Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ИССЛЕДОВАНИЕ АССИМЕТРИЧНЫХ ШИФРОВ**

Студент: Димитриади А.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

1. **Описание приложения**

Приложение позволяет выполнить следующие задачи:

* генерация сверхвозрастающей последовательности (тайного ключа);
* вычисление нормальной последовательности (открытого ключа);
* зашифрование сообщения, состоящего из ФИО;
* расшифрование сообщения;
* оценка времени выполнения операций зашифрования и расшифрования.

1. **Методика выполнения поставленных задач**

Сверхвозрастающей называется последовательность, в которой каждый последующий член больше суммы всех предыдущих. Генерация сверхвозрастающей последовательности была достигнута следующей функцией, рисунок 2.1.

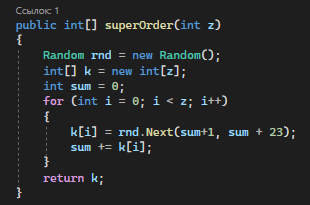


Рисунок 2.1 –Функция генерации тайного ключа

Алгоритм вычисления нормальной последовательности представлен на рисунке 2.2.

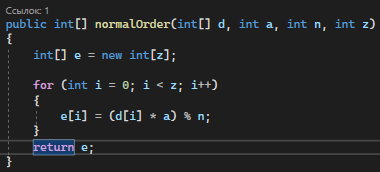


Рисунок 2.2 – Функция вычисления открытого ключа

Данная функция вычисляет элементы последовательности *e*={} по формуле: *=×a (mod n)*, где – члены тайного ключа, n больше суммы всех чисел последовательности, причем НОД (*a*,*n*) = 1.

Для зашифрования сообщения *M* каждый его символ был представлен в двоичной форме. После этого была реализована последовательная проверка каждого символа на равенство единице или нулю. Алгоритм шифрования представлен на рисунке 2.3.

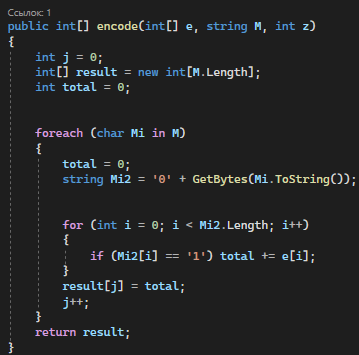


Рисунок 2.3 – Функция зашифрования

Для дешифрования сообщения, использовался предварительно сгенерированный секретный ключ *d*. Алгоритм следующий:

Необходимо найти значение , которое удовлетворяет условию ;

Каждый символ шифрованного текста преобразуется следующим образом: ;

Используя полученное значение , с помощью секретного ключа *d* и известного алгоритма распаковки, происходит получение расшифрованных символов , (нашего исходного сообщения). На рисунке 2.4 представлена реализация данного алгоритма.

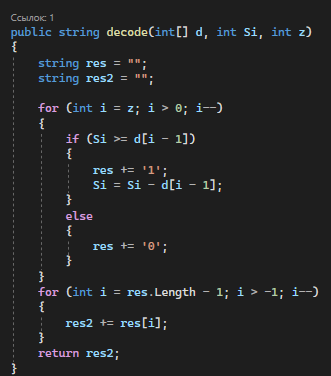


Рисунок 2.4 – Функция дешифрования

Результат выполнения приложения представлен на рисунке 2.5.

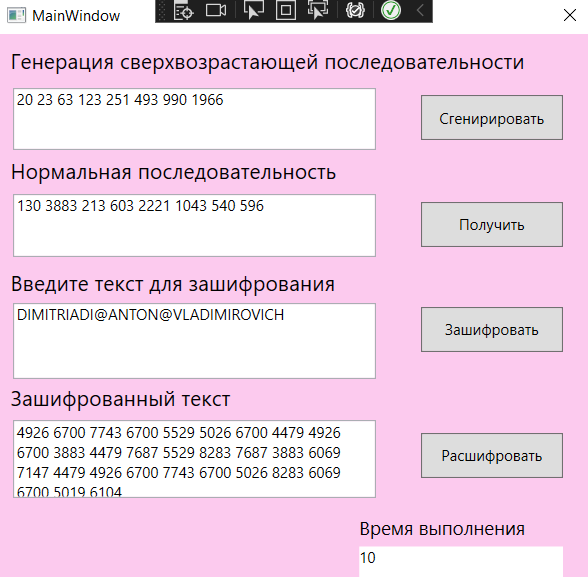


Рис. 2.5 – Результат работы приложения

Была проведена оценка времени затрат на шифрование/дешифрование данных, рисунок 2.6.

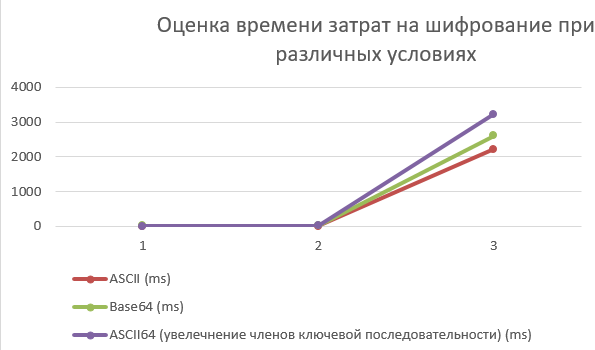


Рис. 2.6 – Оценочный график

**Вывод**

В ходе лабораторной работы были приобретены практические навыки разработки и использования приложений для реализации асимметричных шифров. Было разработано приложение для реализации методов генерации ключевой информации и ее использования. Также была оценена скорость зашифрования/расшифрования.