Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов  
на основе эллиптических кривых

**Задание II**

Студент: Яскович М.Э.

ФИТ 3 курс 6 группа

Преподаватель: Сазанова Д.В.

Минск 2023

## 1. Описание приложения

Приложение написано на языке программирования Java и реализиует следующие операции:

* зашифрование/расшифрование собственного имени на основе ЭК, указанной в задании I.

## 2. Методика выполнения поставленных задач

## 2.1. Алгоритм RSA

Генерирующая точка G = (0,1). Тайный ключ d = 50. Параметр k = 11.

Также примем к сведению, что шифруемым блоком является один символ сообщения.

Для реализации зашифрования и расшифрования применим алгоритм Эль-Гамаля. При использовании ЭК зашифрование предполагает представление сообщения в виде точки Р (или представления каждого блока сообщения в виде разных точек Рi) ЭК с известной точкой G и известным Q. Соответственно шифртекст – это две точки на той же ЭК: С1 и C2.

Предположим, что шифруемое сообщение М – это точка Р на ЭК. Сторона А выбирает некоторое случайное число k и далее выполняет вычисления с использованием открытого ключа стороны В:

С1 = kG, С2 = P + kQ.

Программная реализации процесса зашифрования представлена на рисунке 2.1.

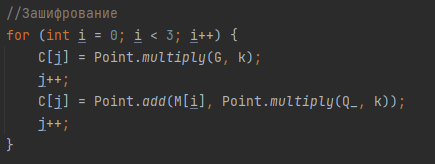


Рис. 2.1 – Зашифрование в ЭК

Получатель для расшифрования сообщения вычисляет:

P = С2 – dC1.

Программная реализация расшифрования представлена на рисунке 2.2.

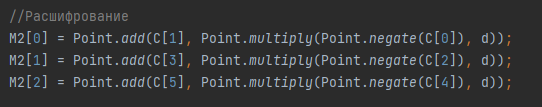


Рис. 2.2 – Расшифрование в ЭК

Результаты проделанных выше операций представлены на рисунке 2.3.

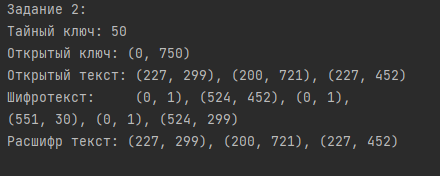


Рис. 2.3 – Результат зашифрования/расшифрования

Открытый ключ Q = G\*d, где G – генерирующая точка, d – тайный ключ. Как упоминалось ранее, на рисунке видно, что одному символу исходного открытого текста соответствует два символа шифротекста. Именно поэтому их количество – 6.

Как видно из рисунка 2.3, открытый и расшифрованный тексты совпадает, что говорит о корректной работе разработанного приложения.

## Вывод

В ходе лабораторной работы было разработано приложения для реализации алгоритмов зашифрования/расшифрования информации на основе ассиметричной криптографии и ЭК, алгоритмов генерации и верификации ЭЦП на основе асимметричной криптографии и ЭК, оценена криптостойкость систем на основе ЭК.