**Задание**

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 n**,

где **n = p·q, p и q** – большие простые числа, **Н0 = 100** – произвольное начальное значение, **Mi** – i-й блок сообщения M = {M1, M2, …, Mk}.

Вычисления функции необходимо выполнять по модулю числа ***q*.** Числа ***q, p, h, x, k*** 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 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.

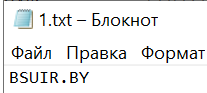
При проверке ЭЦП предусмотреть возможность выбора файла для проверки. На экран вывести результаты проверки: сообщение о том верна подпись или нет; вычисленные при проверке значения параметров.

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

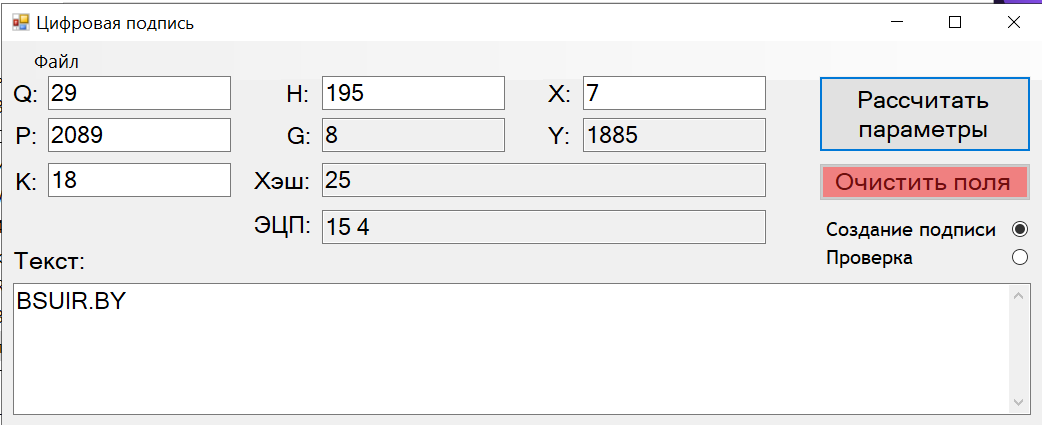
При нахождении обратного элемента ***s−1mod q*** или ***k−1 mod q*** использовать ***малую теорему Ферма*** в виде: ***s−1mod q= sq-2 mod q***

**Тесты**

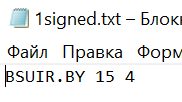
Исходный тест:



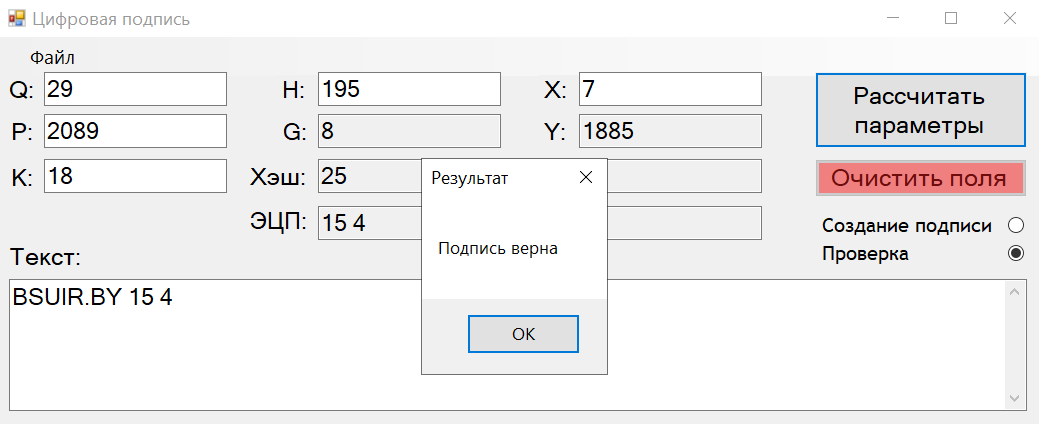
Создание подписи:



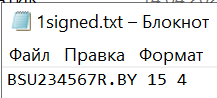
Сохранённый подписанный файл:



Проверка подписи:



Изменим подписанный файл:



Проверка подписи:

