Отчет к лабораторной работе №3

351002 Хмылко Илья Сергеевич

Вариант 3

Алгоритм Рабина

**Пример поиска случайного первообразного корня**

p = 23, p – 1 = 22 = 2 \* 11

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^22/2 mod 23** | **g^22/11 mod 23** | **Первообразный** |
| 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 | 1 | 8 | - |
| 11 | 22 | 6 | + |
| 12 | 1 | 6 | - |
| 13 | 1 | 8 | - |
| 14 | 22 | 6 | + |
| 15 | 22 | 22 | + |
| 16 | 1 | 3 | - |
| 17 | 22 | 12 | + |
| 18 | 1 | 2 | - |
| 19 | 22 | 16 | + |
| 20 | 22 | 8 | + |
| 21 | 22 | 4 | + |
| 22 | 1 | 1 | - |

5, 7, 11, 14, 15, 17, 19, 20, 21 — всего 9 штук.

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

a1 = 13, z = 23 (10101), n = 27

|  |  |  |  |
| --- | --- | --- | --- |
| **а1(основание степени)** | **z(степень)** | **х(результат)** | **Шаги выполнения** |
| 13 | 23 | 1 | 0 - начальное значение |
| 13 | 22 | (13 \* 1) mod 27 = 13 | 1 (23 - нечётное) |
| (13\*13) mod 27 = 7 | 11 | 13 | 2 (22 чётное) |
| 7 | 10 | (13 \* 7) mod 27 = 10 | 3 (11 нечётное) |
| (7 \* 7) mod 27 = 22 | 5 | 10 | 4 (10 чётное) |
| 22 | 4 | (10 \* 22) mod 27 = 4 | 5 (5 нечётное) |
| (22 \* 22) mod 27 =25 | 2 | 4 | 6 (4 чётное) |
| (25 \* 25) mod 27 =4 | 1 | 4 | 7 (2 чётное) |
| 4 | 0 | (4 \* 4) mod 27 = 16 | 8 (1 нечётное) |

1323 mod 27 = 16

**Пример работы расширенного алгоритма Евклида**

A = 125 B = 95

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **d0** | **d1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 125 | 95 | 1 | 0 | 0 | 1 |
| 1 | 1 | 95 | 30 | 0 | 1 | 1 | -1 |
| 2 | 3 | 30 | 5 | 1 | -3 | -1 | 4 |
| 3 | 6 | 5 | 0 | -3 | 19 | 4 | -25 |

x = -3, y = 4

125 \* (-3) + 95 \* 4 = 5

**Проверка работоспособности программы**

**Шифрование текста:**

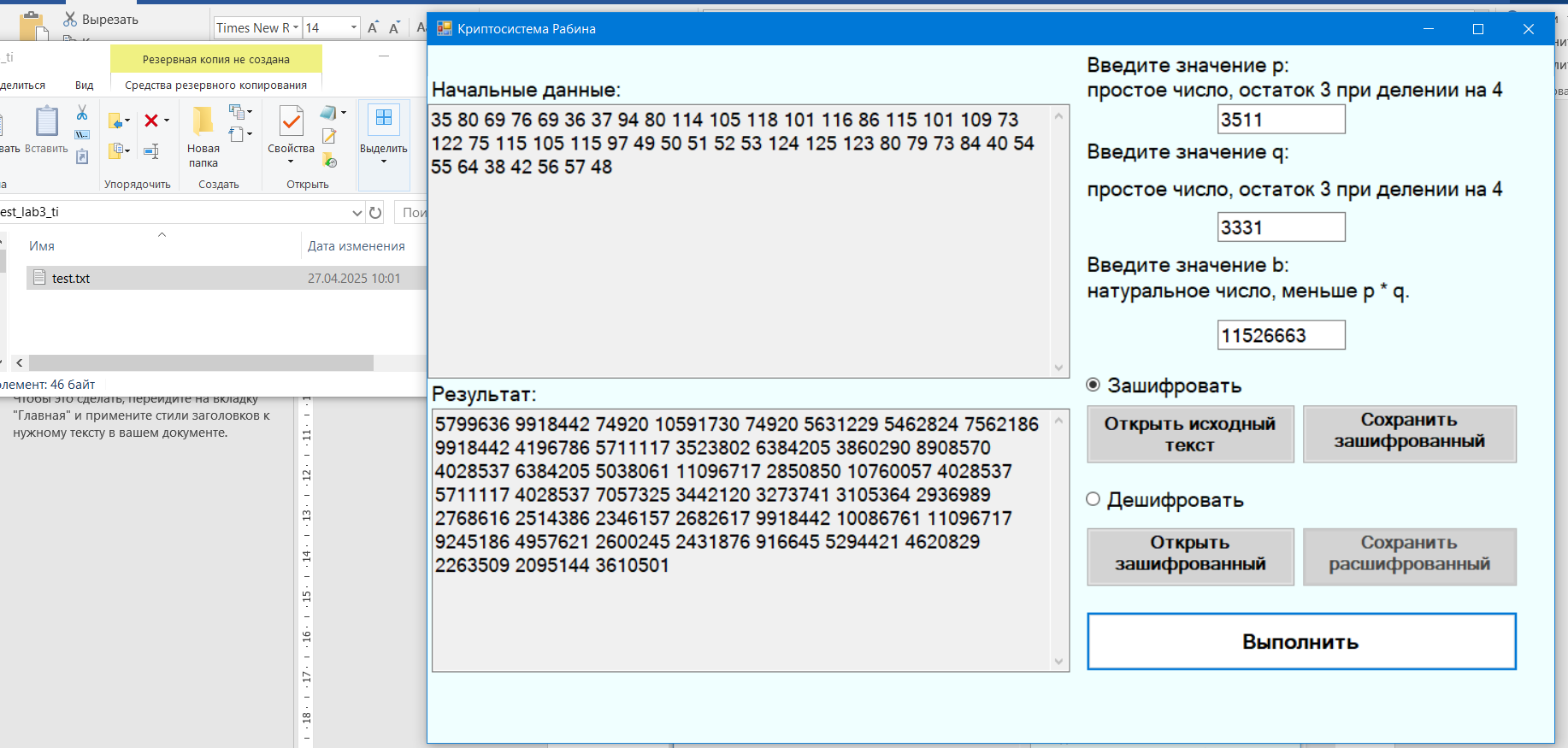
**Исходный текст:**

Исходный текст:

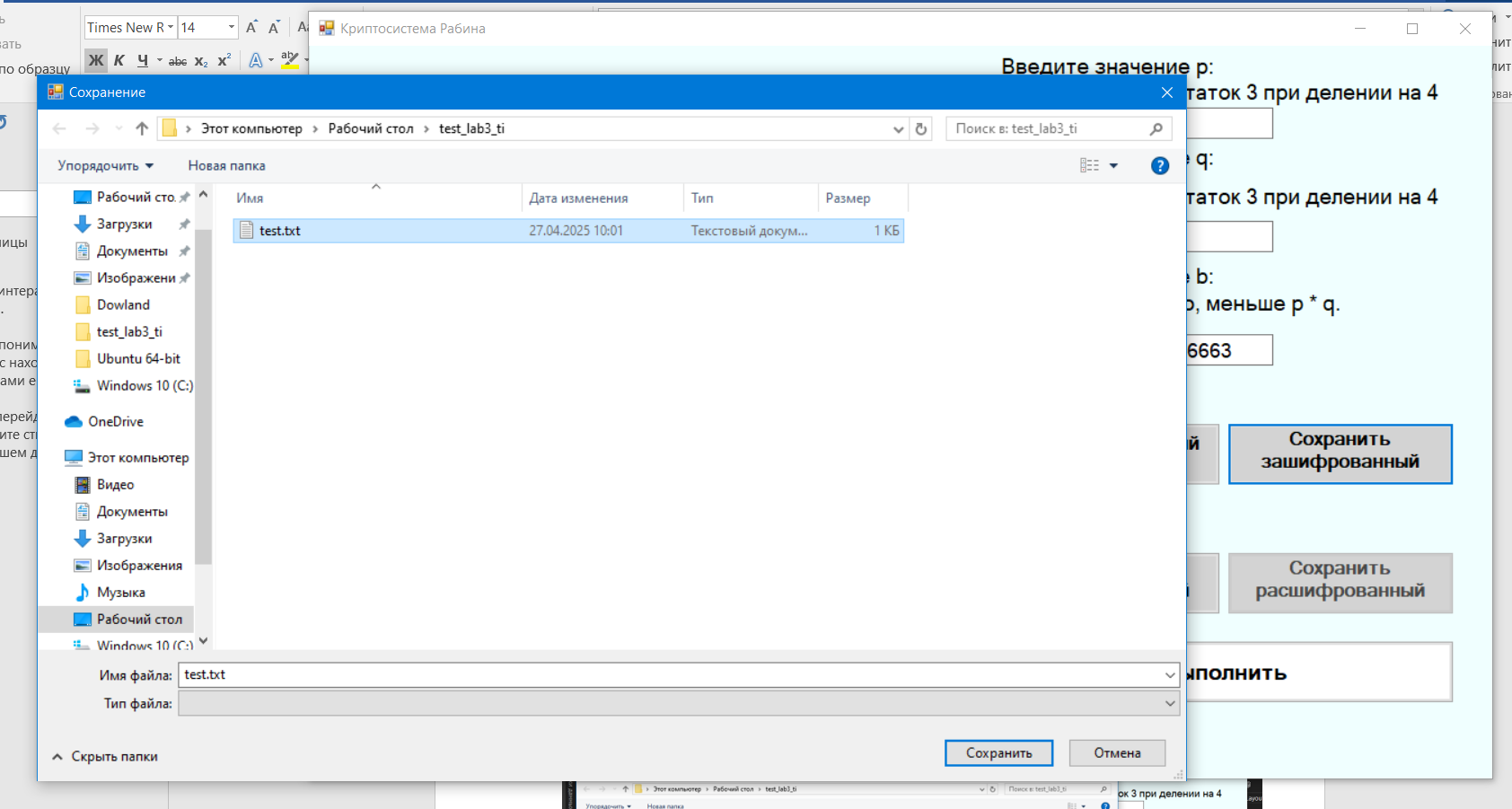
#PELE$%^PrivetVsemIzKsisa12345|}{POIT(67@&\*890

**Окно программы:**

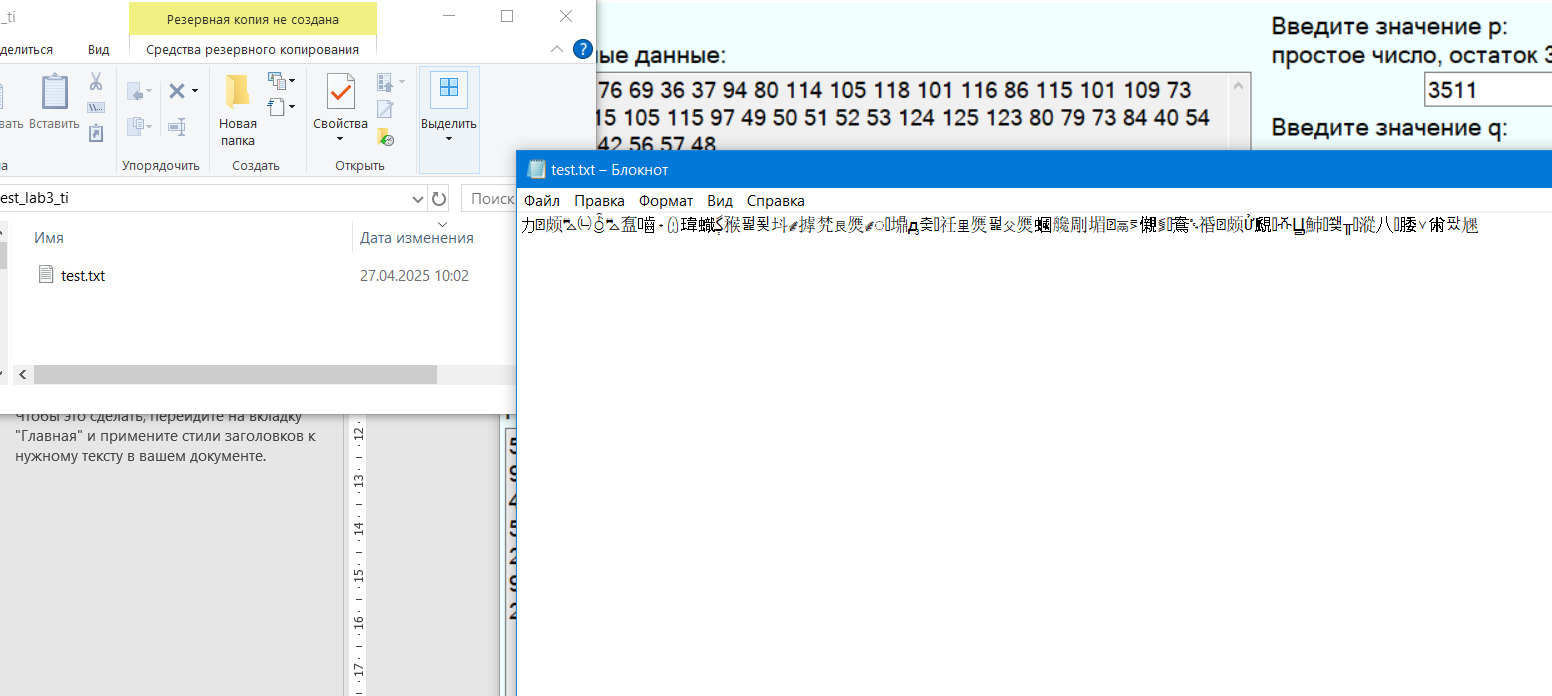
**Шифрование:**

****

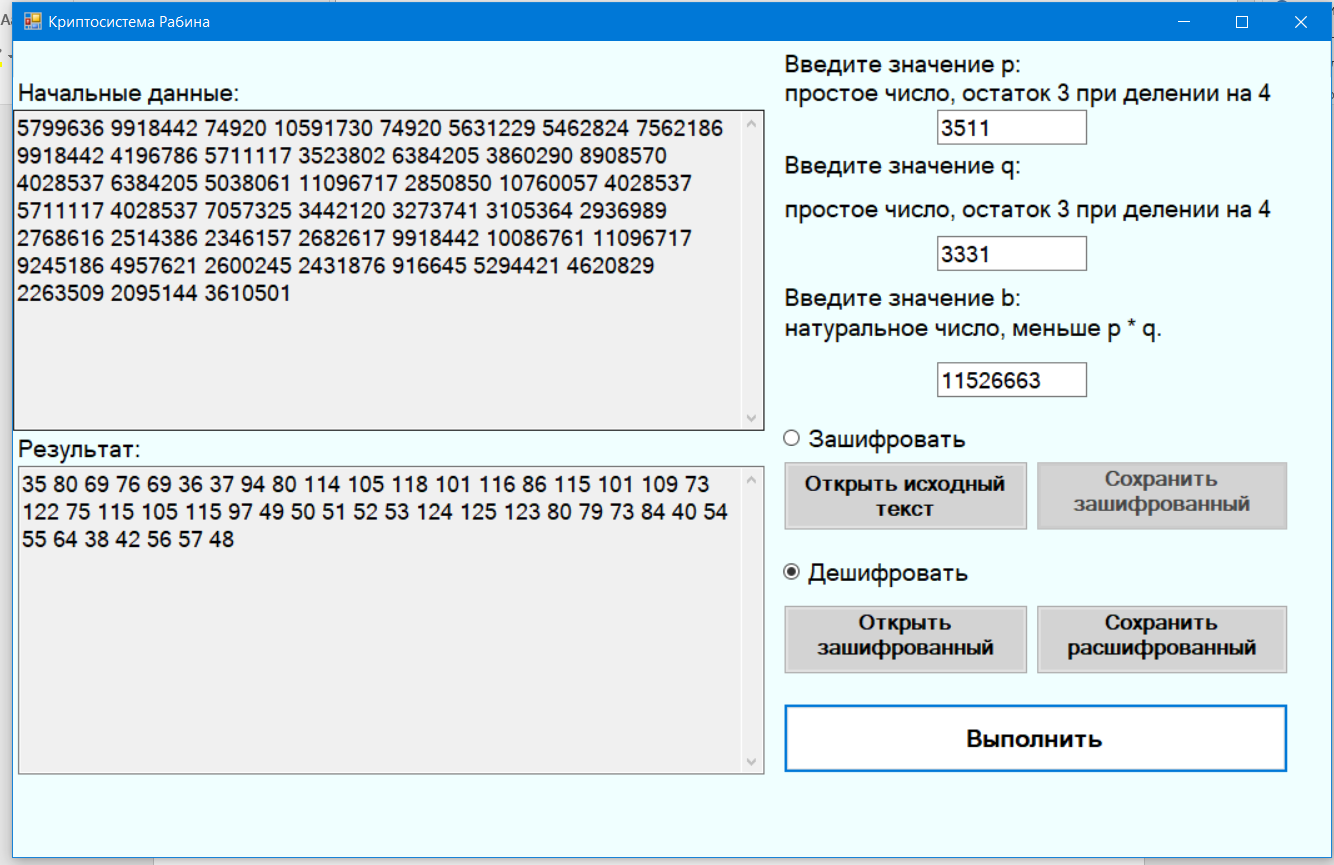
**Сохранение зашифрованного текста в файл:**

****

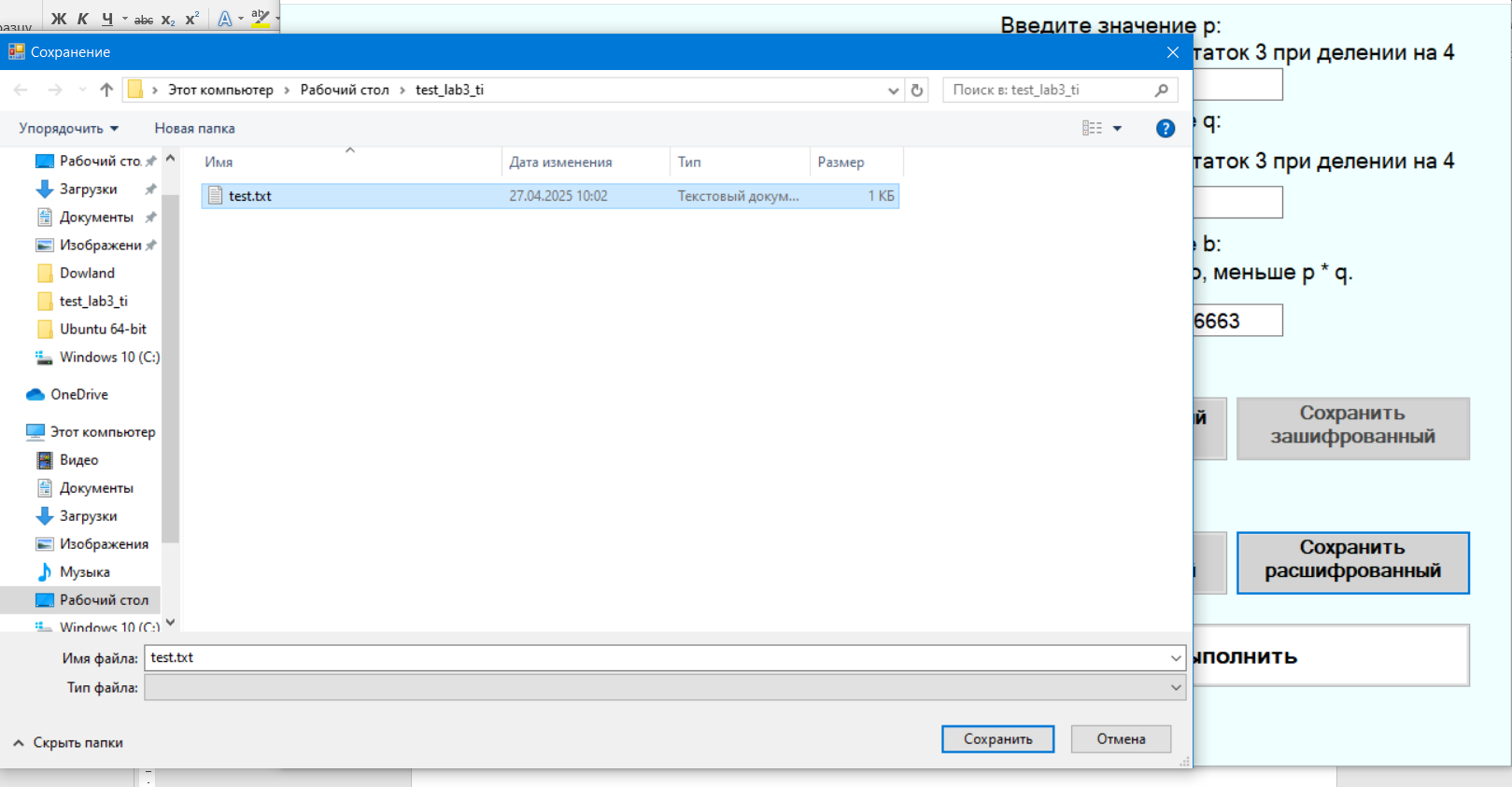
**Результат шифрования:**

****

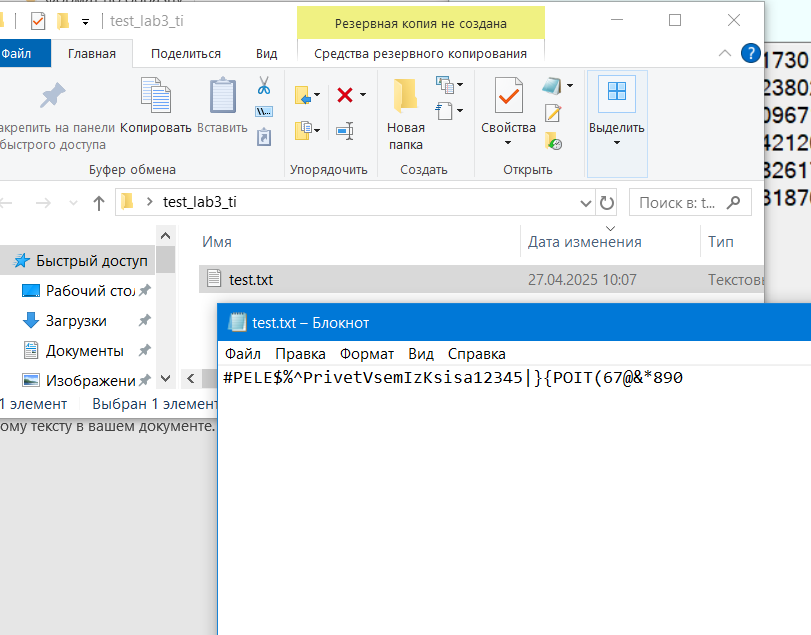
**Дешифрование:**



**Сохранение расшифрованного текста в файл:**



**Значение файла после дешифрования:**

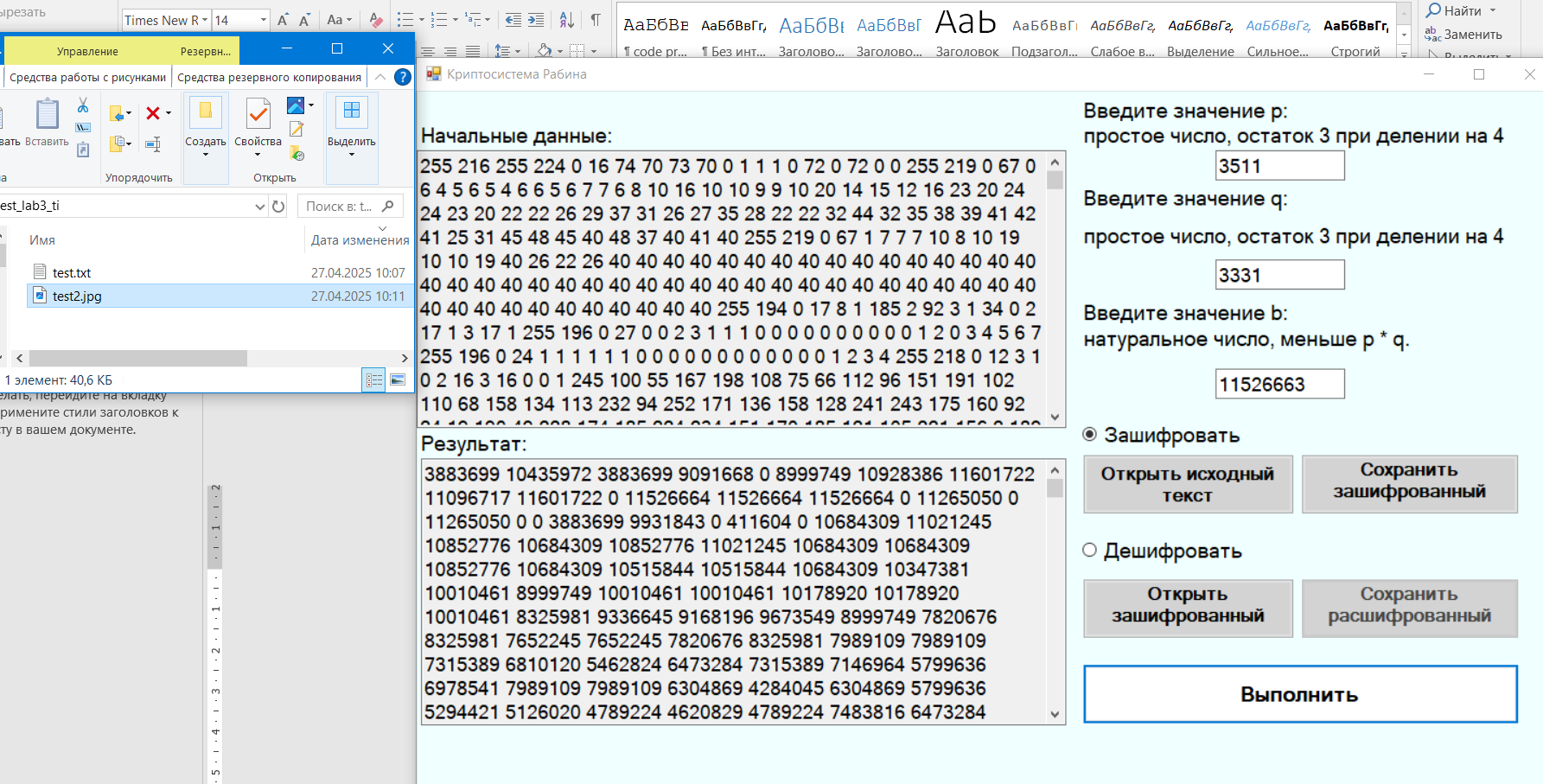


**Шифрование картинки:**

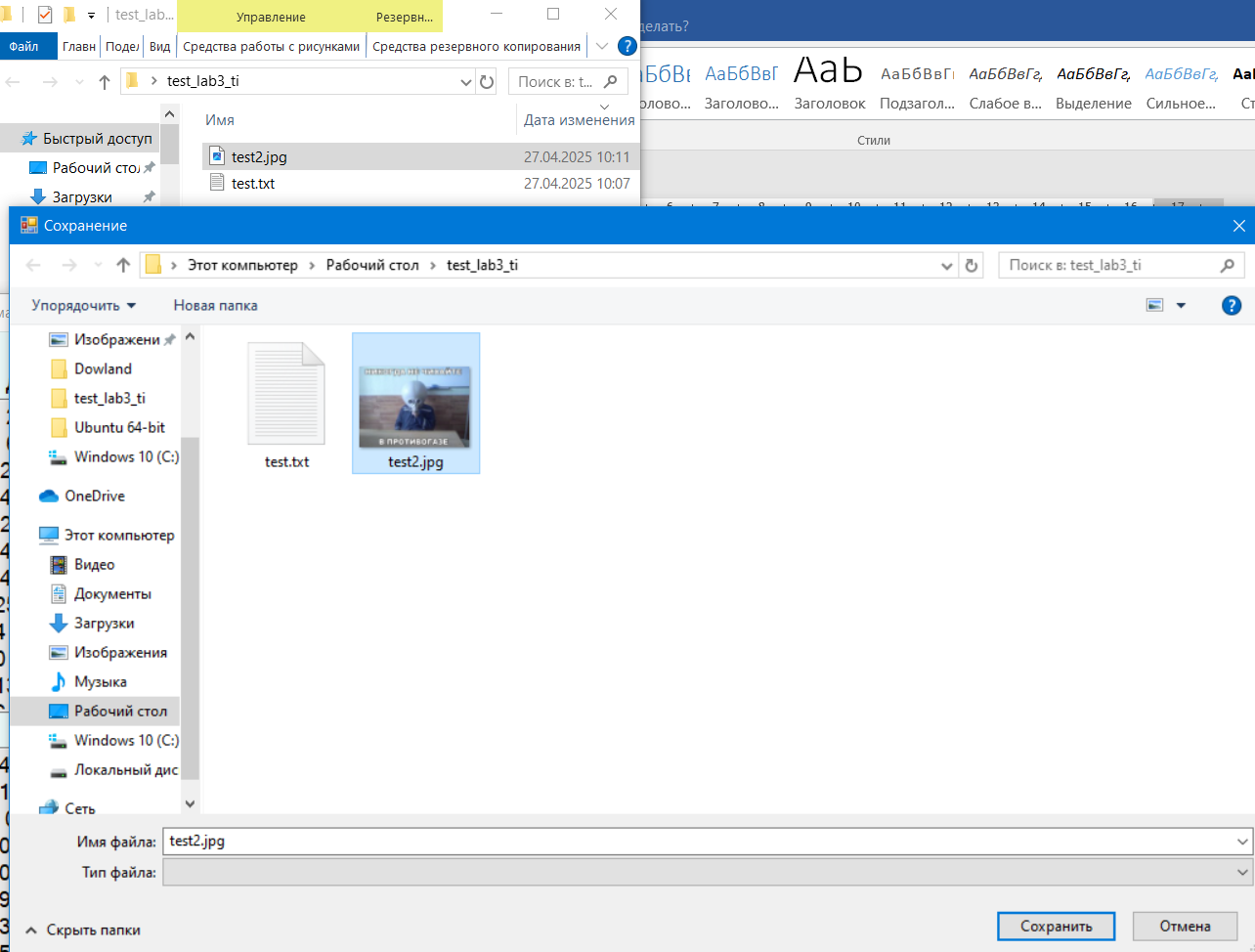
Исходная картинка в формате .jpg:



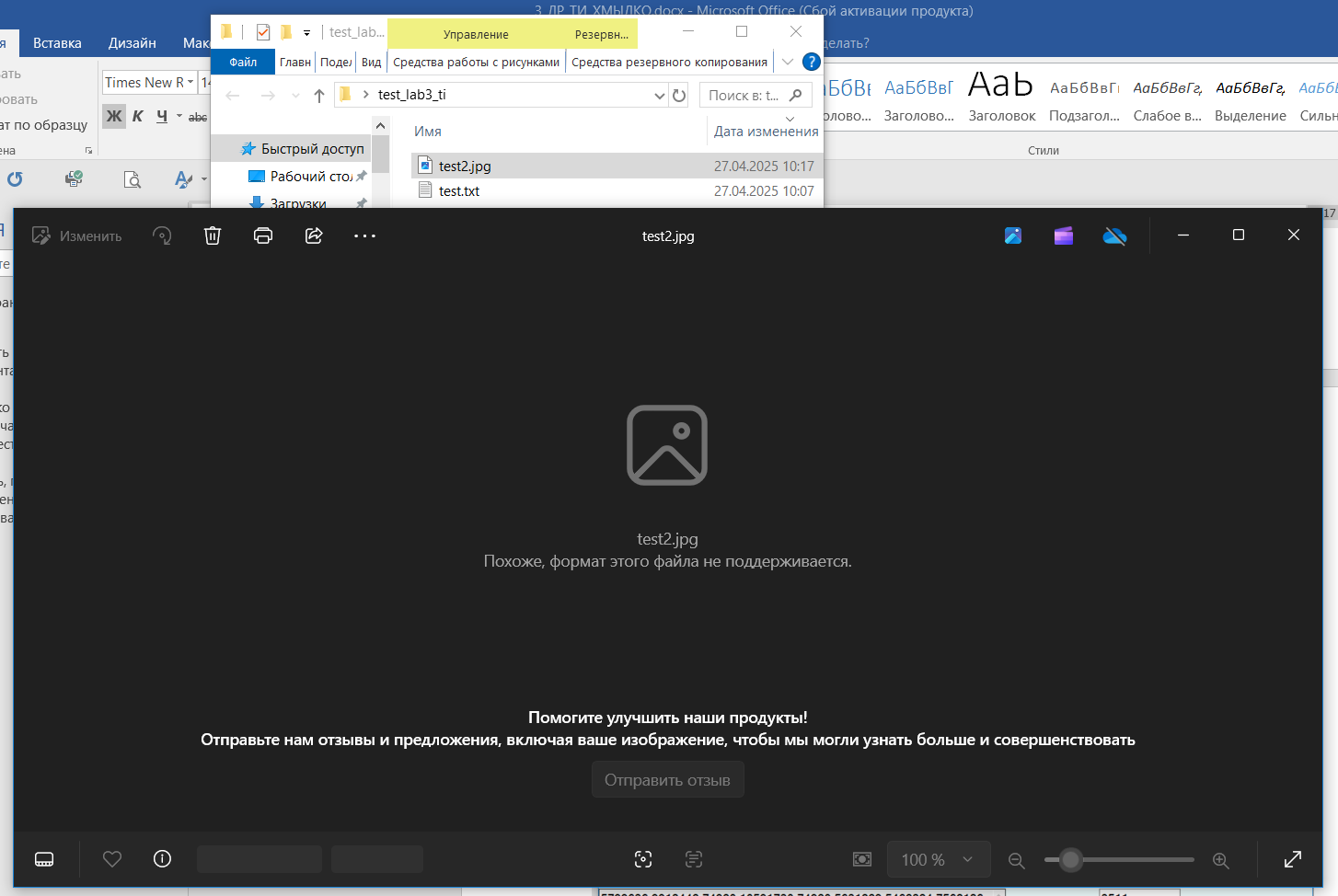
**Шифрование:**

****

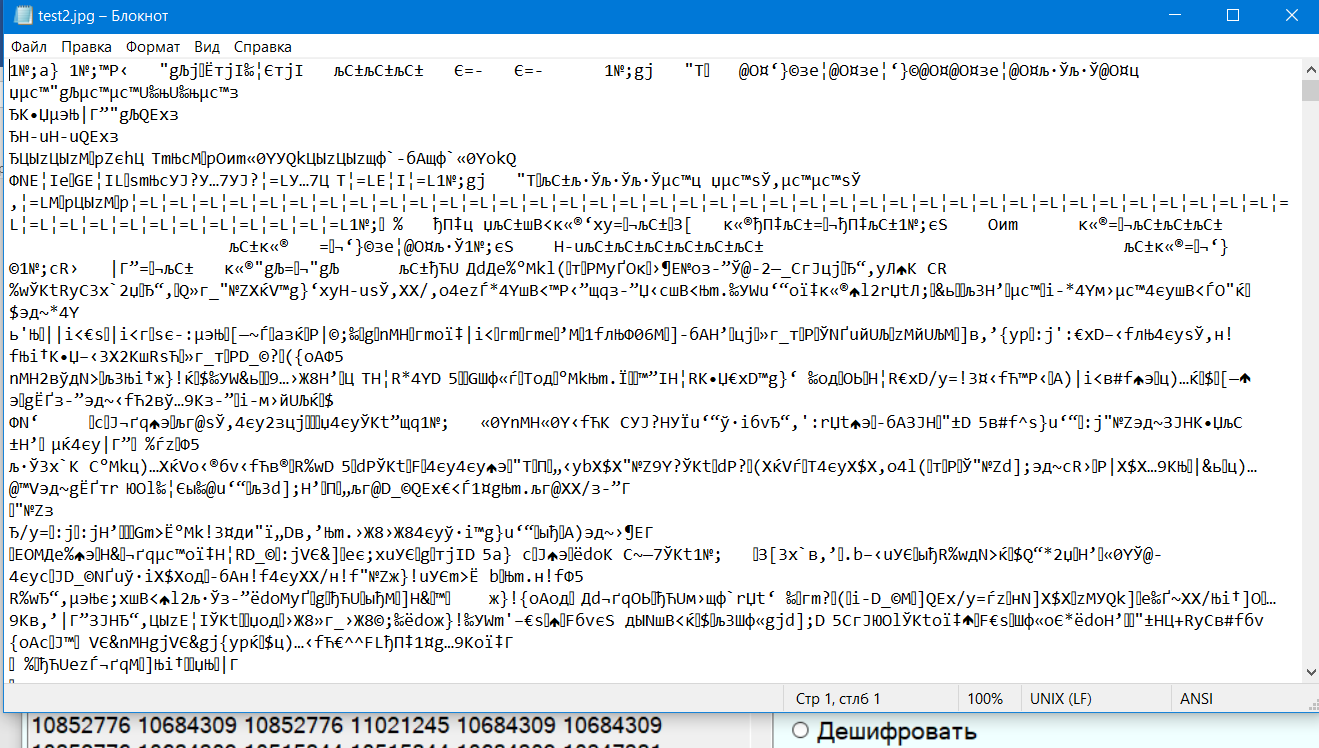
**Сохранение зашифрованной картинки в файл:**

****

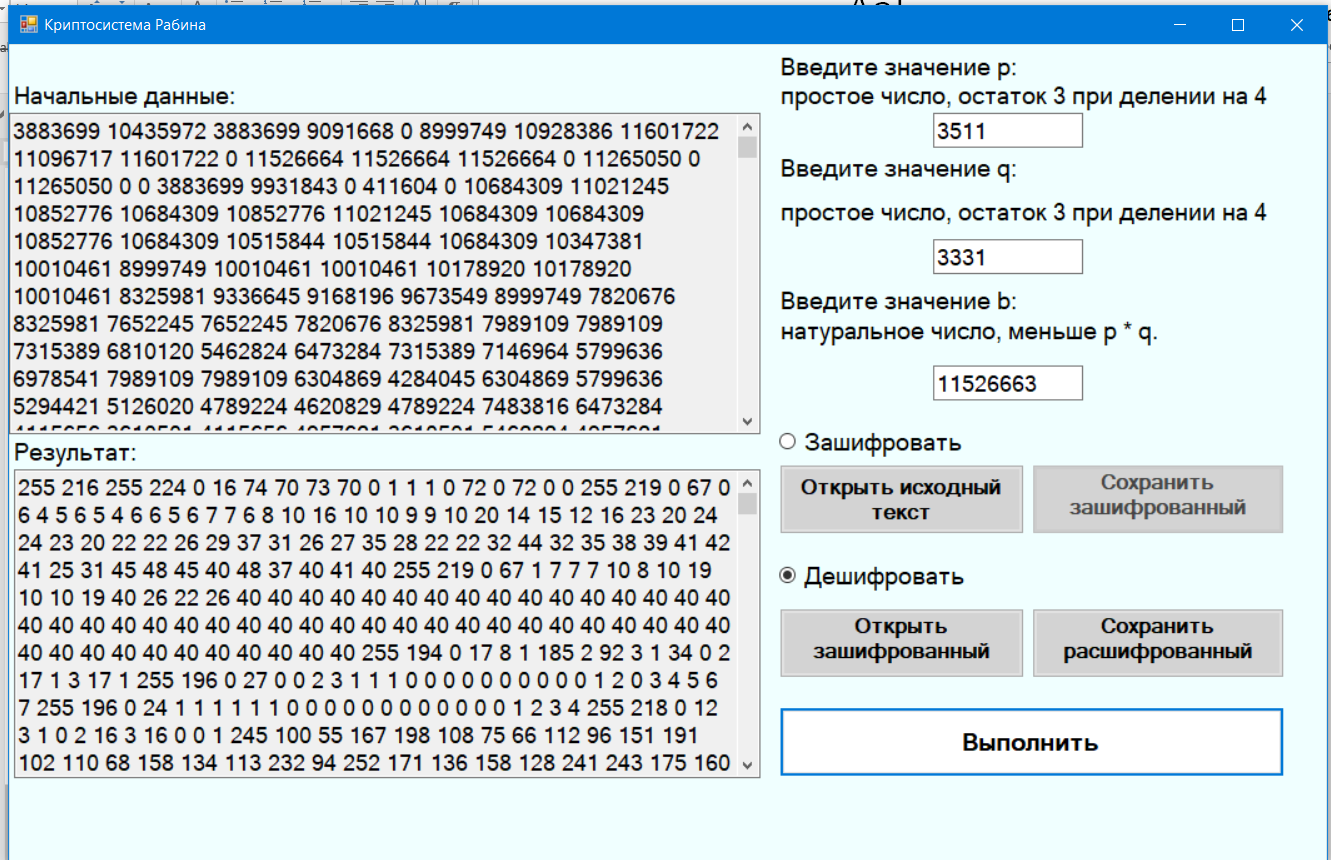
**Результат шифрования:**

****

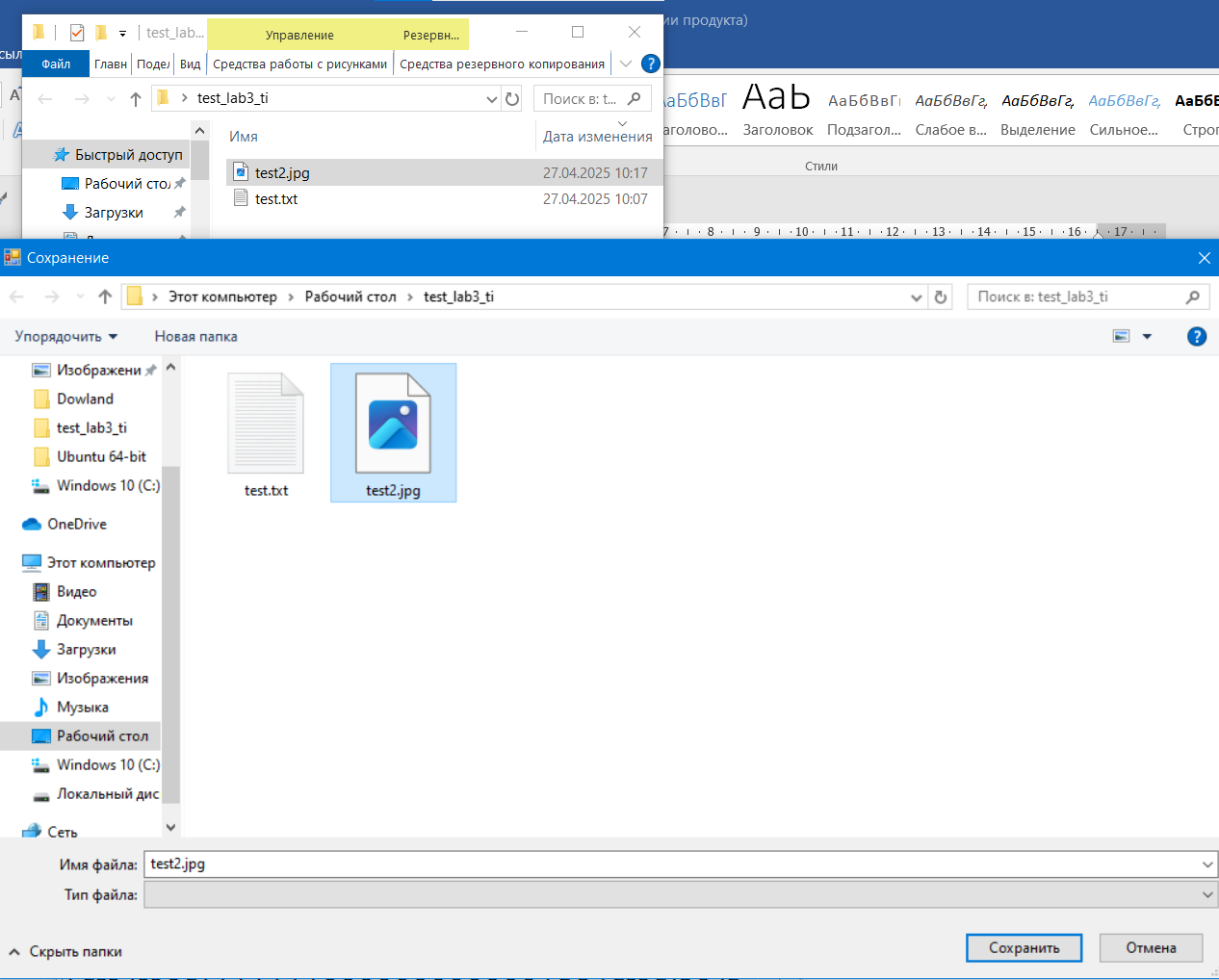
**Содержимое файла после шифрования:**

****

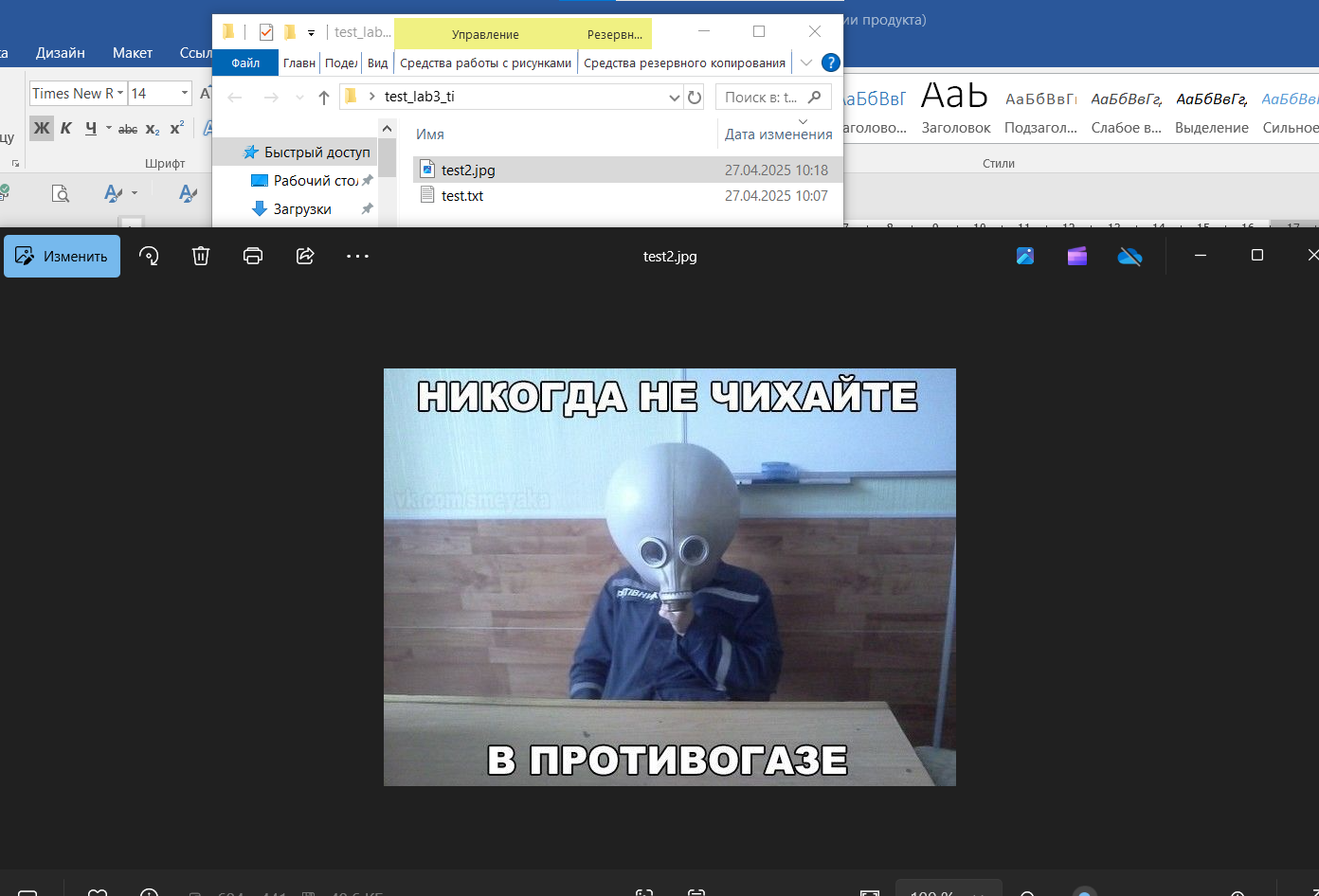
**Дешифрование:**



**Сохранение расшифрованной картинки в файл:**

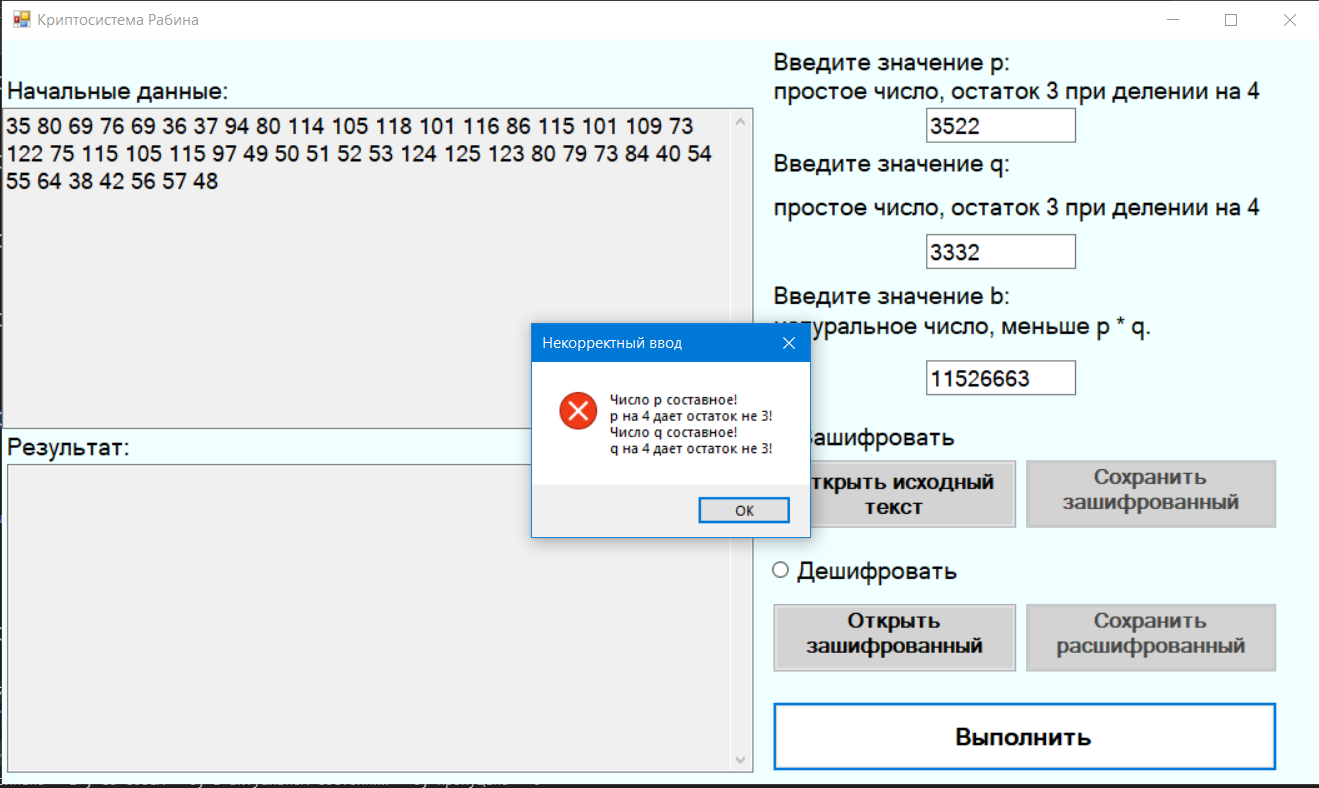


**Результат дешифрования:**

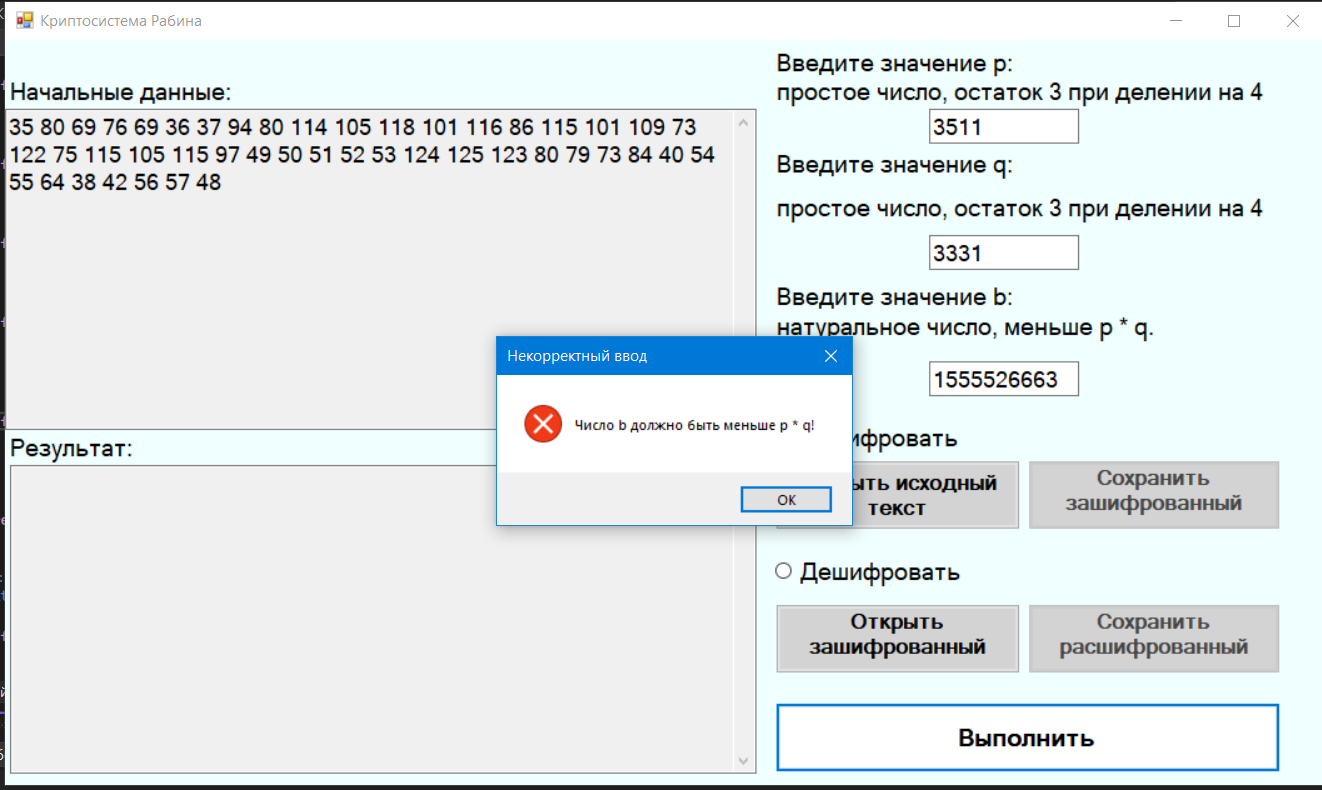
****

**Тестирование ввода некорректных данных**

Если p или q – не простые чилса или при делении на 4 в остатке не 3 – ошибка:



Если b больше чем произведение p\*q - ошибка

****