Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов на основе эллиптических кривых. Часть 2

Студент: Николаева Е.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет выполнить задачу:

* зашифрование/расшифрование собственного имени на основе ЭК;

1. **Методика выполнения поставленных задач**

В данной части лабораторной работы было необходимо создать приложение, реализующее зашифрование и расшифрование текста на основе ЭК. По умолчанию, нам дается точка *G* = (0,1), ключ *d* =19, *k* = 11.

Также примем к сведению, что шифруемым блоком является один символ сообщения, координаты которого мы берем из таблицы.

В основе алгоритмов зашифрования и расшифрования текста лежат функции из первого задания. Это продемонстрированно на рисунке 2.1.



Рис. 2.2 – Алгоритм выполнения функций

Рассмотрим результат работы приложения на рисунке 2.3.

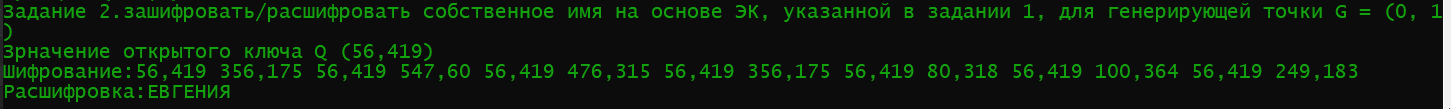


Рис. 2.3 – Выполнение функции шифрования и расшифрования

Увеличим количество буков в тексте. Изображено это на рисунке 2.4. Как видно, при увеличении буков пропорционально увеличивается количество символов при расшифровке.

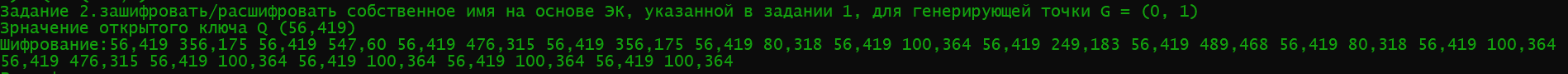


Рис. 2.4 – Выполнение функции шифрования

**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.