УО «Белорусский государственный университет   
информатики и радиоэлектроники»

Кафедра ПОИТ

Отчёт по лабораторной работе № 4  
по предмету «Теория информации»  
Вариант 1

Выполнила:

Сучёк Е.А.

гр. 351003

Проверила:

Болтак С.В.

Минск 2025

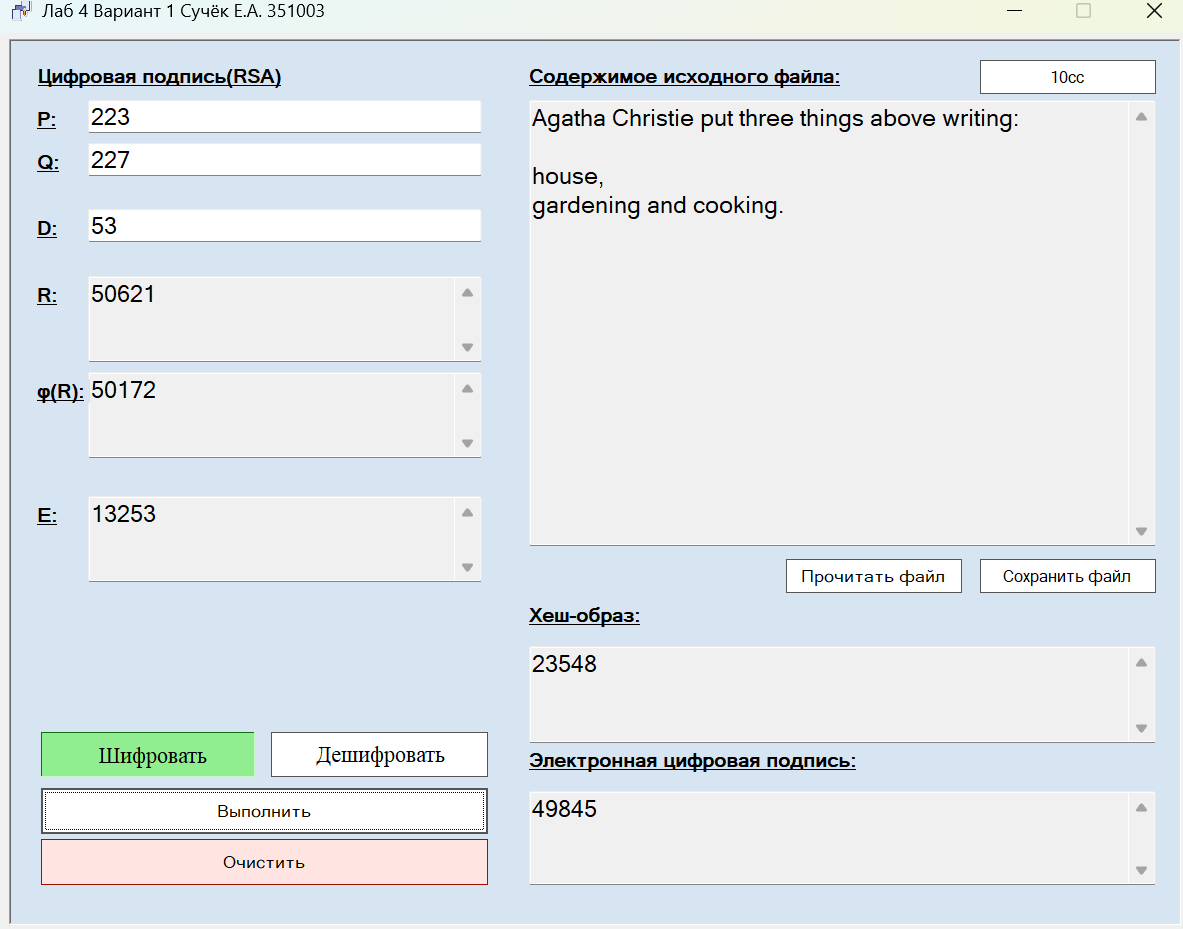
**Задание:**

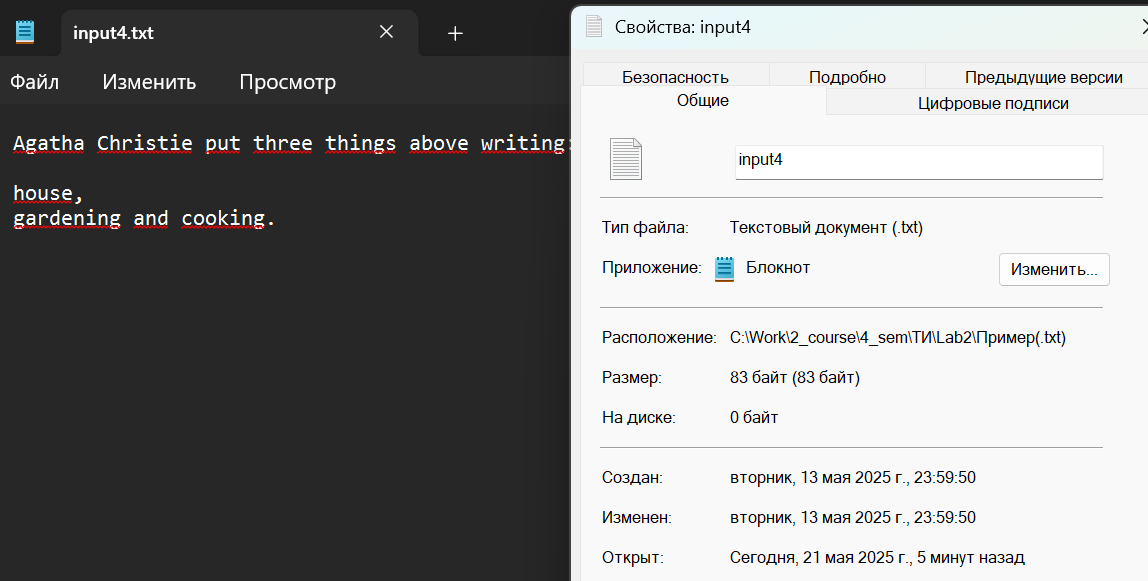
Реализовать программное средство, выполняющее вычисление и проверку электронной цифровой подписи (**ЭЦП**) текстового файла **на базе алгоритма RSA**. Для вычисления хеш-образа сообщения использовать функцию 3.2 из методических материалов (стр.22, **Н0=100**). Числа ***p* и *q***, а также закрытый ключ 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.

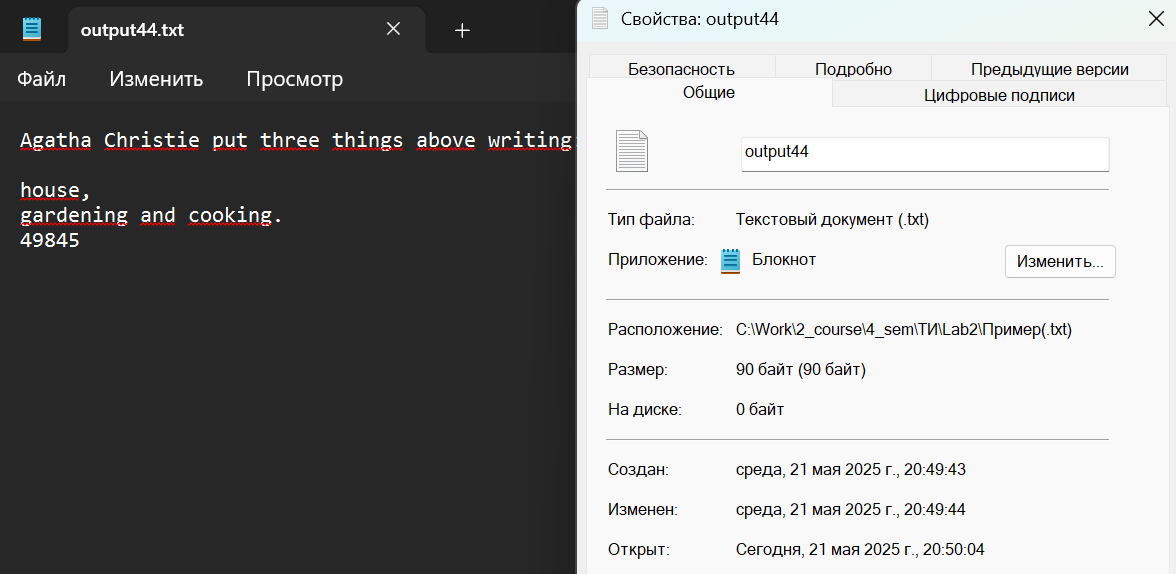
Для возведения в степень использовать быстрый алгоритм возведения в степень по модулю.

**Пример выполнения программы:**

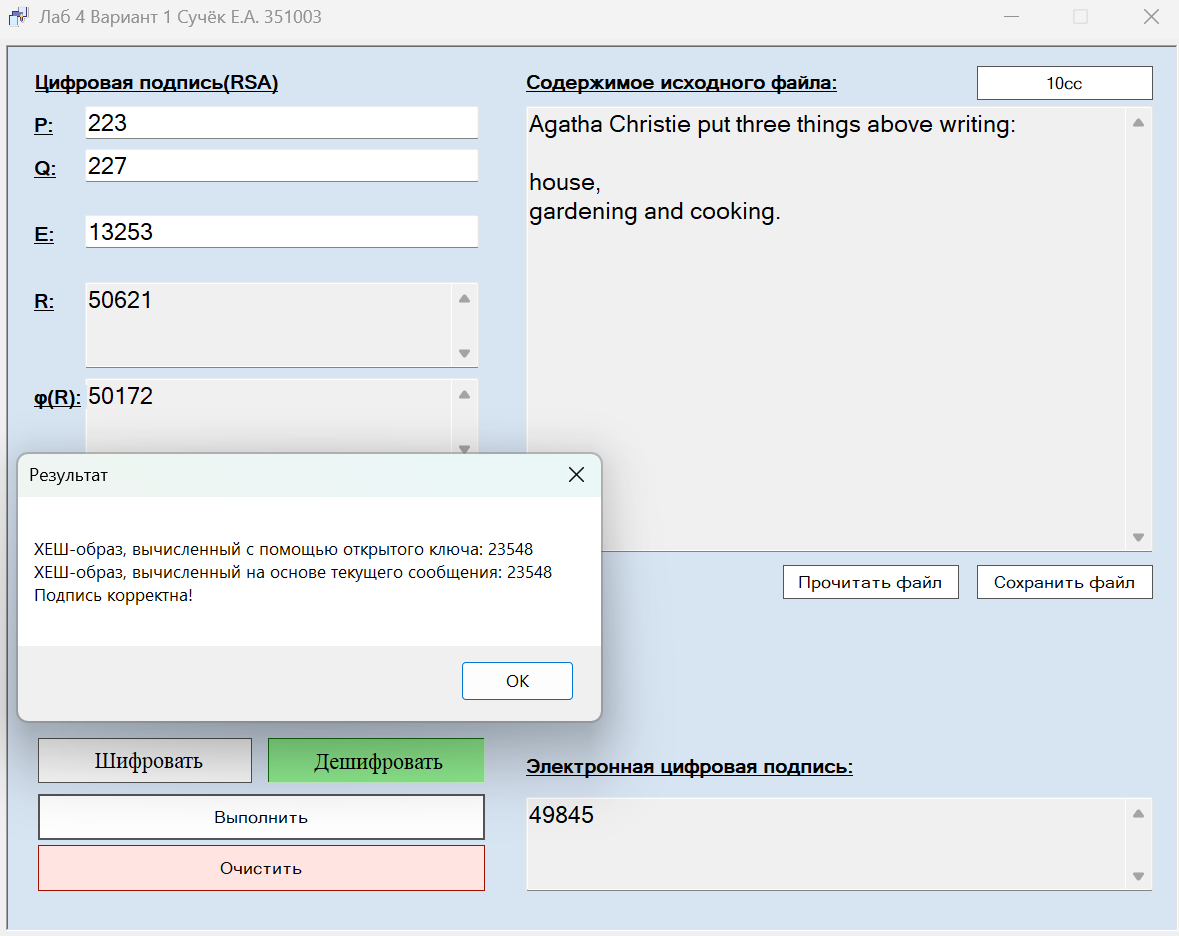
**Процесс добавления цифровой подписи:**



**Содержимое исходного файла:**

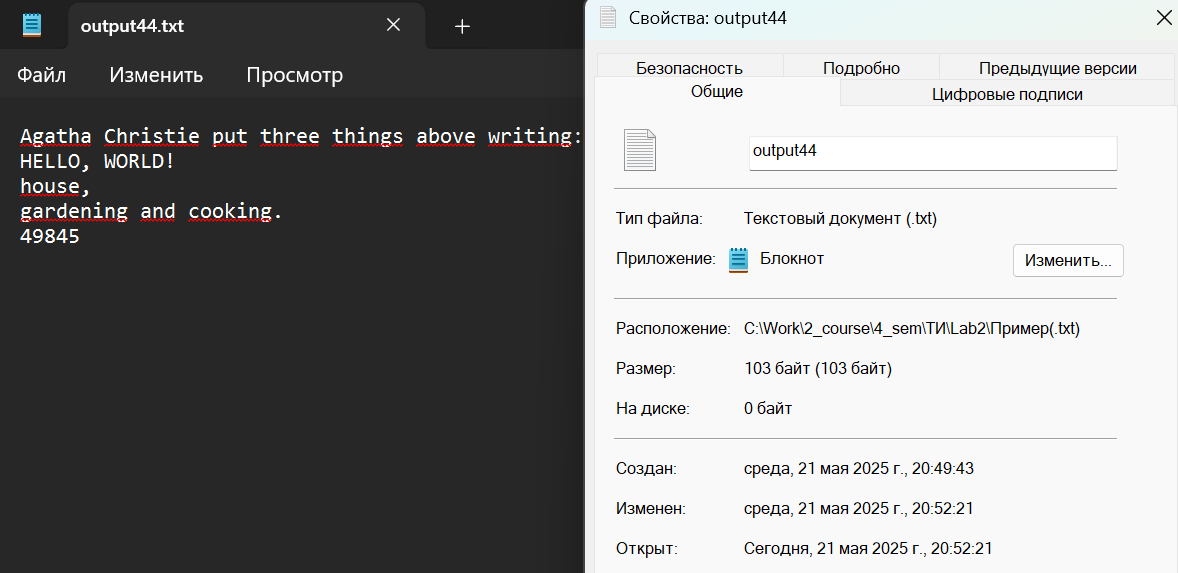
**Содержимое файла с подписью:**

**Процесс проверки цифровой подписи:**

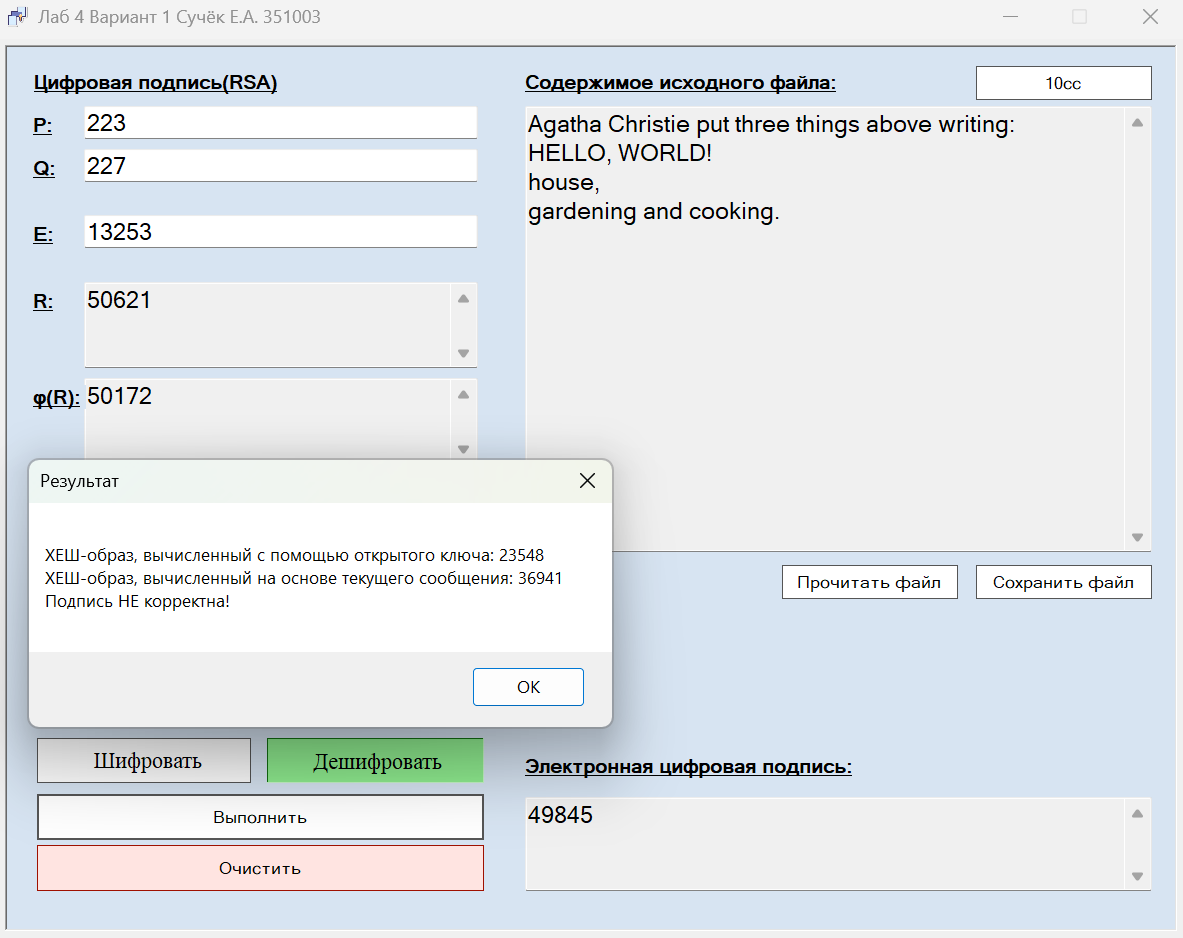


**Изменим файл с цифровой подписью:**

**Содержимое изменённого файла:**

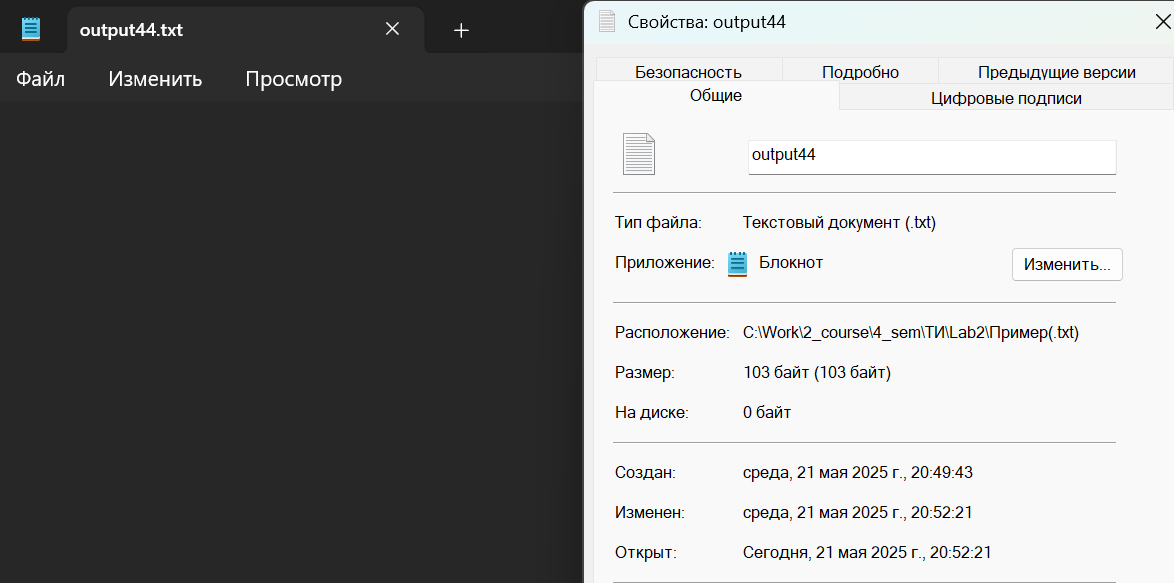


**Процесс проверки изменённого файла:**

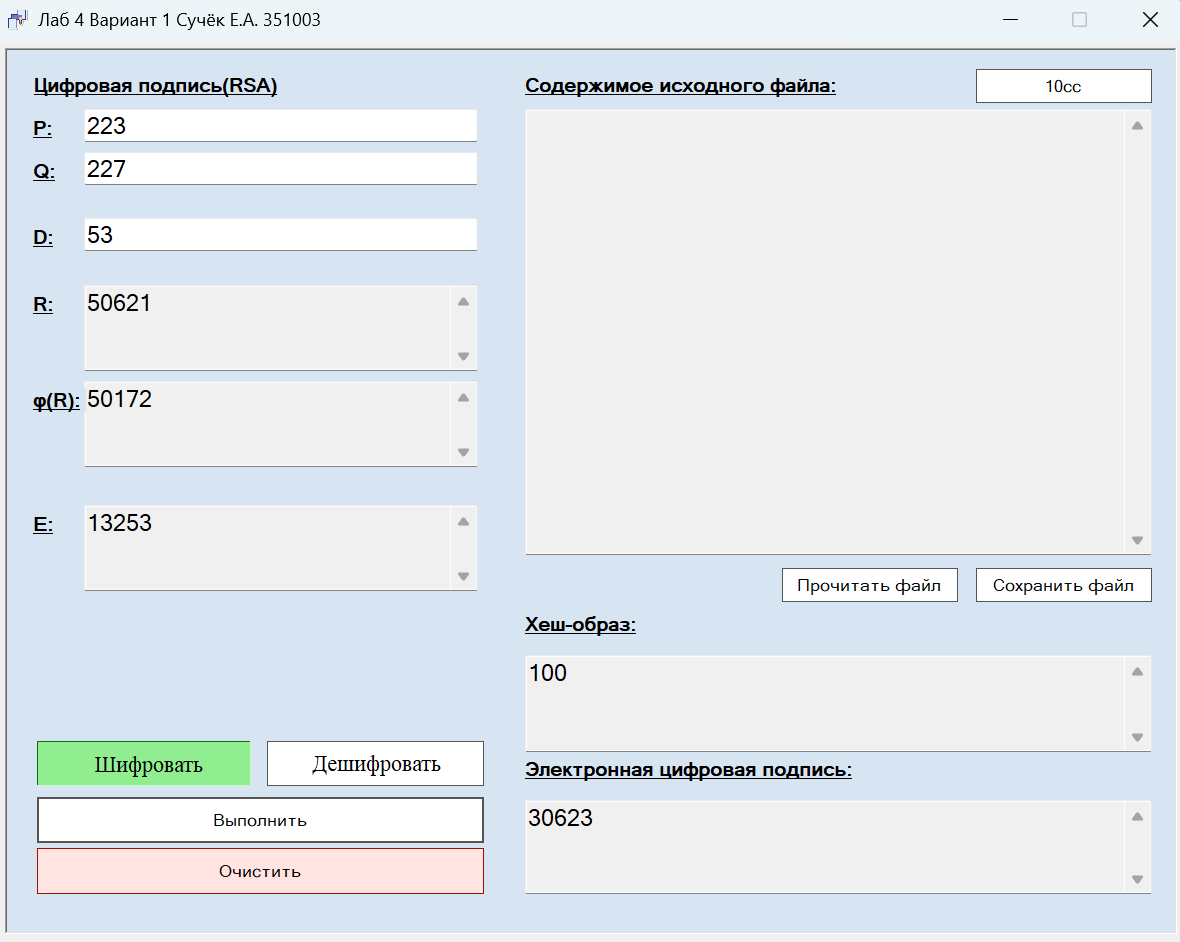
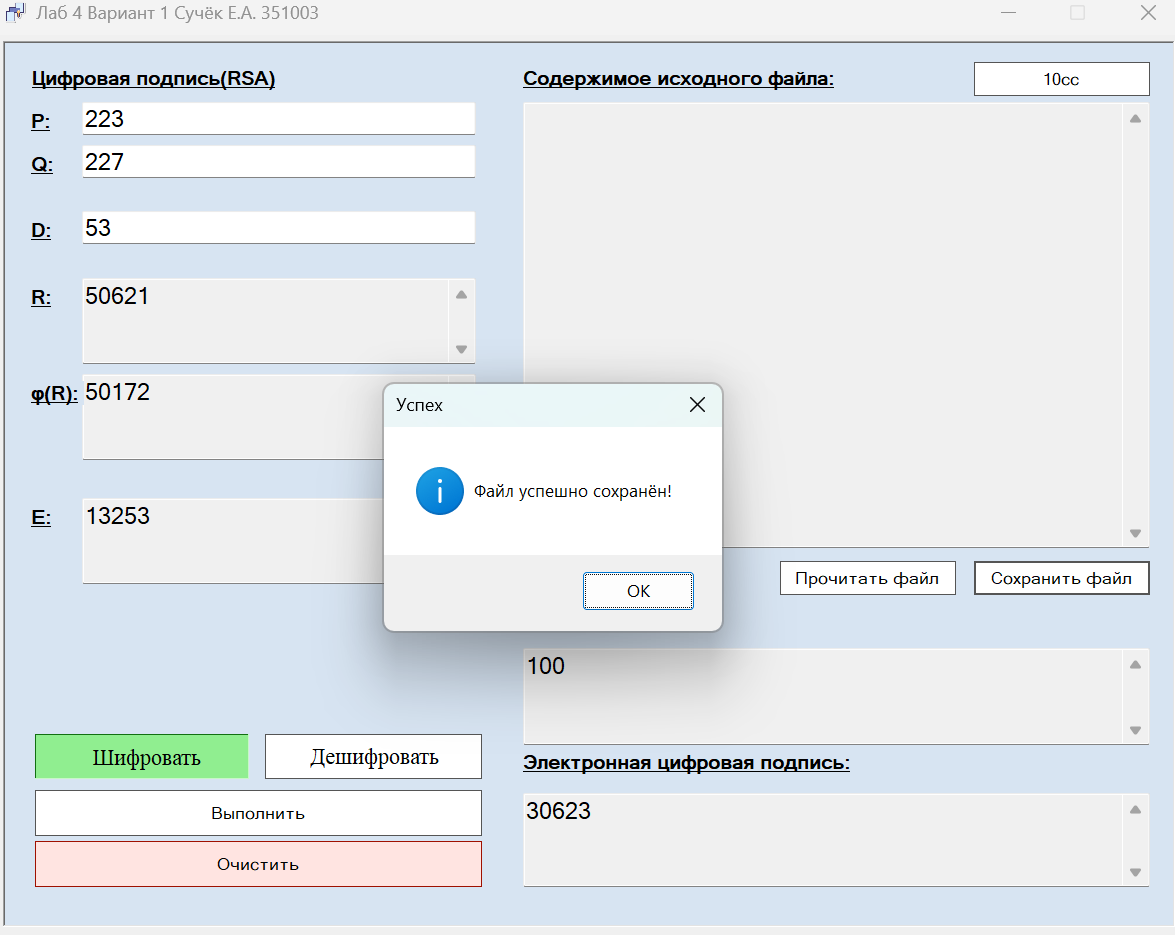


**Цифровая подпись для пустого файла:**

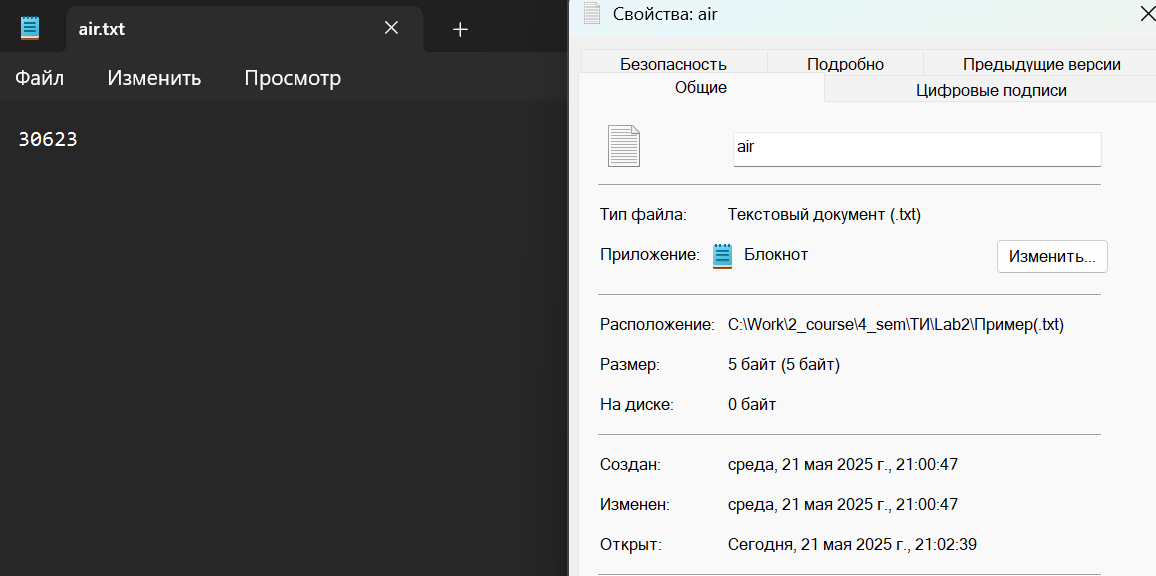
**Содержимое файла:**



**Процесс вычисления цифровой подписи:**

**Содержимое файла с цифровой подписью:**



**Процесс проверки цифровой подписи:**

