БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №8**

**«Исследование асимметричных шифров RSA**

**и Эль-Гамаля**»

**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 RSA и Эль-Гамаля.

**Ход работы**

**Задание.** Разработать приложение, которое реализует зашифрование сообщения (Potapeyko Polina Pavlovna), расшифрование сообщения, оценку времени зашифрования и расшифрования с использованием алгоритмов RSA и Эль-Гамаля.

**RSA**

Первым действием нужно выбрать два больших простых числа p и q равной длины (рисунок 1).



Рисунок 1 – Простые числа p и q

Далее необходимо высчитать число n как произведение p и q (рисунок 2).



Рисунок 2 – Число n

Затем случайным образом выбирается открытый ключ е, такой что е и (p-1)(q-1) взаимно простые, а также с помощью расширенного алгоритма Евклида вычисляется закрытый ключ d (d^-1 = e mod (p-1)(q-1)) (рисунок 3).



Рисунок 3 – Полученные открытый и закрытый ключи e и d соответственно

Для получения зашифрованного сообщения само сообщение разбивается на блоки, и каждый блок возводится в степень е (открытый ключ) и берется по модулю n (рисунок 4).

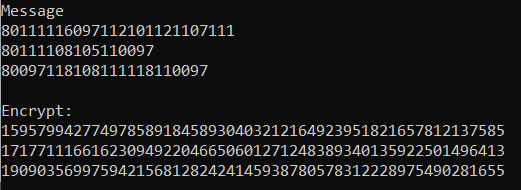


Рисунок 4 – Разбитое на блоки и зашифрованное сообщение

Время зашифрования сообщения представлено на рисунке 5.



Рисунок 5 – Время зашифрования

Для расшифрования каждого зашифрованного блока берется сам зашифрованный блок, возводится в степень d (закрытый ключ) и берется по модулю n. Результат расшифрования и время расшифрования представлены на рисунке 6.

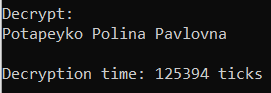


Рисунок 6 – Время расшифрования и расшифрованное сообщение

**Эль-Гамаль**

Первоначально производится вычисление ключевой информации: выбирается простое число p, число g (g<p), которое является первообразным корнем числа p, далее выбирается число х (x<p) и вычисляется число y как g^x mod p (рисунок 7).

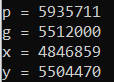


Рисунок 7 – Числа p, g, x, y

Для зашифрования сообщение разбивается на блоки, для каждого блока выбирается случайное число k (1<k<p-1), находятся числа а (a=g^k mod p) и b ((y^k\*m)mod p) (рисунок 8).

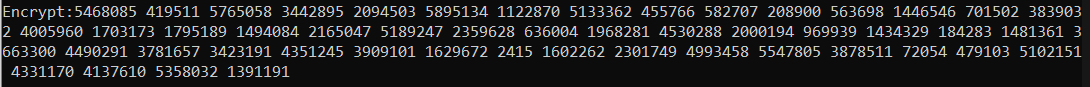


Рисунок 8 – Зашифрованное сообщение

Время зашифрования представлено на рисунке 9.



Рисунок 9 – Время зашифрования

Для расшифрования необходимо найти обратное значение числа a^x по модулю p, затем умножив b на а^(p-x-1) по модулю p расшифруем сам блок шифртекста. Расшифрованное сообщение и время операции расшифрования представлены на рисунке 10.

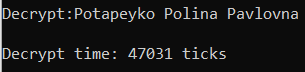


Рисунок 10 – Расшифрованное сообщение и время расшифрования

**Вывод:** в ходе лабораторной работы были закреплены теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров RSA и Эль-Гамаля, разработано приложение для реализации асимметричного зашифрования/расшифрования на основе алгоритмов RSA и Эль-Гамаля, выполнен анализ криптостойкости асимметричных шифров RSA и Эль-Гамаля, оценена скорость зашифрования/расшифрования реализованных шифров.