УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №4

по предмету

Теория Информации

Вариант 2

Выполнил:

Пуренок А.С.

Проверил:

Болтак С.В.

Группа 351004

Минск 2025

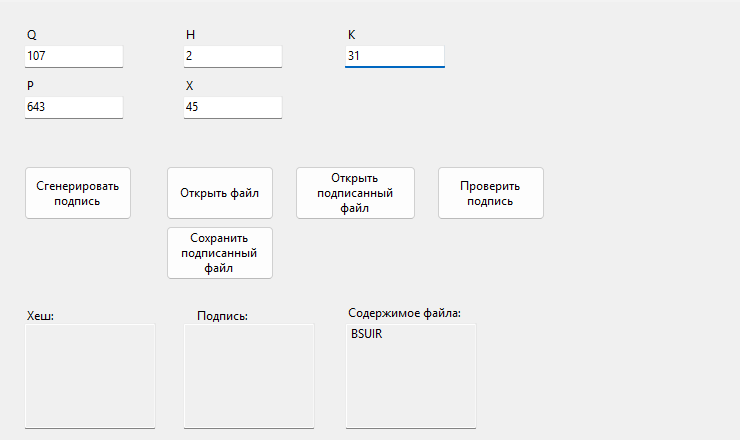
**Задание:**

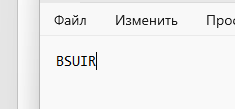
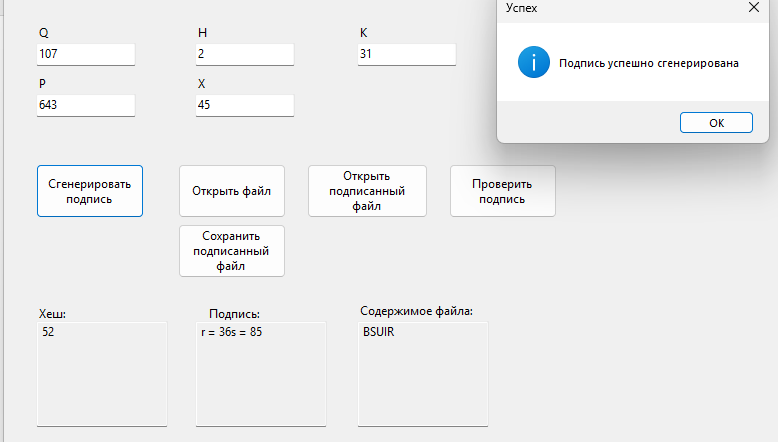
Реализовать программное средство, выполняющее вычисление и проверку электронной цифровой подписи (**ЭЦП**) текстового файла **на базе алгоритма DSA**. Для вычисления хеш-образа сообщения использовать функцию 3.2 из методических материалов (стр.22, **Н0=100),** вычисления функции необходимо выполнять 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:

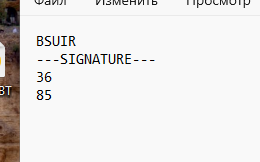
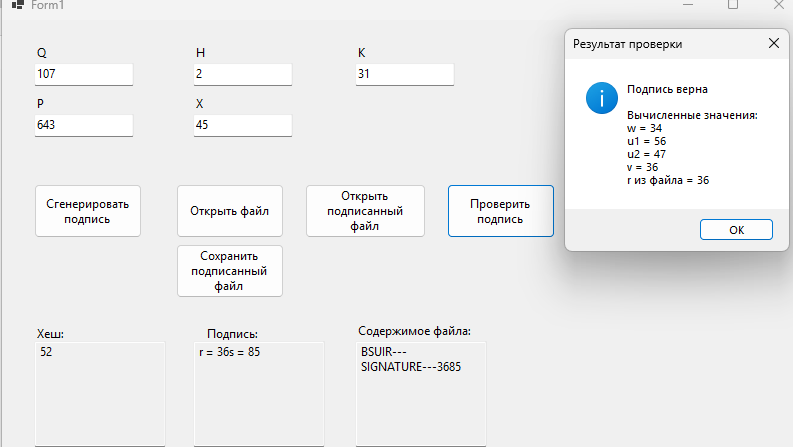
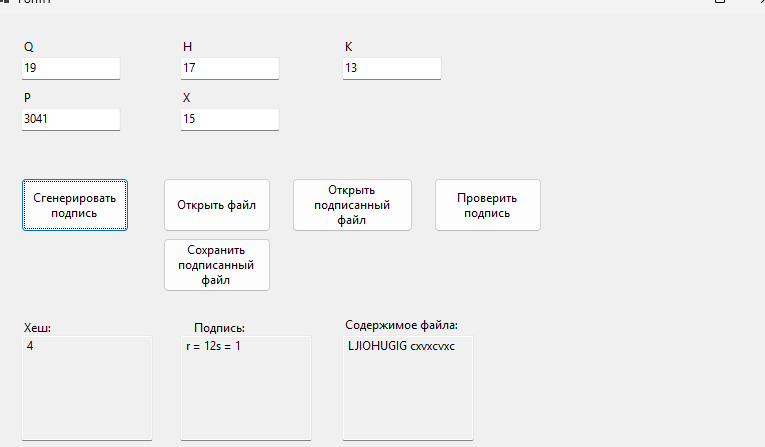
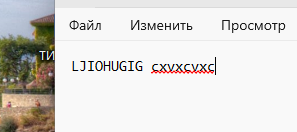
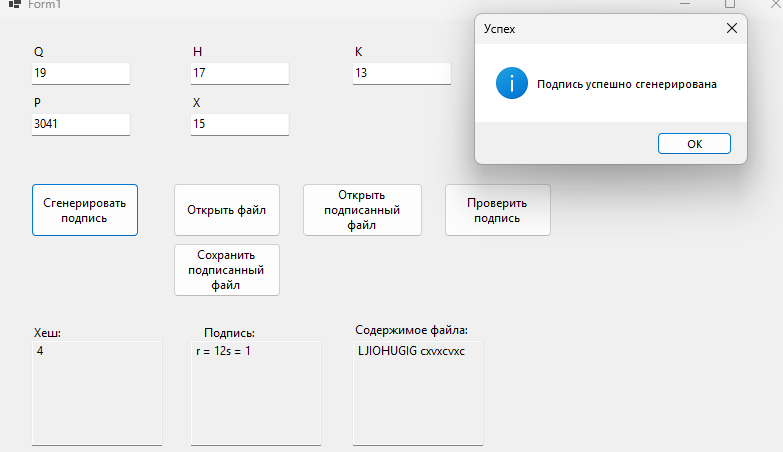
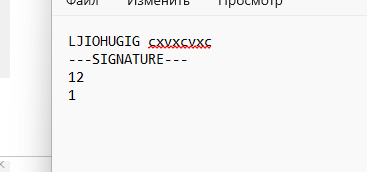
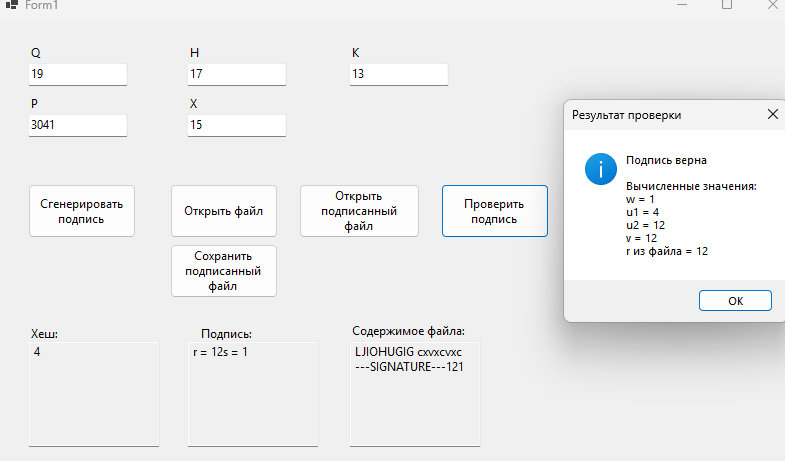
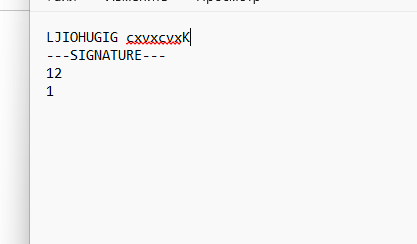
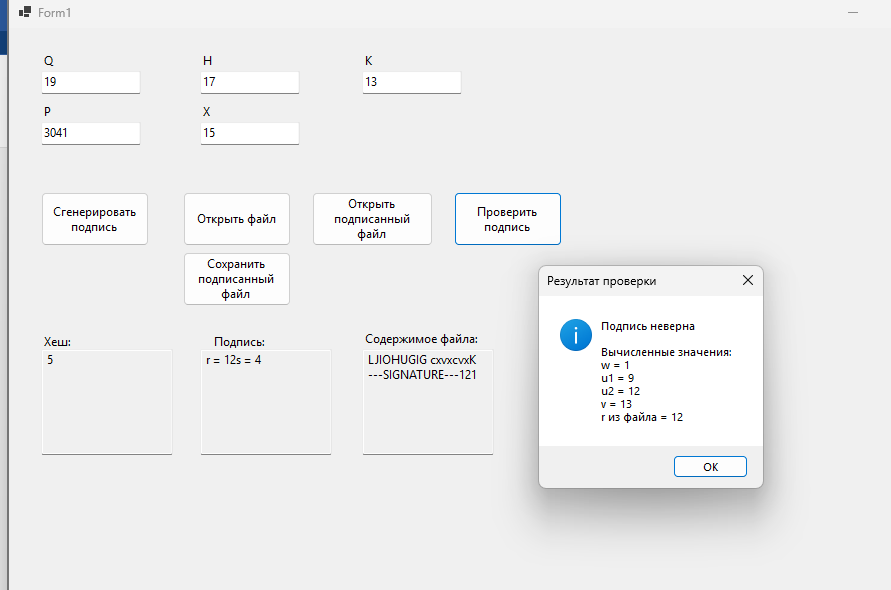
1 – сообщение о том верна подпись или нет;

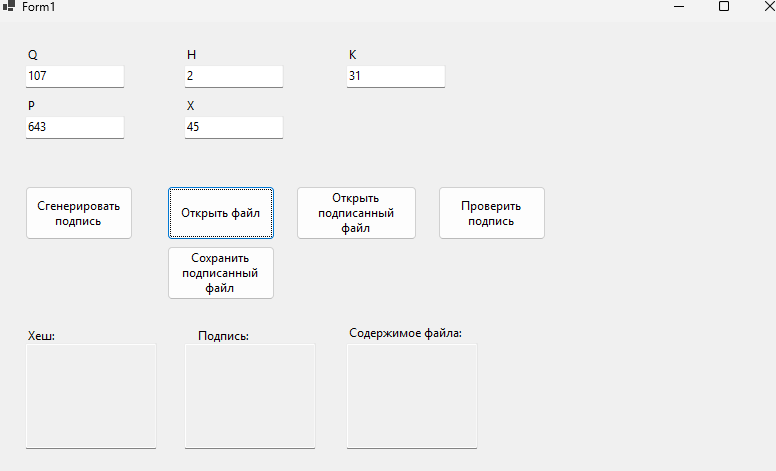
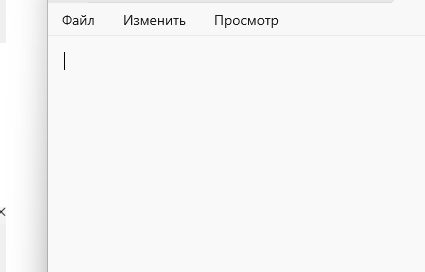
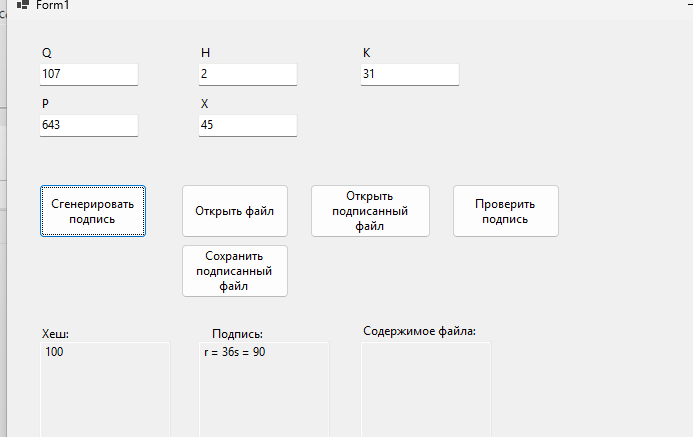
2 – вычисленные при проверке значения.

**ТЕСТ №1**

****

**Входной текст:  
  
  
  
Генерация цифровой подписи:  
  
  
  
Подписанный файл:**

**  
  
Проверка подписи:  
  
  
  
Результат: Подпись верна  
  
ТЕСТ №2  
  
  
Входной текст:  
  
  
  
Генерация цифровой подписи:  
  
  
  
Подписанный файл:  
  
  
Проверка:  
  
  
  
Результат: Подпись верна  
  
Изменим файл на:  
  
  
И проверим подпись:  
**

**Результат: Подпись неверна!  
  
  
ТЕСТ №3  
  
Вычисление хеша пустого файла:  
  
  
  
Содержимое файла:  
  
  
   
Результат:  
  
  
   
Хеш был вычислен!**