Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов  
на основе эллиптических кривых

**Задание II**

Студент: Шулаков А.А.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

## 1. Описание приложения

Приложение написано на языке программирования C# и реализиует следующие операции:

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

## 2. Методика выполнения поставленных задач

Генерирующая точка *G* = (0,1). Тайный ключ *d* = 43. Параметр *k* = 8.

Также примем к сведению, что шифруемым блоком является один символ сообщения, координаты которого представлены в таблице 2.1.

Таблица 2.1 – Координаты символа

|  |  |
| --- | --- |
| Ш | (218, 150) |
| У | (209, 669) |
| Л | (200, 721) |

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 *Р*i) 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.

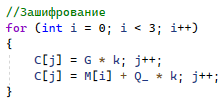


Рис. 2.1 – Зашифрование в ЭК

Получатель для расшифрования сообщения вычисляет:

*P = С2 – dC1.*

Программная реализация расшифрования представлена на рисунке 2.2.

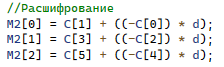


Рис. 2.2 – Расшифрование в ЭК

Результаты проделанных выше операций представлены на рисунке 2.3.

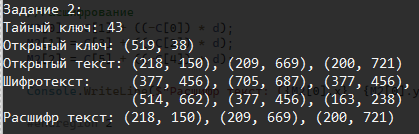


Рис. 2.3 – Результат зашифрования/расшифрования

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.

# **3. Анализ результатов**

Анализ результатов показывает, что время выполнения операции шифрования составило всего 55.3 микросекунды (или 0.0553 миллисекунды). Это свидетельствует о том, что шифрование было выполнено очень быстро. Такое низкое время выполнения может быть полезным в приложениях, где требуется обработка большого объема данных или быстрый отклик системы.

В целом, низкое время выполнения шифрования является позитивным показателем, что говорит о эффективности алгоритма и хорошей производительности системы.

Также следует обратить внимание на точность выполнения операций шифрования и расшифрования, совпадение расшифрованного сообщения с исходным, а также убедиться, что значения точек на ЭК находятся в рамках заданных параметров и соответствуют ожидаемым координатам. Также необходимо проверить корректность вычисления открытого ключа *Q* и убедиться, что он соответствует ожидаемому значению.

## 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.