УО «Белорусский государственный университет информатики и радиоэлектроники»

Отчет по лабораторной работе №4

по предмету «Теория информации»

Вариант 1

Выполнил:

Наривончик А.М.

Гр. 351004

Проверил:

Болтак С.В.

Минск 2025

**Тест 1**

**Исходный файл**: test 1.txt

**Содержимое файла:** Price Range

**P** = 73

**Q** = 11

**R** = 803

**Ф(r)** = 720

**D** = 59

**Вычисленное значение E** = 659

**Вычисленный хэш-образ:** 291

**Значение цифровой подписи**: 218

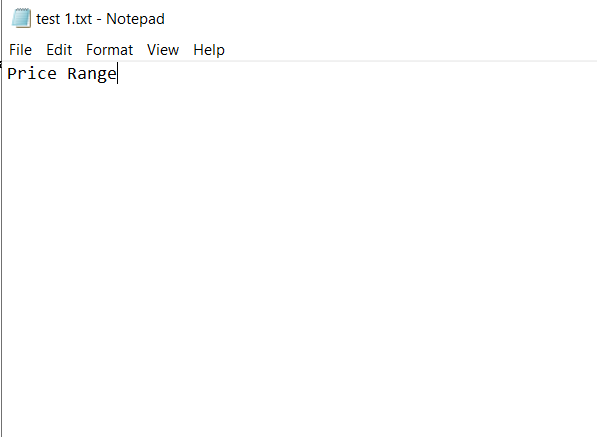


Рисунок 1.1 – исходный файл test 1.txt

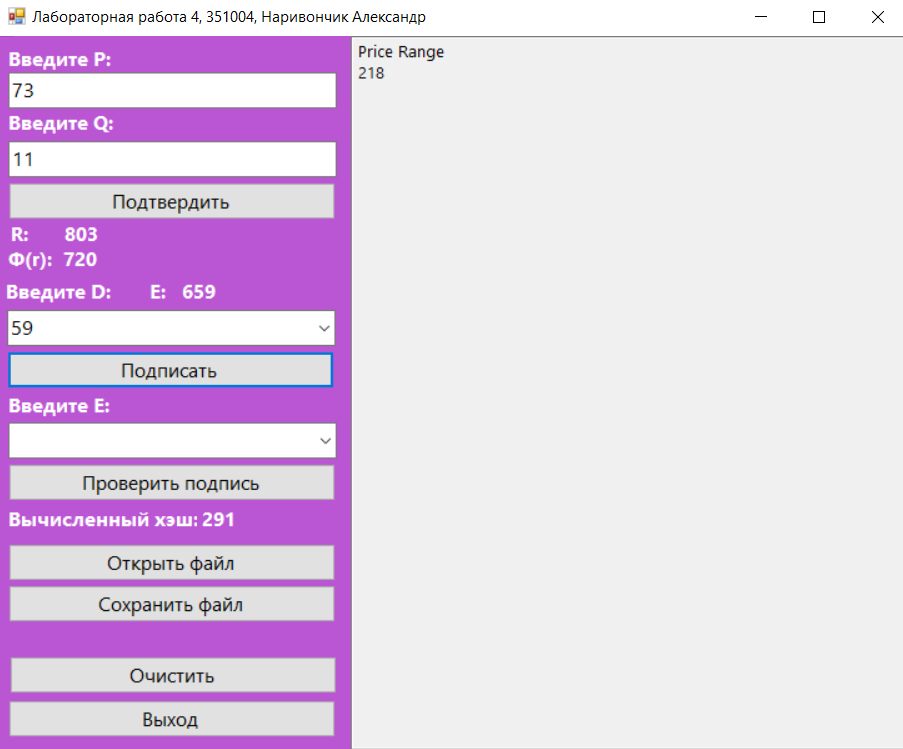


Рисунок 1.2 – подпись файла test 1.txt



Рисунок 1.3 – подписанный файл test\_1\_with\_signature.txt

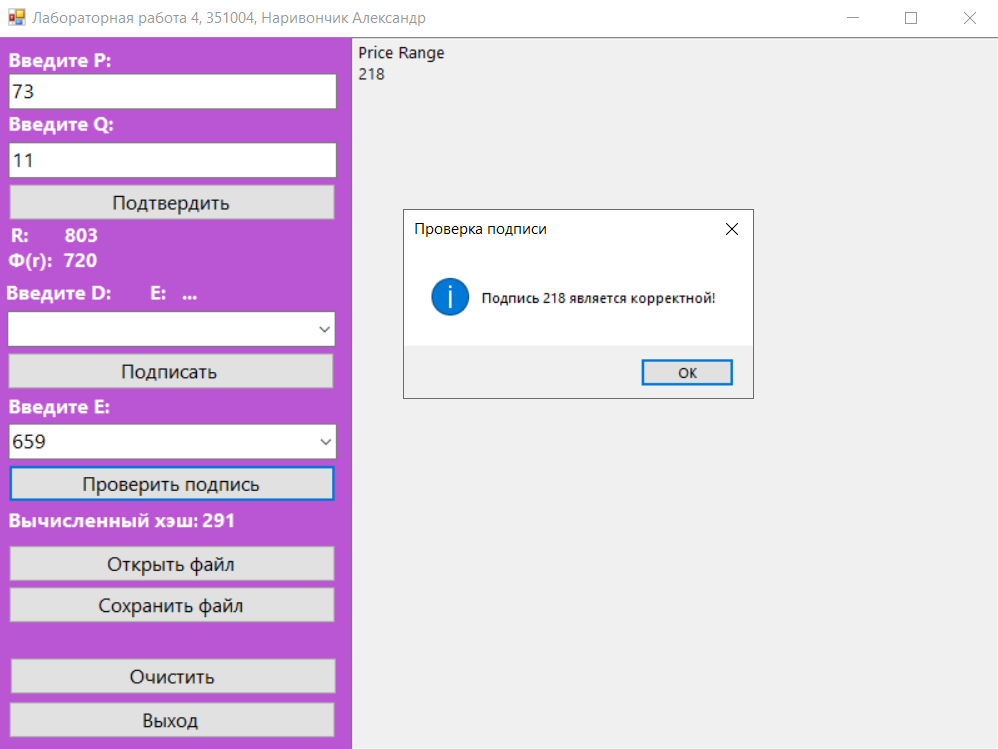


Рисунок 1.4 – проверка подписи в файле test\_1\_with\_signature.txt

**Тест 2   
(***модифицированный подписанный файл, применение неправильного открытого ключа****)***

**Исходный файл**: test 2.txt

**Содержимое файла:**

some text some text

some text some text

some text some text

some text some text

some text some text

some text some text

**P** = 13

**Q** = 29

**R** = 377

**Ф(r)** = 336

**D** = 101

**Вычисленное значение E** = 173

**Вычисленный хэш-образ:** 16

**Значение цифровой подписи**: 152

**Содержимое измененного подписанного файла:**

some virus some virus

aaaa VIRUS AAAA VIRUS

some text some text

some text virus virus

some text some text

some virus some text

152

**Значение его хэш-образа:** 82

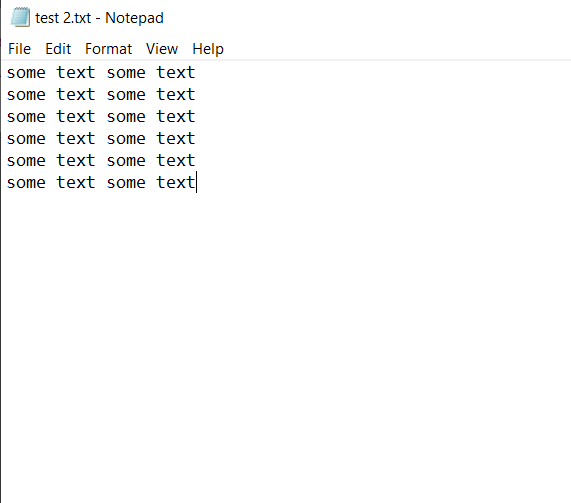


Рисунок 2.1 – исходный файл test 2.txt

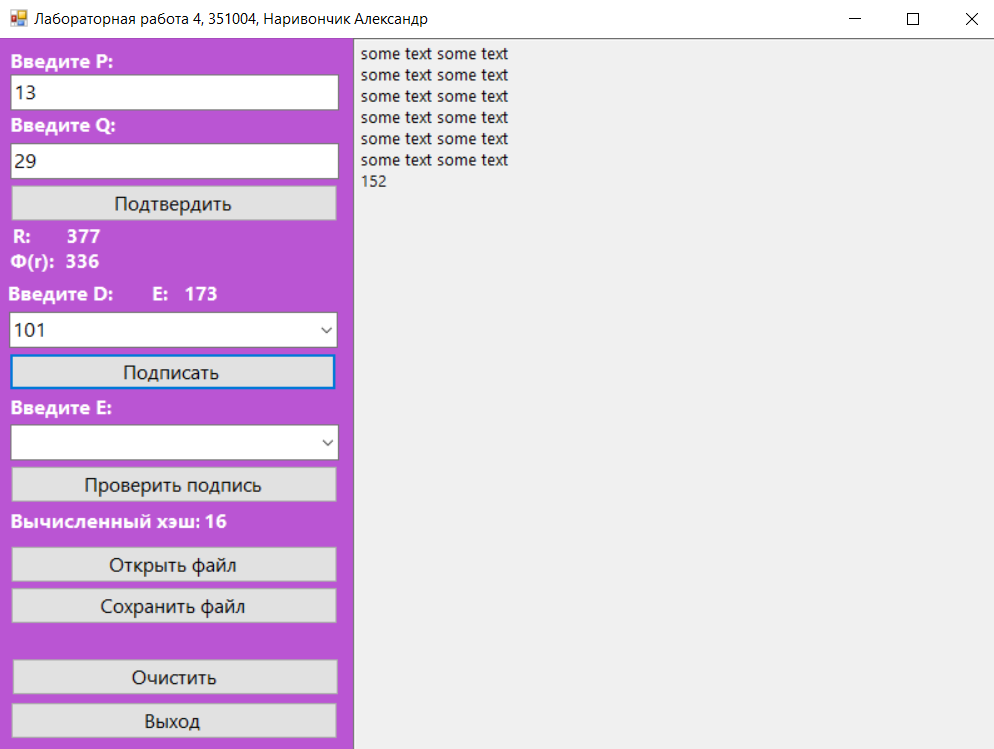


Рисунок 2.2 – подписанный файл test 2.txt

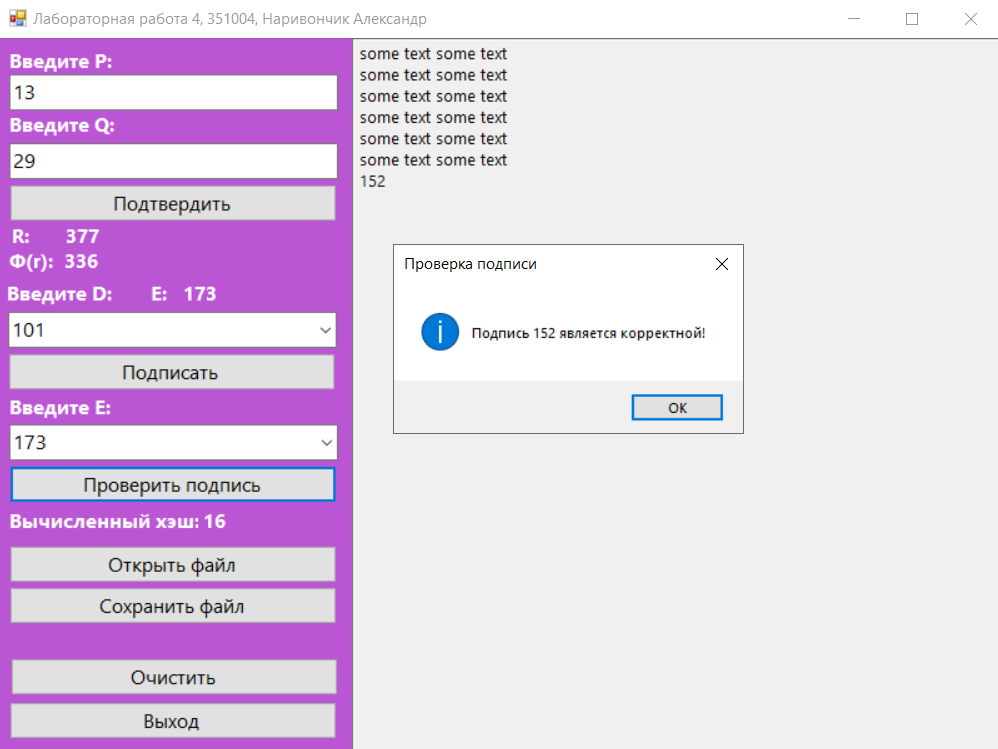


Рисунок 2.3 – проверка подписи с правильным открытым ключом E

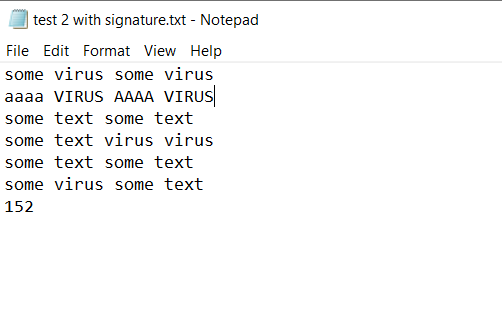


Рисунок 2.4 – модифицированный test\_2\_with\_signature.txt

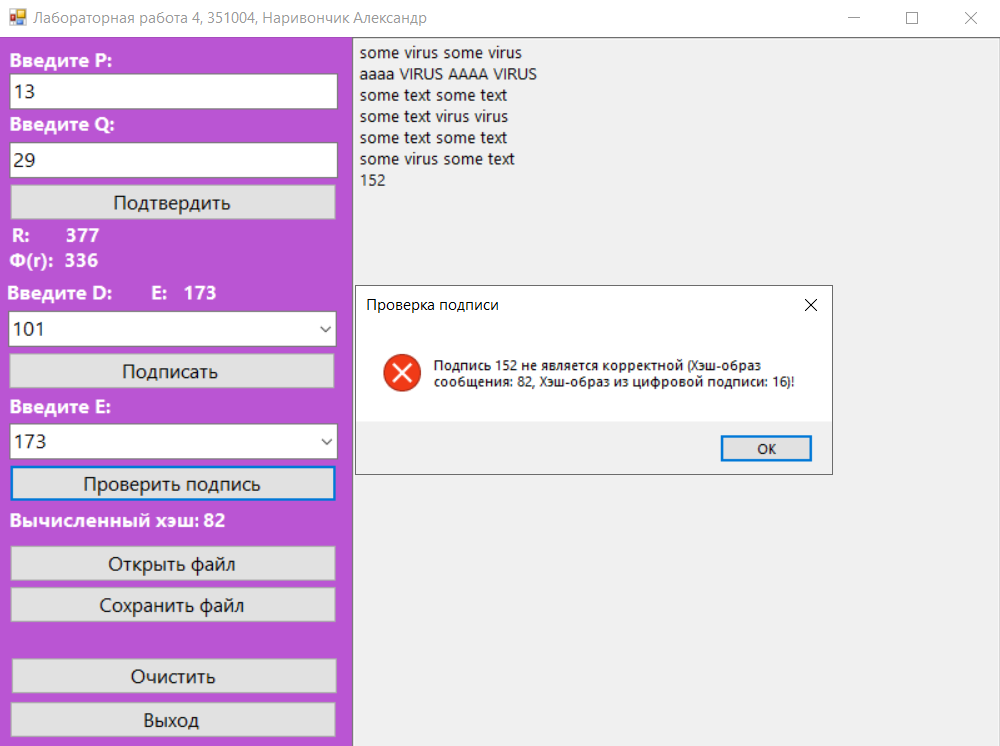


Рисунок 2.5 – проверка подлинности подписи модифицированного файла

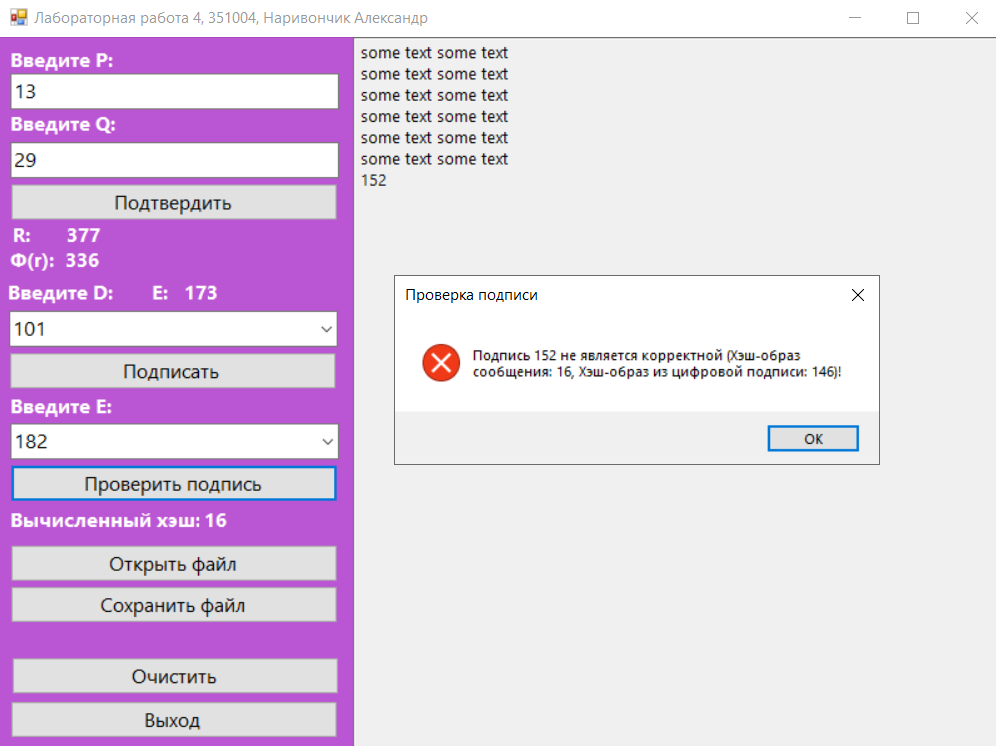


Рисунок 2.6 - проверка подлинности подписи файла с неправильным открытым ключом

**Тест 3  
(***подпись пустого файла***)**

**Исходный файл**: test 3.txt

**Содержимое файла:** (*пустой*)

**P** = 41

**Q** = 59

**R** = 2419

**Ф(r)** = 2320

**D** = 133

**Вычисленное значение E** = 157

**Вычисленный хэш-образ:** 100

**Значение цифровой подписи**: 2306

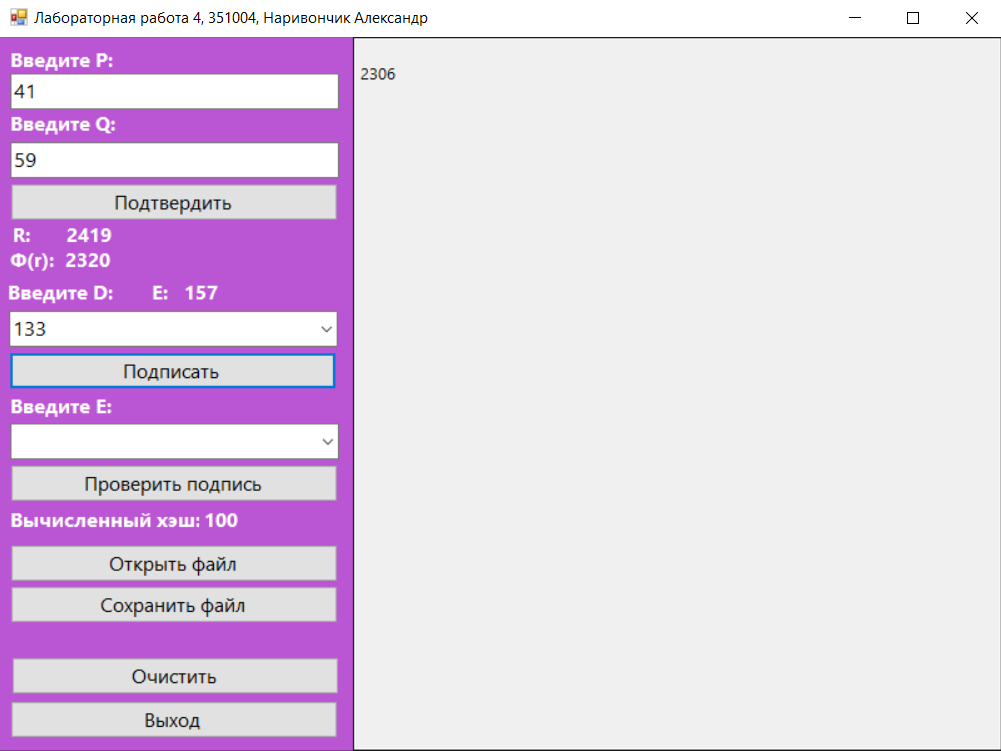
****

Рисунок 3.1 – подпись пустого файла test 3.txt

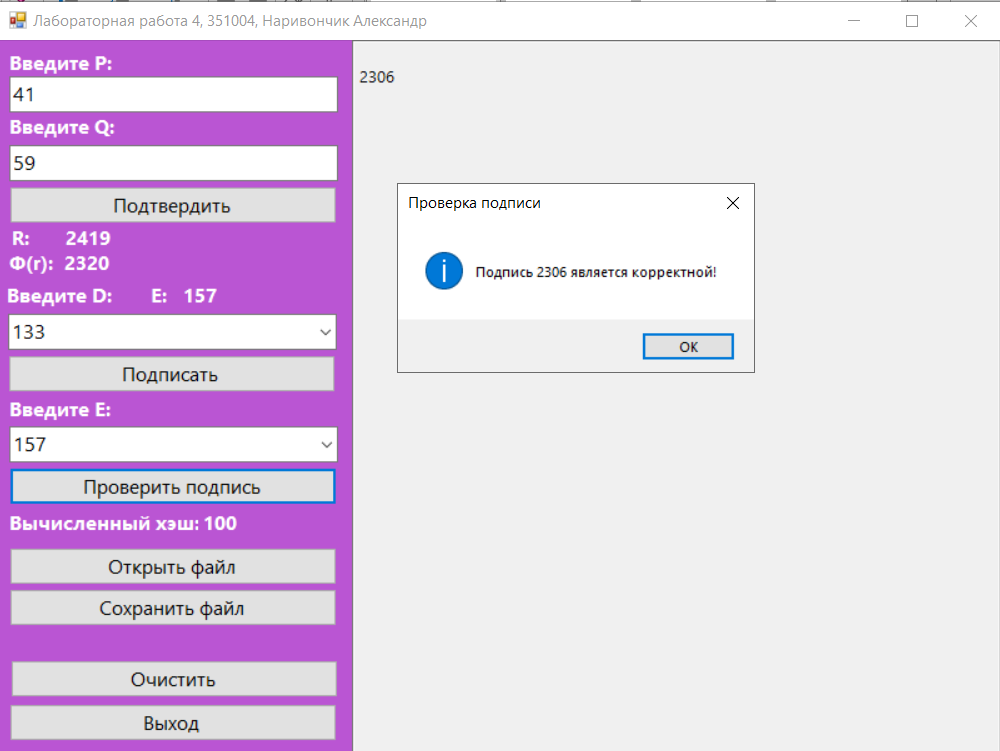
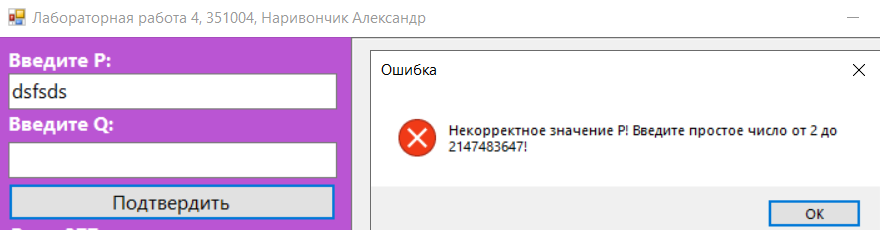
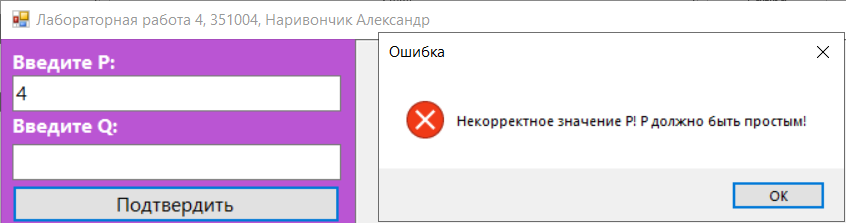
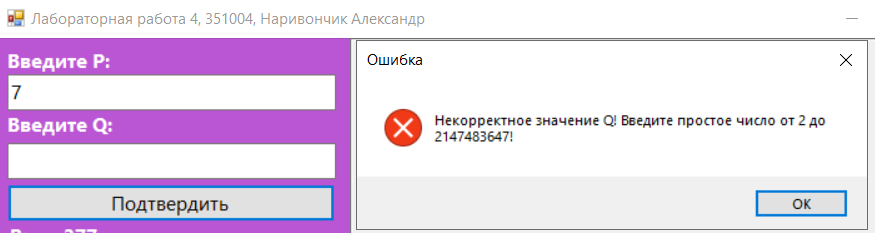
****

Рисунок 3.2 – проверка подписи файла test\_3\_with\_signature.txt

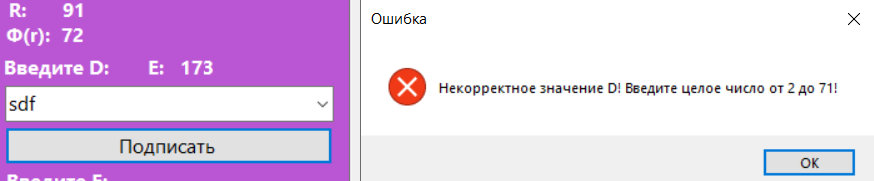
**Тест 4 (***невалидный P или Q***)**

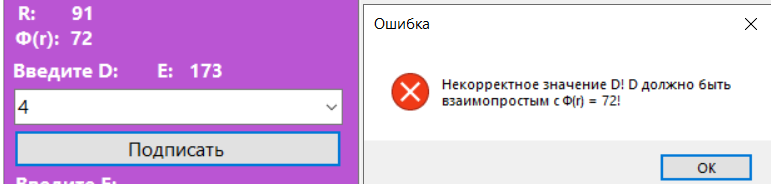
****

****

****

**Тест 5 (***невалидный D или D невзаимнопростой с Ф(r)***)**

****

****