УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №3

по предмету «Теория информации»

Выполнил:

Кравченко В.В.

гр. 351002

Проверила:

Болтак С.В.

Минск 2025

**Вариант №2.**

Реализовать шифратор и дешифратор *алгоритма* ***Эль-Гамаля*** файла c произвольным содержимым, используя алгоритм быстрого возведения в степень, а также реализовать вычисление открытого ключа ***g*** при данном значении ***p***, используя алгоритм нахождения первообразного корня по модулю. Значения параметров ***p*, *x*** и ***k***задаются пользователем*.* Программа должна осуществлять проверку ограничений на вводимые пользователем значения параметров алгоритма. Организовать вывод содержимого зашифрованного файла на экран в виде чисел в 10-й системе счисления. Вывести значение ***g*** на экран. Результат работы программы – зашифрованный/расшифрованный файл/ы.

Используя алгоритм из методички, искать все первообразные корни по модулю ***p.*** Все найденные корни вывести на экран и предложить для шифрования ввести на выбор любой из найденных

**Поиск первообразного корня**

p = 41, p – 1 = 40 = 2 \* 2 \* 2 \* 5

g^40/2 mod 41 => g^20 mod 41

g^40/5 mod 41 => g^8 mod 41

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^20 mod 41** | **g^8 mod 41** | **Первообразный** |
| 2 | 1 | 10 | Нет |
| 3 | 40 | 1 | Нет |
| 4 | 1 | 18 | Нет |
| 5 | 1 | 18 | Нет |
| 6 | 40 | 10 | Да |
| 7 | 40 | 37 | Да |
| 8 | 1 | 16 | Нет |
| 9 | 1 | 1 | Нет |
| 10 | 1 | 16 | Нет |
| 11 | 40 | 16 | Да |
| 12 | 40 | 18 | Да |
| 13 | 40 | 10 | Да |
| 14 | 40 | 1 | Нет |
| 15 | 40 | 18 | Да |
| 16 | 1 | 37 | Нет |
| 17 | 40 | 16 | Да |
| 18 | 1 | 10 | Нет |
| 19 | 40 | 37 | Да |
| 20 | 1 | 37 | Нет |
| 21 | 1 | 37 | Нет |
| 22 | 40 | 37 | Да |
| 23 | 1 | 10 | Нет |
| 24 | 40 | 16 | Да |
| 25 | 1 | 37 | Нет |
| 26 | 40 | 18 | Да |
| 27 | 40 | 1 | Нет |
| 28 | 40 | 10 | Да |
| 29 | 40 | 18 | Да |
| 30 | 40 | 16 | Да |
| 31 | 1 | 16 | Нет |
| 32 | 1 | 1 | Нет |
| 33 | 1 | 16 | Нет |
| 34 | 40 | 37 | Да |
| 35 | 40 | 10 | Да |
| 36 | 1 | 18 | Нет |
| 37 | 1 | 18 | Нет |
| 38 | 40 | 1 | Нет |
| 39 | 1 | 10 | Нет |
| 40 | 1 | 1 | Нет |

6 7 11 12 13 15 17 19 22 24 26 28 29 30 34 35 — кол-во 16 .

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

a1 = 8, z = 17 (10011), n = 37

a1^z mod n = x

|  |  |  |  |
| --- | --- | --- | --- |
| **а1** | **z** | **х** | **Шаг** |
| 8 | 17 (нечет) | 1 | 0 |
| 8 | 16 (чет) | (8 \* 1) mod 37 = 8 | 1 |
| (8\*8) mod 37 = 27 | 8 (чет) | 8 | 2 |
| (27\*27) mod 37 = 26 | 4 (чет) | 8 | 3 |
| (26\*26) mod 37 = 10 | 2 (чет) | 8 | 4 |
| (10\*10) mod 37 = 26 | 1 (чет) | 8 | 5 |
|  | 0 | (26\*8) mod 37 = 23 | 6 |

8^17 mod 37 = 23

**Пример работы расширенного алгоритма Евклида**

A = 111 B = 98

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **шаг** | **q** | **d0** | **d1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 111 | 98 | 1 | 0 | 0 | 1 |
| 1 | 1 | 98 | 13 | 0 | 1 | 1 | -1 |
| 2 | 7 | 13 | 7 | 1 | -7 | -1 | 8 |
| 3 | 1 | 7 | 6 | -7 | 8 | 8 | -9 |
| 4 | 6 | 6 | 1 | 8 | -15 | -9 | 17 |

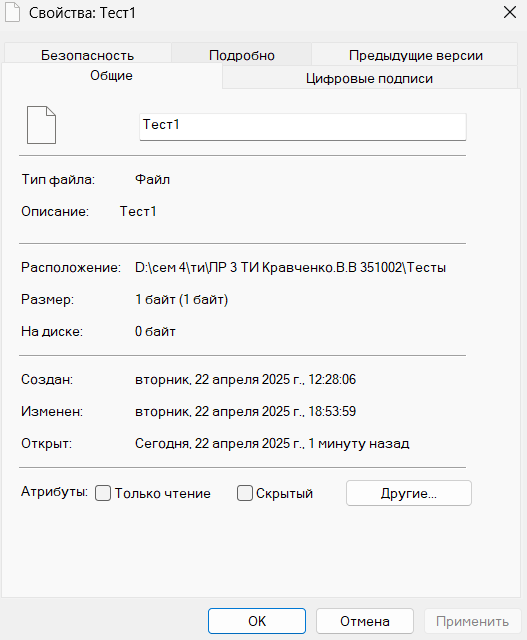
x = -15, y = 17

140 \* (-15) + 135 \* 17 = 1

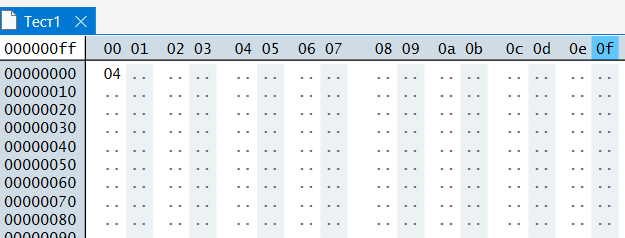
**Группа А – Проверка работоспособности программы**

1. Проверка работоспособности программы для малых файлов.

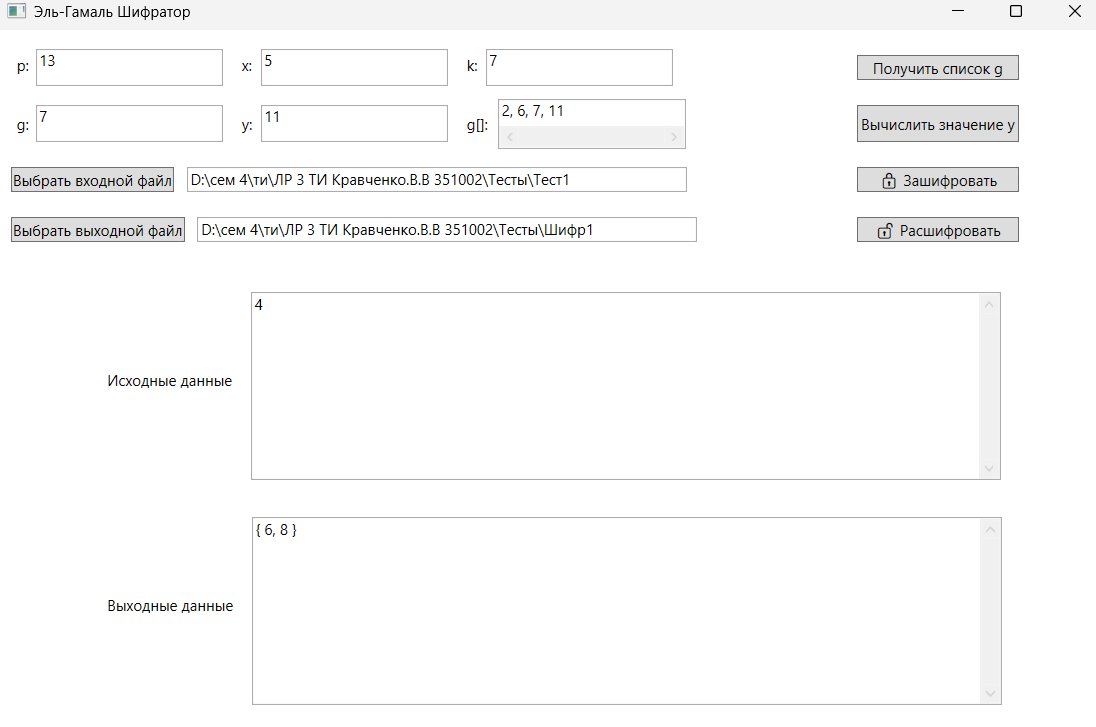
Исходный файл: Тест1



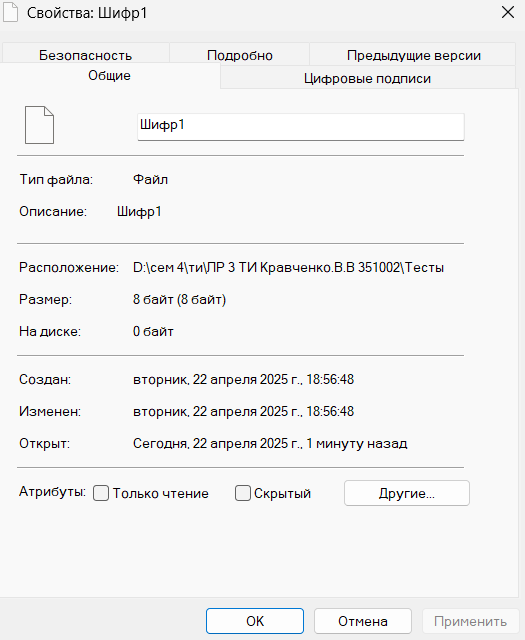
Содержимое файла до шифрования в приложении Hex Editor (для просмотра содержимого файлов в шестнадцатеричном формате):



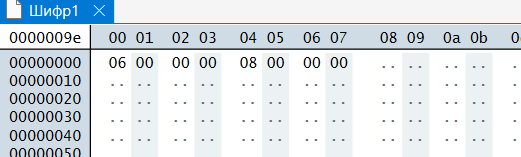
Начальное состояние:



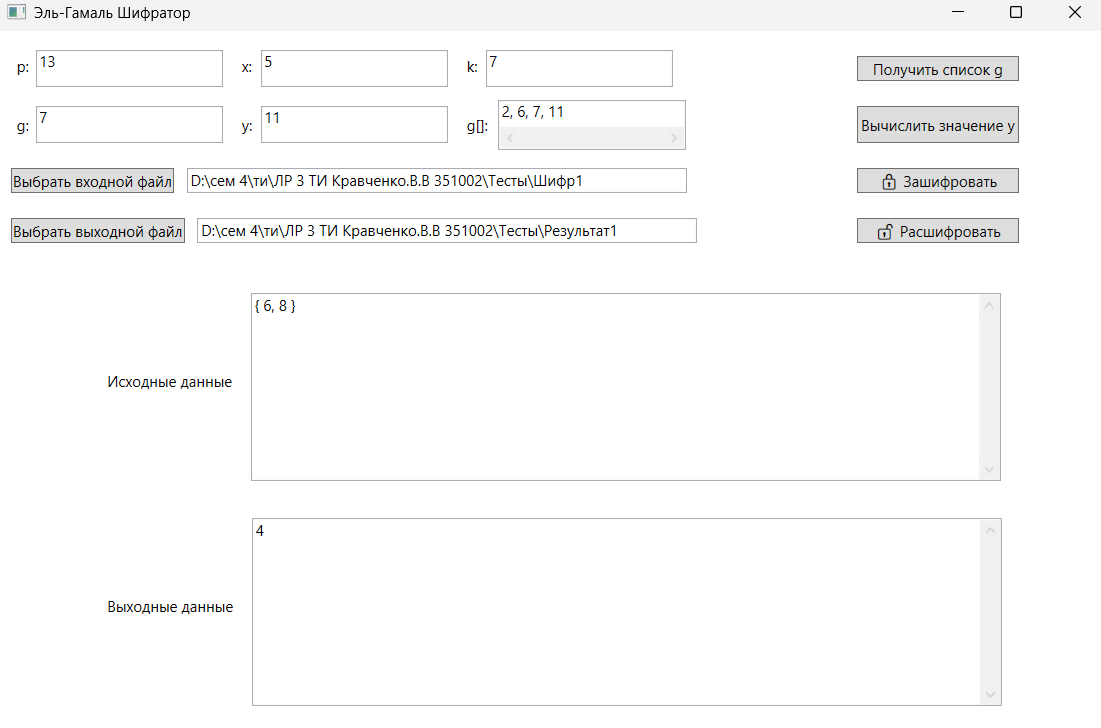
Выходной файл: Шифр1



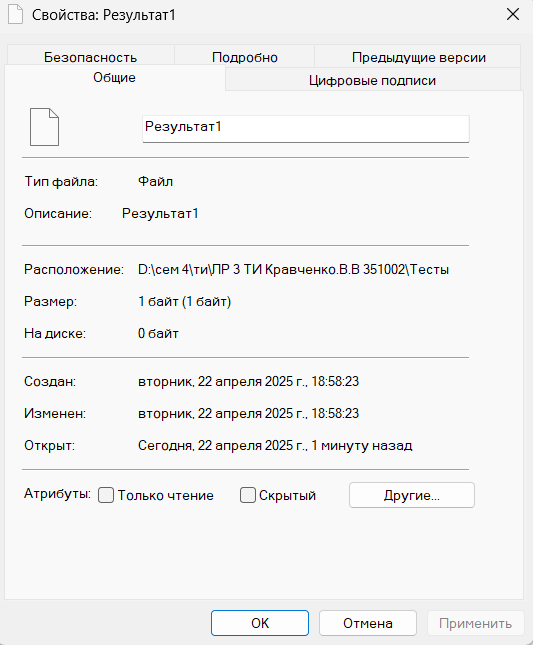
Содержимое файла до шифрования в приложении Hex Editor (для просмотра содержимого файлов в шестнадцатеричном формате):



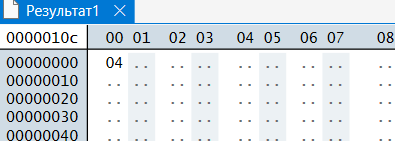
Расшифровка файла Шифр1 с тем же ключом:



Выходной файл: Результат1

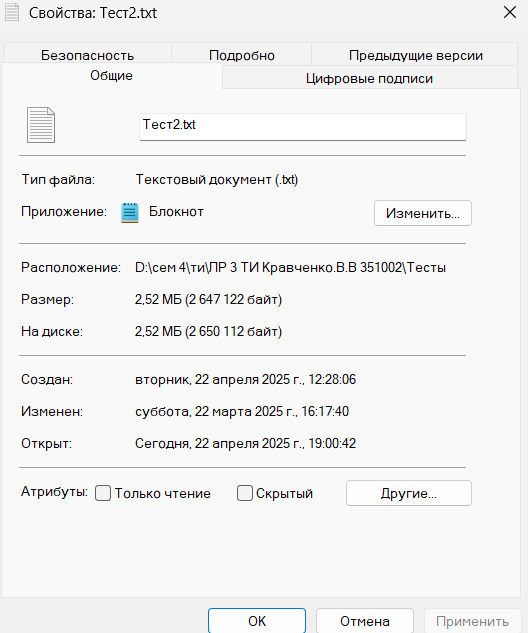


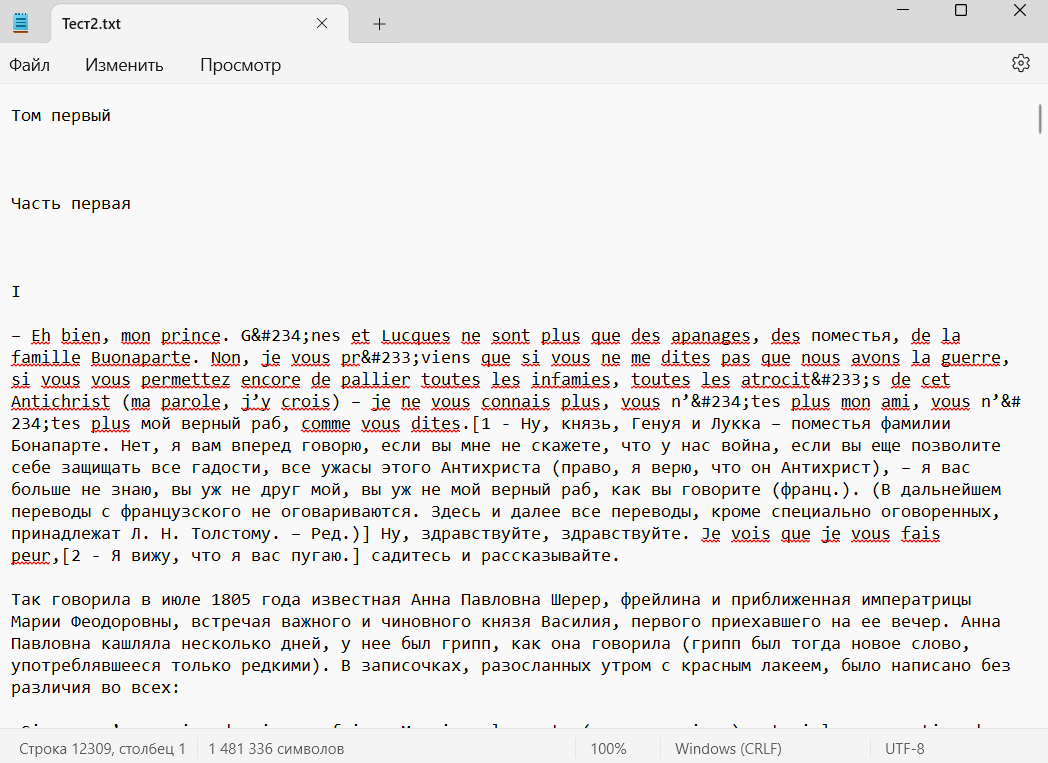
Содержимое файла до шифрования в приложении Hex Editor (для просмотра содержимого файлов в шестнадцатеричном формате):



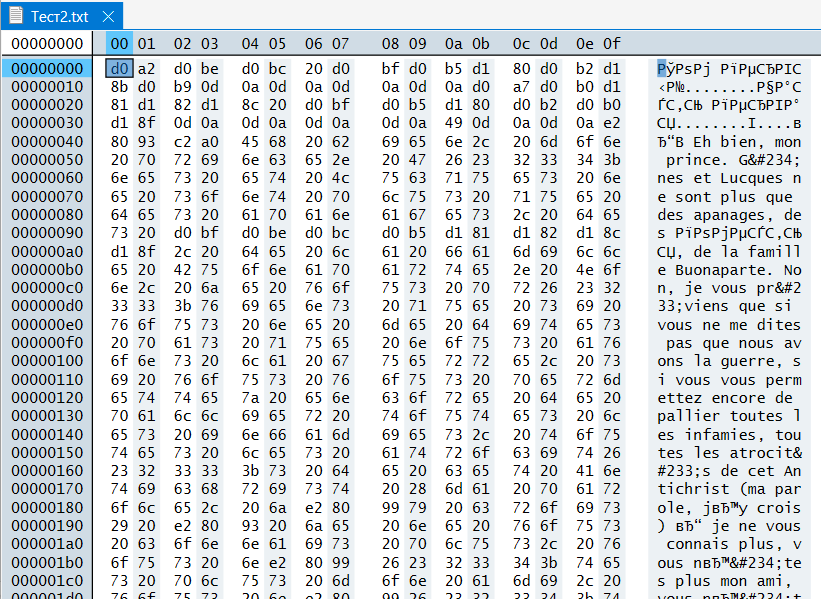
2. Проверка работоспособности программы для больших файлов

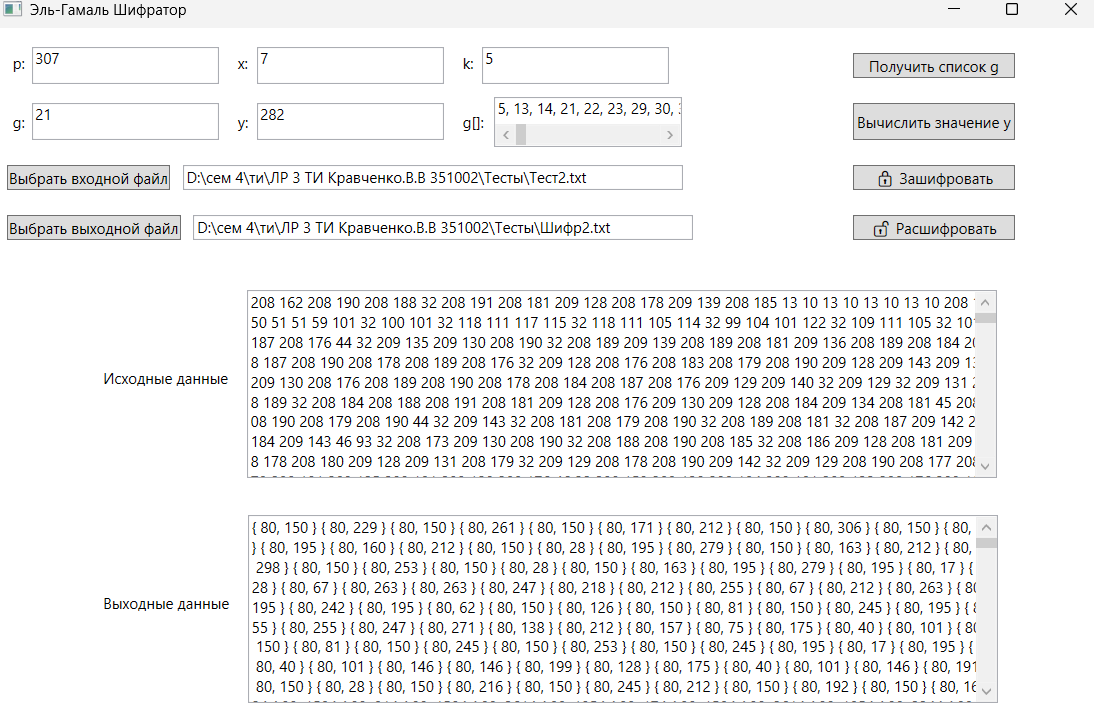
Исходный файл: Тест2.txt



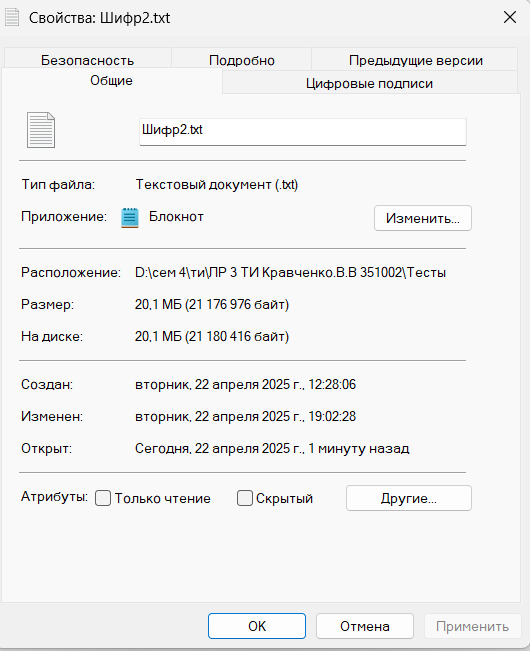
Содержимое файла до шифрования:  
 

Содержимое файла до шифрования в приложении Hex Editor

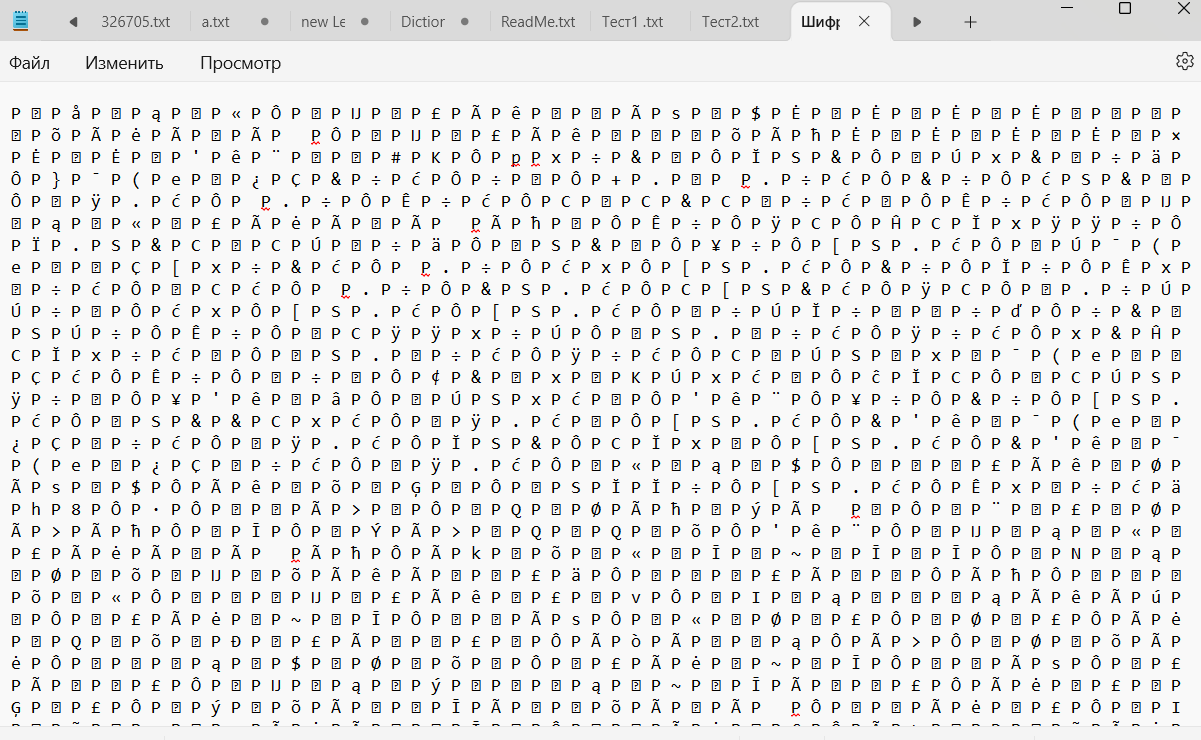




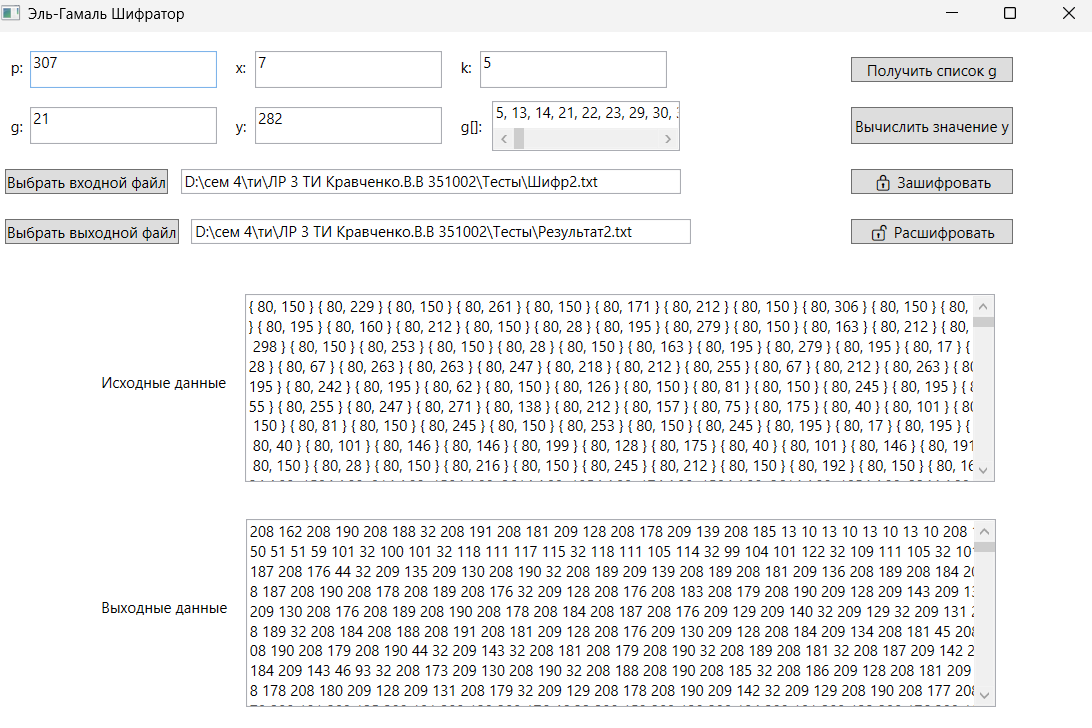
Выходной файл: Шифр2.txt



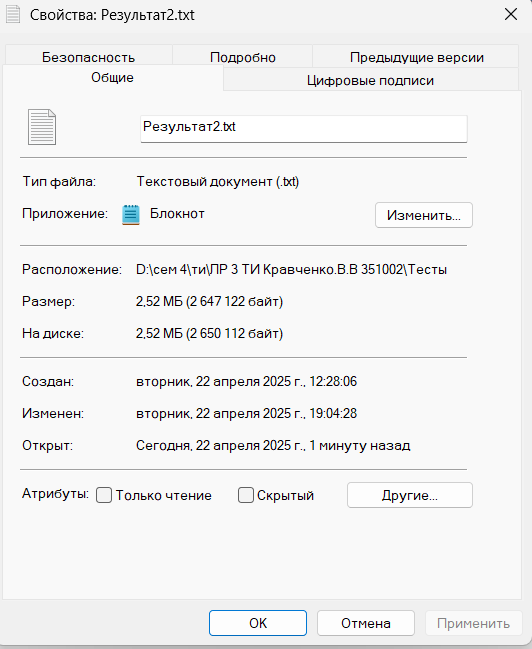
Содержимое файла после шифрования:



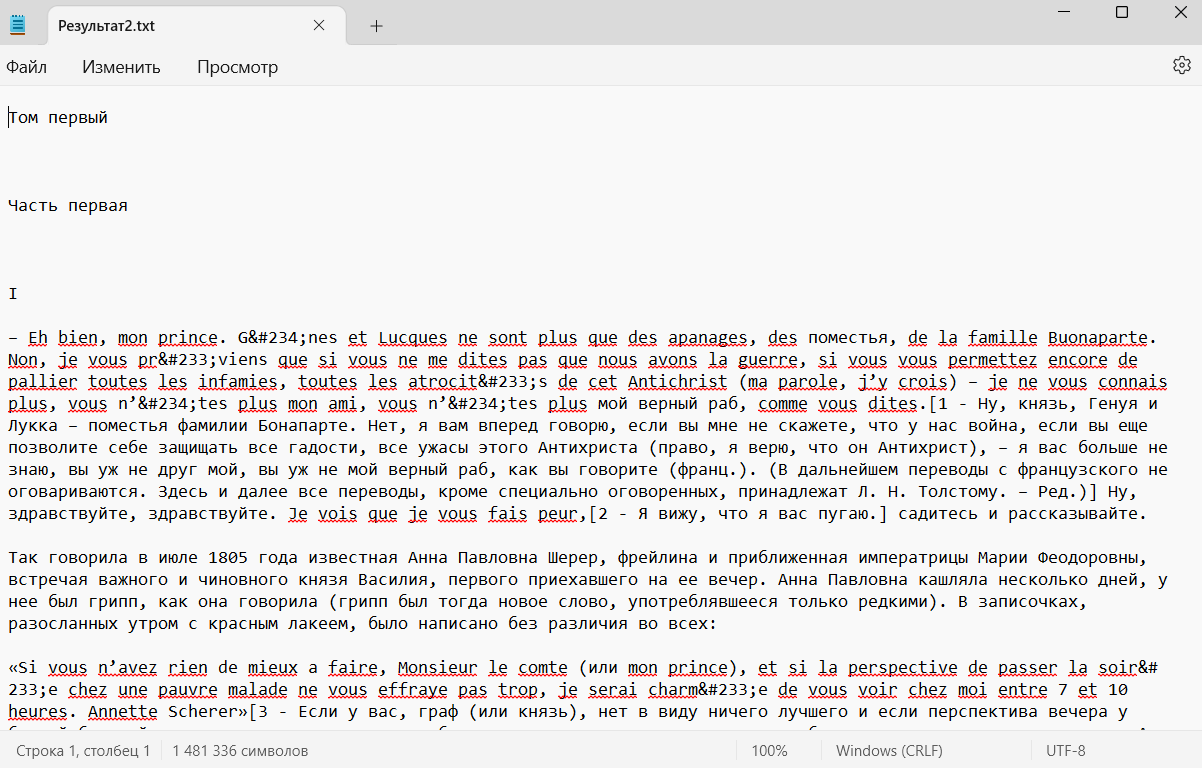
Дешифрование:



Выходной файл: Результат2.txt

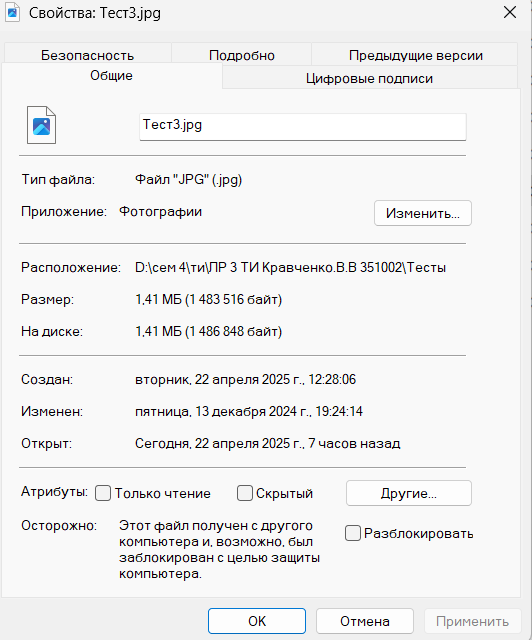


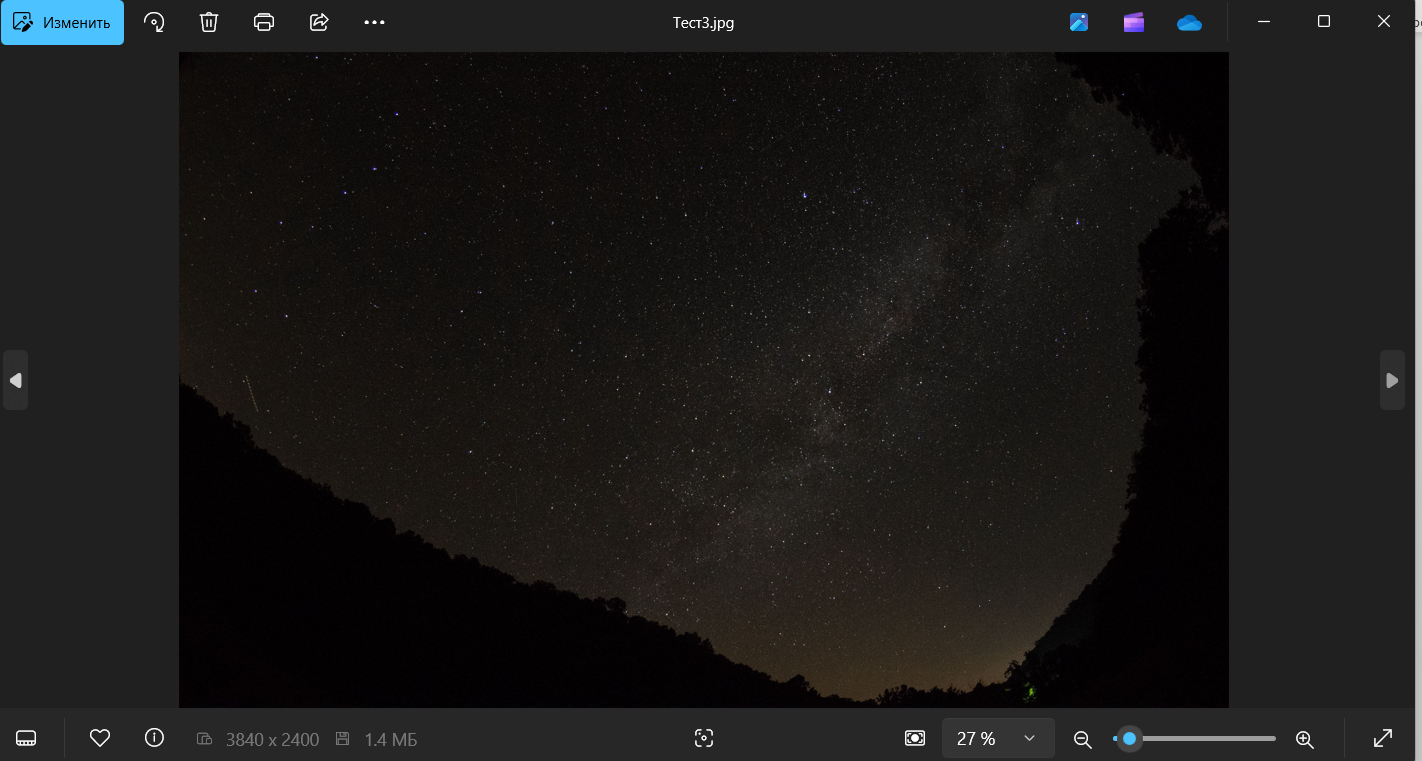
Содержимое файла после дешифрования:



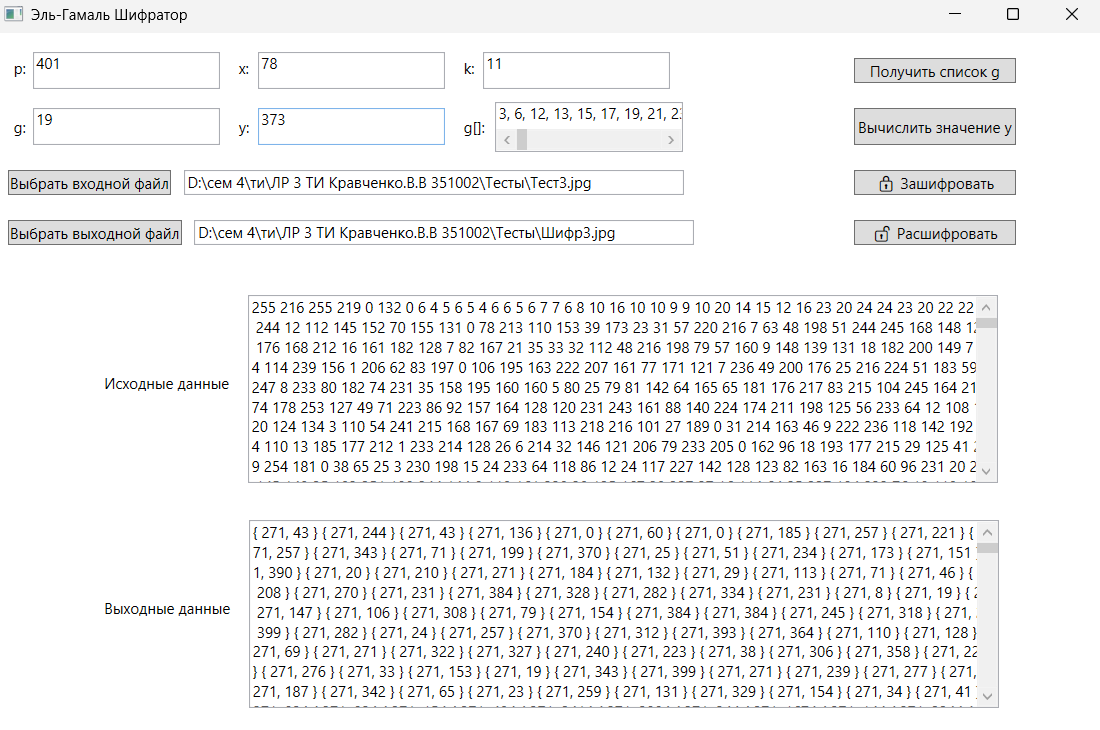
3. Проверка работоспособности программы для изображения

Исходный файл: Тест3.jpg

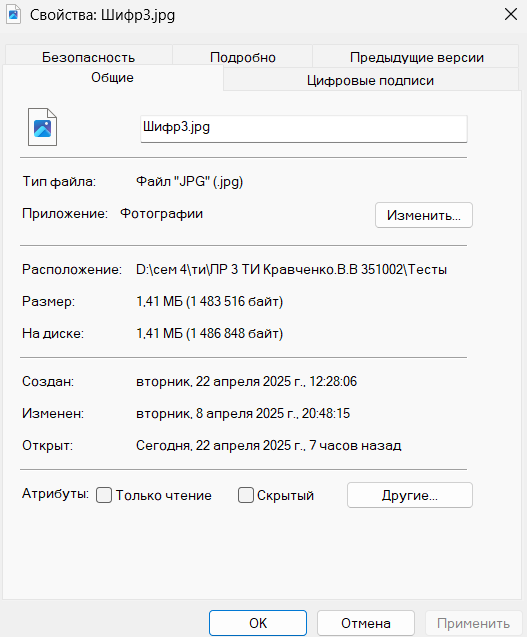


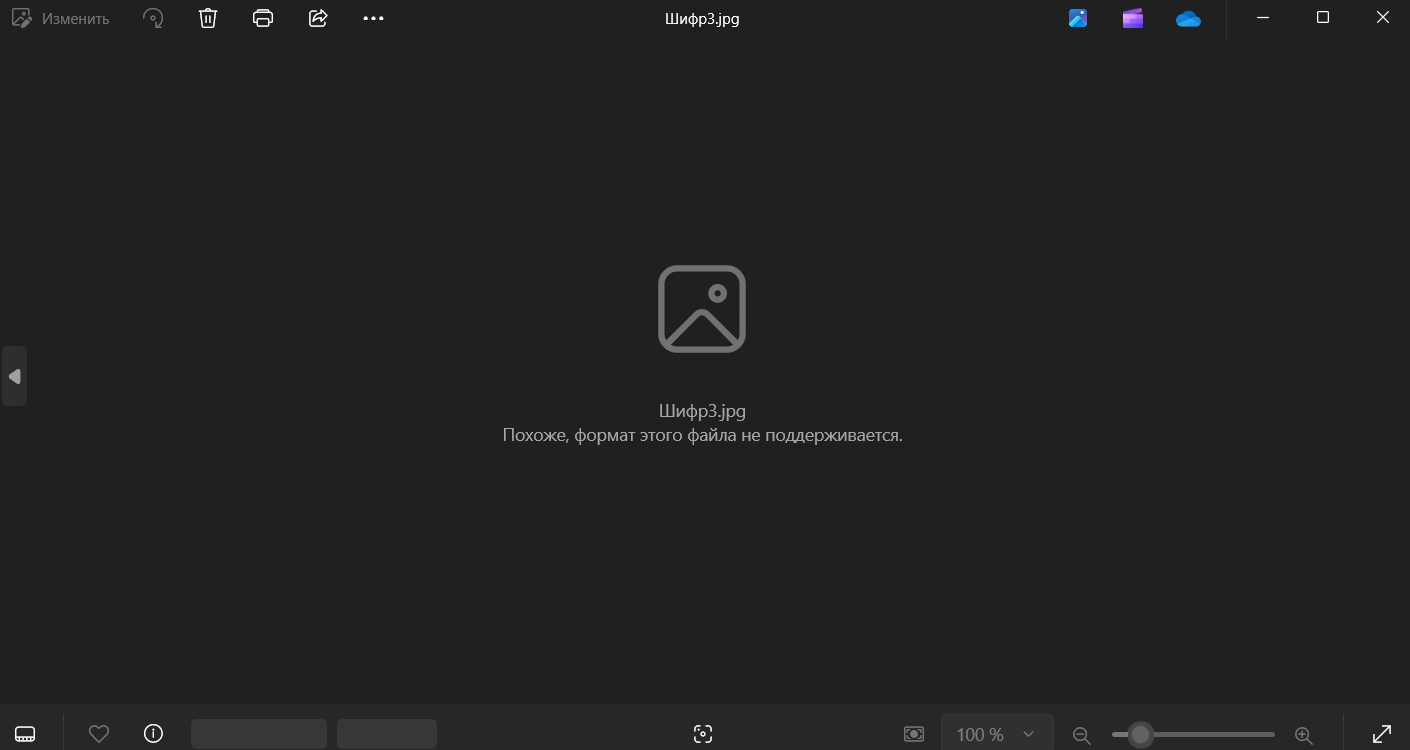


Шифрование

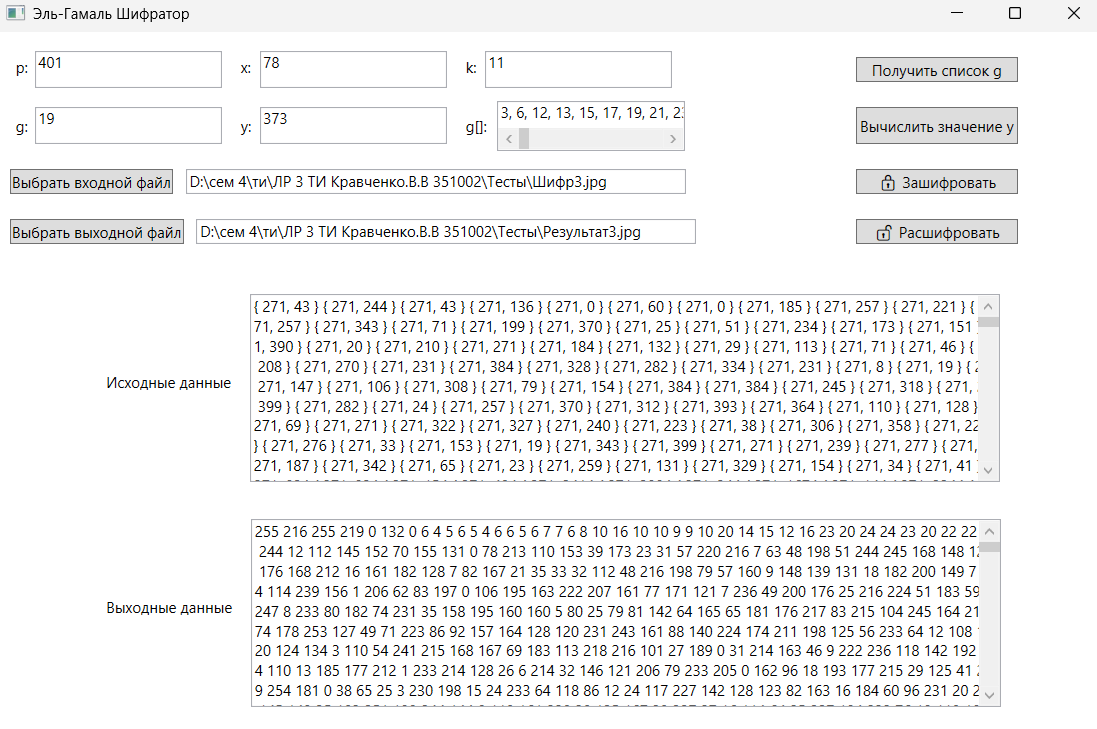


Содержимое файла после шифрования:

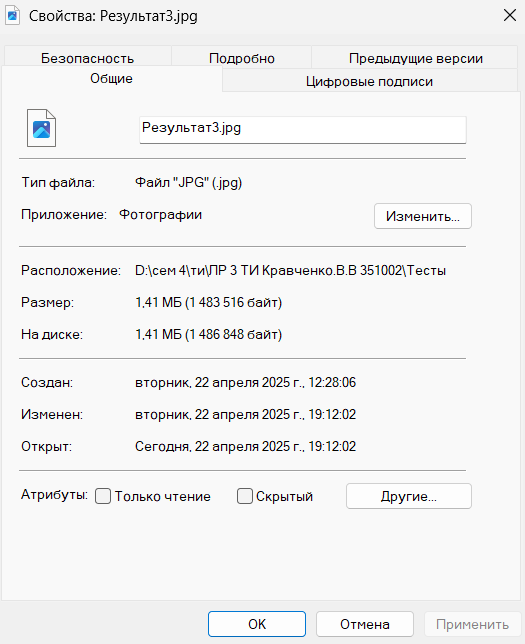




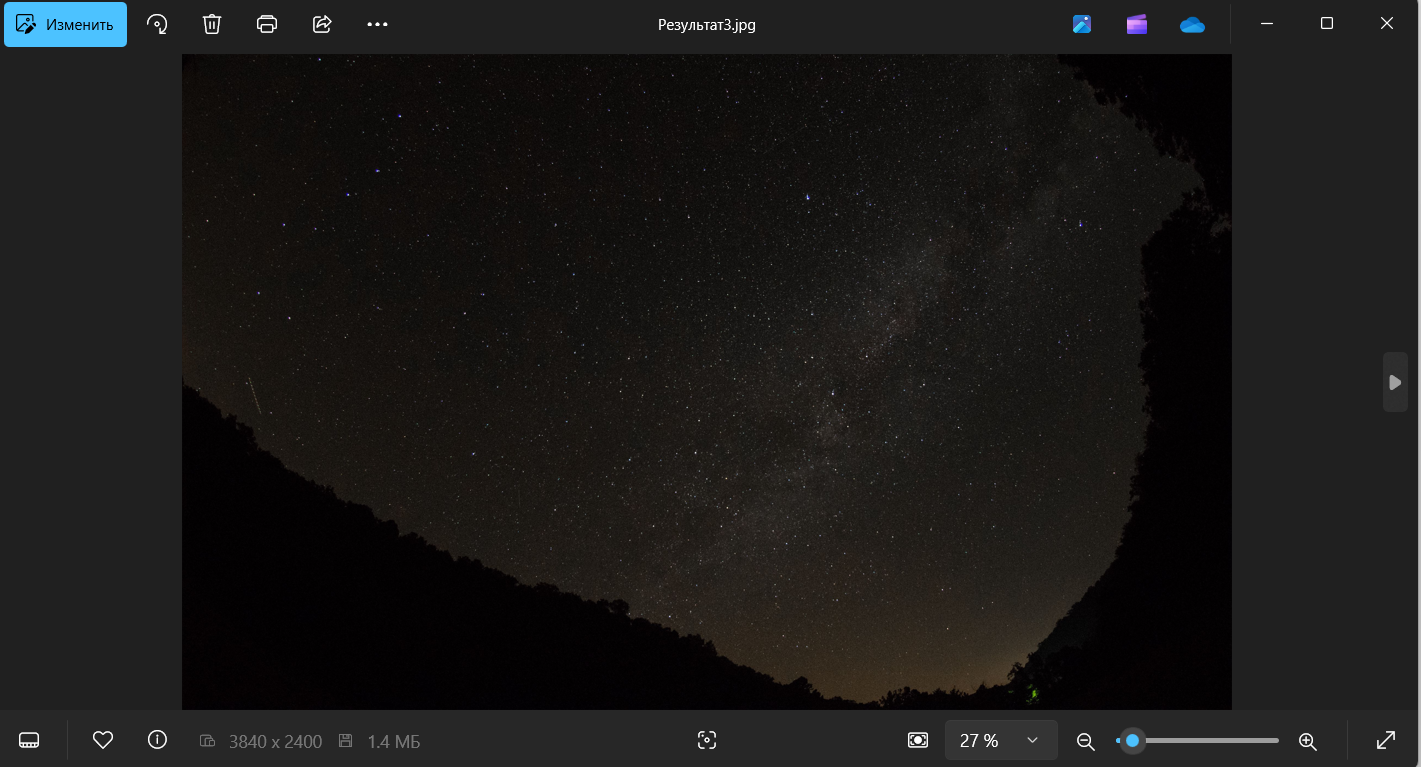
Дешифрование:



Выходной файл: Результат3.jpg



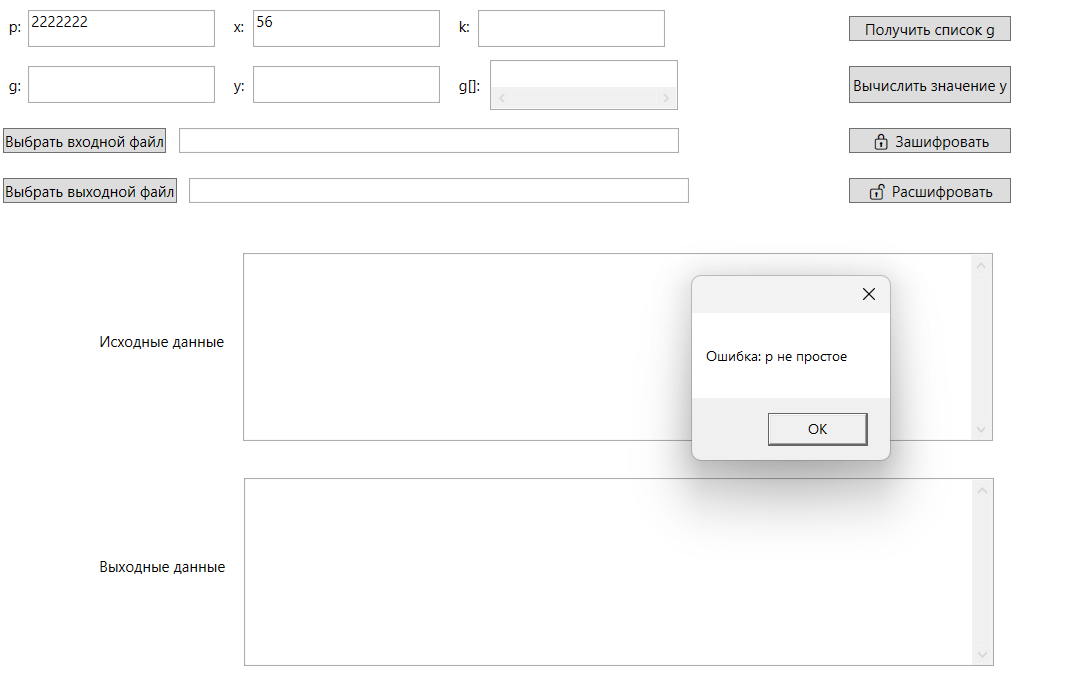
Содержимое файла после дешифрования:



**Группа Б – Проверка корректности вводимых данных**

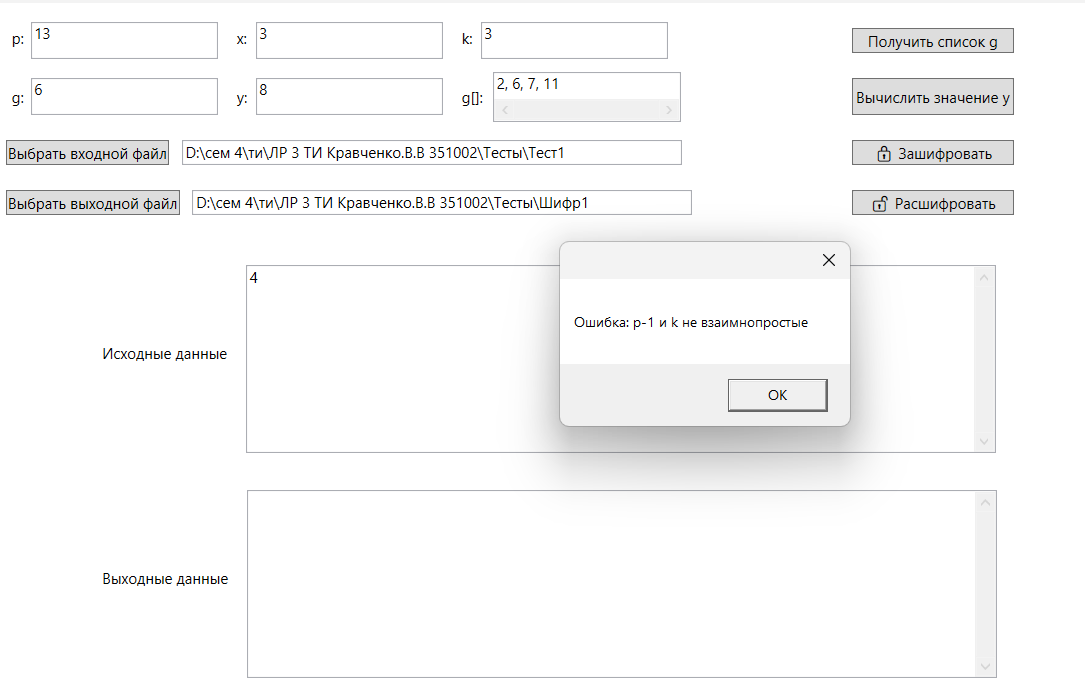
4. Проверка работоспособности программы при p не простом

Программа выдаёт сообщение об ошибке и просит пользователя ввести корректное значение



5. Проверка работоспособности программы при k не взаимопростом с p-1

Программа выдаёт сообщение об ошибке и просит пользователя ввести корректное значение k



6. Проверка работоспособности программы при некорректном значении g

Программа выдаёт сообщение об ошибке и просит пользователя ввести корректное значение g

