Отчет к лабораторной работе №3

Вариант 3

Мухин Дмитрий 351004

Алгоритм Рабина

**Пример поиска случайного первообразного корня**

p = 17, p – 1 = 16 = 2 \* 2 \* 2 \* 2

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^12/2 mod 13** | **g^12/3 mod 13** | **Первообразный** |
| 2 | 12 | 3 | + |
| 3 | 1 | 3 | - |
| 4 | 1 | 9 | - |
| 5 | 12 | 1 | - |
| 6 | 12 | 9 | + |
| 7 | 12 | 9 | + |
| 8 | 12 | 1 | + |
| 9 | 1 | 9 | - |
| 10 | 1 | 3 | - |
| 11 | 12 | 3 | + |
| 12 | 1 | 1 | - |

2, 6, 7, 11 – первообразные корни

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

7^13 mod 20 = 7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Шаг | a (основание) | z (степень) | x (результат) | Действия |
| 0 | 7 | 13 | 1 | Стартовые значения |
| 1 | 7 | 13 | 7 | x = (1 \* 7) mod 20 = 7 (z нечётное) |
| 2 | 9 | 6 | 7 | a = (7 \* 7) mod 20 = 9, z = z div 2 = 6 |
| 3 | 1 | 3 | 7 | a = (9 \* 9) mod 20 = 1, z = z div 2 = 3 |
| 4 | 1 | 3 | 7 | x = (7 \* 1) mod 20 = 7 (z нечётное) |
| 5 | 1 | 1 | 7 | a = (1 \* 1) mod 20 = 1, z = z div 2 = 1 |
| 6 | 1 | 1 | 7 | x = (7 \* 1) mod 20 = 7 (z нечётное) |
| 7 | 1 | 0 | 7 | конец (z = 0) |

**Пример работы расширенного алгоритма Евклида**

a = 1239, b = 568

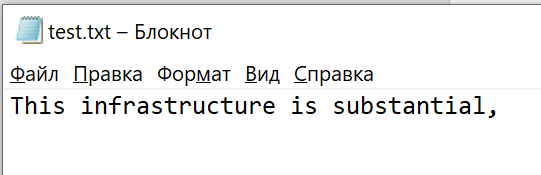
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **a₀** | **a₁** | **x₀** | **x₁** | **y₀** | **y₁** |
| 0 | - | 568 | 1239 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1239 | 568 | 0 | 1 | 1 | 0 |
| 2 | 2 | 568 | 103 | 1 | -2 | 0 | 1 |
| 3 | 5 | 103 | 53 | -2 | 11 | 1 | -5 |
| 4 | 1 | 53 | 50 | 11 | -13 | -5 | 6 |
| 5 | 1 | 50 | 3 | -13 | 24 | 6 | -11 |
| 6 | 16 | 3 | 2 | 24 | -397 | -11 | 182 |
| 7 | 1 | 2 | 1 | -397 | 421 | 182 | -193 |
| 8 | 2 | 1 | 0 | 421 | -1239 | -193 | 568 |

x0 = -193, y0 = 421

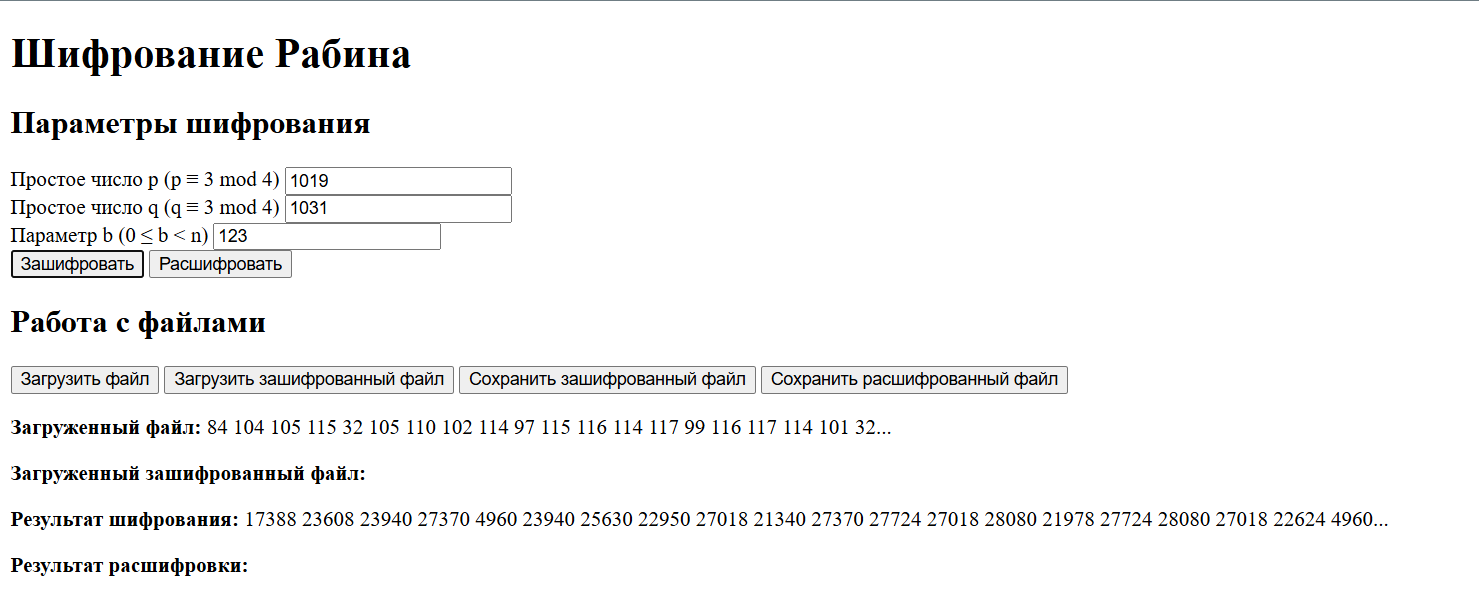
(−193)⋅1239+421⋅568=−239127+239128=1

**Проверка работоспособности программы**

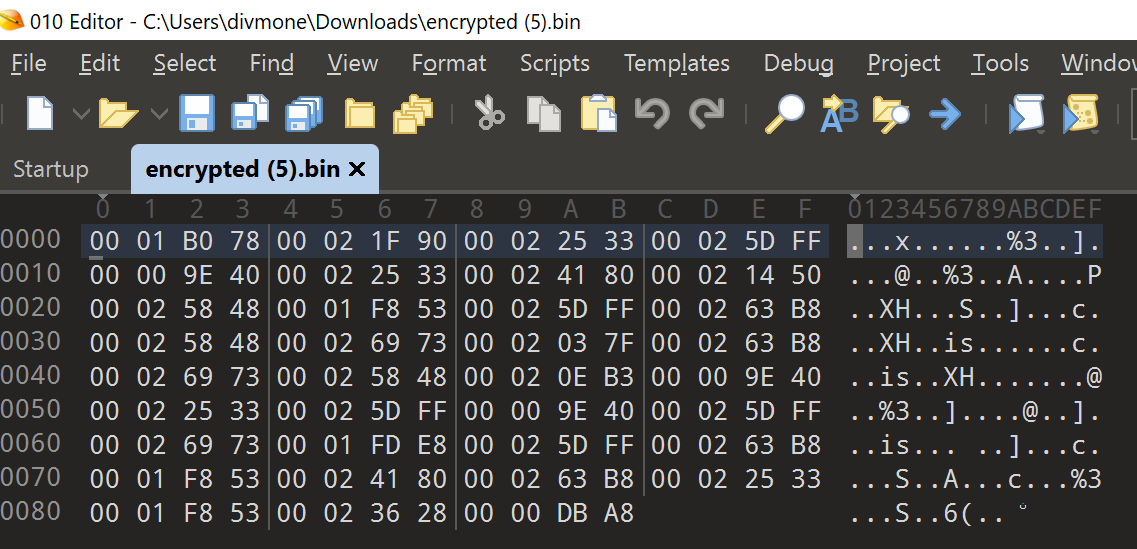
**Исходный текст:**

****

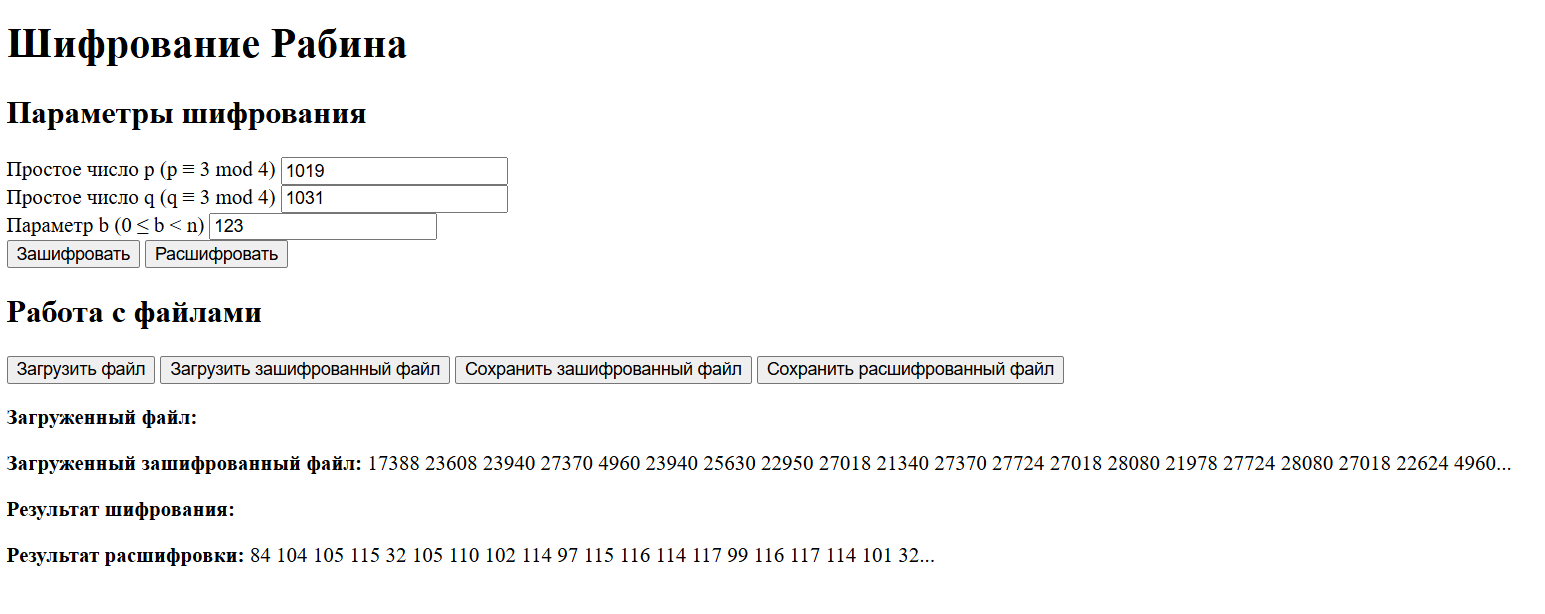
**Окно программы:**

****

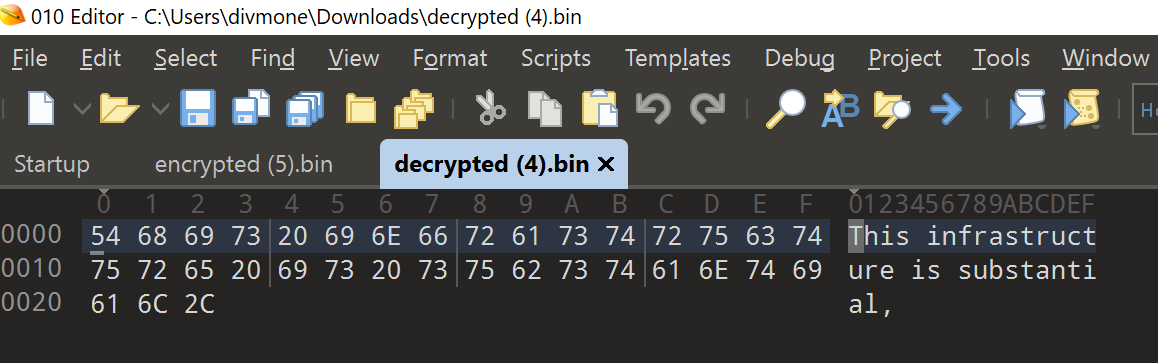
**Результат шифрования:**

****

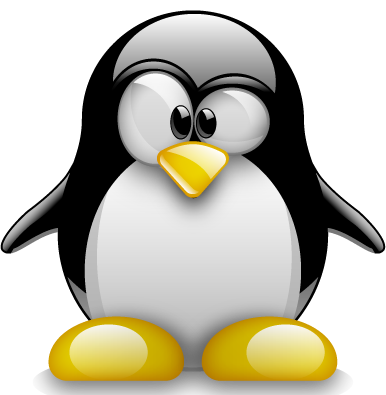
**Дешифрование:**

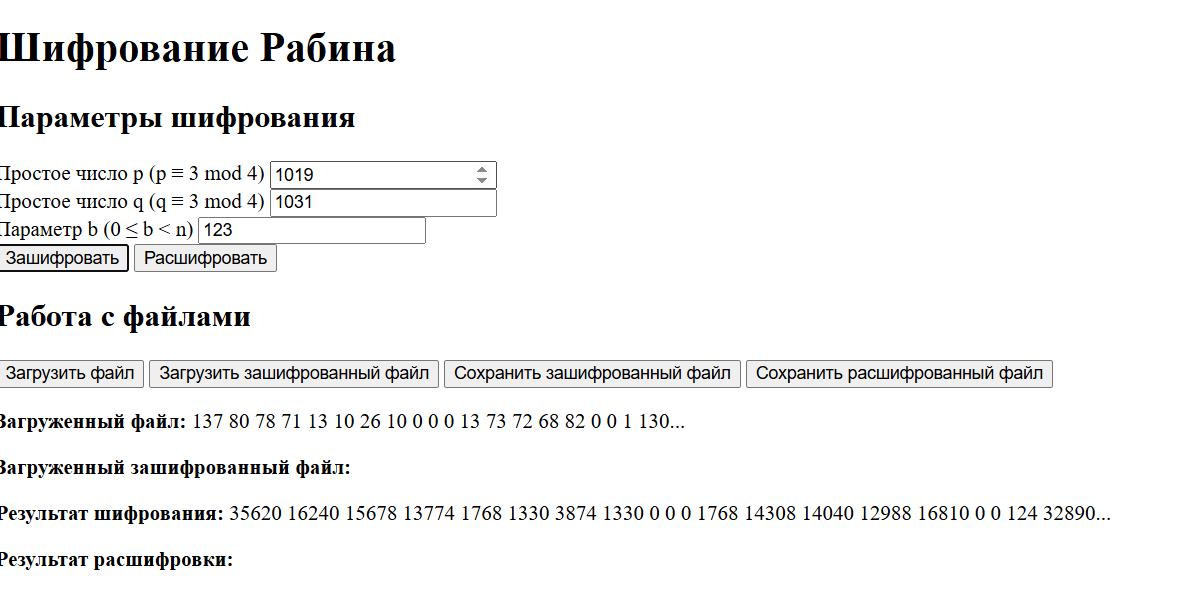
****

**Значение файла после дешифрования:**

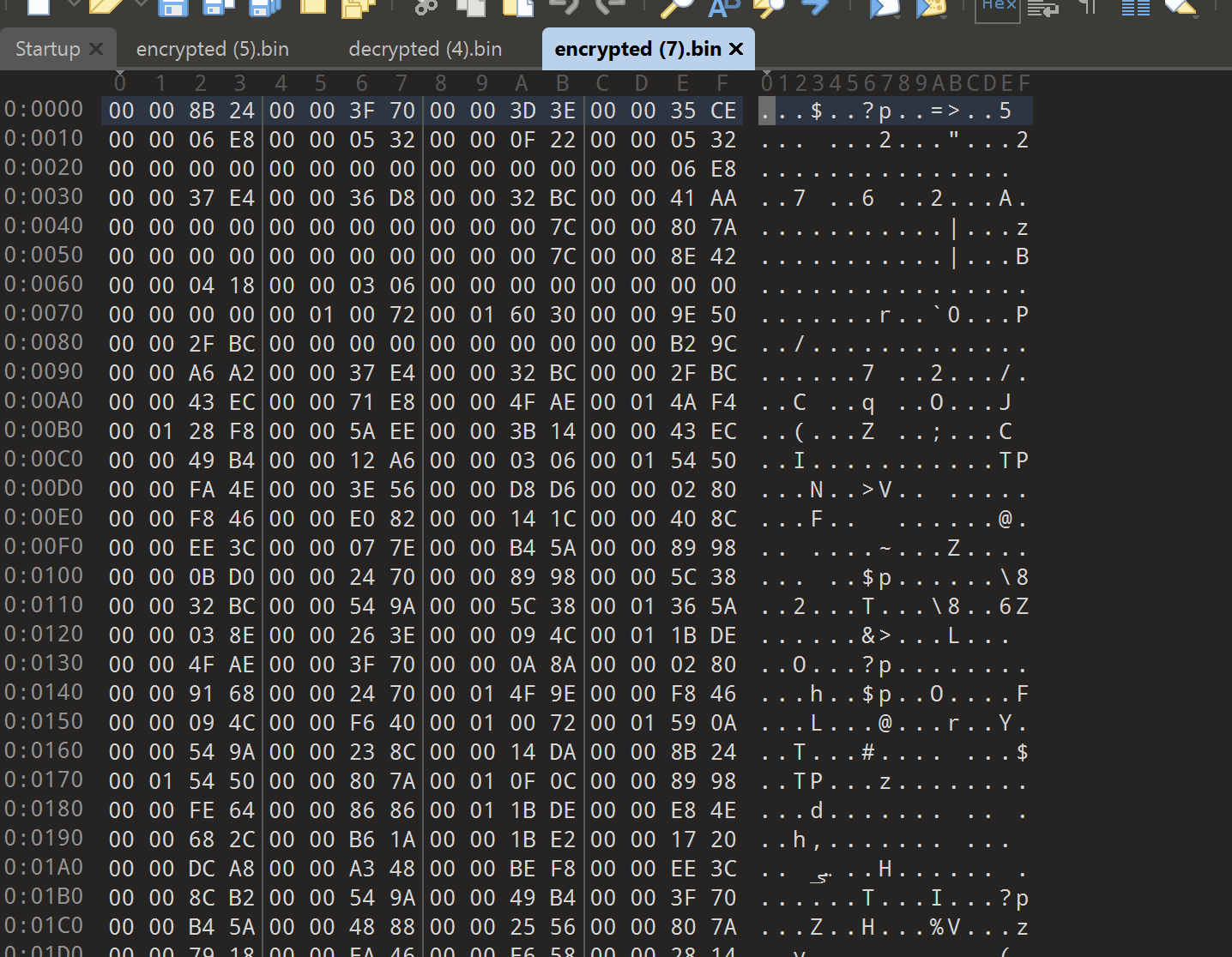
****

Шифрование картинки:

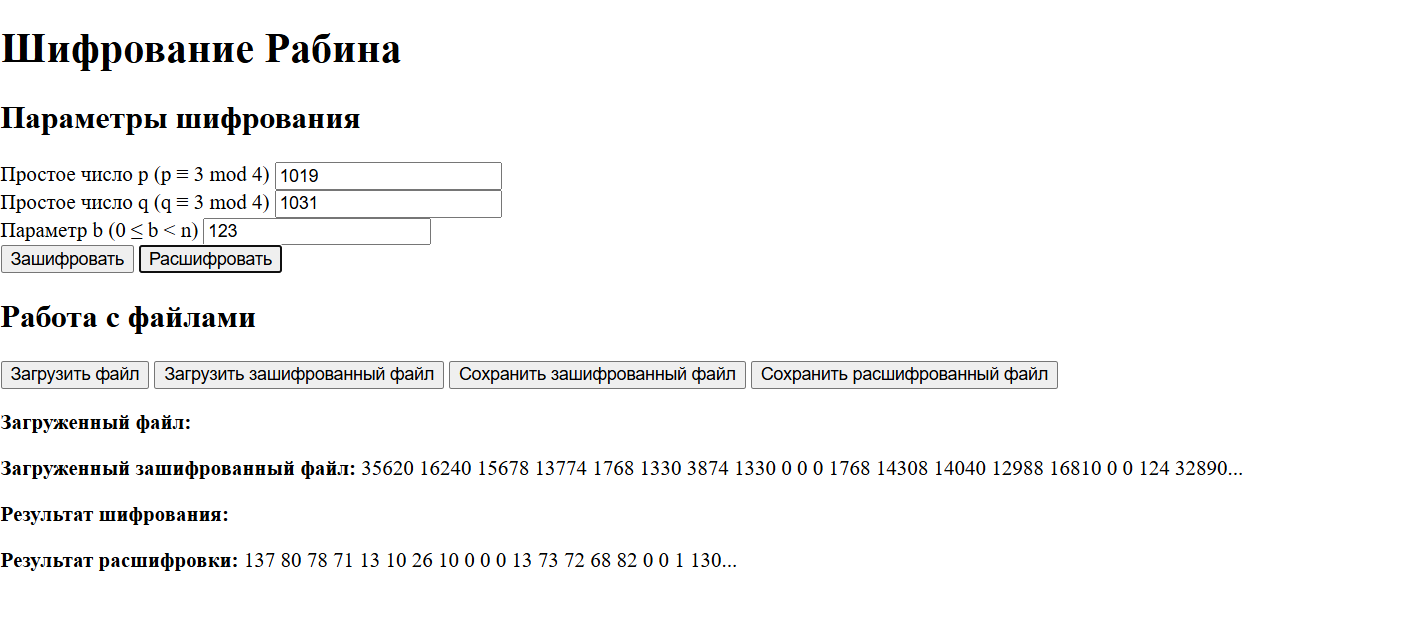


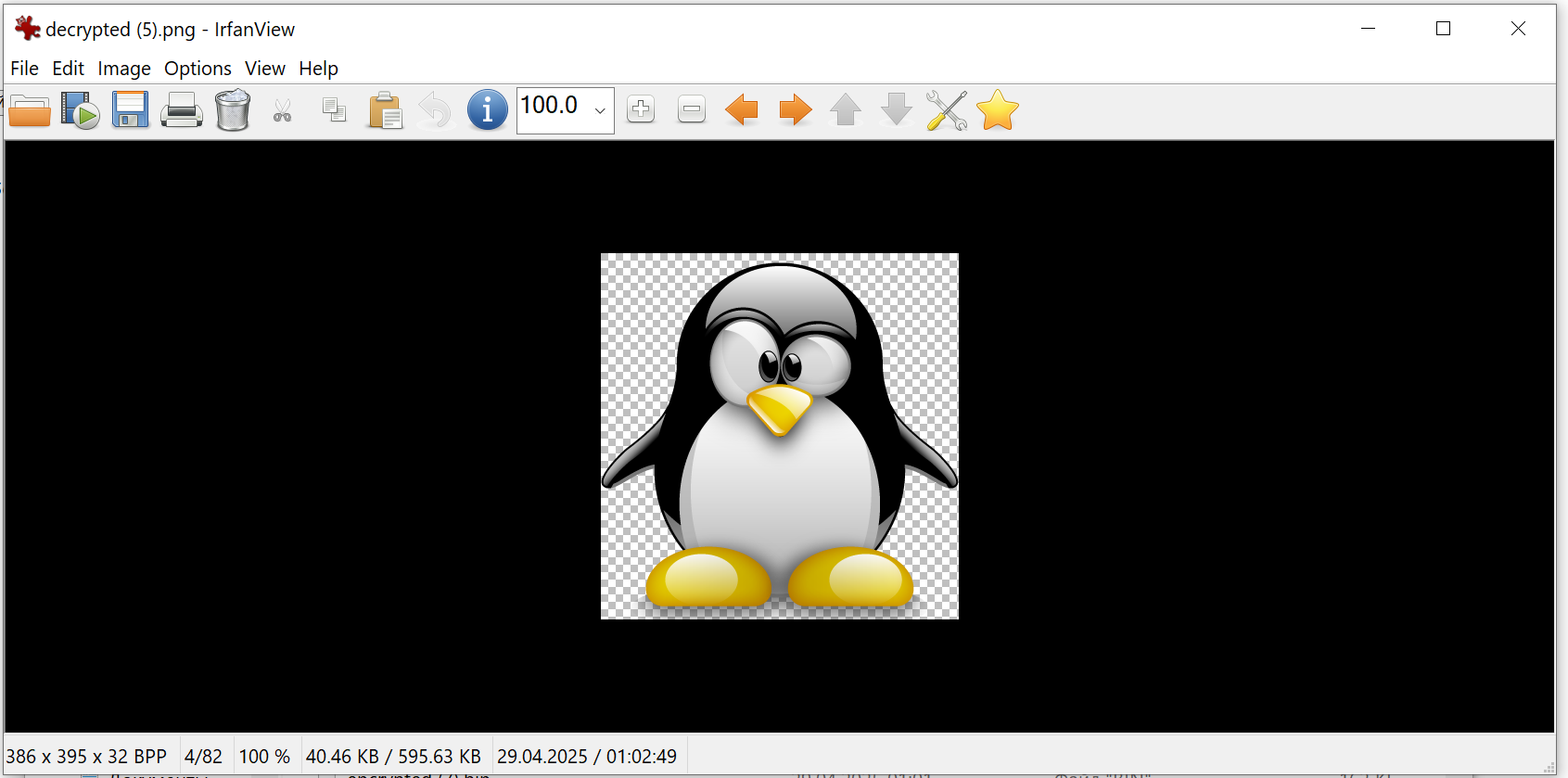
****

Содержимое зашифрованного файла:



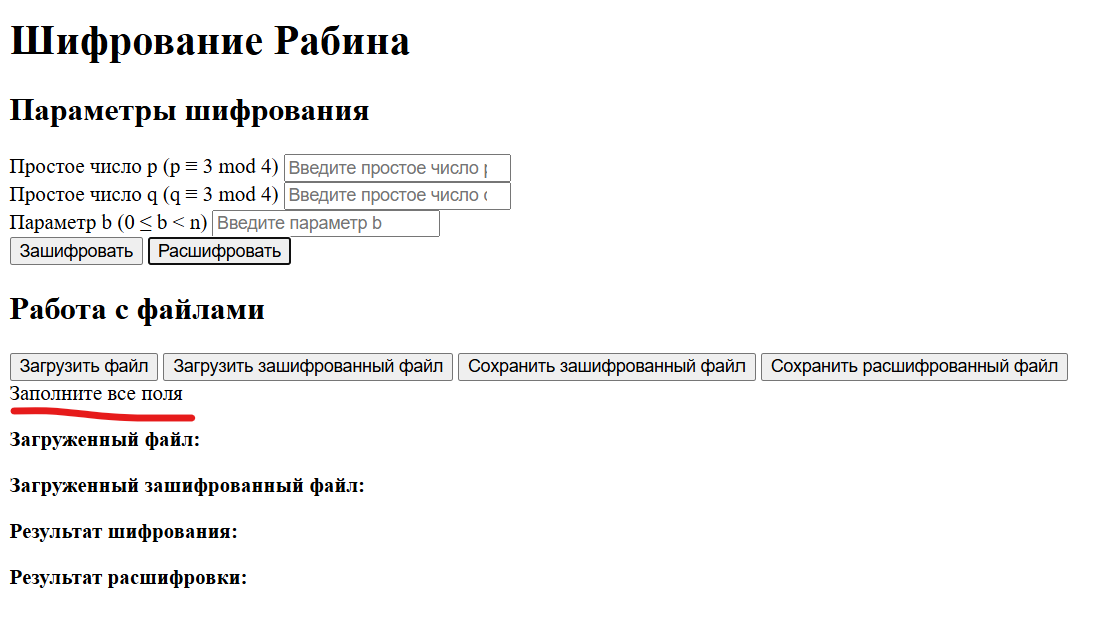
Дешифрование:

 Файл после дешифрования:

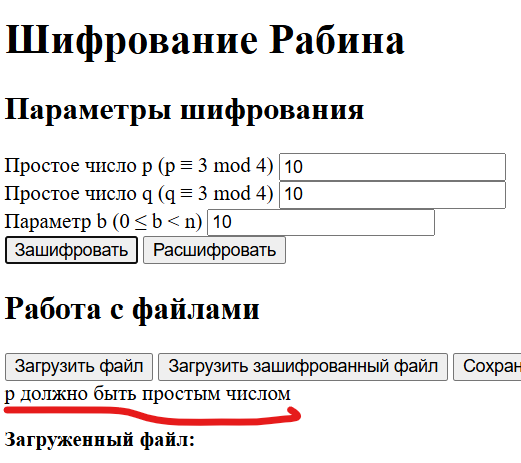


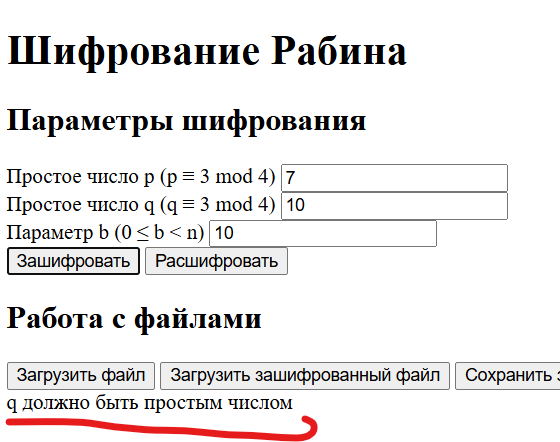
Тесты при некорректных вводных данных:





P или Q не простые





Не загружен файл:

