Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование алгоритмов генерации

и верификации электронной цифровой подписи

Студент: Николаева Е.В.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет выполнить 2 задачи:

* генерация и верификация ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра;
* оценку времени выполнения указанных процедур при реальных ключевых параметрах.

1. **Методика выполнения поставленных задач**

## 2.1. Алгоритм RSA

Алгоритм генерации подписи RSA заключается в выборе простых чисел *p*, *q*, вычислении числа *n*=*p*×*q* и функции Эйлера *φ*(*n*)=(*p*-1)(*q*-1), выборе случайного числа e, взаимно простого с *φ*(*n*), нахождение числа *d*, такого что *e*×*d* = 1mod(*p*-1)(*q*-1), вычислении хеш-образа сообщения *h*=*H*(*M*), и в конце в вычислении ЭЦП: *S* = *hd* mod *n*.

Функция, где вычисляется ЭЦП с помощью переменных *d*, *e* и *φ*(*n*), приведена на рисунке 2.1. Функция верификации ЭЦП представлена на рисунке 2.2. Для функции верификации необходимо вычислить *h* = *Se* mod *n*, а после сравнить значение с хеш-образом. Результат работы RSA представлен на рисунке 2.3.

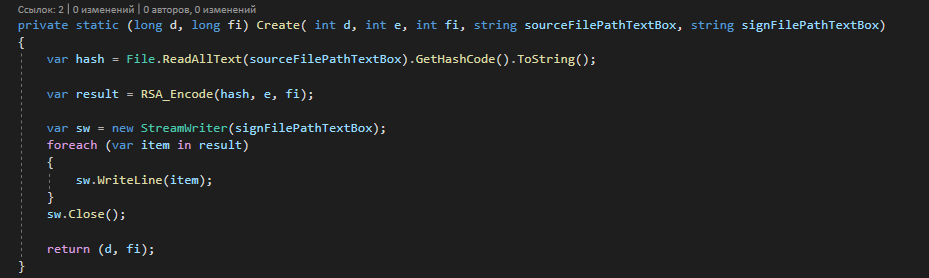


Рис. 2.1 – Генерация ЭЦП

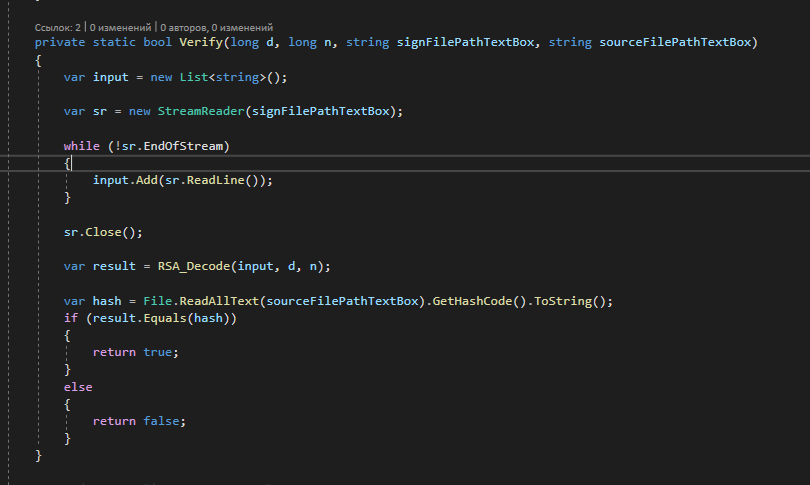


Рис. 2.2 – Функция верификации ЭЦП

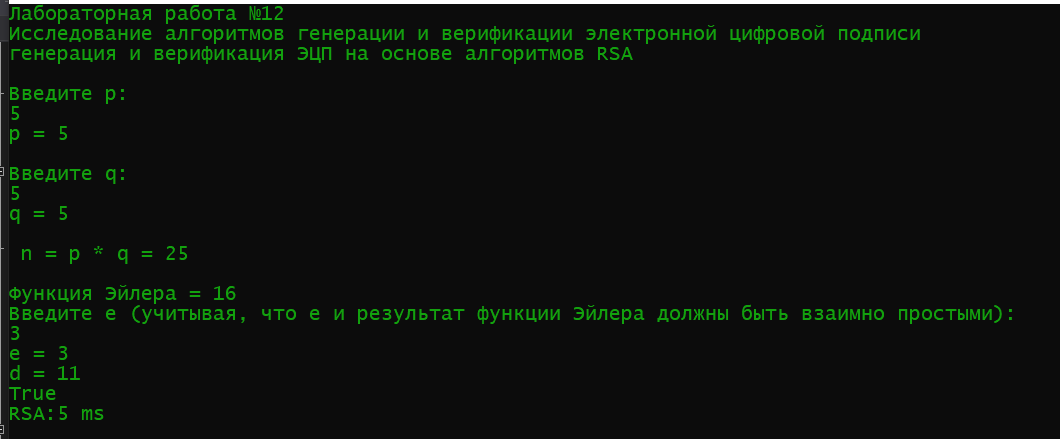


Рис. 2.3 – Результат работы алгоритма

## 2.2. Алгоритм Эль-Гамаля

Алгоритм генерации подписи RSA заключается в выборе простых чисел *p*, вычислении числа *q*- первообразный корень по модулю *p*, выборе случайного числа х, что меньше р, вычисление *y* = *gx*mod*p*.

Для верификации подлинности полученного сообщения необходимо проверить равенство *ya*×*ab* (mod *p*) = *gh*(mod*p*). Результат работы Эль-Гамаля представлен на рисунке 2.4

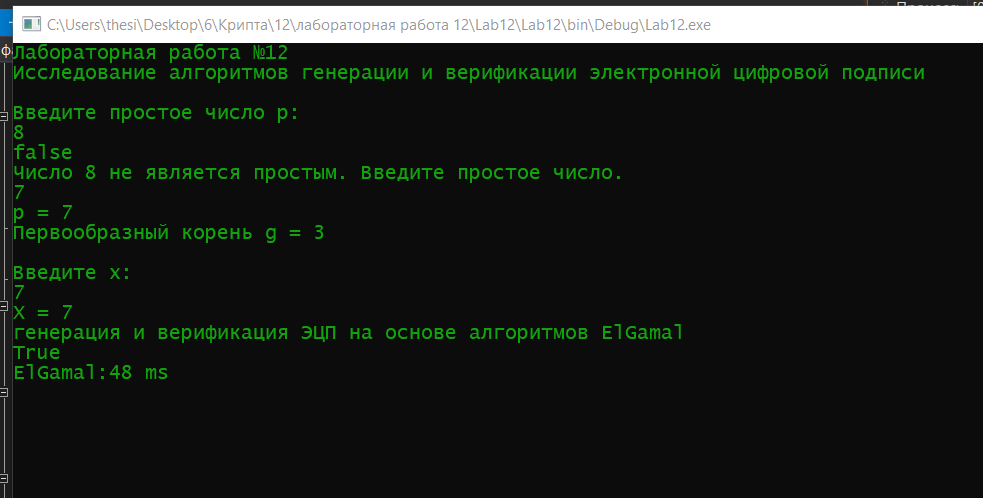


Рис. 2.4 – Результат работы алгоритма

## 2.3. Алгоритм Шнорра

Алгоритм генерации ключевой информации заключается в следующих шагах: генерация простых чисел *p*, *q*, вычисление (*p*-1) – делителя, выбор любого *g*≠1, такого что *g*×*q* = 1 mod *p*, выбор любого числа *х*<*q* – это и будет закрытый ключ, вычисление *y* = *g*–*X*mod*p*;

Для проверки подписи на подлинность необходимо вычислить *X*=*gb*×*yh* (mod *p*), после чего проверить выполняется ли равенство вычисленного ранее *h* хеш-образа и *H*(*М*||*X*) хеш-образа конкатенации полученного сообщения с вычисленным значением *Х*. Если равенство выполняется, подпись верифицирована. Результат работы Алгоритма Шнорра представлен на рисунке 2.5

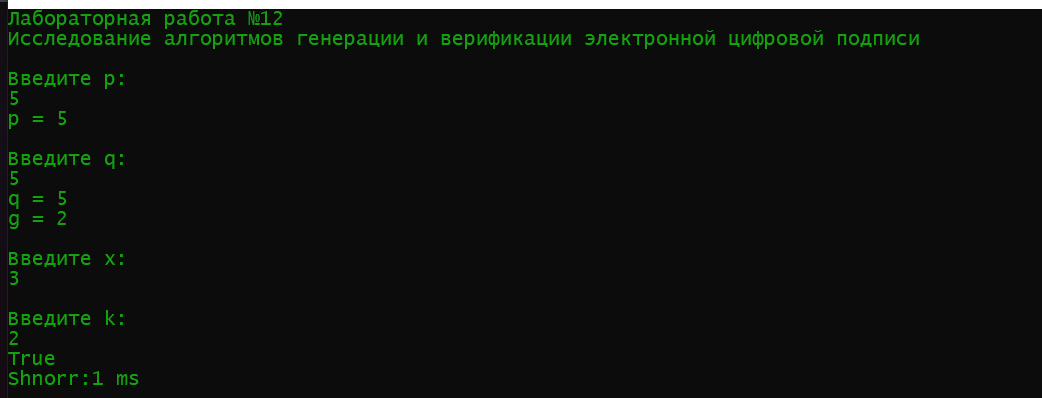


Рис. 2.5 – Результат работы алгоритма

## 3. Оценка времени выполнения указанных процедур

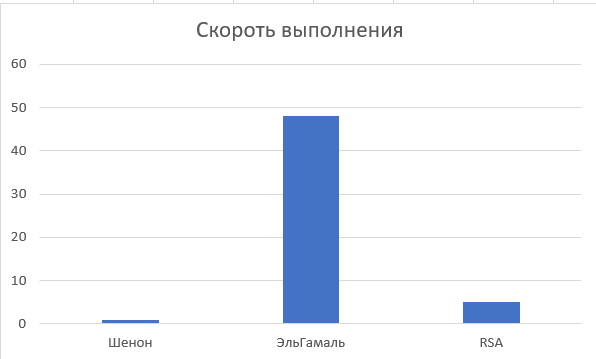


Рис. 2.6 – График скорости работы алгоритма

На графике видно, что процедура Шенона является самой быстрой. Это можно объяснить тем, что у Шенона самый маленький размер подписи. После же идет RSA и Эль-Гамаль, где размер подписи намного больше Шенона и вычисления являются более трудозатратным.

**Вывод**

В ходе лабораторной работы были изучены алгоритмы генерации и верификации электронной цифровой подписи, а также приобретены практические навыки их реализации. Также была оценена скорость генерации и верификации ЭЦП.