УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №4

по предмету

Теория Информации

Вариант 1

Выполнил:

Романовский М.И.

Проверила:

Болтак С.В.

Группа 351004

Минск 2025

**Задание:**

Реализовать программное средство, выполняющее вычисление и проверку электронной цифровой подписи (**ЭЦП**) текстового файла **на базе алгоритма RSA**. Для вычисления хеш-образа сообщения использовать функцию 3.2 из методических материалов (стр.22, **Н0=100**). Числа ***p* и *q***, а также закрытый ключ ввести с клавиатуры. Произвести все необходимые проверки для параметров, вводимых с клавиатуры. В отдельное поле вывести полученный хеш сообщения в 10 с/cч. ЭЦП вывести как целое число. Сформировать новое сообщение, состоящее из исходного сообщения и добавленной к нему цифровой подписи. При проверке ЭЦП предусмотреть возможность выбора файла для проверки. На экран вывести результат проверки:

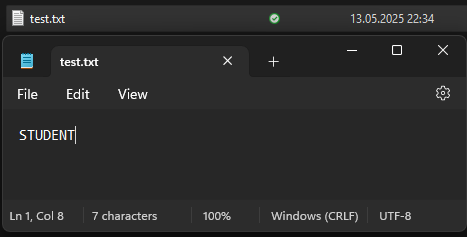
1 – сообщение о том верна подпись или нет;

2 – вычисленные при проверке значения.

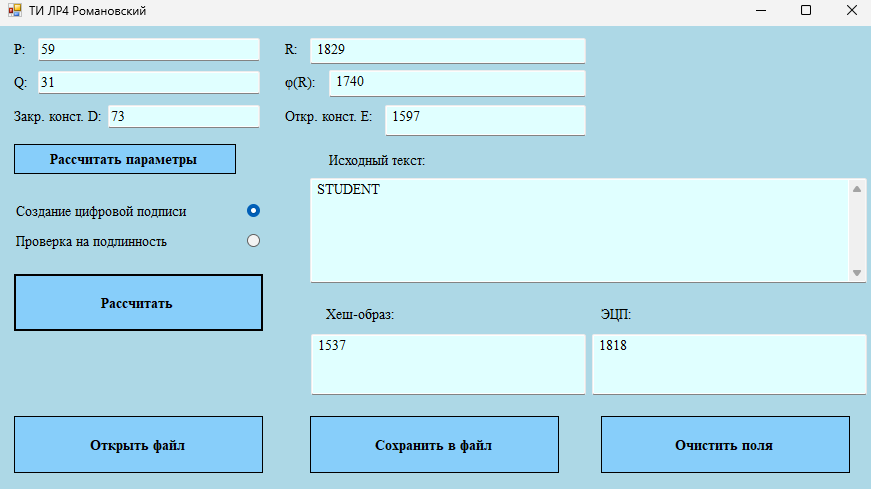
Для возведения в степень использовать быстрый алгоритм возведения в степень по модулю.

**Тесты на разных файлах**

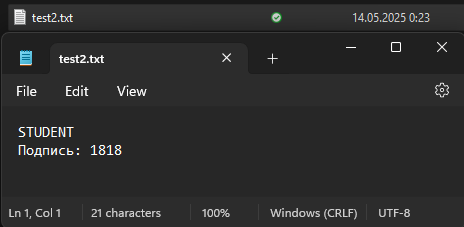
1. Текстовый файл с верной подписью:

Исходное содержимое:  


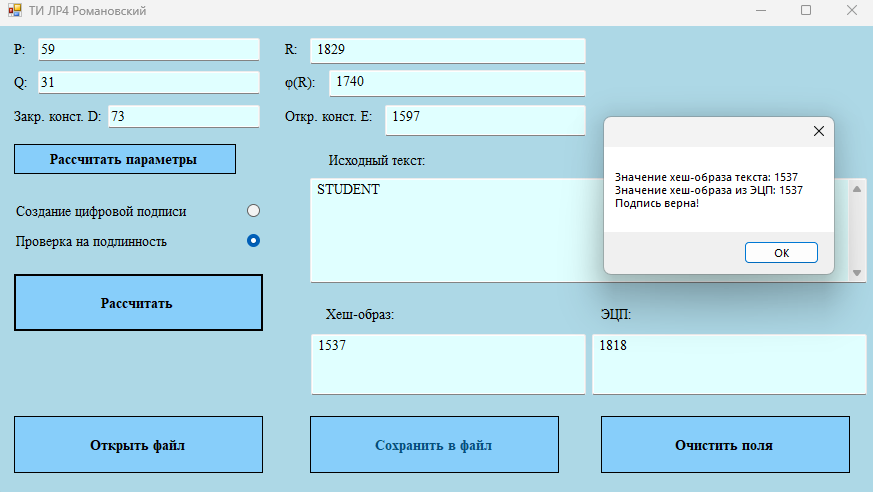
Результат создания цифровой подписи:



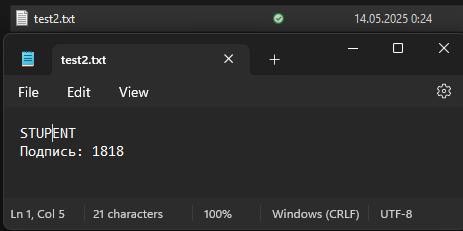
Отображение подписанного содержимого в файле:



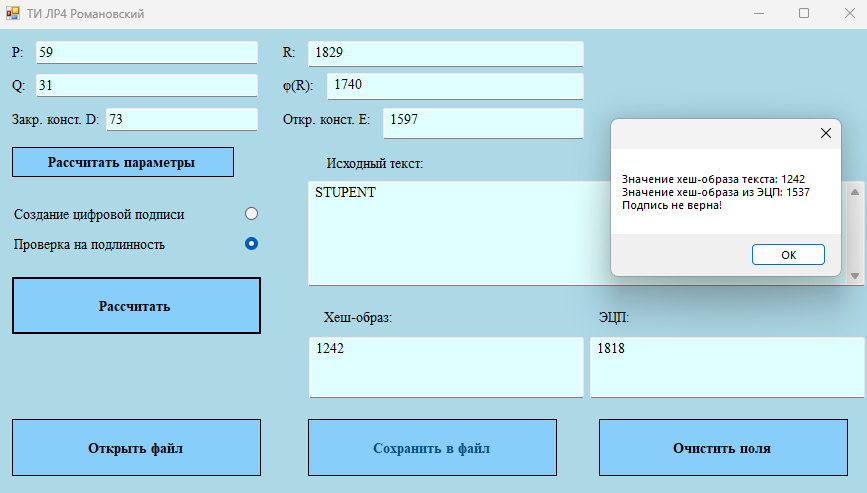
Результат проверки подписи:



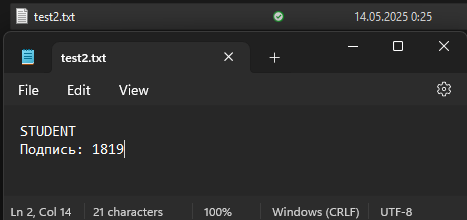
1. Текстовый файл с измененным содержимым и правильной подписью:

Исходное содержимое:  


Результат проверки подписи:



1. Текстовый файл с правильным содержимым и измененной подписью:

Исходное содержимое:  


Результат проверки подписи:

