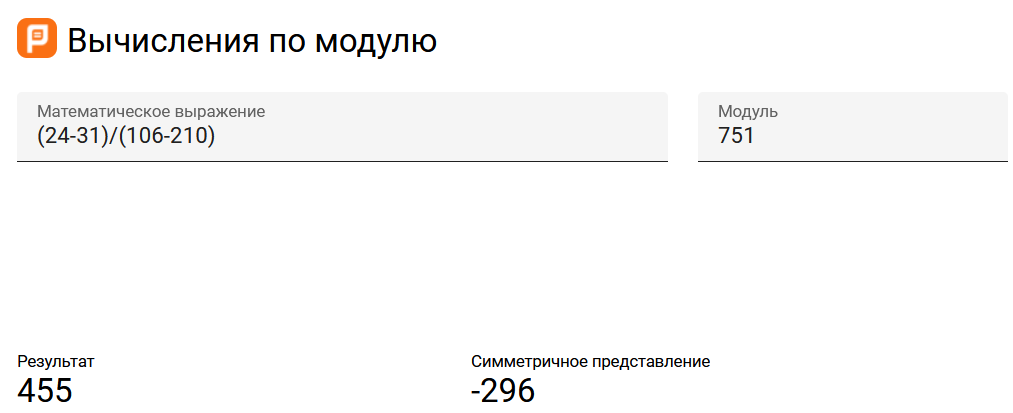


Рисунок 1.2 – Вычисление *λ*

Тогда координаты новой точки:

Для вычисления выполнения операций над точками кривой в приложении был использован Python модуль ECPy, позволяющий работать с эллиптическими кривыми. Результаты вычислений представлены на рисунке 1.3.

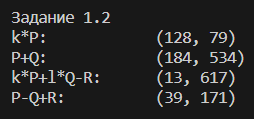


Рисунок 1.3 – Вычисленные значения для задания 1.2

**Задание 2**: Создать приложение для зашифрования / расшифрования собственной фамилии (или имени – по выбору) на основе ЭК, указанной в задании 1, для генерирующей точки G = (0, 1). k = 11.

Перед зашифрованием каждую букву сообщения необходимо представить в виде точки, принадлежащей заданной эллиптической кривой. Таблица для перевода представлена на странице 165 методического пособия.

При шифровании методом эллиптических кривых тайным ключом является целочисленный параметр *d*. В соответствии с вариантом 10, параметр *d* равен 18. Открытый ключ *Q* вычисляется по формуле:

Каждый зашифрованный символ (блок) сообщения представляет из себя 2 подблока (C1 и C2), которые также являются точками заданной ЭК и вычисляются по формулам:

Где *k* – случайное целое число (в данном случае 11); *P* – точка ЭК, представляющая символ сообщения.

Результаты шифрования и расшифрования с помощью приложения представлены на рисунке 2.1.

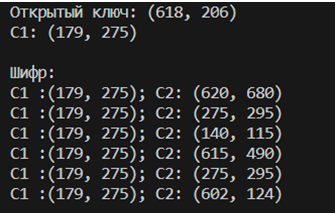


Рисунок 2.1 – Шифрование сообщения методом ЭК

**Задание 3.** Создать оконное приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA: ЭК Е751 (–1, 1) c генерирующей точкой G = (416, 55); порядок точки q = 13; d = 18.

**Генерация ЭЦП:**

1. Выбрать число k (1 < k < q), q – порядок точки G.

2. Вычислить точку k\*G = (х, у), вычислить r ≡ x mod q; при r = 0 изменить k и повторить шаг.

3. Вычислить t ≡ k–1 mod q (например, на основе расширенного алгоритма

Евклида).

4. Вычислить s = (t (H(M) + d\*r)) mod q; при s = 0 изменить k и повторить алгоритм.

Стороне В отсылаются сообщение М и ЭЦП (числа r и s).

**Верификация ЭЦП.** Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над М и полученной ЭЦП.

1. Проверить выполнение условия: 1 < r, s < q; если условие не  
выполняется, то легитимность подписи не подтверждается, в противном случае – выполняются дальнейшие шаги.

2. Вычисляются Н(М) и w ≡ s–1 mod q.

3. Вычисляются u1 ≡ w\*Н(М) (mod q), u2 ≡ w\*r (mod q).

4. Вычисляются G\*u1 + Q\*u2 = (x', y'), v ≡ x' mod q.

5. Сравниваются v и r; если равенство выполняется, подтверждается легитимность подписи и целостность полученного сообщения.

Использование ЭЦП на основе ЭК в приложении через модуль ECPy:

d = 18

Q = ec.mul\_point(d, G)

print(f"Открытый ключ: ({Q.x}, {Q.y})")

print(f"Тайный ключ: {d}")

message = b"VALERIA"

signer = ECDSA()

public\_key = ECPublicKey(Q)

private\_key = ECPrivateKey(d, ec)

sig = signer.sign(message, private\_key)

print(f"Проверка подписи: {signer.verify(message, sig, public\_key)}")

Листинг 3.1 – Код для ЭЦП на основе ЭК

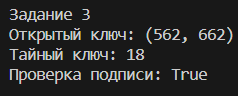


Рисунок 3.1 – Вывод консоли для задания 3

**Контрольные вопросы:**

**1. Дать определение эллиптической кривой.**

Эллиптическая кривая – математический объект, который может быть определен над любым полем. Представляет собой множество точек, описываемых уравнением Вейерштрасса**.**

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

При этом константы *a* и *b* должны удовлетворять условию:

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

Основные операции над точками ЭК включают в себя сложение, умножение на скаляр, а также проверку принадлежности точки к кривой. Ниже приведены правила для выполнения этих операций:

1. **Сложение точек на ЭК.** Сложение двух точек на кривой ЭК определяется следующим образом:

* Если точки имеют разные координаты x, то: λ = (y2 – y1) / (x2 – x1)
* Если точки имеют одинаковые координаты x и y, то: λ = (3x12 + a) / (2y1)
* Вычисляем новую координату x точки-результата: x3 = λ2 – x1 – x2
* Вычисляем новую координату y точки-результата: y3 = λ (x1 – x3) – y1

2. **Умножение точки на скаляр.** Умножение точки на скаляр (целое число) происходит путём выполнения нескольких операция сложения умножаемой точки.

3. **Проверка принадлежности точки к кривой.** Проверка, принадлежит ли точка к кривой над, происходит следующим образом:

* Проверяем, что точка имеет координаты (*x*, *y*), которые удовлетворяют уравнению кривой: y2=x3+ax+b
* Проверяем, что координаты точки лежат в диапазоне, определяемом порядком группы точек на кривой.

**4.** **Что такое «рациональная точка».**

Рациональная точка – это точка на плоскости, у которой обе координаты являются рациональными числами, то есть числами, которые могут быть представлены в виде отношения двух целых чисел.

**5. Как производится умножение точки ЭК?**

Умножение точки на ЭК – это операция, которая выполняется путем последовательного сложения точки с самой собой определенное количество раз.

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

Для облегчения выполнения подобных операций вычисляются промежуточные значения скалярных произведений, которые потом складываются между собой. Например, при k = 20 порядок действий следующий:

*2P = P + P;*

*4P = 2P + 2P;*

*5P = 4P + P;*

*10P = 5P + 5P;*

*20P = 10P + 10P;*

То есть смысл состоит в том, чтобы по максимуму свести промежуточные вычисления к операциям удвоения точки.

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

1. Инициализируем переменную *Q = O*, где *O* – это точка в бесконечности на кривой ЭК.

2. Представляем число k в двоичном виде.

3. Для каждого бита bi числа *k* в двоичном представлении, начиная с младшего бита:

* + Удваиваем точку *Q: Q = 2Q*.
  + Если bi равен 1, то прибавляем к точке *Q* исходную точку *P*:

*Q = Q + P.*

4. После прохождения всех битов числа *k*, точка *Q* будет равна *kP*.

5. Возвращаем точку *Q*.

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

from ecpy.curves import Curve, Point

from ecpy.keys import ECPublicKey, ECPrivateKey

from ecpy.ecdsa import ECDSA

ec = Curve.get\_curve('secp256k1')

ec.\_domain['a'] = 2

ec.\_domain['b'] = 3

ec.\_domain['field'] = 67

d = 4

G = Point(2, 22, ec)

g2 = ec.add\_point(G, G)

print(f"2G: ({g2.x}, {g2.y})")

g4 = ec.add\_point(g2, g2)

print(f"4G: ({g4.x}, {g4.y})")

Листинг 4.1 – Получение значения точки d\*G на Python

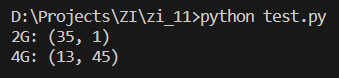


Рисунок 4.1 – Вывод консоли

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

Операции над точками на эллиптических кривых над конечными полями производятся с помощью арифметики в конечных полях (например, полях Галуа), тогда как операции над точками на эллиптических кривых над действительными числами производятся с помощью арифметики действительных чисел.

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

**11. Из какого числа точек состоит ЭК E11(6, –9)? Дать их координаты.**

Чтобы подсчитать число точек ЭК, можно перебрать все сочетания возможных значений *x* и *y*, так как их значения не могут быть больше *p* = 11.

p = 11

for x in range(0, p):

    y\_sq = (x\*\*3 + 6\*x - 9) % p

    for y in range(0, p):

        if (y\*\*2) % p == y\_sq:

            print(f"({x}, {y})")

            if y != 0:

                print(f"({x}, {p - y})")

            break

Листинг 4.2 – Нахождение всех точке ЭК над полем

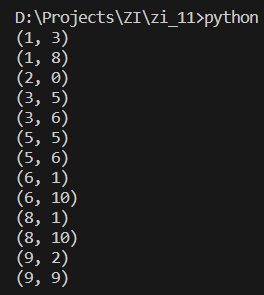


Рисунок 4.2 – Координаты 13 точек ЭК

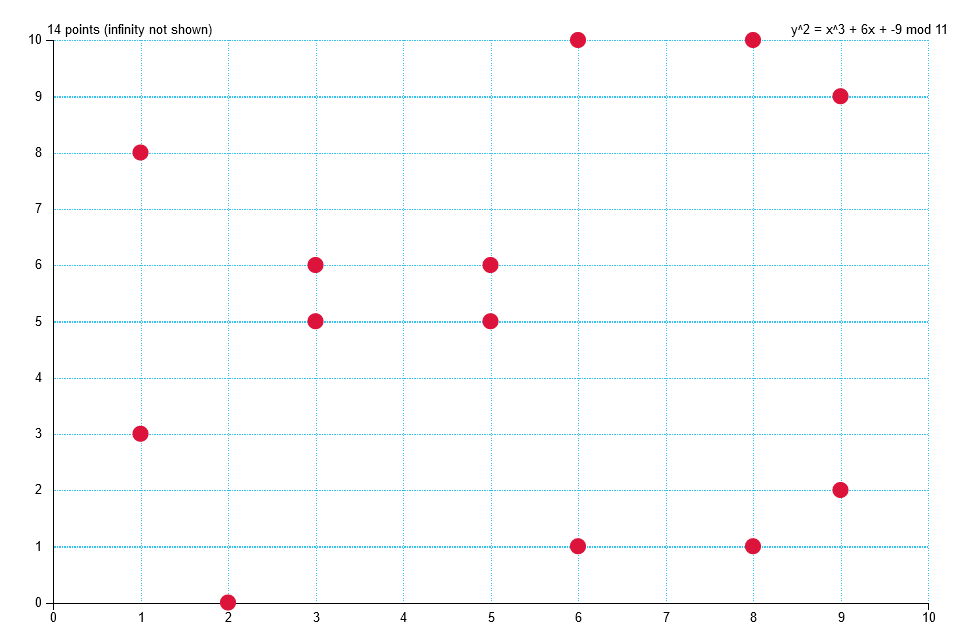


Рисунок 4.3 – Проверка вычисленных точек ЭК через онлайн-приложение

**12. Найти все точки ЭК E11(1, 2).**

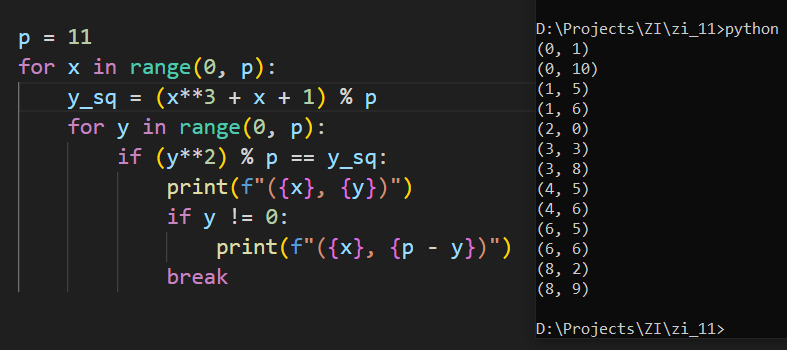


Рисунок 4.4 – Точки для ЭКE11(1, 2)

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

Криптостойкость систем на основе эллиптических кривых (ЭК) основана на сложности задачи дискретного логарифмирования на кривых ЭК. В частности, для заданной точки P и числа k, которое является секретным ключом, найти точку *Q = kP* является вычислительно сложной задачей, к которой пока нет эффективных алгоритмов решения. Одно из наиболее распространенных применений ЭК в криптографии – это создание криптографических систем на основе ЭК, таких как ECDSA (эллиптическая криптография с открытым ключом) и ECDH (эллиптический протокол Диффи-Хеллмана), которые используются для аутентификации и обмена ключами в интернет-протоколах SSL/TLS.

**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) определяется как количество точек на кривой, которые можно получить, умножая данную точку на натуральное число.

Формально, пусть *P* - фиксированная точка на кривой ЭК. Тогда порядок точки *P* – это наименьшее натуральное число n такое, что *nP = O*, где *O* – это точка в бесконечности на кривой ЭК.

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

Базовая точка (генератор) на эллиптической кривой – это фиксированная точка P, которая используется в криптографии на основе эллиптических кривых для генерации случайных ключевых значений и подписей. Роль базовой точки заключается в том, что она позволяет генерировать другие точки на кривой, которые могут быть использованы для создания ключей или подписей. В частности, любую точку *Q* на кривой можно представить в виде кратной суммы базовой точки *P*, т.е. *Q = kP*, где *k* - целое число. Это свойство позволяет использовать базовую точку для генерации случайных значений *k*, которые могут быть использованы в криптографии для создания ключей и подписей.

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

1. Выбор параметров ЭК: выбираются параметры эллиптической кривой, такие как коэффициенты *a* и *b*, модуль *p* и базовая точка *P*.

2. Генерация закрытого ключа: случайным образом выбирается целое число *d*, которое является закрытым ключом пользователя.

3 Вычисление открытого ключа: открытым ключом пользователя является точка *Q = dP*, т.е. результат умножения базовой точки на закрытый ключ.

4. Обмен ключами: для установления защищенного соединения пользователи обмениваются открытыми ключами и с помощью них вычисляют общий секретный ключ.

5. Вычисление общего секретного ключа: общий секретный ключ вычисляется путем умножения открытого ключа другого пользователя на закрытый ключ текущего пользователя, т.е. *K = dQ = d*(*kP*), где *k* - закрытый ключ другого пользователя.

**17. Сгенерировать ключевую информацию на основе кривой E11(1, 2).**

Алгоритм для базовой точки (2,1):

1. Выбрать случайное секретное число *a*, например, *a* = 4.
2. Вычислить публичный ключ *A = a* \* *P* = 4 \* (2,1) = (10,0).
3. Отправить публичный ключ *A* = (10,0) другой стороне.
4. Другая сторона выбирает свое случайное секретное число *b*, например, *b* = 5, вычисляет свой публичный ключ *B = b*\**P* = 5\*(2,1) = (4,2) и отправляет его первой стороне.
5. Обе стороны вычисляют общий секретный ключ *K* = *a\*B* = *b\*A* = 4\*(4,2) = (10,0).

**Вывод:** В ходе лабораторной работы были рассмотрены операции над точками эллиптических кривых. Также, было разработано приложение, позволяющее зашифровывать, расшифровывать и подписывать сообщения с помощью метода эллиптических кривых.