Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов на основе

эллиптических кривых.

Задание 2.

Студент: Раченок И.А.

ФИТ 3 курс 4 группа

Преподаватель:

Сазонова Дарья Владимировна

Минск 2023

## 1. Описание приложения

Приложение позволяет выполнить следующие задачи:

* зашифрование/расшифрование собственной фамилии или имени на основе ЭК;
* вычислять самостоятельно значение открытого ключа *Q*;

## 2. Методика выполнения поставленных задач

Зашифрованное сообщение М или каждый зашифрованный блок (mi) этого сообщения состоят из двух чисел.

Блок шифртекста () мы обозначали двумя символами и и вычисляли как ≡ mod *p*, ≡ ( ) mod *p*. Поскольку символы *а* и *b* мы зарезервировали в текущей работе для обозначения параметров ЭК, то блок шифртекста сейчас будем обозначать соответственно символами и .

При использовании ЭК зашифрование предполагает представление сообщения в виде точки *Р* (или представления каждого блока сообщения в виде разных точек ) ЭК с известной точкой *G* и известным *Q*. Соответственно шифртекст – это две точки на той же ЭК: и . 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*: = *kG*, = *P* + *kQ*. Получатель для расшифрования сообщения вычисляет: *P* = – *d*. Знак «–» в означает сложение с инверсией: инверсией по отношению к точке (*х*, *у*) является точка (*х*, –*у*) на ЭК.

Функции зашифрования/расшифрования представлены на рисунке 2.1.

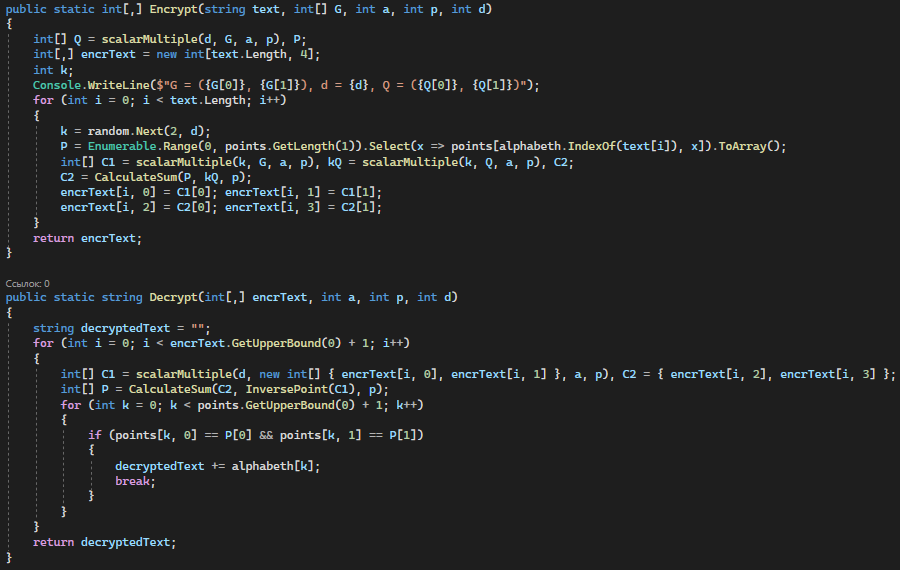


Рисунок 2.1 – Функции зашифрования/расшифрования для работы с ЭК

Основной код представлен на рисунке 2.2.



Рисунок 2.2 – Основной код запуска программы

Результат выполнения зашифрования и расшифрования представлен на рисунке 2.3.

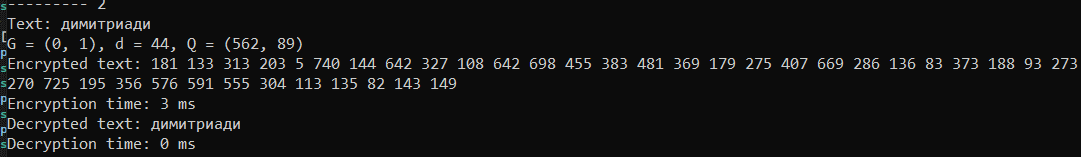


Рисунок 2.3 – Результат шифрования

Как можно увидеть, алгоритм работает корректно, зашифрование и расшифрование проходит корректно.

## 3. Анализ результатов

Анализ результатов проводился путем оценки скорости выполнения зашифрования/расшифрования текста на основе ЭК, рисунок 3.1.

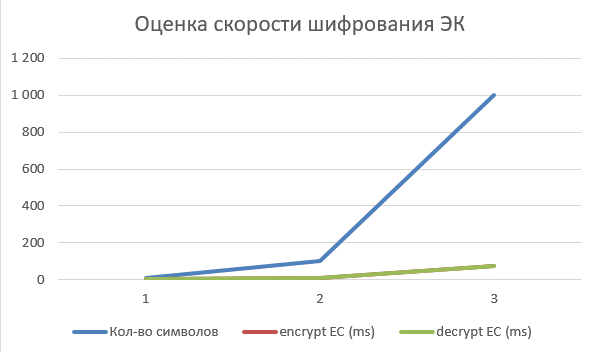


Рисунок 3.1 – Анализ результатов выполнения шифрования данных

На основе графика можно сделать вывод что расшифрование данных на основе ЭК производится очень быстро, и можно смело использовать этот метод шифрования в виду быстрой скорости исчисления.

## Вывод

В ходе лабораторной работы было разработано приложение для реализации зашифрования и расшифрования на основе ЭК. Усвоены навыки работы с ЭК, и с их основными методами.