**Вариант 1**

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.

**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 3.2 из методических материалов (стр.22, **Н0=100),** вычисления функции необходимо выполнять по модулю числа ***q*.** Числа ***q, p, h, x* и *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* для чего 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 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.

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***