МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №13-1**

**″Исследование криптографических алгоритмов на основе эллиптических кривых″**

Выполнила студентка 3 курса 5 группы Максимчикова Ю. С.

Проверила: Блинова Е. А.

Минск 2020

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

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию и геометрическому представлению операций над эллиптическими кривыми (ЭК): по алгоритмам согласования ключевой информации на основе ЭК, алгоритмам зашифрования/расшифрования информации на основе асимметричной криптографии и ЭК, алгоритмам генерации и верификации электронной цифровой подписи на основе асимметричной криптографии и ЭК, оценке криптостойкости систем на основе ЭК.
* Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для потокового зашифрования/расшифрования.
* Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теория.** 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: 4a3+27b2 ≠ 0. Данное уравнение 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, обладающими следующими свойствами:

* единичный элемент – это бесконечно удалённая 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.

В соответствии с этим можем сформулировать 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;

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 положительное 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

Если Р = (х1, у1) и Q = (х2, у2), то Р + Q = (х3, у3) определяется в соответствии с правилами: x3= λ2 – х1 – х2; у3= λ (х1–х3) – у1, где λ = ( у2 – у1)/( х2 – х1), если Р ≠ Q и λ = (х1)2+а)/2 у1, если Р = Q.

Из этого следует, что число λ – угловой коэффициент секущей, проведенной через точки Р = (х1, у1) и Q = (х2, у2). При Р = Q секущая превращается в касательную, чем и объясняется наличие двух формул для вычисления λ.

ЭК над конечными полями.Именно этот тип ЭК будет нас интересовать в плане практического применения. Конечное поле – это множество конечного числа элементов. 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 удаленная) О; а и b – вещественные числа. Прежде, чем приступить к алгебраическим операциям над точками кривой, такими как суммирование двух разных точек на ЭК и удвоение точек, кратко проанализируем операции для расчета точек, принадлежащих ЭК. Должны быть приняты некоторые предположения, такие как площадь, на которой будут рассчитываться точки кривой, и функция кривой.

Если требуется, например, точку Р сложить саму с собой z раз, то это означает, что нужно выполнить вычисление zР. Для реализации этой операции существует простой метод на основе операции сложения точек. Число z представляется в двоичном виде. И далее вычисляются необходимые составляющие общей суммы на основе весовых (единичных) разрядов двоичного числа z.

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 неравенству: p + 1 – 2(p)½ ≤ m ≤ p + 1 + 2(p)½.

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.

**Задание.** В первой части данной лабораторной работы необходимо было разработать приложение для поиска точек ЭК для значений x в диапазоне [xmin, xmax], а также для выполнения операций над точками кривой: а) kР, б) Р + Q, в) kР + lQ – R, г) Р – Q + R.

Исходными были следующие данные (вариант 11): ЭК вида у2 = х3 – х + 1 (mod 751): а = –1, b = 1, р = 751, т. е. Е751(–1, 1), xmin = 586, xmax = 620, k = 7, l = 7, P(59, 365), Q(59, 386), R(105, 382).

В первой части задания нужно было вычислить значение y для указанного диапазона значений x. Данные вычисления проводились по формуле y = √x\*x\*x – x + 1 (mod 751). Фрагмент кода, выполняющий данные вычисления представлен на рисунке 1.

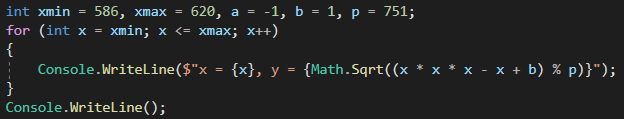


Рис. 1 – Вычисления значений y при различных x

Во второй части задания нужно было выполнить различные операции над точками ЭК. Вычисление результата операций предполагает вычисление λ, поэтому была разработана функция для её вычисления, когда точки не равны, и её перегруженная версия в случае когда точки равны.

Реализация функции для вычисления λ, когда точки не равны, представлена на рисунке 2.

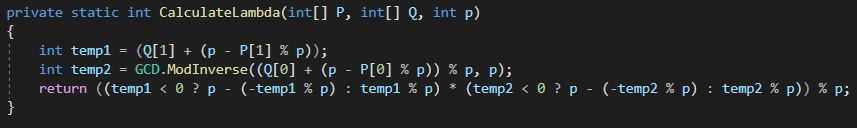


Рис. 2 – Функции для вычисления λ, когда точки не равны

Реализация функции для вычисления λ, когда точки равны, представлена на рисунке 3.

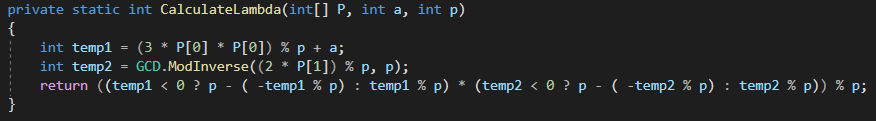


Рис. 3 – Функции для вычисления λ, когда точки равны

Для вычисления P + Q была разработана функция, представленная на рисунке 4.

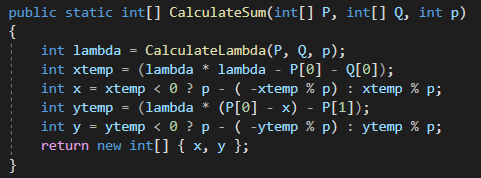


Рис. 4 – Функции для вычисления P + Q

Для вычисления P + P = 2P была разработана функция, представленная на рисунке 5.

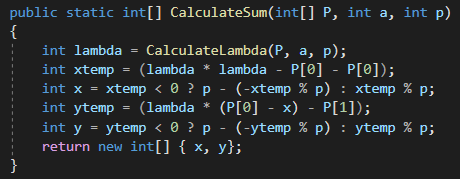


Рис. 5 – Функции для вычисления P + P = 2P

Результаты работы приложения представлены ниже рисунке 6.

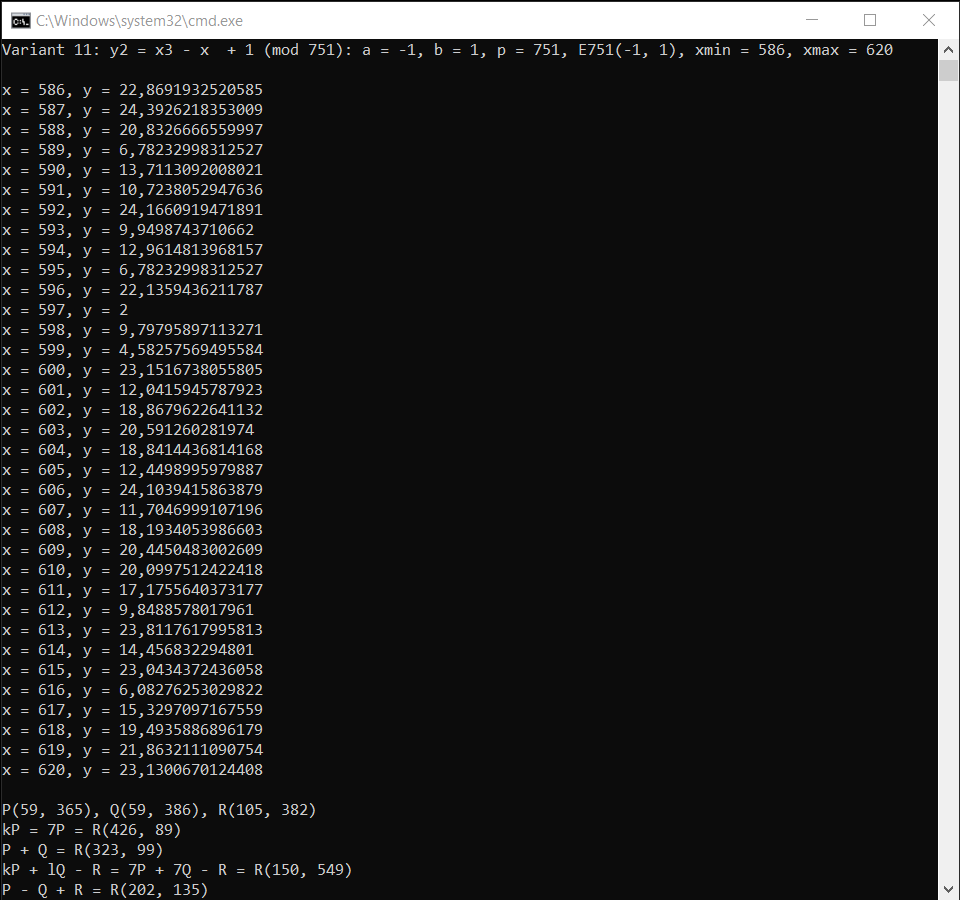


Рис. 6 – Результаты работы приложения

Вывод: в результате данной лабораторной работы было разработано приложение для поиска точек ЭК для значений x в диапазоне [xmin, xmax], а также для выполнения операций над точками кривой.