Отчет к лабораторной работе №3

Голубева Анастасия

Вариант 2

1. **Быстрое возведение в степень по модулю:**

a1 = 5, z = 13 (1101), n = 23

5¹³ mod 23 = 5 \* 5^13 mod 23 = 5 \* (5⁶)² mod 23 = 5 \* ((5²)²)² mod 23 = 17

|  |  |  |  |
| --- | --- | --- | --- |
| a1(основание степени) | z(степень) | x(результат) | Шаги выполнения |
| 8 | 12 | 1 | 0 |
| 1 | 6 | 1 | 1 |
| 1 | 3 | 1 | 2 |
| 1 | 2 | 1 | 3 |
| 1 | 1 | 1 | 4 |
|  | 0 | 1 | 5 |

812 mod 21 = 1

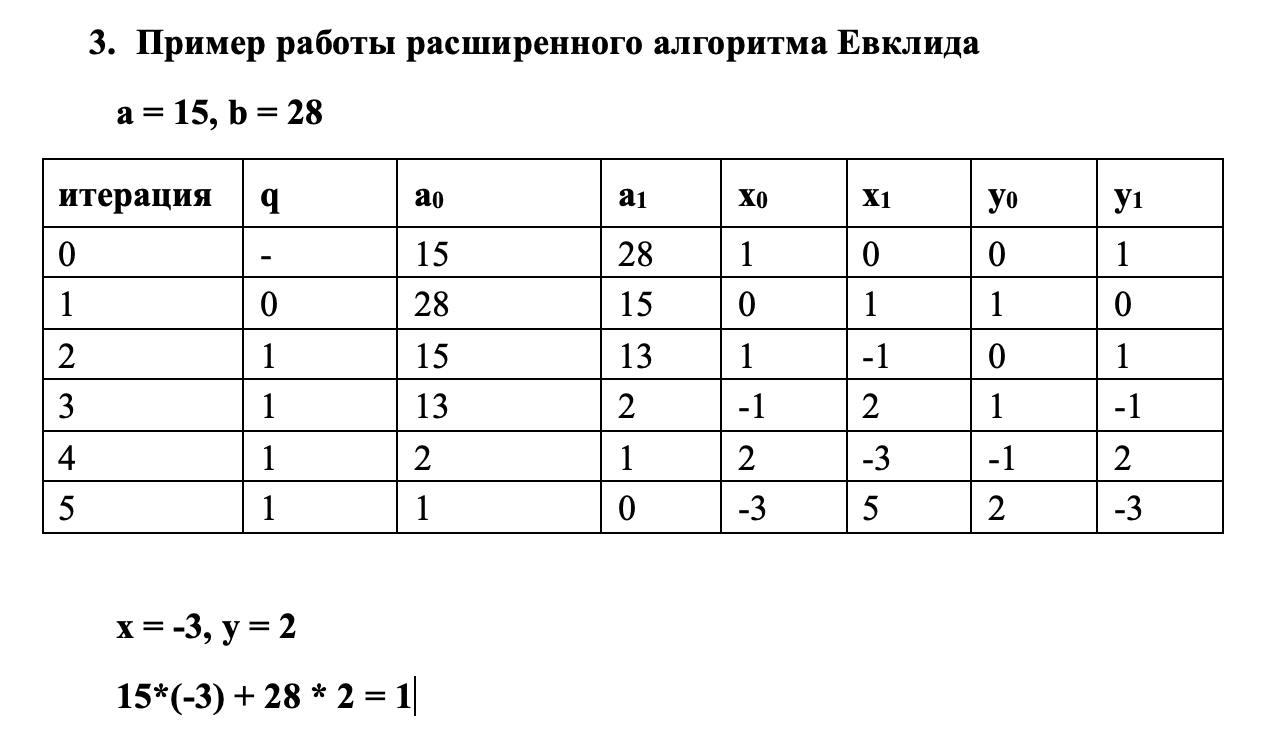
1. **Поиск всех первообразных корней числа**

p = 41

p – 1 = 40= 2\*2\*2\*5

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

6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35– первообразные корни

**Проверка работоспособности программы**

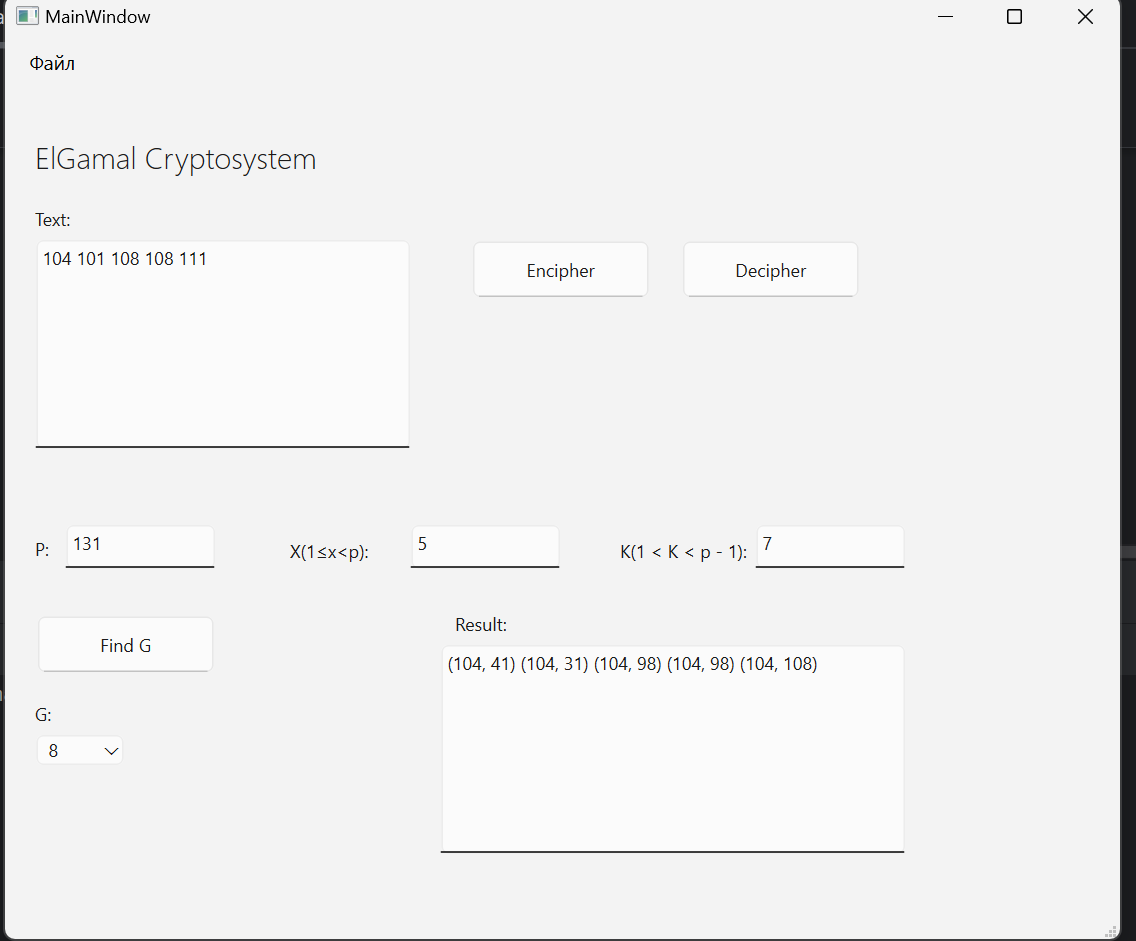
1. **Исходный текст:**

Исходный текст:

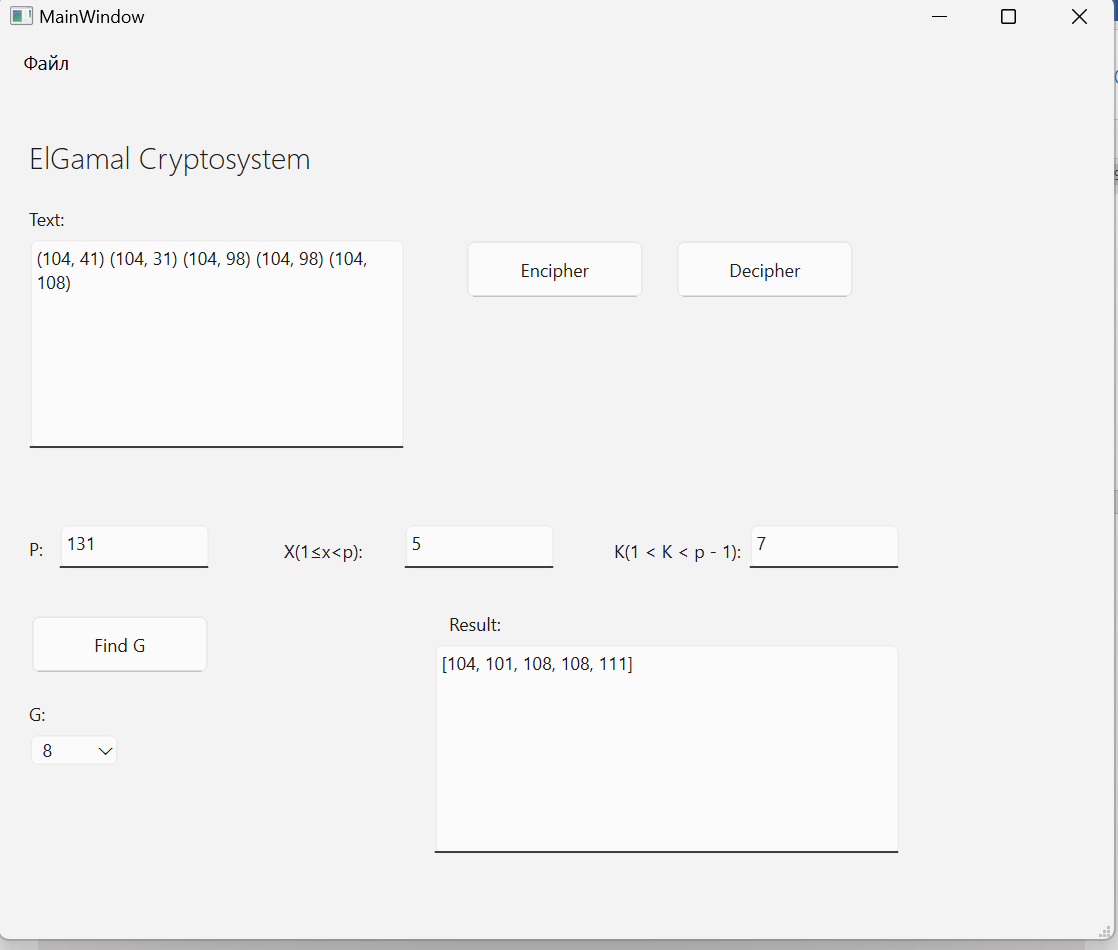
hello

**Окно программы:**

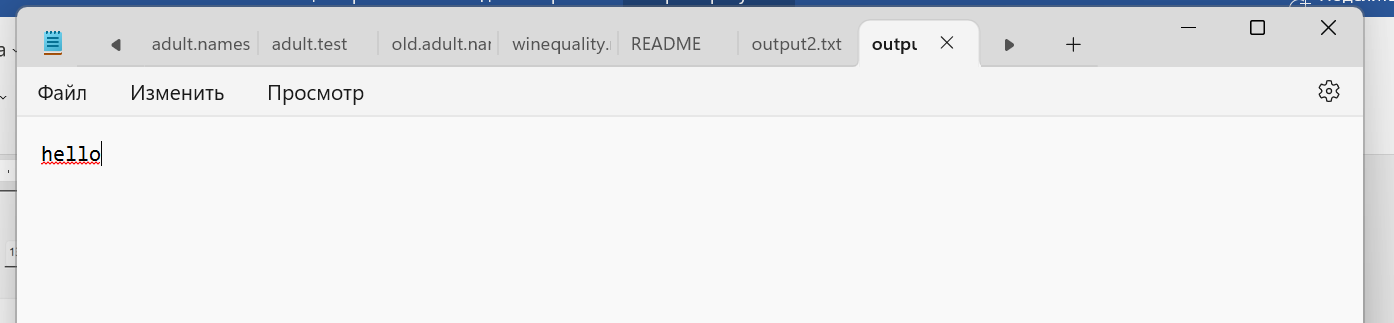
**Шифрование:**

****

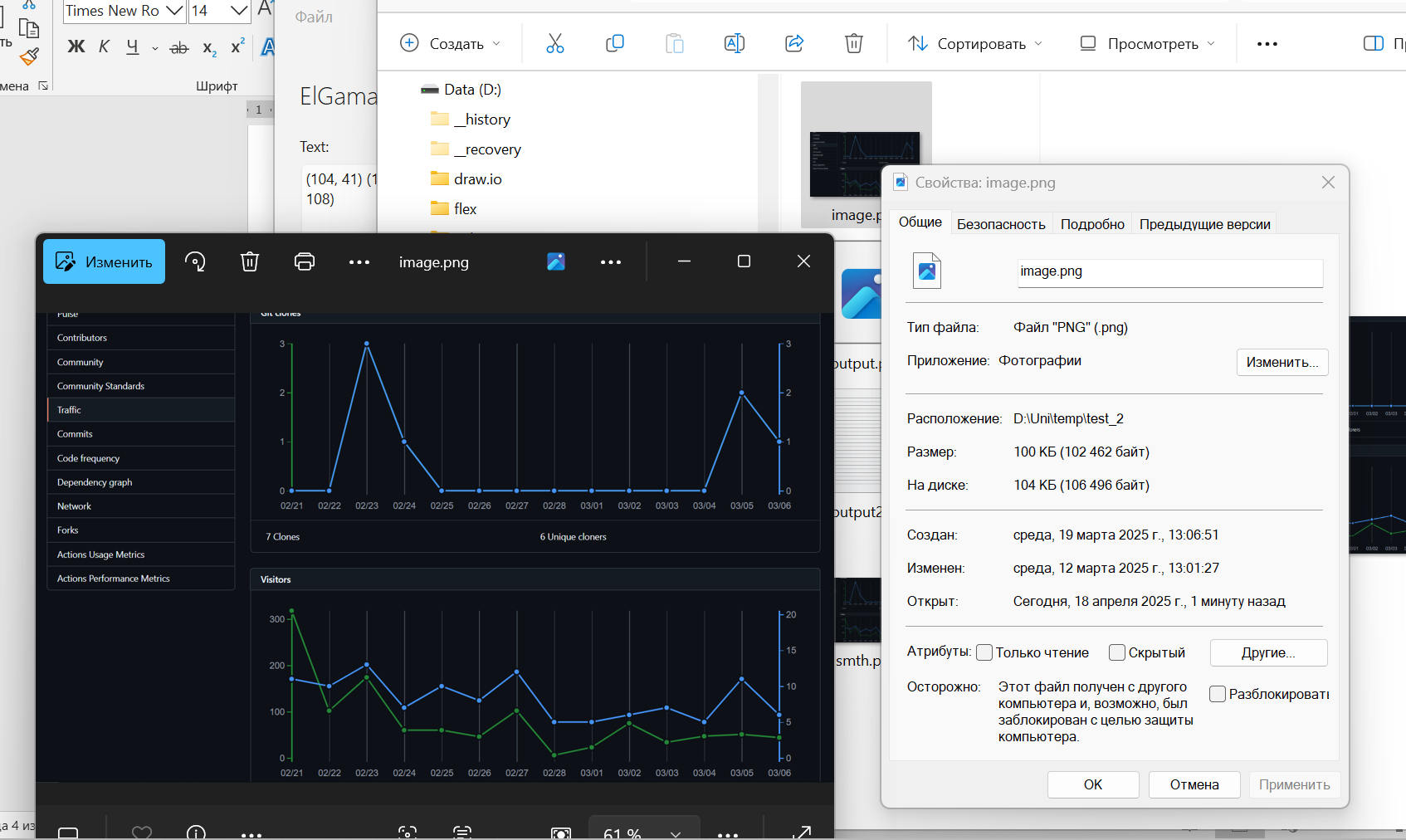
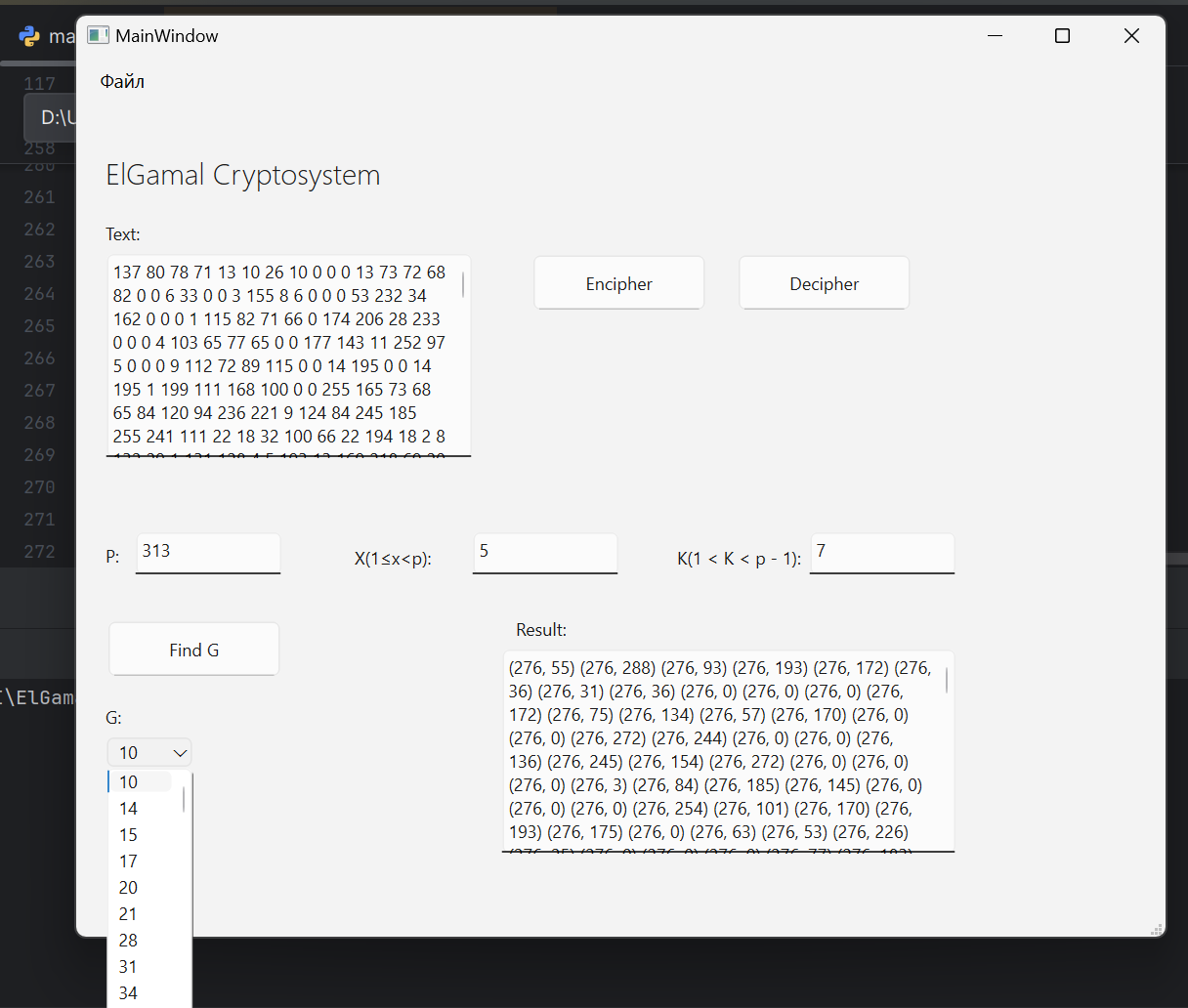
**Дешифрование:**

****

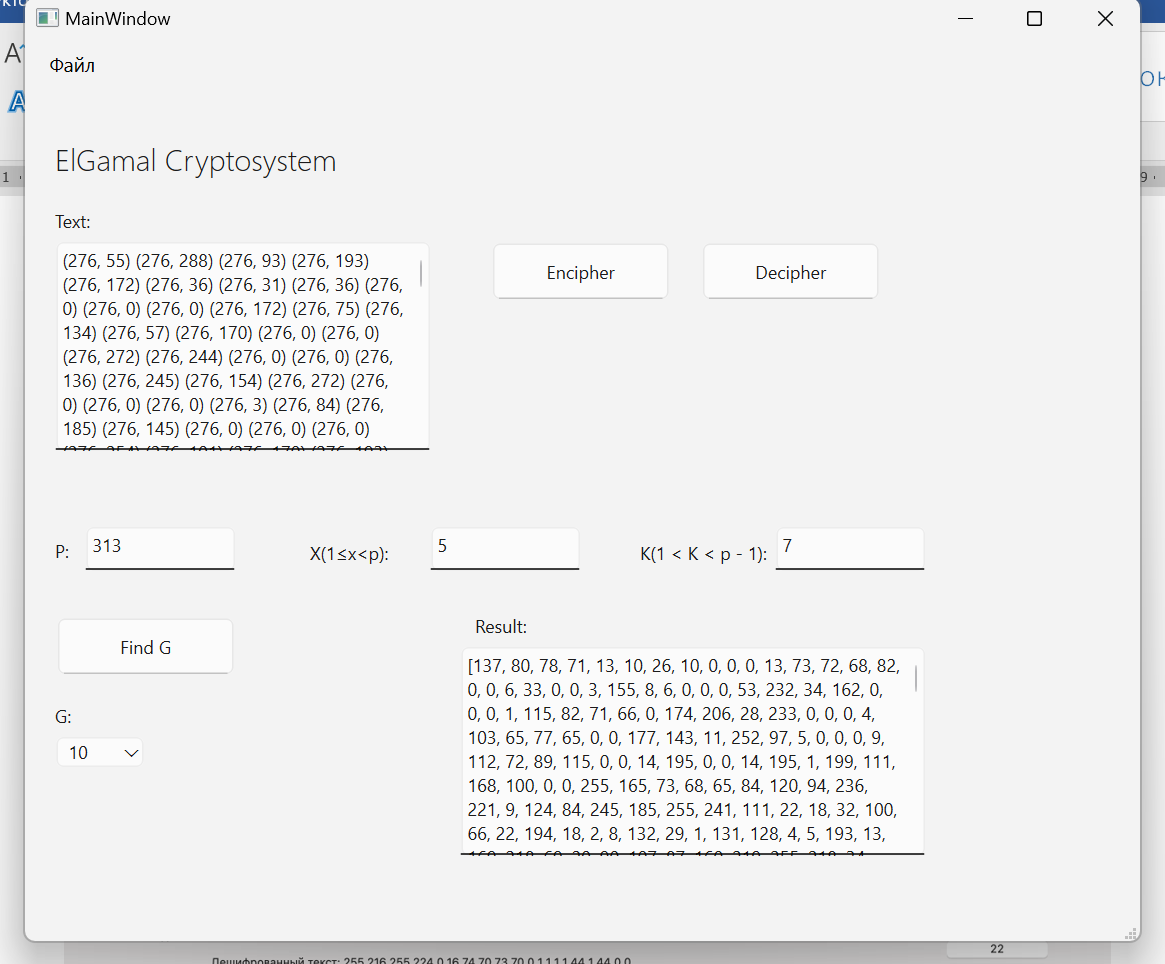
**Значение файла после дешифрования:**

****

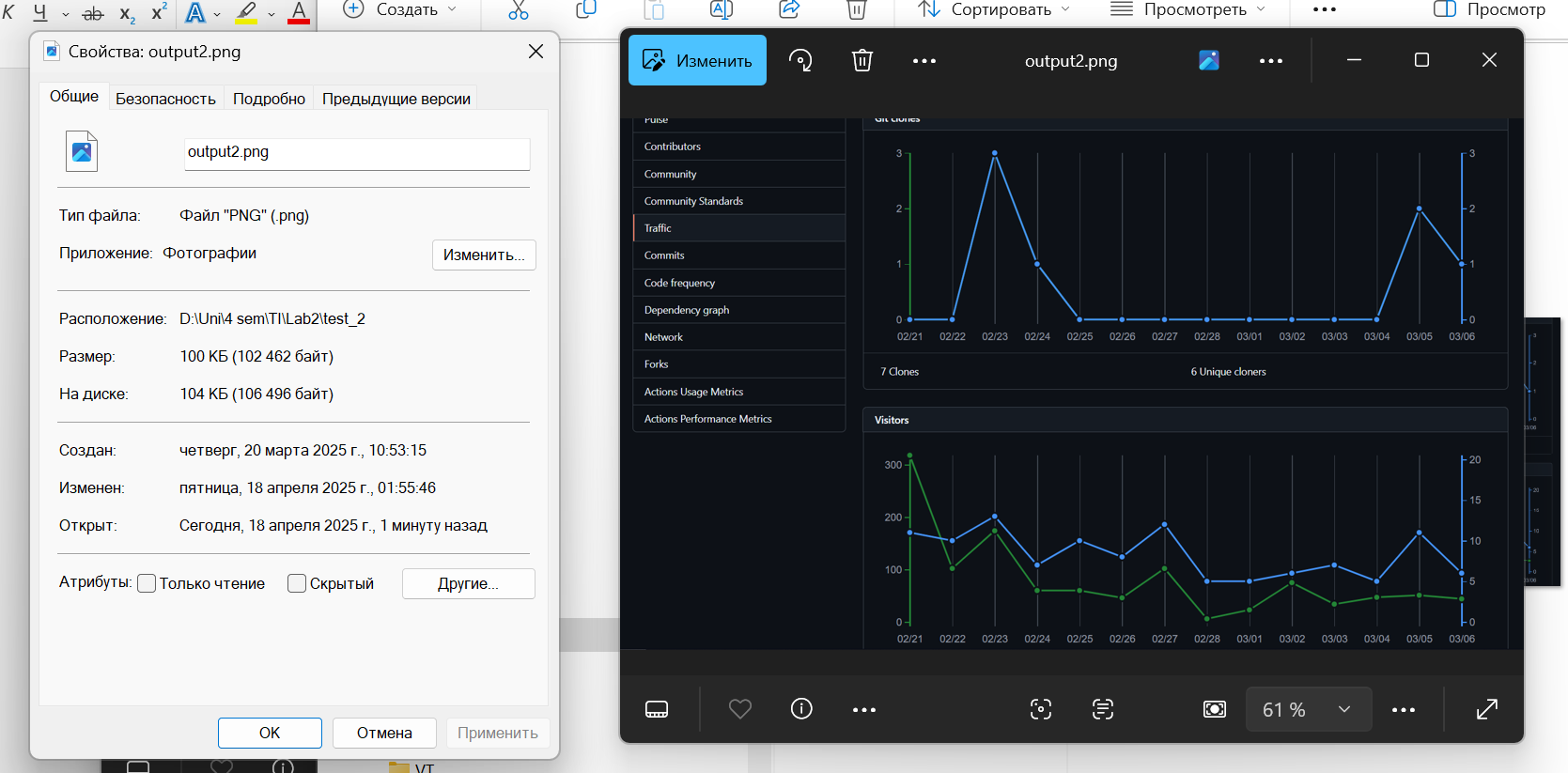
1. **Шифрование картинки:**

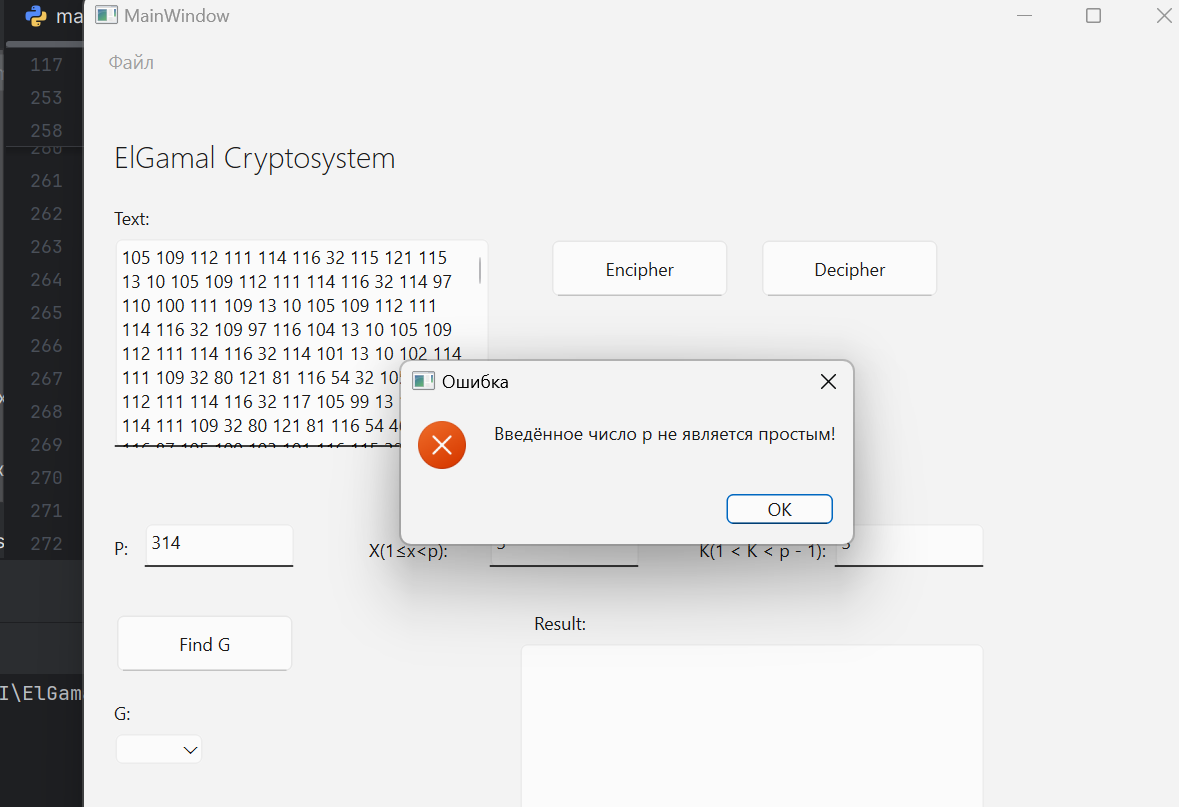
Дешифрование:



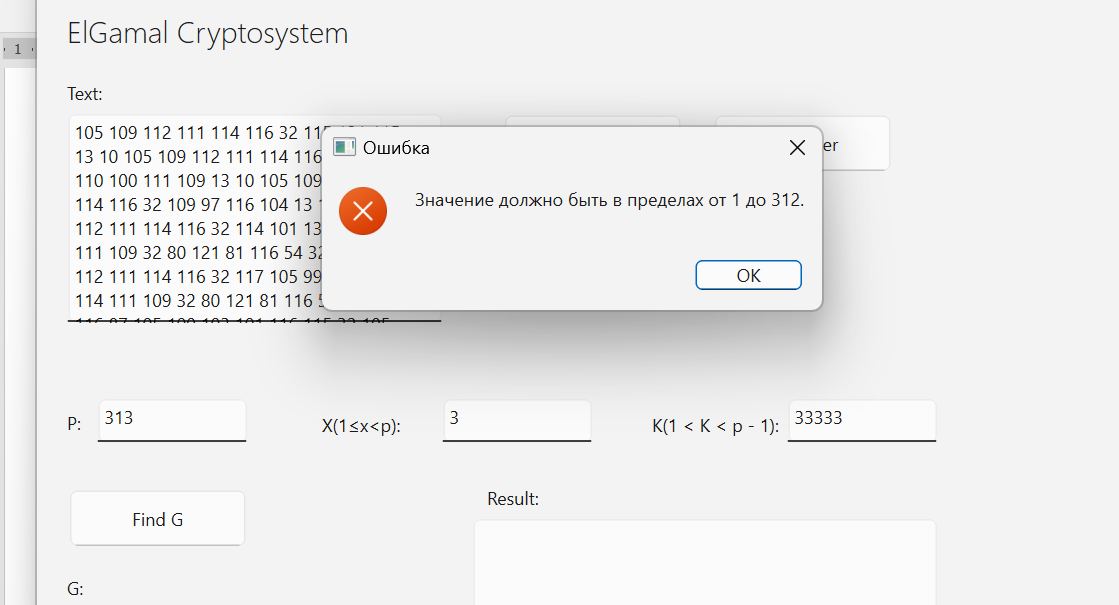
Файл после дешифрования:



Ввод некорректных данных:  
p – не простое - ошибка :



Если к не попадает в промежуток:



Если к и p не взаимно простые:

