Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Исследование криптографических алгоритмов на основе эллиптических кривых

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Дубалеко В.В.

Минск 2020

1. **Теоретические сведения**

Определение 1. Эллиптические кривые – математический объект, который может быть определен над любым полем.

Определение 2. 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

Определение 3. Частью ЭК является бесконечно удаленная точка (также известная как идеальная точка), которую мы обозначим символом О.

Определение 4. Группа – непустое множество с определенной на нем бинарной операцией, называемой сложением и удовлетворяющей нескольким аксиомам.

Определение 5. 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;

Определение 2. Электронная цифровая подпись – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа

Классическая технология использования ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь Мо), а его хеша, H(Mо). Это сокращает время генерации/верификации подписи и снижает вероятность появления случайных ошибок в итоговом документе.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать приложение для нахождения точек ЭК и выполнения операций над точками.

Первой частью задания было нахождение точек для определенной эллиптической кривой для значений х которые были указаны в таблице.

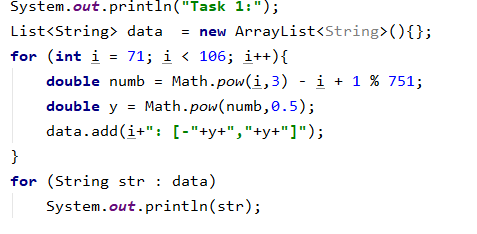


Рисунок 2.1 – Нахождение точек ЭК

Для того что бы приступить к выполнению второй части задания было необходимо написать функции для нахождения суммы для двух одинаковых и различных точек.

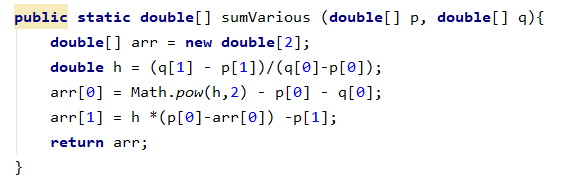


Рисунок 2.1 – Листинг кода для сложения разных точек

Кроме сложения двух разных точек так же есть листинг кода для двух разных точек.

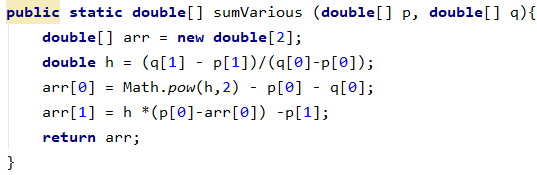


Рисунок 2.2 – Листинг кода для сложения одинаковых точек

После того как были написаны функции для нахождения суммы для двух одинаковых и разных точек можно было приступать к самому заданию. В пункте а от нас требовалось найти сумму точки P с самой собой некоторое k раз. Для выполнения этого действия использовались операции сложения и удваивания.

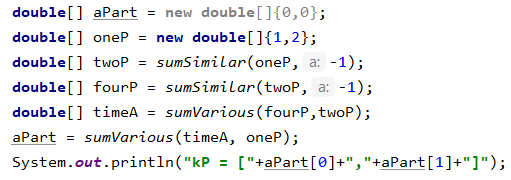


Рисунок 2.3 – Листинг кода для выражения Kp

Следующим пунктом было найти сумму двух точек для которых использовалась выше написанная функция сложения.

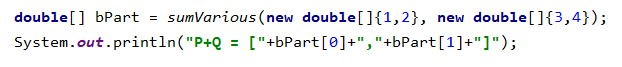


Рисунок 2.4 – Листинг кода для выражения P+Q

Третьим в очереди было выражение которое от нас требовало, что бы мы высчитывали kР + lQ – R.

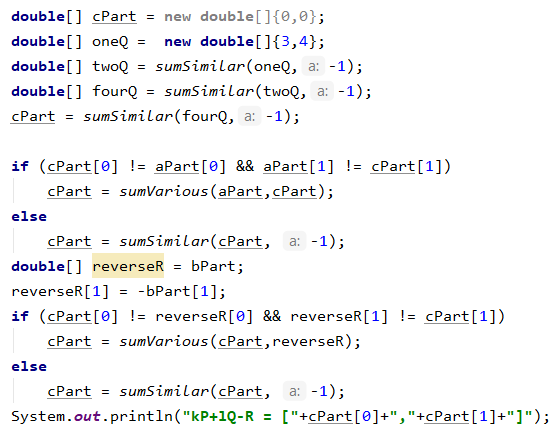


Рисунок 2.5 – Листинг кода выражения kР + lQ – R

В последнее пункте выражение было высчитано выражение P-Q+R.

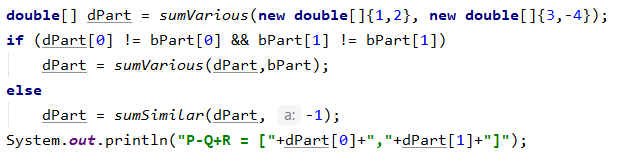


Рисунок 2.6 –Листинг кода выражения P-Q+R

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по эллиптическим кривым. А также, разработал приложение работы с ними.