УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №4

по предмету «Теория информации»

Вариант 2

Выполнил:

Колбеко В.С.

гр. 351003

Проверила:

Болтак С.В.

Минск 2025

**Вариант №2**

Реализовать программное средство, выполняющее вычисление и проверку электронной цифровой подписи (**ЭЦП**) текстового файла **на базе алгоритма DSA**. Для вычисления хеш-образа сообщения использовать функцию

**Hi = (Hi−1 + Mi)2 mod q**,

где **q** – большое простое число, **Н0 = 100** – произвольное начальное значение, **Mi** – i-й блок сообщения M = {M1, M2, …, Mk}.

Числа ***q, p, h, x, k*** ввести с клавиатуры, произвести все необходимые проверки для параметров, вводимых с клавиатуры. В отдельное поле вывести полученный хэш сообщения в 10 с/cч.

ЭЦП вывести как два целых числа (если одно из полученных значений ***r*** или***s*** будет равно 0, то необходимо повторить вычисления для другого значения ***k*** – предложить повторно ввести ***k*** с клавиатуры). 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 результаты проверки:

* сообщение о том верна подпись или нет;
* вычисленные при проверке значения параметров.

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

При нахождении обратного элемента ***s−1mod q*** или ***k−1 mod q*** использовать ***малую теорему Ферма*** в виде: ***s−1mod q= sq-2 mod q­***.

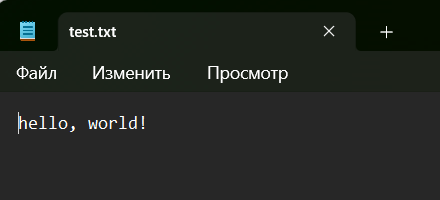
1. **Проверка корректной подписи текстового файла.**

**Шифрование:**

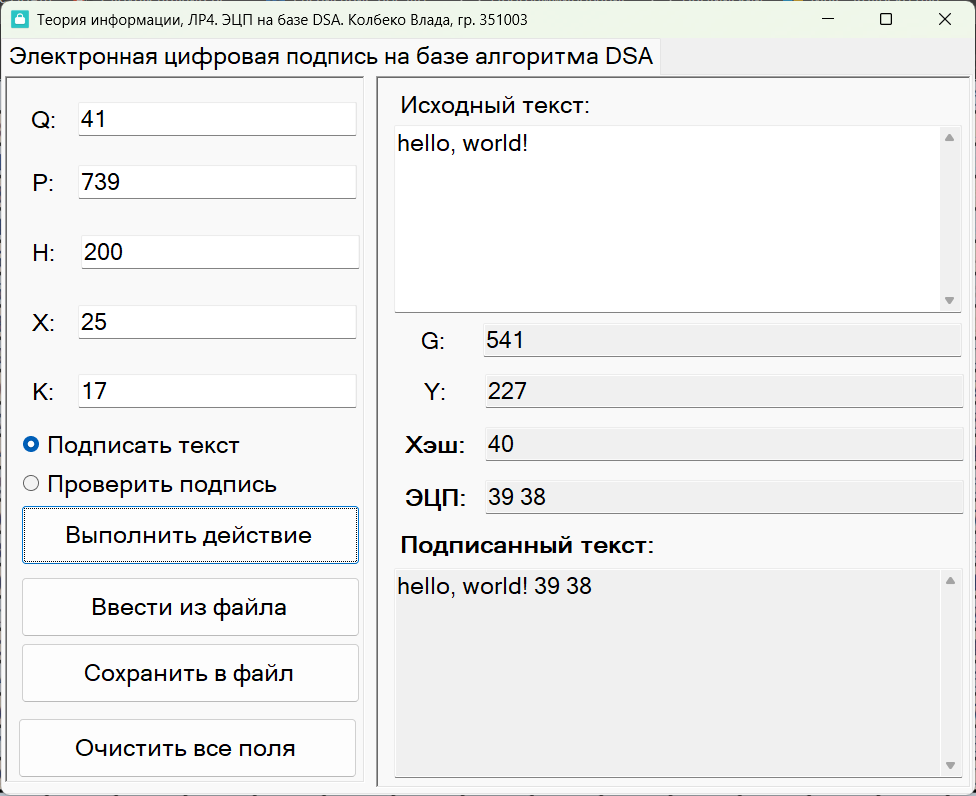
Файл ввода: test.txt

Файл вывода: test\_signed.txt

Содержимое файла ввода:



Результат подписи файла:

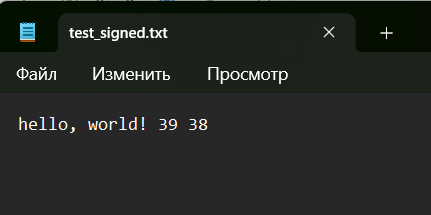


1. **Проверка корректной работы проверки подписи.**

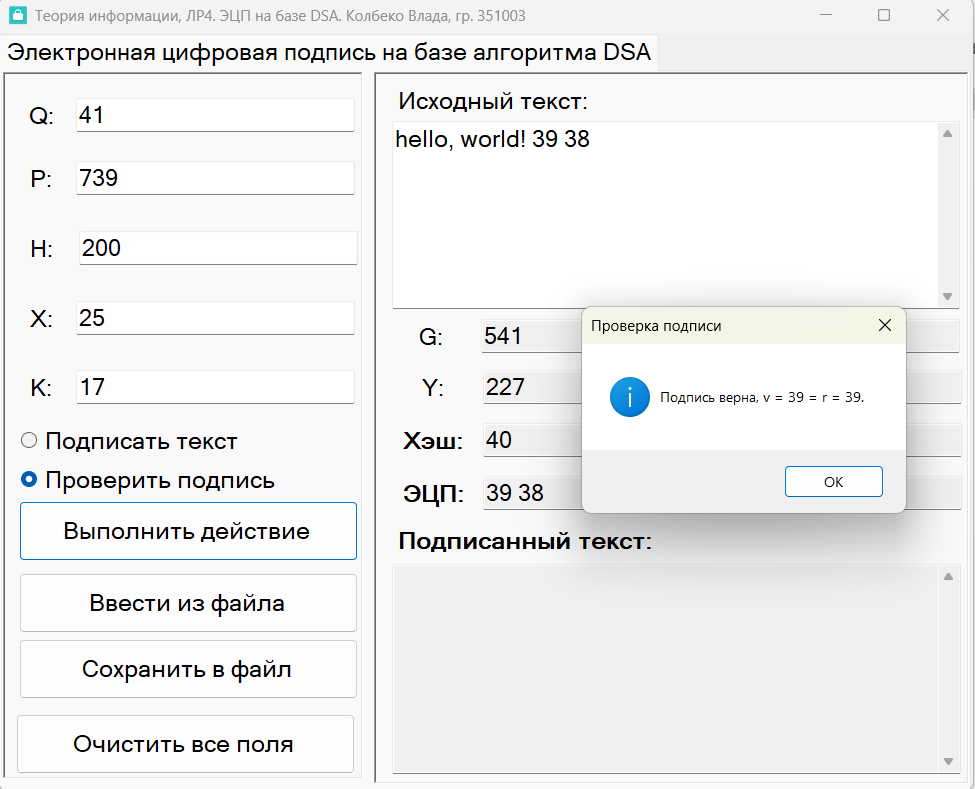
**Корректный файл:**

Файл ввода: test\_signed.txt

Содержимое файла ввода:



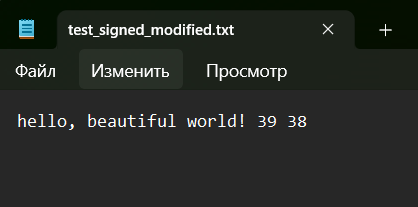
Результат проверки подписи:



**Модифицированный файл:**

Файл ввода: test\_signed\_modified.txt

Содержимое файла ввода:



Результат проверки подписи:

