Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №12**

Студент: Бобрович Г.С.

ФИТ 3 курс 7 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Разработать авторское оконное приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться результатами выполнения предыдущих лабораторных работ, а также доступными библиотеками либо программными кодами.**

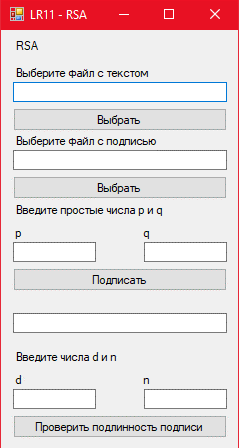
****

Рисунок 1.1 — Приложение 1 (RSA)

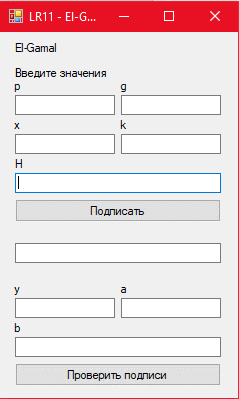
****

Рисунок 1.2 — Приложение 1 (Эль-Гамаль)

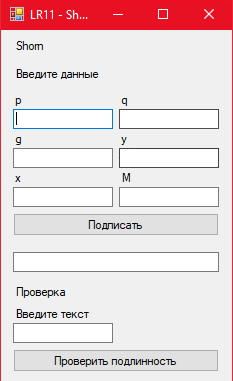
****

Рисунок 1.3 — Приложение 1 (Шнорр)

Проверим работоспособность приложения 1:

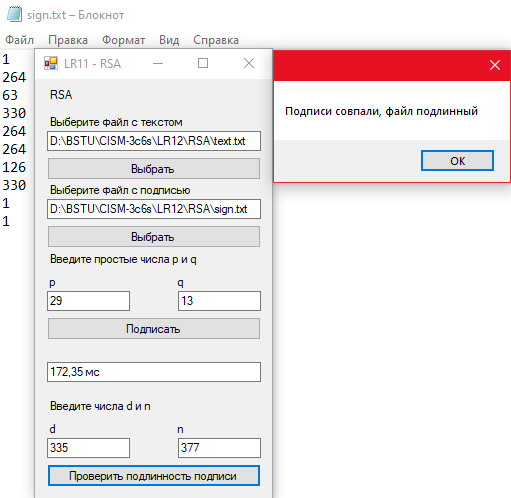


Рисунок 1.4 — Результат RSA

Проверим работоспособность приложения 2:

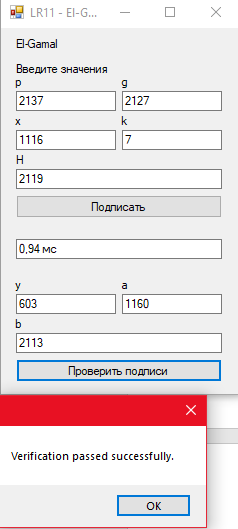


Рисунок 1.5 — Результат E-G

Проверим работоспособность приложения 3:

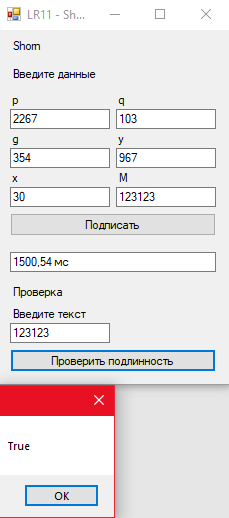


Рисунок 1.6 — Результат Шнорра

Оценим время выполнения каждого алгоритма:

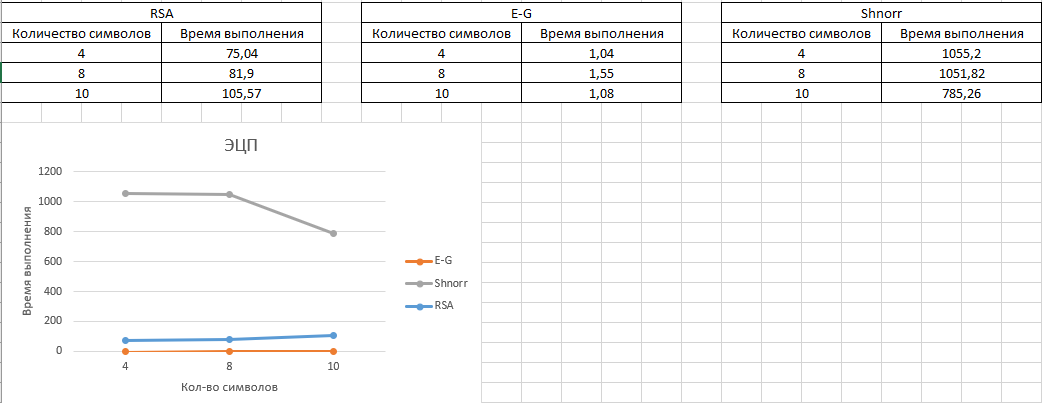


Рисунок 1.7 — Время выполнения

**Вывод**

В ходе лабораторной работы были изучены алгоритмы генерации и верификации электронной цифровой подписи и приобретены практических навыков их реализации.