Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**Защита информации и надёжность информационных систем**

**Лабораторная работа №10**

ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ RSA И ЭЛЬ-ГАМАЛЯ

Студент: Вайсера Р.Л.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова

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.

**Практическое задание**

Было разработано приложение, шифрующее и расшифровывающее сообщения, используя шифры RSA и Эль-Гамаля.

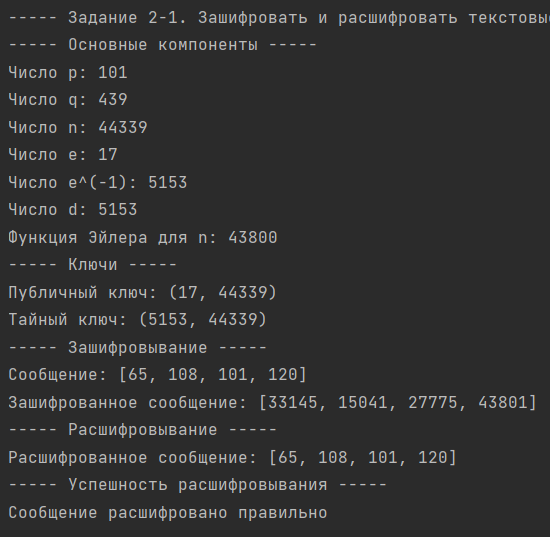
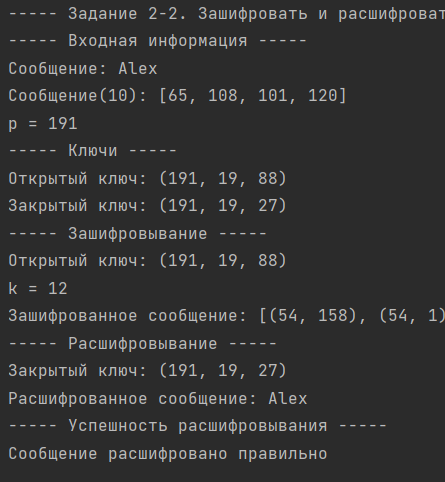
Вывод программы представлен на рисунке 1.

Рис. 1 – вывод консоли программы

Рис. 2 – вывод консоли программы

В алгоритме RSA сначала выбираются два простых числа *p* и *q.* Рассчитывается число *n,* которое равно произведению *p*×*q.* Затем случайно выбирается компонент *e*, такой, что *e* взаимно простое с произведением   
(*p*-1) × (*q*-1). На следующем шаге мы находим число *d*, такое, что

*e*×*d* = 1 (mod (*p*-1) × (*q*-1)).

Для зашифрования сообщения состоящее из *r* блоков следует воспользоваться следующей формулой:

*ci*≡(*mi*)*e* mod(*n*)

Где *mi* ­­– часть исходного сообщения, а *ci* – часть зашифрованного сообщения.

А для расшифрования сообщения нужно воспользоваться следующей формулой:

*mi*≡(*ci*)*d* mod(*n*)

В алгоритме Эль-Гамаля сначала выбирается простое число *p*, далее выбирается число *g*, такое, что *g* является первообразным корнем *g*, далее выбираем число *x* меньшее *p*. И вычисляем число *y* по следующей формуле.

*y* ≡ *gx* mod *p*

Для зашифрования сообщения состоящее из *r* блоков нужно вычислить для каждого блока пару чисел *ai* и *bi* по следующей формуле:

*ai*≡*gk* mod *p*

*bi*≡(*yk*×*mi*)mod *p*

Для расшифрования нужно воспользоваться следующей формулой:

*m*i ≡ (*bi*(*ai*)*р–x*–1) mod *p*

В алгоритме RSA зашифрованный текст будет такого же объема, как и исходный, а в алгоритме Эль-Гамаля зашифрованная информация будет занимать в 2 раза больше места, чем исходная.

Время выполнения алгоритма Эль-Гамаля занимает больше время, чем выполнения алгоритма RSA. График зависимости времени выполнения операций шифрования и расшифрования представлено н рисунке 2.

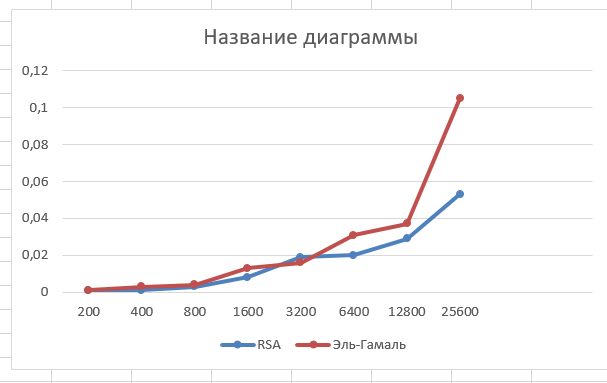


Рис. 3 – График зависимости времени выполнения операций шифрования и расшифрования

Так же была построена таблица зависимости скорости вычисления *y* по следующей формуле:

*у* ≡ *ax* mod *n*

От параметров *a*, *x*, *n*.

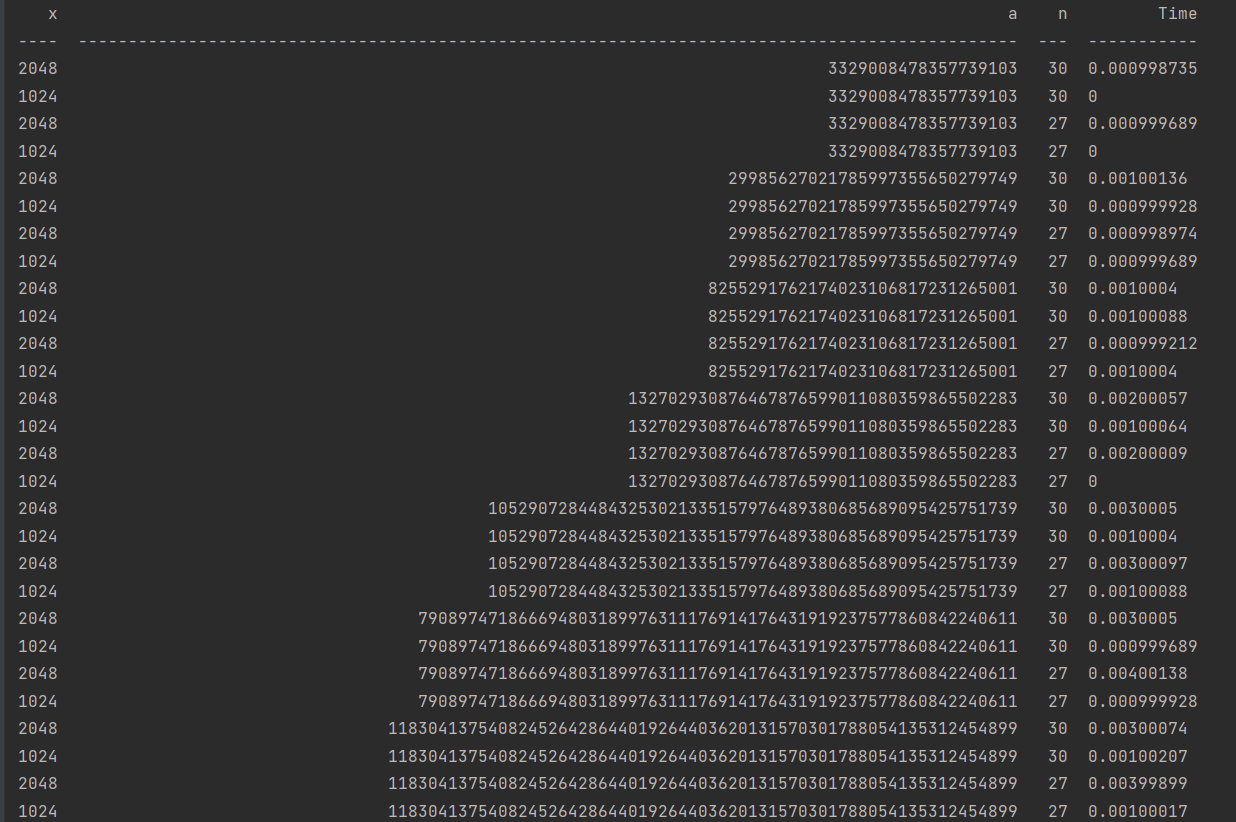


Рис. 4 – табличная форма зависимости времени вычисления параметра *y*

**Вывод**: в ходе лабораторной работы было разработано приложение для шифрования и расшифрования сообщения с помощью шифров RSA и Эль-Гамаля.