Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №10**

Студент: Бобрович Г.С.

ФИТ 3 курс 7 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Изучить и приобрести практические навыки разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.**

**1. С помощью простого консольного приложения составить табличную или графическую форму зависимости времени вычисления параметра *у*, зависящего 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 битов).**

**2. Разработать авторское оконное приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться доступными библиотеками либо программными кодами.**

****

Рисунок 1.1 — Результат выполнения задания 1

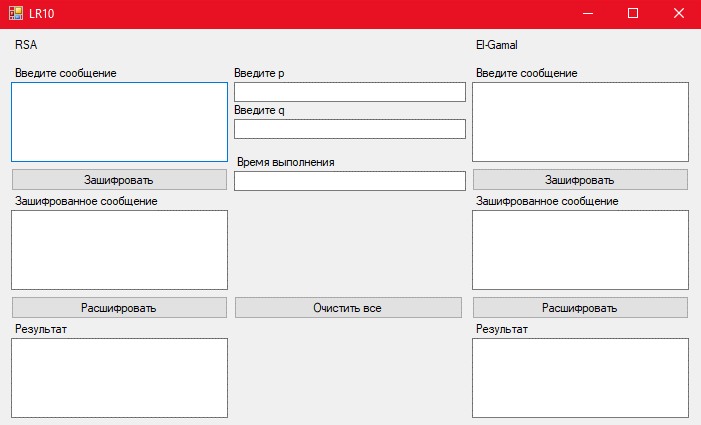


Рисунок 1.2 — Приложение задания 2

Проверим работу второго приложения. Сперва, проверим работу шифрования RSA:

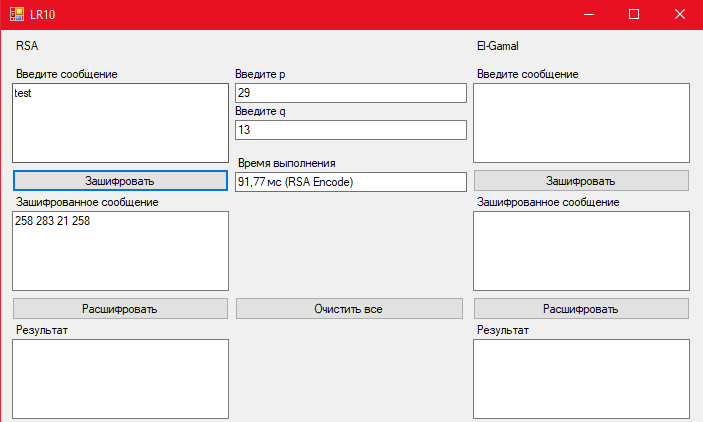


Рисунок 1.3 — Результат зашифрования с помощью алгоритма RSA

Далее, расшифруем полученное сообщение:

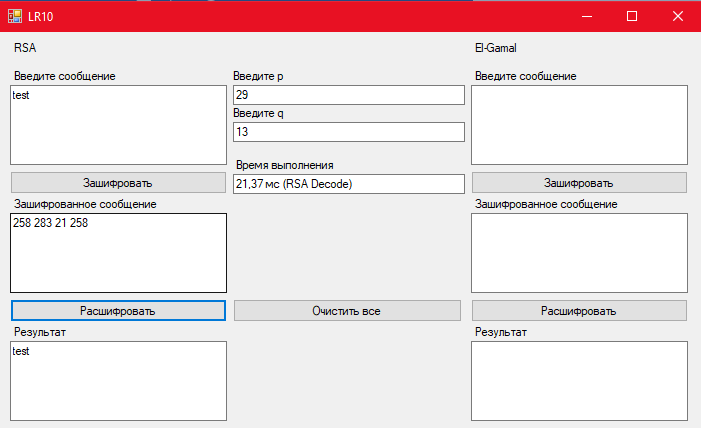


Рисунок 1.4 — Результат расшифрования с помощью алгоритма RSA

Теперь попробуем выполнить шифрование с помощью алгоритма Эль-Гамаля:

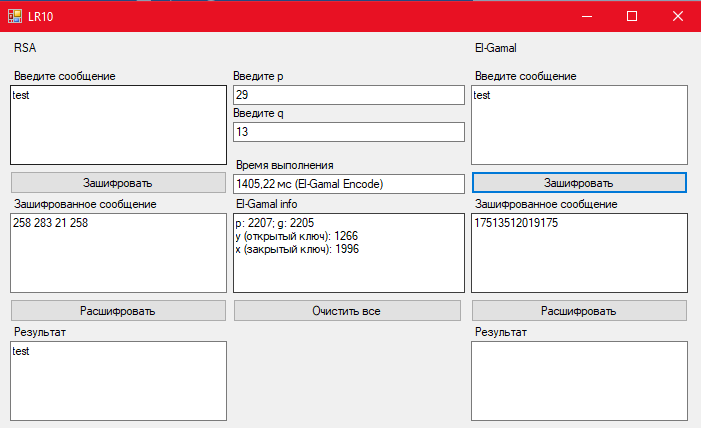


Рисунок 1.5 — Результат зашифрования с помощью алгоритма Эль-Гамаля

И расшифруем, используя тот же алгоритм:

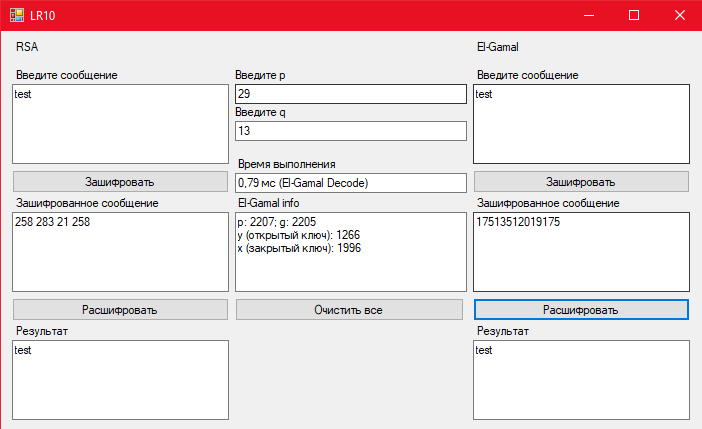


Рисунок 1.6 — Результат расшифрования с помощью алгоритма Эль-Гамаля

Сравним время выполнения при зашифровании и расшифровании с использованием разных алгоритмов

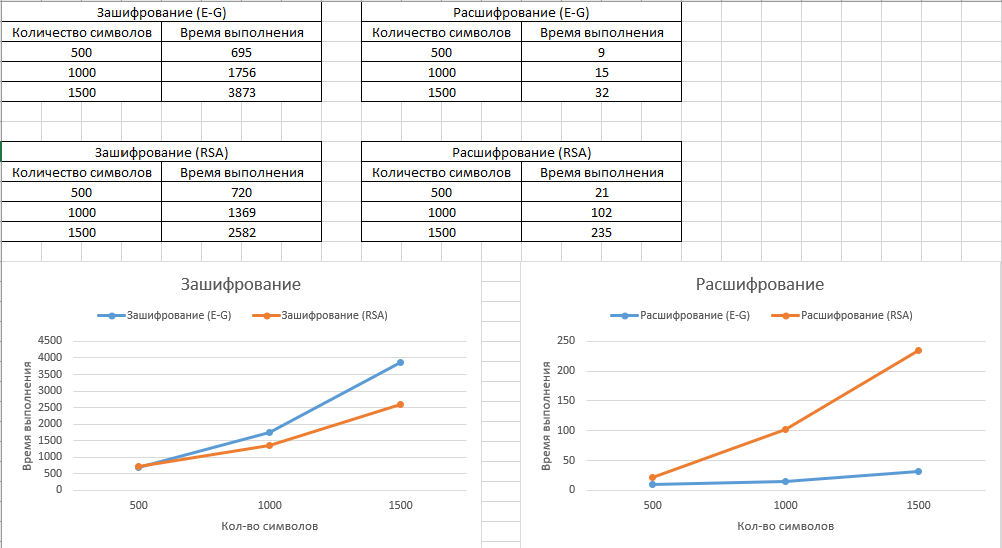


Рисунок 1.7 — Графики сравнения времени выполнения приложения 2

Точно так же сравним время вычисления параметра *у* в зависимости от значения *х*:

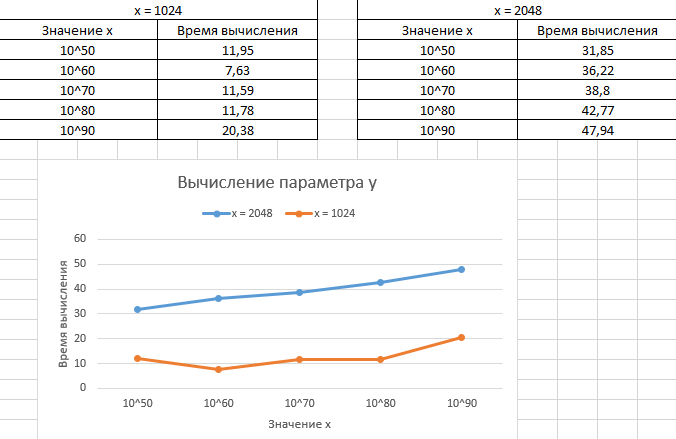


Рисунок 1.8 — График сравнения времени выполнения приложения 1

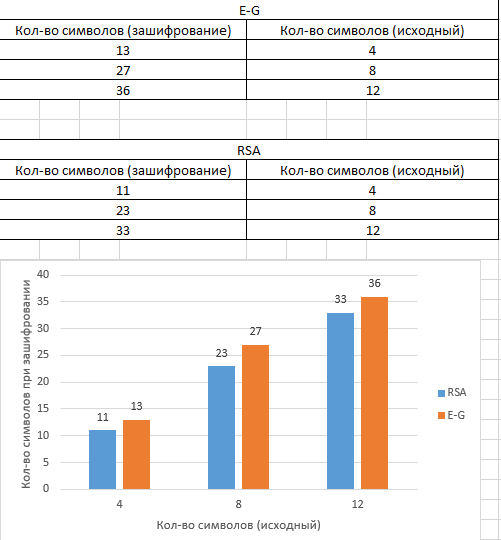


Рисунок 1.9 — Задание 3

**Вывод**

В ходе выполнения лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.