МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №10**

**″ИССЛЕДОВАНИЕ АЛГОРИТМОВ ГЕНЕРАЦИИ И ВЕРИФИКАЦИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ″**

Выполнил:

Cтудент 3 курса 2 группы

Говоронок В.А.

Проверил:

Преподаватель-стажер

Копыток Д.В.

Минск 2021

Цель: изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций генерации и верификации электронной цифровой подписи (ЭЦП).

2. Получить навыки практической реализации методов генерации и верификации ЭЦП на основе хеширования подписываемых сообщений и алгоритмов RSA, Эль-Гамаля и Шнорра, а также DSA.

3. Разработать приложение для реализации заданных алгоритмов генерации и верификации ЭЦП.

4. Оценить скорость генерации и верификации ЭЦП.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

Выполнение работы:

Программная реализация выполнена на языке C# с использованием консольного приложения и формы.

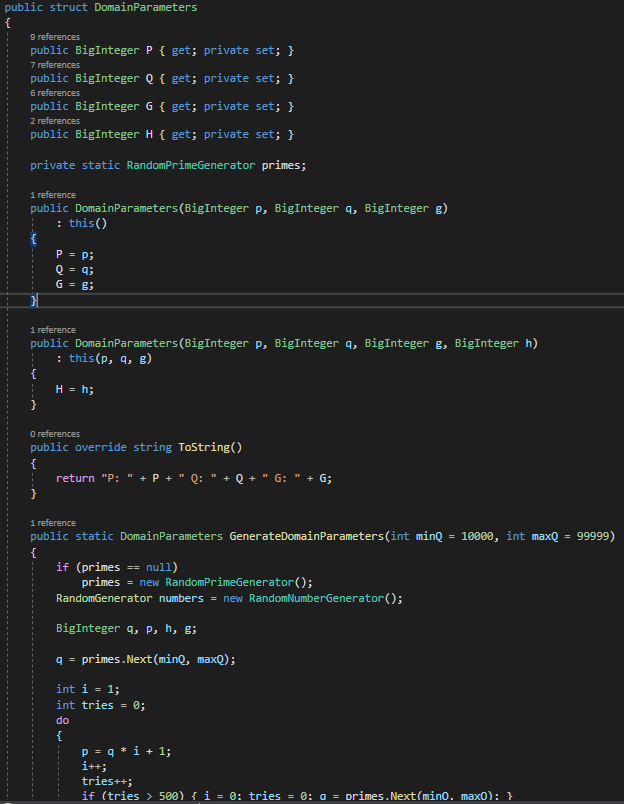


Рисунок 1 – Пример кода

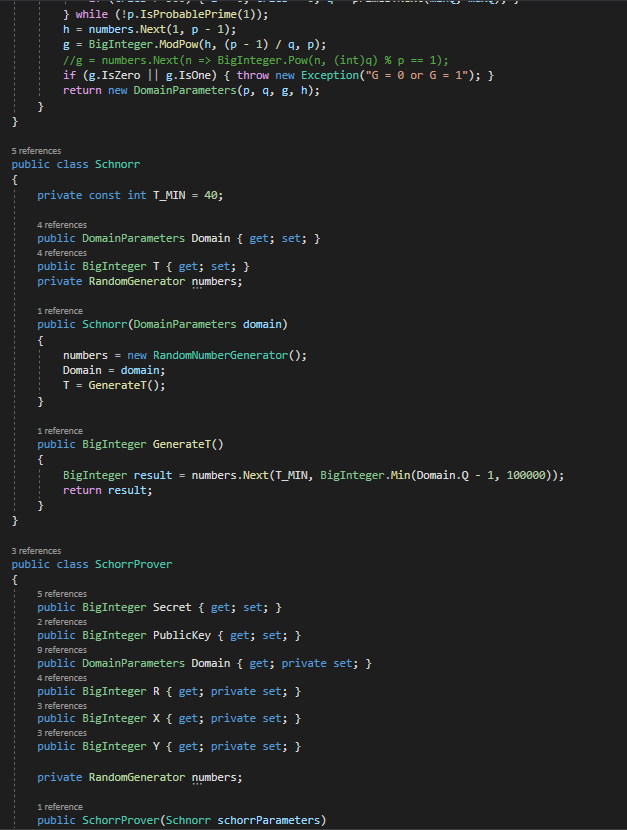


Рисунок 2 – Пример кода

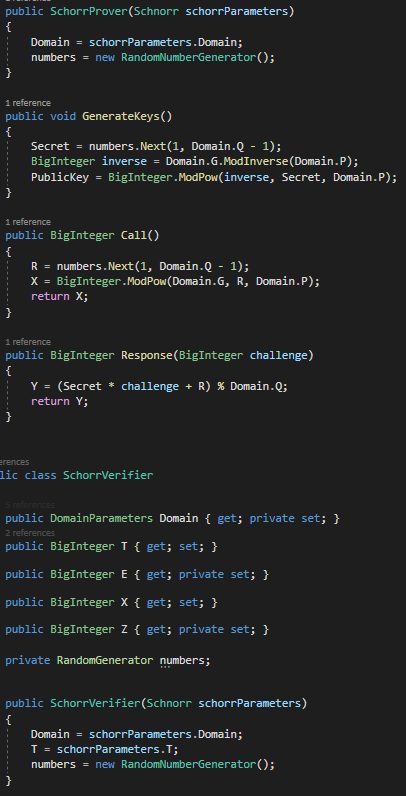
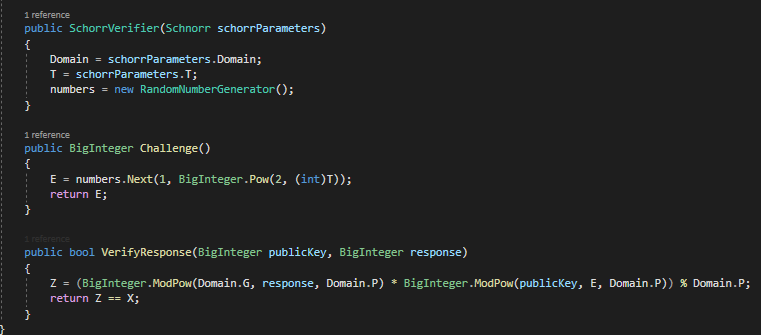


Рисунок 3 – Пример кода

Рисунок 4 – Пример кода

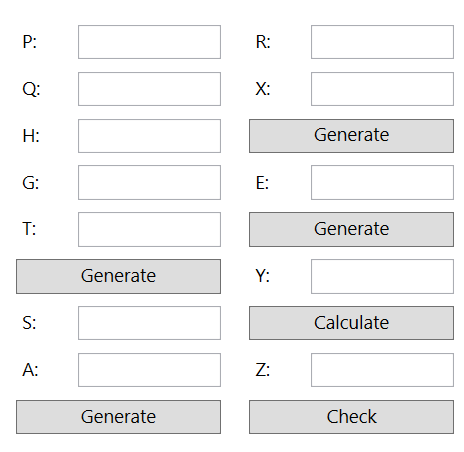


Рисунок 5 – Визуализация программы

Вывод: в результате данной лабораторной работы было разработано приложение для реализации заданных алгоритмов генерации и верификации ЭЦП.