УО «Белорусский государственный университет информатики и радиоэлектроники»

Отчет по лабораторной работе №3

по предмету «Теория информации»

Вариант 2

Выполнил:

Наривончик А.М.

Гр. 351004

Проверил:

Болтак С.В.

Минск 2025

**Пример работы алгоритма быстрого возведения в степень с модульной арифметикой**

**az mod n:**

a = 7,

z = 13,

n = 22

|  |  |  |  |
| --- | --- | --- | --- |
| **а (основание степени)** | **z (степень)** | **х (результат)** | **шаги выполнения** |
| 7 | 13 | 1 | 0 |
| 7 | 13 – 1 = 12 | (1 \* 7) mod 22 = 7 | 1  (13 нечетное) |
| (7\*7) mod 22 = 5 | 12 / 2 = 6 | 7 | 2  (12 четное) |
| (5\*5) mod 22 = 3 | 6 / 2 = 3 | 7 | 3  (6 четное) |
| 3 | 3 – 1 = 2 | (7 \* 3) mod 22 = 21 | 4  (3 нечетное) |
| (3\*3) mod 22 = 9 | 2 / 2 = 1 | 21 | 5  (2 четное) |
| 9 | 1 – 1 = 0 | (21 \* 9) mod 22 = 13 | 6  (1 нечетное) |
|  | 0 | Результат: 13 | 7 |

**Примеры работы алгоритмов**

**Пример поиска всех первообразных корней по модулю p**

p = 23,

p – 1 = 22 = 2 \* 11

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g22/2 mod 23** | **g22/11 mod 23** | **Является первообразным?** |
| 2 | 1 | 4 | - |
| 3 | 1 | 9 | - |
| 4 | 1 | 16 | - |
| 5 | 22 | 2 | + |
| 6 | 1 | 13 | - |
| 7 | 22 | 3 | + |
| 8 | 1 | 18 | - |
| 9 | 1 | 12 | - |
| 10 | 22 | 8 | + |
| 11 | 22 | 6 | + |
| 12 | 1 | 6 | - |
| 13 | 1 | 8 | - |
| 14 | 22 | 12 | + |
| 15 | 22 | 18 | + |
| 16 | 1 | 3 | - |
| 17 | 2 | 13 | + |
| 18 | 1 | 2 | - |
| 19 | 18 | 16 | + |
| 20 | 19 | 9 | + |
| 21 | 13 | 4 | + |
| 22 | 22 | 1 | - |

5, 7, 10, 11, 14, 15, 17, 19, 20, 21 – первообразные корни

**Пример работы расширенного алгоритма Евклида**

A = 43 B = 12

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a** | **b** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 43 | 12 | 1 | 0 | 0 | 1 |
| 1 | 43/12=3 | 12 | 7 | 0 | 1 | 1 | -3 |
| 2 | 12/7=1 | 7 | 5 | 1 | -1 | -3 | 4 |
| 3 | 7/5=1 | 5 | 2 | -1 | 2 | 4 | -7 |
| 4 | 5/2=2 | 1 | 1 | 2 | -5 | -7 | 18 |

x1 = -5, y1 = 18

-5 \* 43 + 18 \* 12 = 1 – НОД = 1, следовательно числа взаимно простые

**Тест 1 (***текст***)**

**Исходный файл**: test1.txt

P = 73

G = 11

X = 3

K = 19

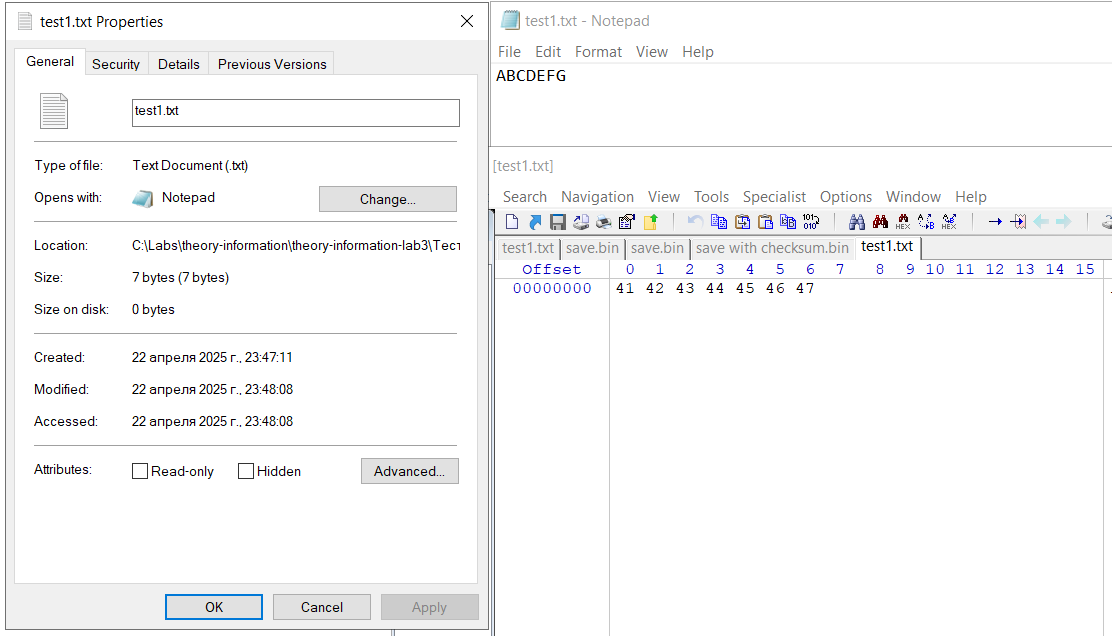


Рисунок 1.1 – исходный файл test1.txt

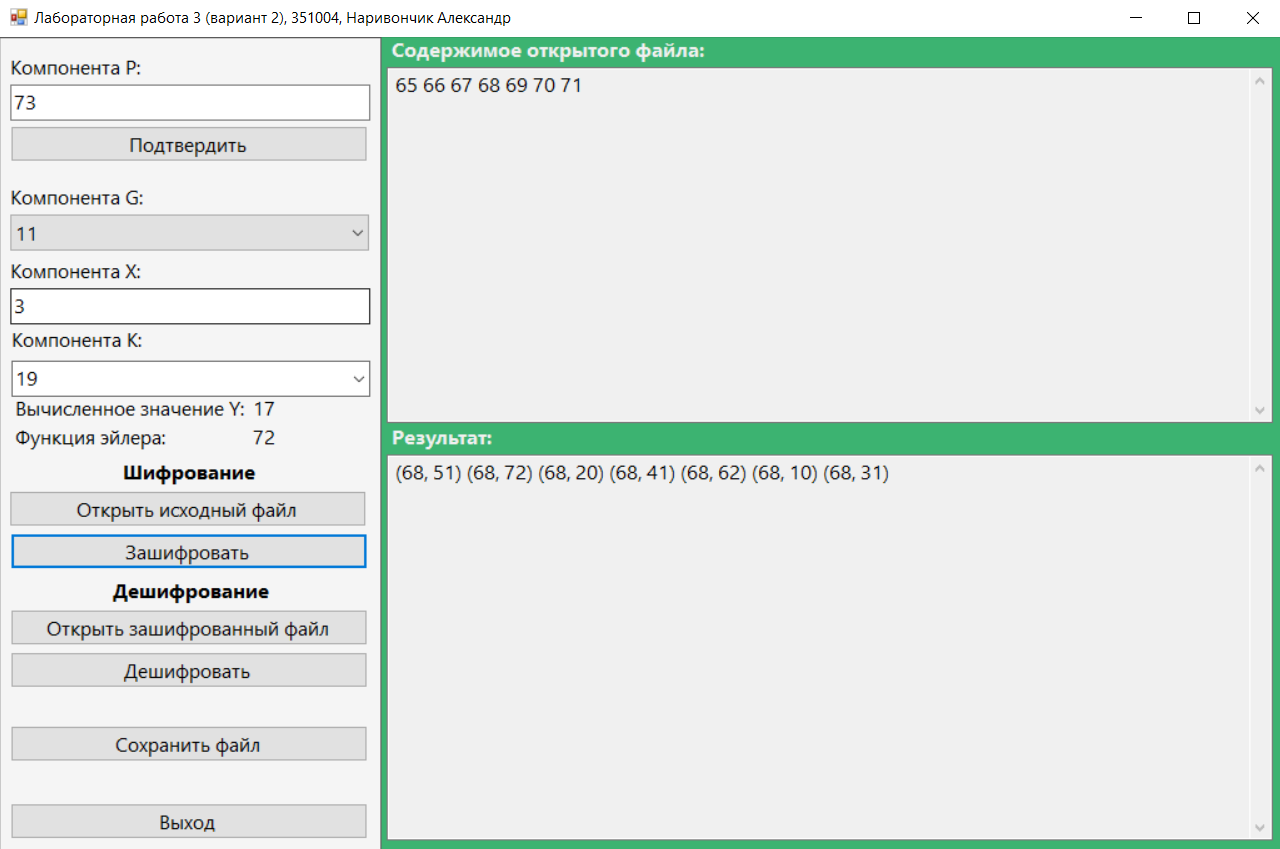


Рисунок 1.2 – шифрование файла test1.txt

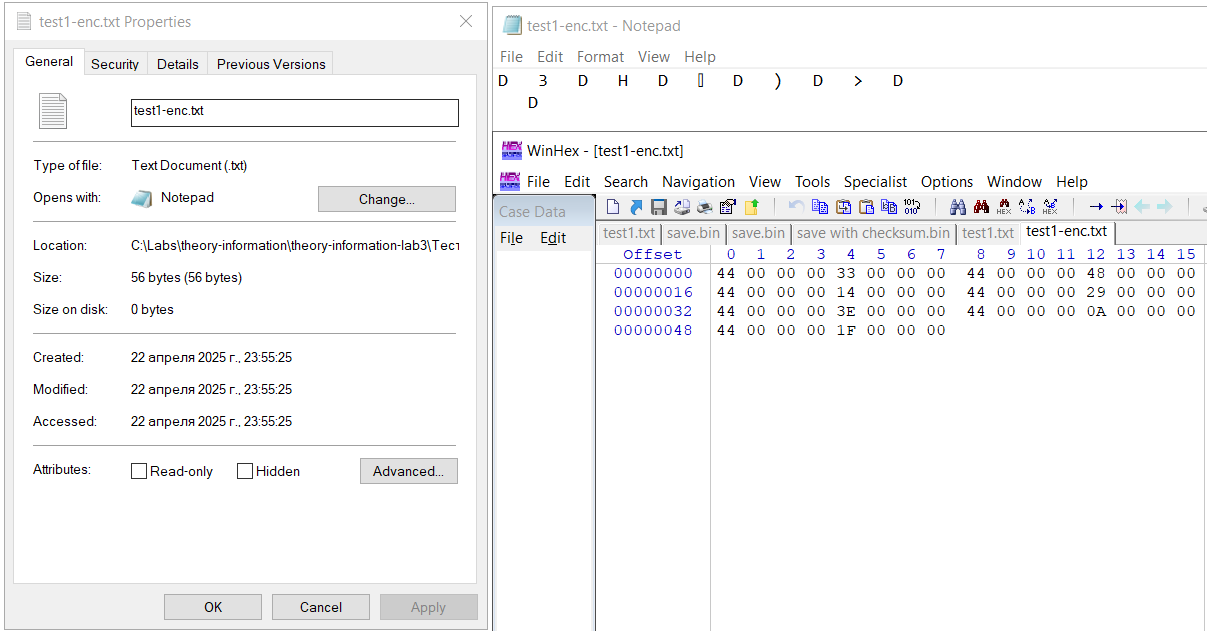


Рисунок 1.3 – зашифрованный файл test1-enc.txt

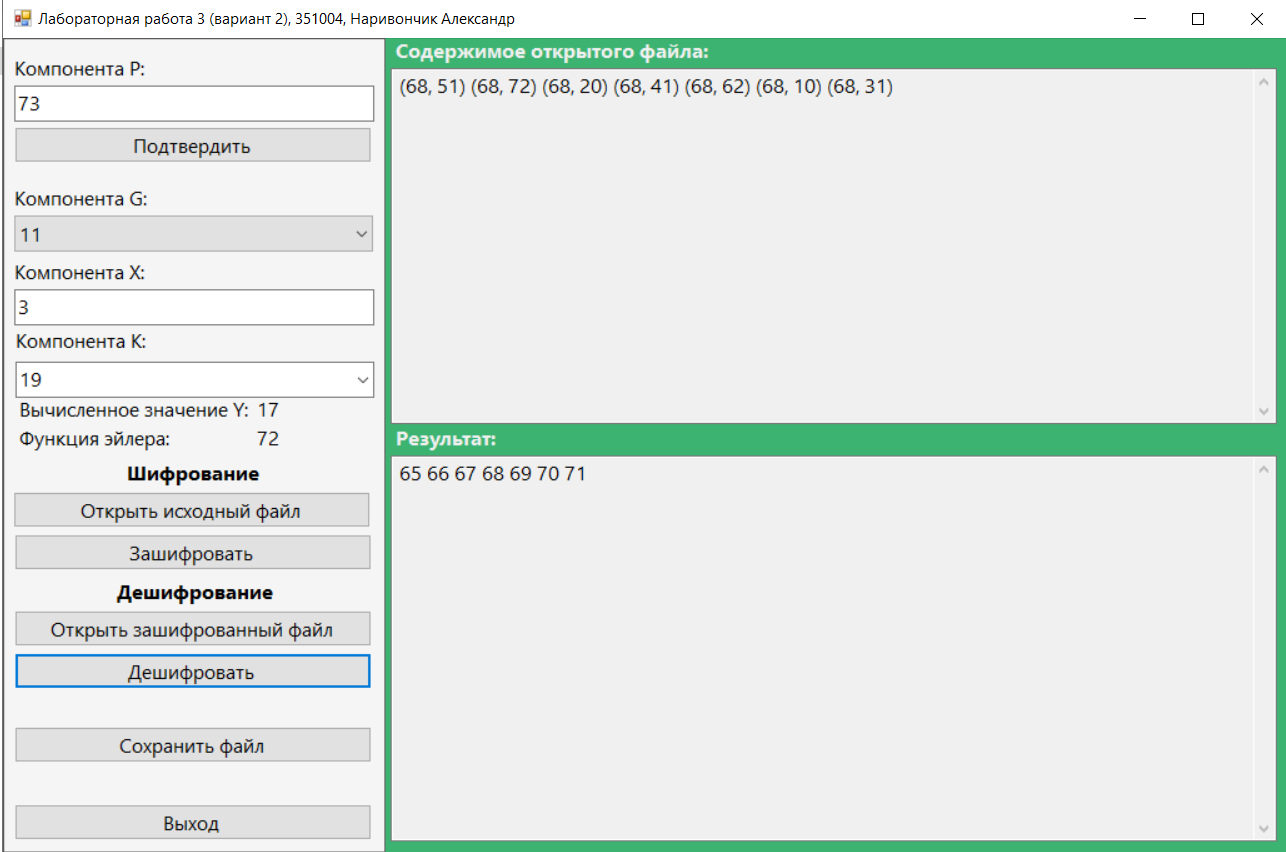


Рисунок 1.4 –дешифрование test1-enc.txt

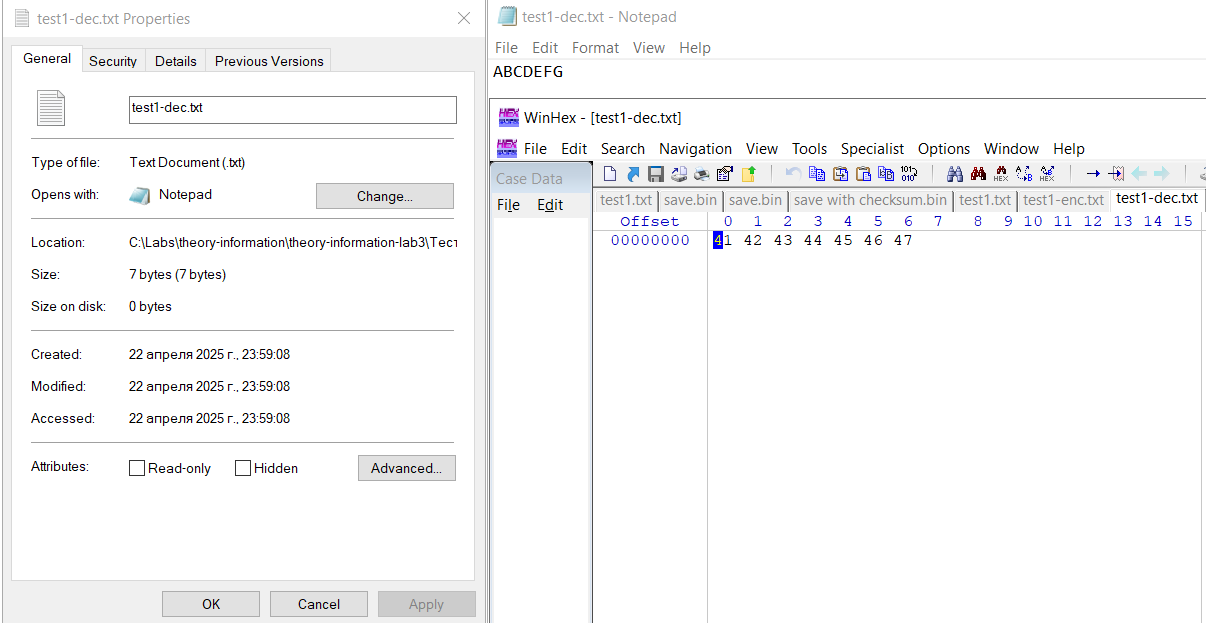


Рисунок 1.5 – дешифрованный test1-dec.txt

**Тест 2 (***изображение***)**

**Исходный файл**: test2.jpg

P = 257

G = 14

X = 7

K = 39



Рисунок 2.1 – исходный файл test2.jpg

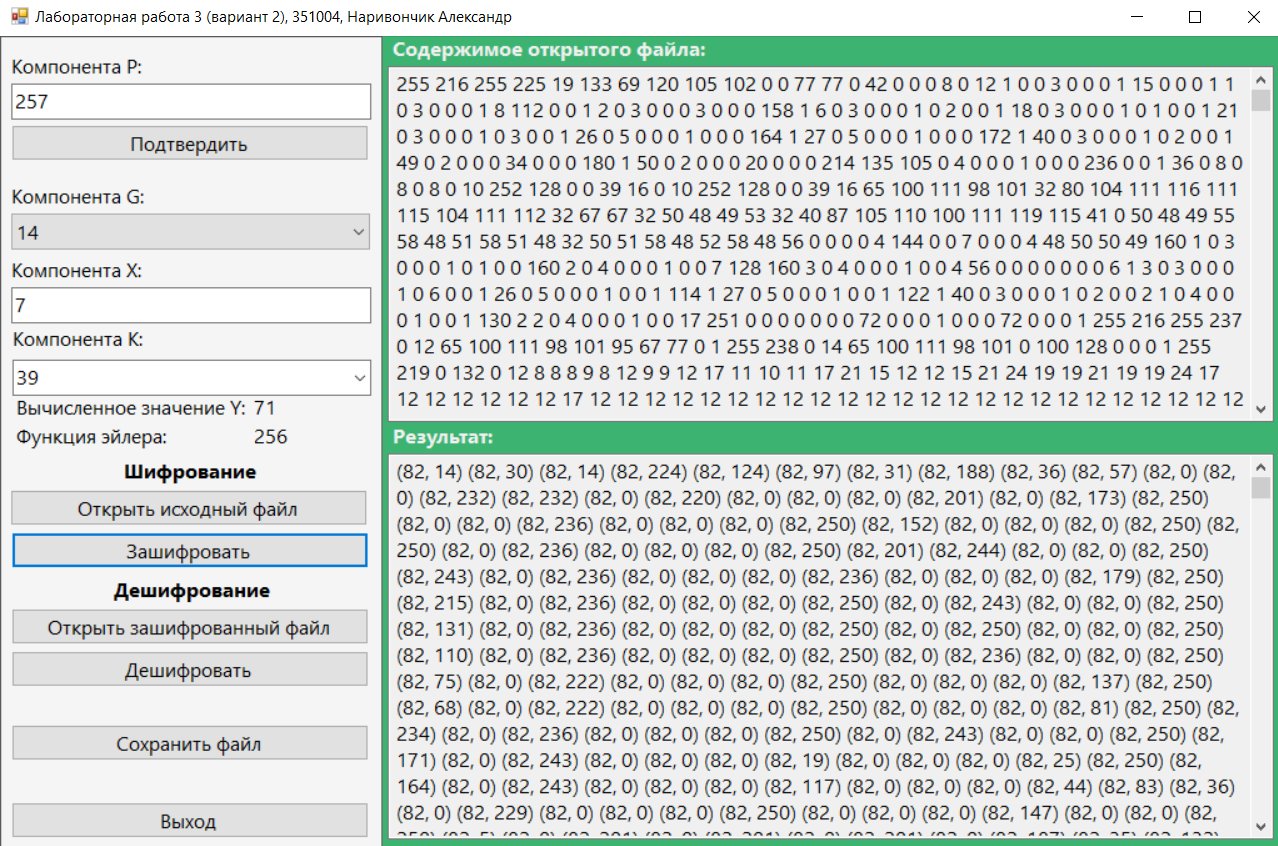


Рисунок 2.2 – шифрование test2.jpg

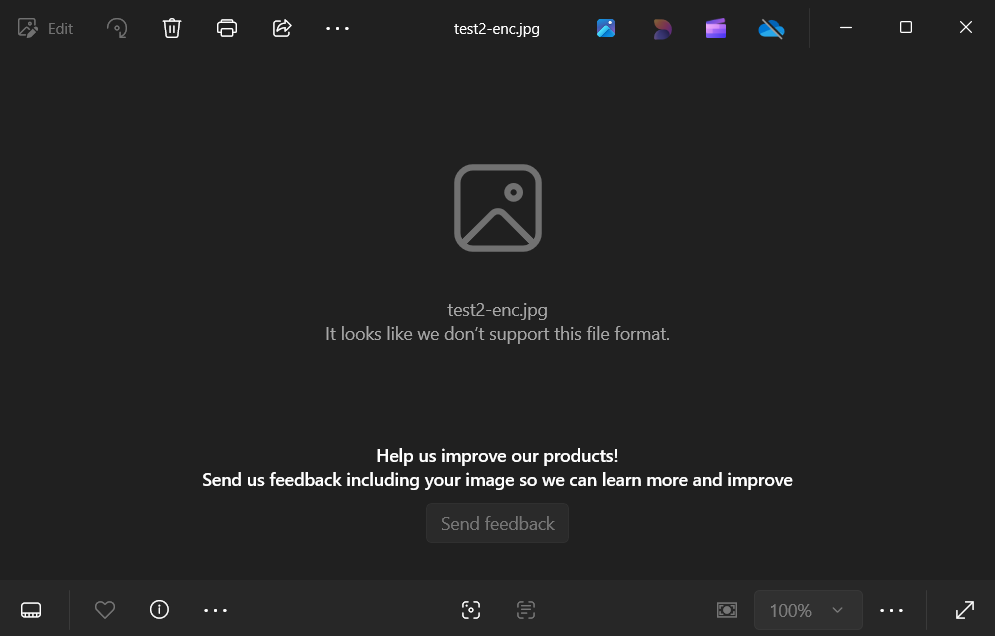


Рисунок 2.3 – зашифрованный test2-enc.jpg

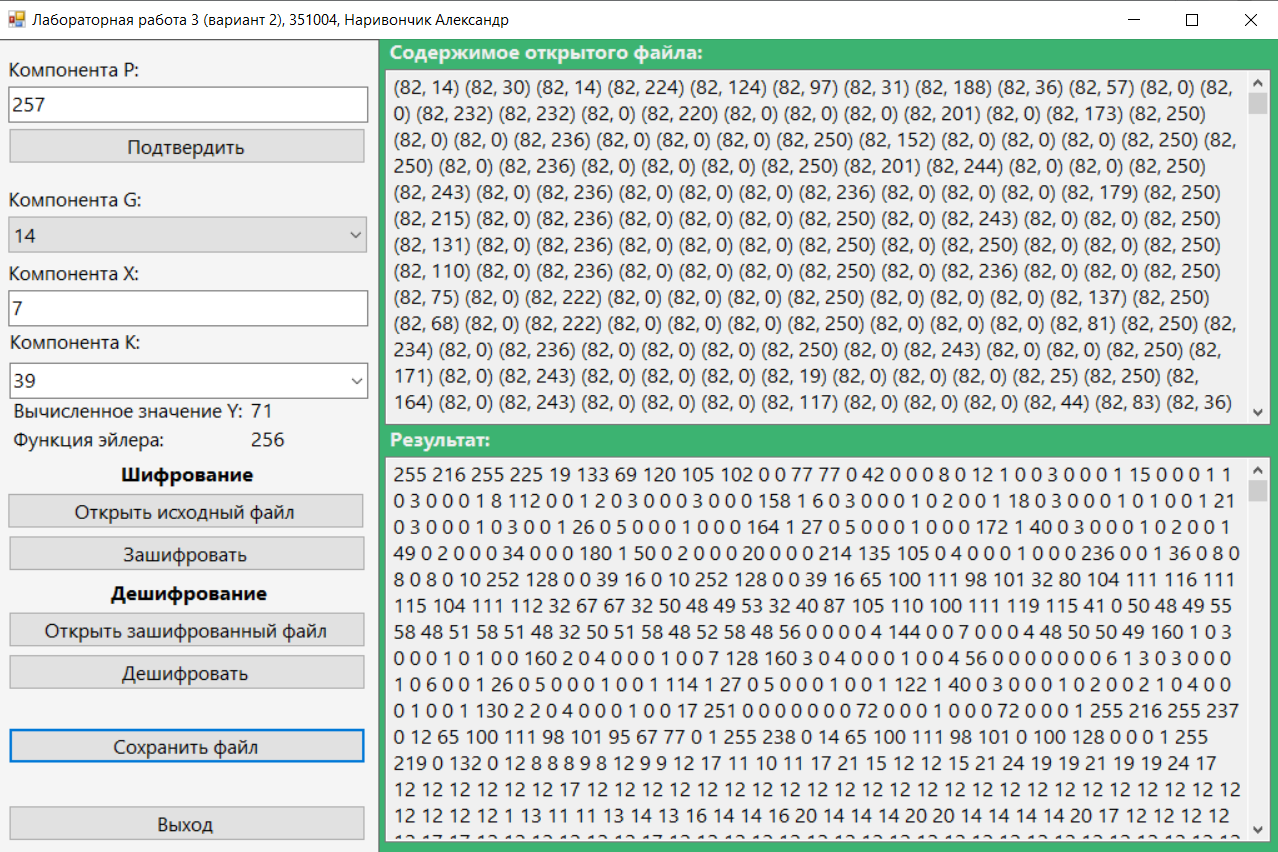
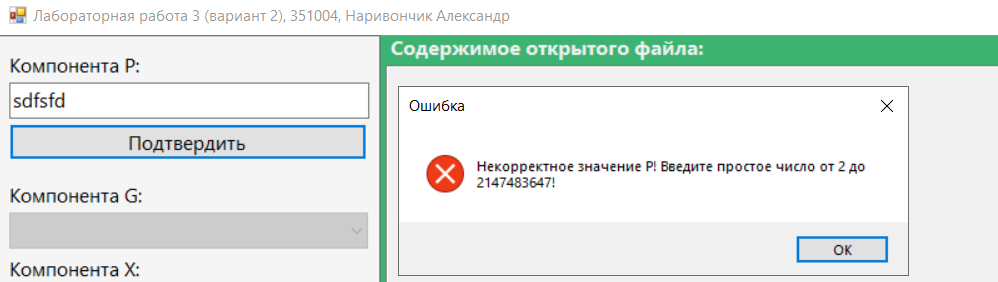


Рисунок 2.4 – дешифрование test2-enc.jpg

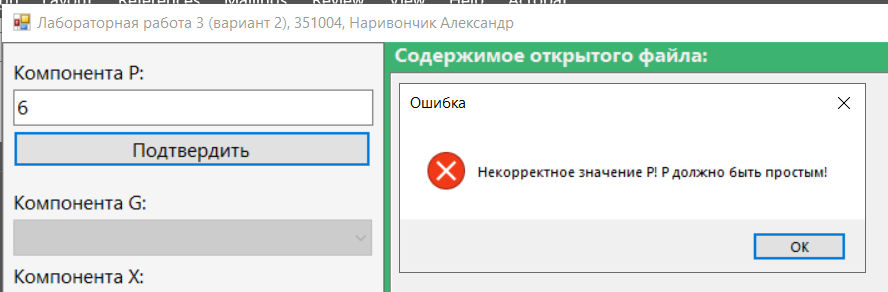


Рисунок 2.5 - дешифрованный файл test2-decrypted.jpg

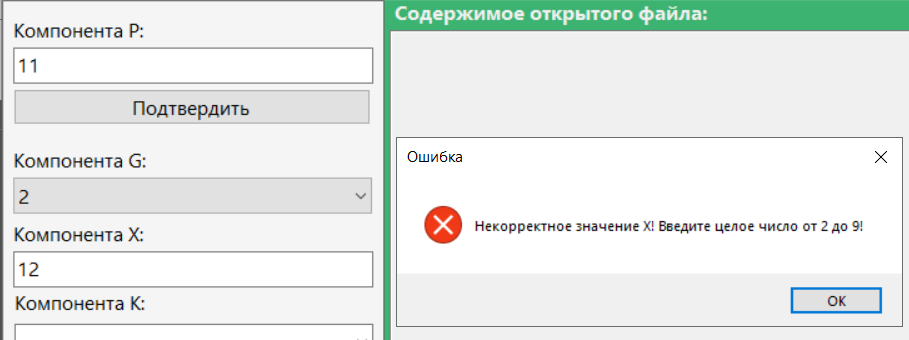
**Тест 3 (***невалидный P***)**

****

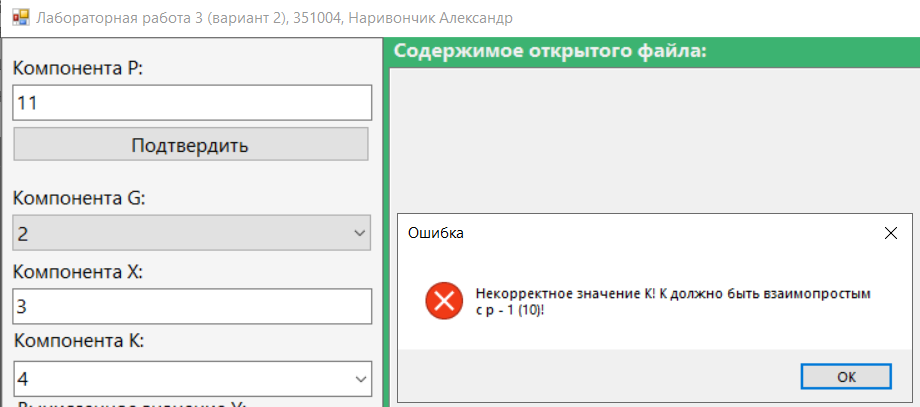
**Тест 4 (***составное число P***)**

****

**Тест 5 (***X принадлежит неверному диапазону***)**

****

**Тест 6 (***K не взаимно простое с P-1***)**

****