Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет по лабораторной работе №11**

**«Изучение криптографических алгоритмов на основе эллиптических кривых»**

Выполнил:

студентка 3 курса 2 группы

Черноок Ю. С.

Проверил:

ассистент

Копыток Д. В.

Минск 2021

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

**Теоретическая часть**

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

Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением у2 = х3 + aх + b,

при этом константы (а и b – вещественные числа) должны удовлетворять условию: 4а3+27b2≠0.

Формула называется уравнением Вейерштрасса, а условие исключает из рассмотрения кривые с особыми точками или особые кривые.

В зависимости от значений a и b ЭК могут принимать на плоскости разные формы.

Частью ЭК является бесконечно удаленная точка (также известная как идеальная точка), которую мы обозначим символом О.

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

На основе последнего определения мы можем определить группу для ЭК.

Группа для ЭК есть непустое множество, элементы которого являются точками ЭК

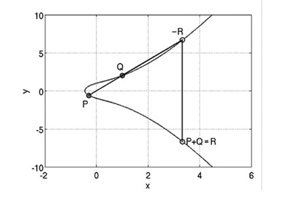


Рисунок 1 – Пояснение к операции сложения двух точек P и Q

эллиптической кривой у2 = х3 + 2х +1 (а = 2, b = 1)

Что будет, если P = Q? В этом случае мы можем говорить об операции удвоения точки: P + Р = 2Р. Обобщив (к точке 2Р можно прибавить еще раз точку Р: 2Р + Р), сформулируем принцип умножения точки Р на целое поло- жительное число n – определяется как сумма n точек Р: nP = P + P + P + …+ P.

Скалярное умножение осуществляется посредством нескольких комбинаций сложения и удвоения точек эллиптической кривой. Например, точка 25P может быть представлена, как 25P = 2(2(2(2P)) + 2(2(2P))) + P.

Понятно, что 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

**ЭК над конечными полями**

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

Поле обозначается как GF(p) или Fp. Здесь операции сложения и умножения работают как в модулярной арифметике.

Например, поле F13 (р = 13) состоит из чисел: 0, 1, … , 12.

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

Формально ЭК над полем задается так: Ер(а, b).

Важно отметить, что, как и ранее, существует точка (бесконечно удален- ная) О; а и b – вещественные числа.

Прежде, чем приступить к алгебраическим операциям над точками кри- вой, такими как суммирование двух разных точек на ЭК и удвоение точек, кратко проанализируем операции для расчета точек, принадлежащих ЭК.

Рассмотрим конкретный пример.

Пусть ЭК формально задается в записью Е13(6, –9). Rоординаты расположения то- чек должны быть ограничены квадратом некоторых чисел по модулю 13 (ле- вая часть основного уравнения – у2). Здесь стоит отметить известную нам цикличность в вычислениях на основе модулярной арифметики. Это видно для нашего случая из табл. 1.

Таблица 1. Цикличность квадратов целых чисел над полем F13



Числа, приведенные после знаков равенства, являются квадратичными вычетами по модулю 13. В данном примере это числа из множества: {1, 3, 4, 9, 10, 12} (обычно число 0 не включают в такие множества).

Важным элементом рассматриваемой технологии является определение точек кривой с целочисленными координатами. Эти задачи в общем случае решаются на основе известных алгоритмов, которые мы здесь опустим. Имея приведенные в табл. 11.1 вычисления квадратов чисел по модулю 13, рас- смотрим ситуацию для х = 0. Подставим это значение в правую часть уравне- ния, имея в виду ЭК Е13(6, –9):

у2 = 03 + 6\*0 – 9 (mod 13),

откуда получим у2 = – 9 (mod 13), у2 = 4 и у = ± 2. Таким образом, пользуясь данными из табл. 11 (смотрим строки с числами 4 справа от знака равенства), определяем, что точками нашей ЭК будут: (0, 2) и (0, 11); здесь мы приняли во внимание то, что значение некоторого целого отрицательного числа (–k) по модулю (р) вычисляется следующим образом:

(–k) modр = – (kmodр) + p.

Следуя приведенной логике рассуждений, определим, например, точки при х = 3: у2 = 33 + 6\*3 – 9 (mod 13) = 36 (mod 13) = 10. Обращаем внимание на 7 и 8 строки левого столбца табл. 11.1 и устанавливаем координаты еще 2- х точек ЭК: (3, 6), (3, 7).

Теперь вернемся к х = 1: у2 = 13 + 6\*1 – 9 (mod 13) = –2 (mod 13) = 11. В табл. 1 не найдено ни одного соответствия. Это означает, что на рассмат- риваемой ЭК нет ни одной точки, координата х которой равна 3.

На рисунке 2 представлены все точки для ЭК Е13(6, –9).

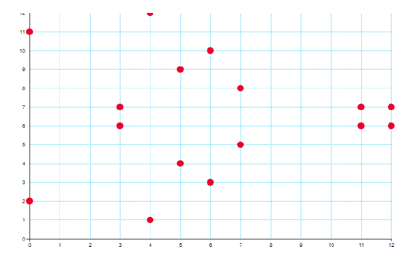


Рисунок 2 – Точки ЭК Е13(6, –9)

На рисунке 3 показаны точки эллиптической кривой (7, 10) из примера 1 для р = 19 (а) и для р = 487 (б).

Из приведенных примеров можно заметить, что для каждого x существу- ет максимум две точки. Отметим также симметрию в расположении точек относительно y = p/2.

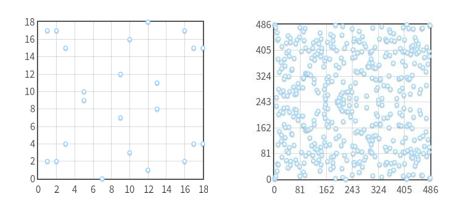


Рисунок 3 – Отображение точек ЭК у2 = х3 – 7х + 10 (mod p)

То, что раньше было непрерывной кривой, теперь стало множеством отдельных точек на плоскости XY, координаты которых (х и у) являются целыми числами.

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).

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

Для ЭК Ер(а, b) порядок m группы точек должен удовлетворять неравен- ству:

Как и в случае с непрерывными ЭК, теперь важным является вычисление некоторого числа d, если мы знаем P и Q для Q = dP. Это и есть задача дискретного логарифмирования для эллиптических кривых.

Эта задача аналогична задаче дискретного логарифмирования, используемой в других криптосистемах, таких как алгоритм DSA, протокол Диффи- Хеллмана и схема Эль-Гамаля.

В криптографии на основе ЭК тайный ключ – это случайное целое d , выбранное из множества {1, 2, ..., q–1}, где q – порядок подгруппы; открытый ключ – это точка Q, такая, что Q = dG, где G – базовая точка подгруппы.

Криптостойкость алгоритмов на основе ЭК определяется, например, для алгоритма ЭЦП в стандарте РБ параметром l, называемым уровнем стойкости и принимающим значения (рекомендуется) из {128, 192, 256}. При этом для взлома ключа злоумышленнику нужно выполнить 2l операций.

**Практическая часть**

В основе задания – ЭК вида у2 = х3 – х + 1 (mod 751): а = –1, b = 1, р = 751, т. е. Е751(–1, 1).

Задание 1. Найти точки ЭК для значений x, принадлежащих промежутку [0;35].

Разработать приложение для выполнения операций над точками кривой:

а) kР, б) Р + Q, в) kР + lQ – R, г) Р – Q + R.

Задание 2. Создать оконное приложение для зашифрования и расшифрования собственной фамилии (или имени – по выбору) на основе ЭК, указанной в задании I, для генерирующей точки G = (0, 1). Тайный ключ – в соответствии с вариантом. Вычислить самостоятельно значение открытого ключа, Q. При этом следует воспользоваться основной формулой (11.8), а также соотношениями (11.3)-(11.5) для случая P = Q; не следует также забывать, что все вычисления производятся по mod 751.

Задание 3. Создать оконное приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA.

На рисунке 4 приведен общий интерфейс программы.

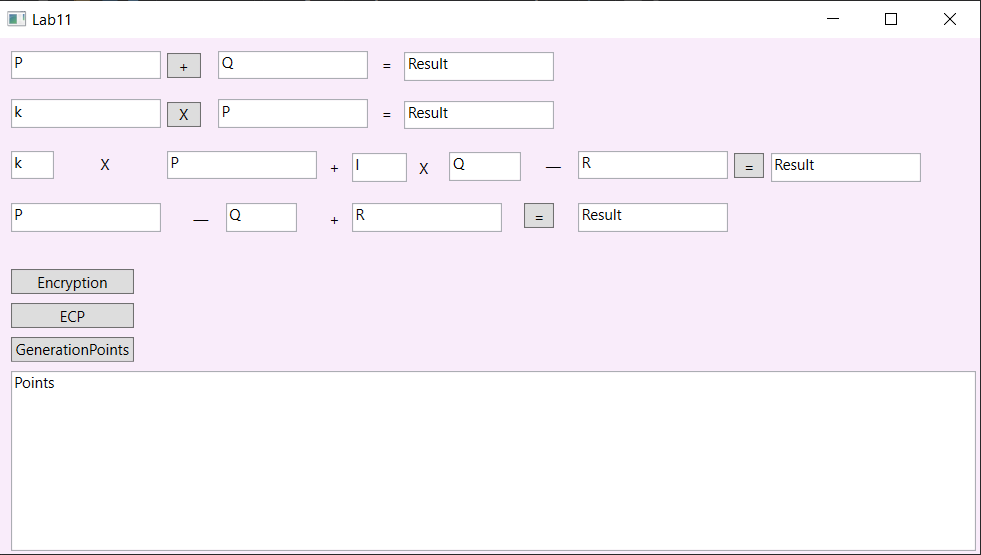


Рисунок 4 – Общий интерфейс программы

Далее на рисунке 5 приведен скриншот выполнения первого задания согласно варианту №1.

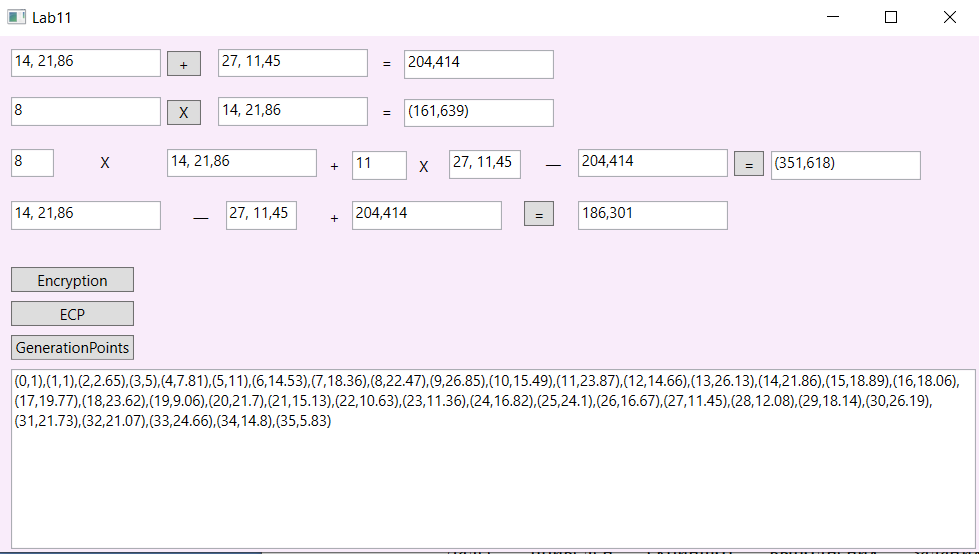


Рисунок 5 – Вычисление значений

Далее на рисунке 6 приведен скриншот выполнения второго задания с шифрованием и расшифрованием.

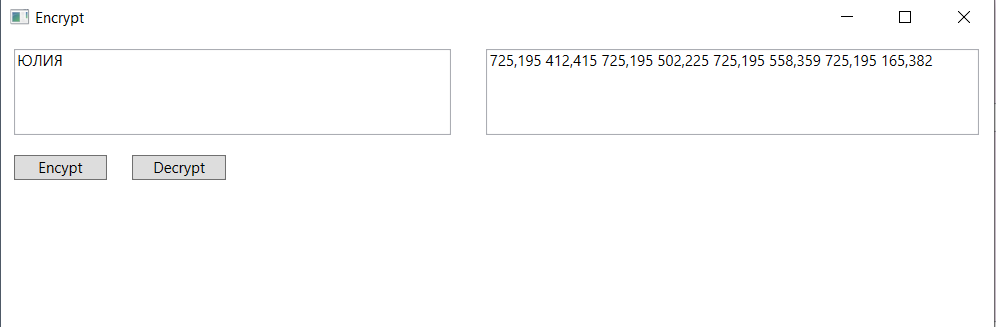


Рисунок 6 – Шифрование и дешифрование имени на основе ЭК

В следующем задании необходимо было реализовать генерацию и верификацию ЭЦП на основе алгоритма ECDSA. Вычислить самостоятельно значение открытого ключа, Q. ЭК Е751(–1, 1) c генерирующей точкой G = (416, 55); порядок точки q = 13. Тайный ключ равен 41. В итоге имеем приложение, которое отображает получившийся открытые ключ и выводит булевское значение, отражающее подлинность ЭЦП (рисунок 7).

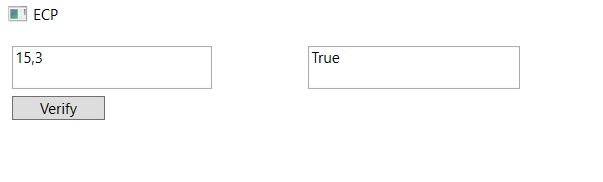


Рисунок 7 – ЭЦП

Вывод: я изучила и приобрела практические навыки разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.