БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №7**

**«Исследование асимметричных шифров»**»

**Выполнила:**

студентка 3 курса 1 группы

Потапейко Полина Павловна

**Проверил:**

Берников Владислав Олегович

Минск 2022

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров.

**Ход работы**

**Задание.** Разработать приложение, которое реализует генерацию сверхвозрастающей последовательности, вычисление нормальной последовательности, зашифрование сообщения (Potapeyko Polina Pavlovna), расшифрование сообщения, оценку времени зашифрования и расшифрования.

На рисунке 1 представлена сгенерированная сверхвозрастающая последовательность (закрытый ключ).



Рисунок 1 – Сгенерированный закрытый ключ

Далее необходимо высчитать используемые для генерации открытого ключа значения n (должно быть больше суммы всех членов закрытого ключа) и а (взаимно простое с n) (рисунок 2).



Рисунок 2 – n и a

Для создания открытого ключа нужно каждый член закрытого ключа умножить на а и произведение взять по модулю n (рисунок 3).



Рисунок 3 – Открытый ключ

Для получения зашифрованного сообщения само сообщение разбивается на блоки, равные числу элементов в последовательности (8, т.к. используется кодировка ASCII), затем складываются элементы открытого ключа, соответствующие 1 в коде ASCII (рисунок 4).

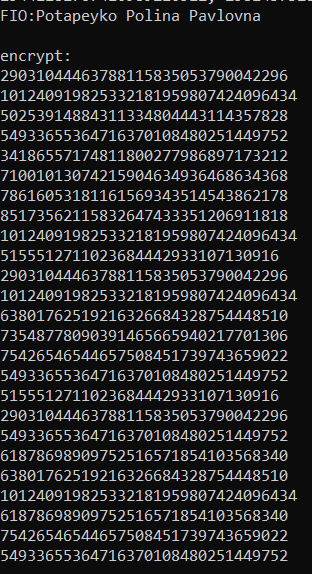


Рисунок 4 – Зашифрованное сообщение

Время зашифрования сообщения представлено на рисунке 5.



Рисунок 5 – Время зашифрования

Для расшифрования сообщения необходимо вычислить а^–1.



Рисунок 6 – а^–1

Затем нужно взять произведение а^–1 и каждого символа шифрграммы по модулю n. Результат расшифрования и время расшифрования представлены на рисунке 7.

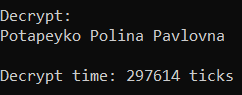


Рисунок 7 – Время расшифрования и расшифрованное сообщение

**Вывод:** в ходе лабораторной работы были закреплены теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров, разработано приложение для реализации заданных методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования, выполнен анализ криптостойкости асимметричных шифров, оценена скорость зашифрования/расшифрования реализованных шифров.