Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по лабораторной работе №13

«Исследование криптографических алгоритмов на основе эллиптических кривых. Часть 1»

Студентка: Пунько А.А,

ФИТ 3 курс 5 группа

Преподаватель: Берников В. О.

Минск 2020

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых (содержит 3 самостоятельных задания, каждое из которых рассчитано на 2 часа аудиторных занятий).

**Задачи:**

1. 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 криптонафии и ЭК,
* алгоритмам генерации и верификации электронной цифровой подписи на основе асимметричной криптографии и ЭК,
* оценке криптостойкости систем на основе ЭК.

2. Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.

3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# Теоретические сведения

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

Нетрудно понять, что вид ЭК также задается парой чисел: a и b. Эта формула называется уравнением Вейерштрасса, а условие исключает из рассмотрения кривые с особыми точками или особые кривые.

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.

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, 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.

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.

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.

Эллиптическая кривая над полем Fp задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю р (mod p), у2 ≡ х3 + aх + b (mod p) и 4a3+27b2 ≠ 0 (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).

# Практическая часть

В данной части лабораторной работы необходимо выполнить следующие задания:

1. Найти точки ЭК для значений х, указанных в таблице по варианту
2. Разработать приложение для выполнения операций над точками кривой: а) kР, б) Р + Q, в) kР + lQ – R, г) Р – Q + R.

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

Результат нахождения всех точек ЭК представлен на рисунке 1.

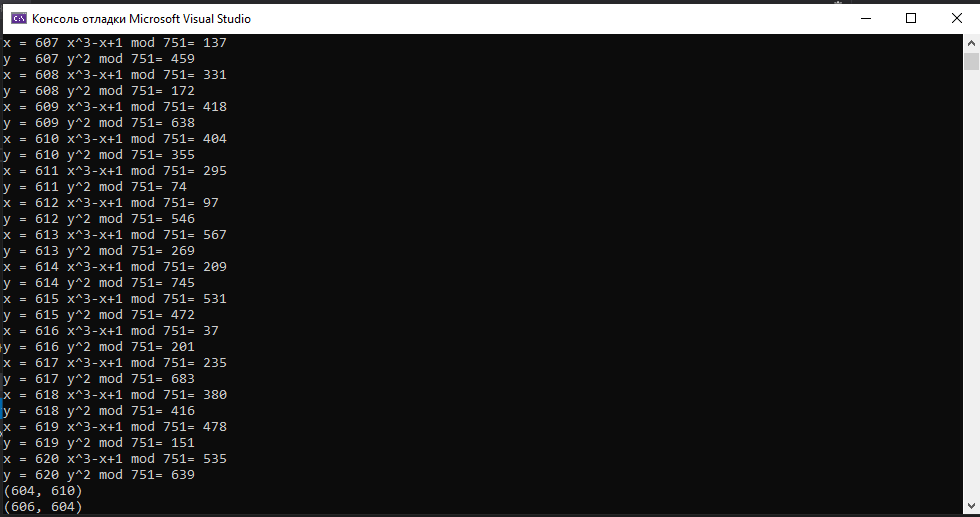


Рисунок 1 – Нахождение всех точек эллиптической кривой

Алгоритм нахождения всех точек ЭК представлен в листинге 1.

int xmin = 583, xmax = 620;

int temp = xmin;

Dictionary<int, int> xValues = new Dictionary<int, int>();

Dictionary<int, int> yValues = new Dictionary<int, int>();

while (temp <= xmax)

{

Console.WriteLine($"x = {temp} x^3-x+1 mod 751= {(temp \* temp \* temp - temp +1) % 751} ");

xValues.Add(temp,( temp \* temp \* temp - temp + 1) % 751 );

Console.WriteLine($"y = {temp} y^2 mod 751= {(temp \* temp ) % 751} ");

yValues.Add(temp, (temp \* temp) % 751);

temp++;

}

foreach (var xx in xValues.Keys)

{

xValues.TryGetValue(xx, out int func1);

foreach (var yy2 in yValues.Values)

{

if (func1 == yy2)

{

var xx1 = yValues.FirstOrDefault(p => p.Value == yy2).Key;

Console.WriteLine($"({xx}, {xx1})");

}

}

}

Листинг 1 – Нахождение всех точек эллиптической кривой

Результат выполнения операций над точками эллиптической кривой представлен на рисунке 2.

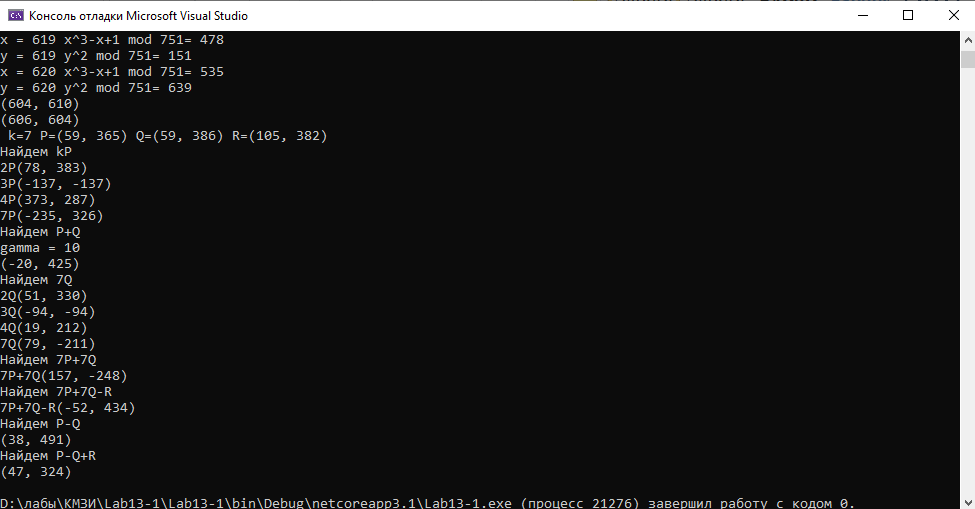


Рисунок 2 – Выполнение операций над точками эллиптической кривой

Алгоритм, выполяющий операции над точками эллиптической кривой, представлен в листинге 2.

int gamma, x, y;

Console.WriteLine(" k=7 P=(59, 365) Q=(59, 386) R=(105, 382)");

Console.WriteLine("Найдем kP");

int gamma1 = (3\*59\*59 - 1)/(2\*365);

int x1 = (gamma1 \* gamma1 - 59 - 59) % 751;

int y1 = ((gamma1 \* 59 - x1) -365) % 751;

Console.WriteLine($"2P({x1}, {y1})");

int gamma2 = (y1 - 365) / (x1 - 59) % 751;

int x2 = (gamma2 \* gamma2 - 59 - x1) % 751;

int y2 = (gamma2 \* 59 - x2 - 365) % 751;

Console.WriteLine($"3P({x2}, {x2})");

int gamma3 = (3 \* x1 \* x1 - 1) / (2 \* y1);

int x3 = (gamma3 \* gamma3 - x1 - x1) % 751;

int y3 = ((gamma3 \* x1 - x3) - y1) % 751;

Console.WriteLine($"4P({x3}, {y3})");

int gamma4 = (y3 - y2) / (x3 - x2) % 751;

int x4 = (gamma4 \* gamma4 - x2 - x3) % 751;

int y4 = ((gamma4 \* x2 - x4) - y2) % 751;

Console.WriteLine($"7P({x4}, {y4})");

int x7p = x4, y7p = y4;

Console.WriteLine("Найдем P+Q");

gamma = ((386 - 365) / (61 - 59)) % 751;

x = (gamma \* gamma - 59 - 61) % 751;

y = (gamma \* (59 - x) - 365)% 751;

Console.WriteLine($"gamma = {gamma}");

Console.WriteLine($"({x}, {y})");

Console.WriteLine("Найдем 7Q");

gamma1 = (3 \* 59 \* 59 - 1) / (2 \* 386);

x1 = (gamma1 \* gamma1 - 59 - 59) % 751;

y1 = ((gamma1 \* 59 - x1) - 386) % 751;

Console.WriteLine($"2Q({x1}, {y1})");

gamma2 = (y1 - 365) / (x1 - 59) % 751;

x2 = (gamma2 \* gamma2 - 59 - x1) % 751;

y2 = (gamma2 \* 59 - x2 - 386) % 751;

Console.WriteLine($"3Q({x2}, {x2})");

gamma3 = (3 \* x1 \* x1 - 1) / (2 \* y1);

x3 = (gamma3 \* gamma3 - x1 - x1) % 751;

y3 = ((gamma3 \* x1 - x3) - y1) % 751;

Console.WriteLine($"4Q({x3}, {y3})");

gamma4 = (y3 - y2) / (x3 - x2) % 751;

x4 = (gamma4 \* gamma4 - x2 - x3) % 751;

y4 = ((gamma4 \* x2 - x4) - y2) % 751;

Console.WriteLine($"7Q({x4}, {y4})");

Console.WriteLine("Найдем 7P+7Q");

gamma4 = (y4 -y7p) / (x4 - x7p) % 751;

x4 = (gamma4 \* gamma4 - x4 - x7p) % 751;

y4 = ((gamma4 \* x7p - x4) - y7p) % 751;

Console.WriteLine($"7P+7Q({x4}, {y4})");

Console.WriteLine("Найдем 7P+7Q-R");

gamma4 = (y4 + 382) / (x4 + 105) % 751;

x4 = (gamma4 \* gamma4 - x4 + 105) % 751;

y4 = ((gamma4 \* 105 - x4) + 382) % 751;

Console.WriteLine($"7P+7Q-R({x4}, {y4})");

Console.WriteLine("Найдем P-Q");

gamma = ((386 + 365) / (61 + 59)) % 751;

x = (gamma \* gamma - 59 + 61) % 751;

y = (gamma \* (59 - x) + 365) % 751;

Console.WriteLine($"({x}, {y})");

Console.WriteLine("Найдем P-Q+R");

gamma = ((y - 382) / (x - 105)) % 751;

x = (gamma \* gamma - 59 + 105) % 751;

y = (gamma \* (105 - x) + 382) % 751;

Console.WriteLine($"({x}, {y})");

Листинг 2 – Выполнение операций над точками эллиптической кривой

# Вывод

В данной лабораторной работе было рассмотрено понятие эллиптической кривой, особенности операций с её точками и было создано приложение, реализующее эти операции.