МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа № 10**

**Исследование асимметричных шифров**

**RSA и Эль-Гамаля**

Разработал: Бай И.О.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

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

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров RSA и Эль-Гамаля.
2. Разработать приложение для реализации асимметричного зашифрования/расшифрования на основе алгоритмов RSA и Эль Гамаля.
3. Выполнить анализ криптостойкости асимметричных шифров RSA и Эль-Гамаля.
4. Оценить скорость зашифрования/расшифрования реализованных шифров.
5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.
6. **Практическая часть**

В данной лабораторной работе необходимо разработать пользовательское приложение, которое должно реализовывать следующие операции:

1. С помощью простого консольного приложения составить табличную или графическую форму зависимости времени вычисления параметра у, функционально заданного выражением вида: *у = ax mod n*, от параметров: *а* (десятичные числа от 5 до 35; можно взять 1 или 2 числа), *х* (числа, желательно – простые, из диапазона от 103 до 10100; для примера взять 5-10 чисел, равномерно распределенных в указанном диапазоне), *n* (для примера взять числа, в двоичном виде состоящие из 1024 и 2048 бит).
2. Разработать авторское оконное приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться доступными библиотеками либо программными кодами.

Приложение должно реализовывать следующие операции:

* зашифрование и расшифрование текстовых документов на основе алгоритмов RSA и Эль-Гамаля;
* определение времени выполнения операций.

Исходный текст для зашифрования – собственные фамилия, имя, отчество. Для численного представления блоков текста можно, в том числе, пользоваться указанными выше кодировочными таблицами.

Ключевую информацию для обоих алгоритмов можно сгенерировать самостоятельно либо воспользоваться, например, одной из утилит криптографической библиотеки OpenSSL, с помощью которой, в частности, можно сгенерировать ключевую информацию для алгоритма RSA.

1. Используя примерно одинаковый порядок ключевой информации, оценить производительность обоих алгоритмов и относительное изменение объемов криптотекстов (по отношению к объемам открытых текстов).

Для выполнения первого задания была написана функция, которая позволяет произвести расчеты времени вычисления *у = ax mod n*.

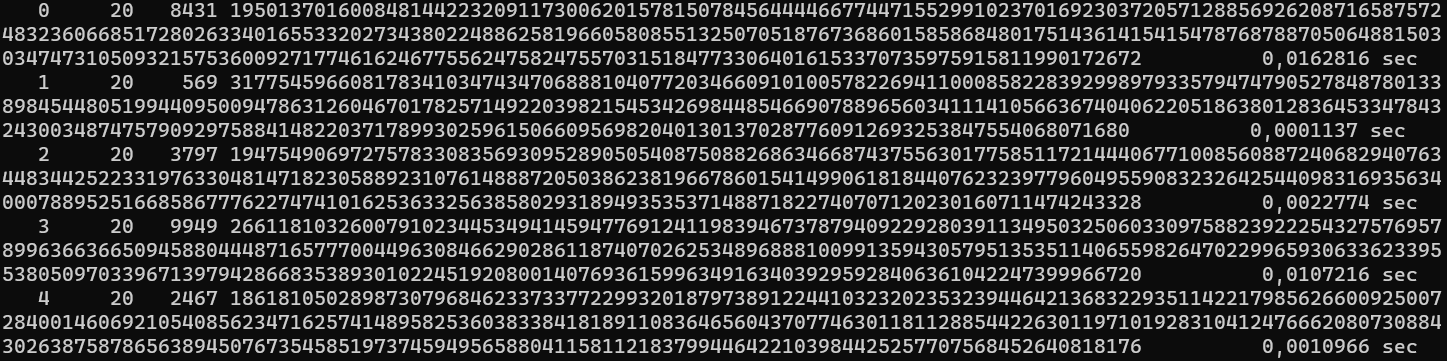


Рисунок 2.1 – Расчет времени вычисления

Сама функция представлена на рисунке 2.2.

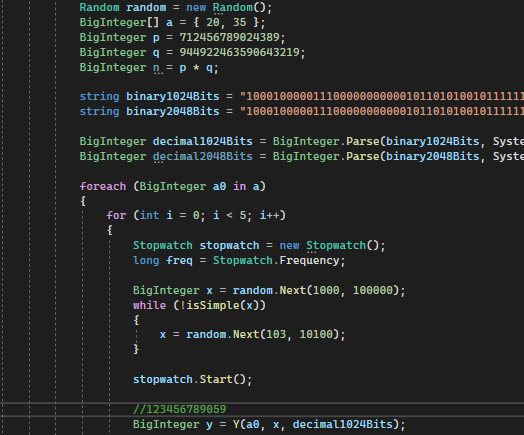


Рисунок 2.2 – Функция расчета времени вычисления

Затем необходимо было реализовать зашифрование/расшифрование сообщений при помощи алгоритма RSA. Для его реализации использовалась библиотека System.Security.Cryptography, которая открывает программный доступ к самым разнообразным криптографическим сервисам, с помощью которых приложения могут шифровать и дешифровать [данные](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5), обеспечивать их целостность, а также обрабатывать цифровые подписи и сертификаты. Реализация функции зашифрования представлена на рисунке 2.3.

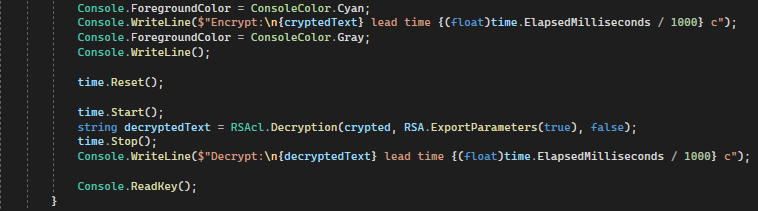


Рисунок 2.3 – Функция шифрования сообщения RSA

Для расшифрования используется функция на рисунке 2.4.

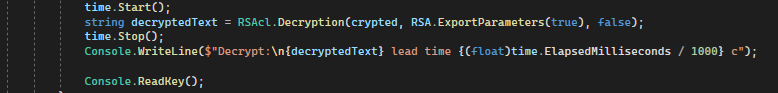


Рисунок 2.4 – Функция расшифрования сообщения RSA

Результат работы программы представлен на рисунке 2.5.

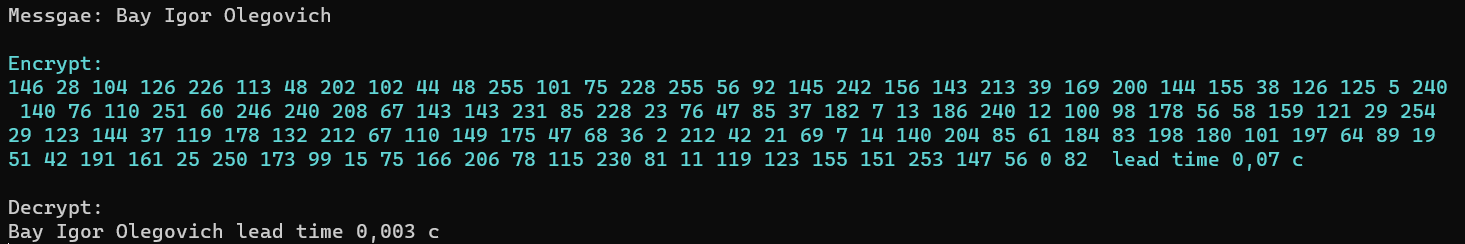


Рисунок 2.5 – Шифрование и расшифрование RSA

После этого было необходимо реализовать зашифрование/расшифрование сообщений при помощи алгоритма Эль-Гамаля. Шифрование сообщения представлено на рисунке 2.6.

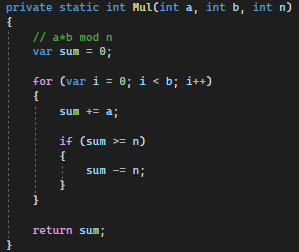


Рисунок 2.6 – Функция шифрования сообщения Эль-Гамаля

Для расшифрования используется функция на рисунке 2.7.

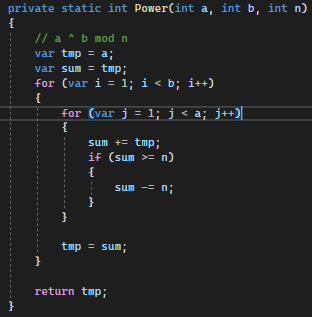


Рисунок 2.7 – Функция расшифрования сообщения Эль-Гамаля

Результат работы программы представлен на рисунке 2.8.

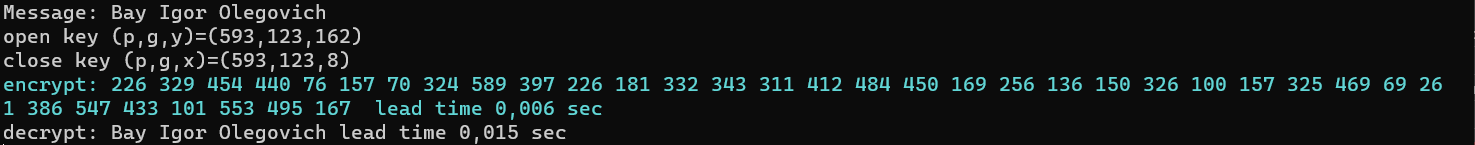


Рисунок 2.8 – Шифрование и расшифрование Эль-Гамаля

Зависимость времени выполнения алгоритмов RSA(оранжевая линия) и Эль-Гамаля(синяя линия), а также изменение длины шифртекста, представлено на рис. 2.9 и 2.10.

Рисунок 2.9 –длина шифр текста алгоритмов RSA и Эль-Гамаля

Рисунок 2.10 –время работы алгоритмов RSA и Эль-Гамаля

**Вывод:** таким образом, в данной лабораторной работе я закрепила теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров RSA и Эль-Гамаля, результатом стало готовое приложение для реализации асимметричного зашифрования/расшифрования на основе этих алгоритмов.