Отчет к лабораторной работе №3

Студент Владислав

Вариант 2

Алгоритм Эль-Гамаля

1. **Пример работы алгоритма быстрого возведения в степень** (без модульной арифметики, студент должен привести пример с модульной арифметикой)

a1 = 11, z = 17, n = 27

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 11 | 17 | 1 | 0 |
| 11 | 16 | (1 · 11) mod 27 = 11 | 1 нечётное (17) |
| (11 · 11) mod 27 = 13 | 8 | 11 | 2 чётное (16) |
| (13 · 13) mod 27 = 7 | 4 | 11 | 3 чётное (8) |
| (7 · 7) mod 27 = 22 | 2 | 11 | 4 чётное (4) |
| (22 · 22) mod 27 = 25 | 1 | 11 | 5 чётное (2) |
| 25 | 0 | (11 · 25) mod 27 = 5 | 6 нечётное (1) |

1117 mod 27 = 5

1. **Пример поиска случайного первообразного корня** (студент должен привести пример поиска всех первообразных корней по заданному модулю)
2. p=23, p – 1 = 22 = 2\*11

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

3, 5, 6, 7, 9, 11, 13, 14, 17, 18, 21– первообразные корни

**3.Пример работы расширенного алгоритма Евклида** (числа не взаимно простые, студент должен привести пример с взаимно простыми числами)

**a = 70 b = 43**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 70 | 43 | 1 | 0 | 0 | 1 |
| 1 | 4 | 43 | 27 | 0 | 1 | 1 | -1 |
| 2 | 1 | 27 | 16 | 1 | -1 | -1 | 2 |
| 3 | 1 | 16 | 11 | -1 | 2 | 2 | -3 |
| 4 | 1 | 11 | 5 | 2 | -3 | -3 | 5 |
| 5 | 2 | 5 | 1 | -3 | 8 | 5 | -13 |
| 6 | 5 | 1 | 0 | 8 | -43 | -13 | 70 |

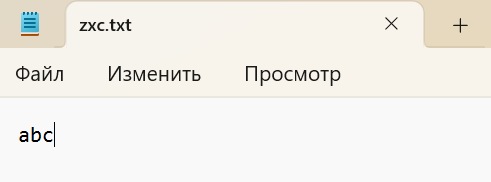
**x1 = 8 y1 = -13**

**70⋅8+43⋅(−13)=560−559=1**

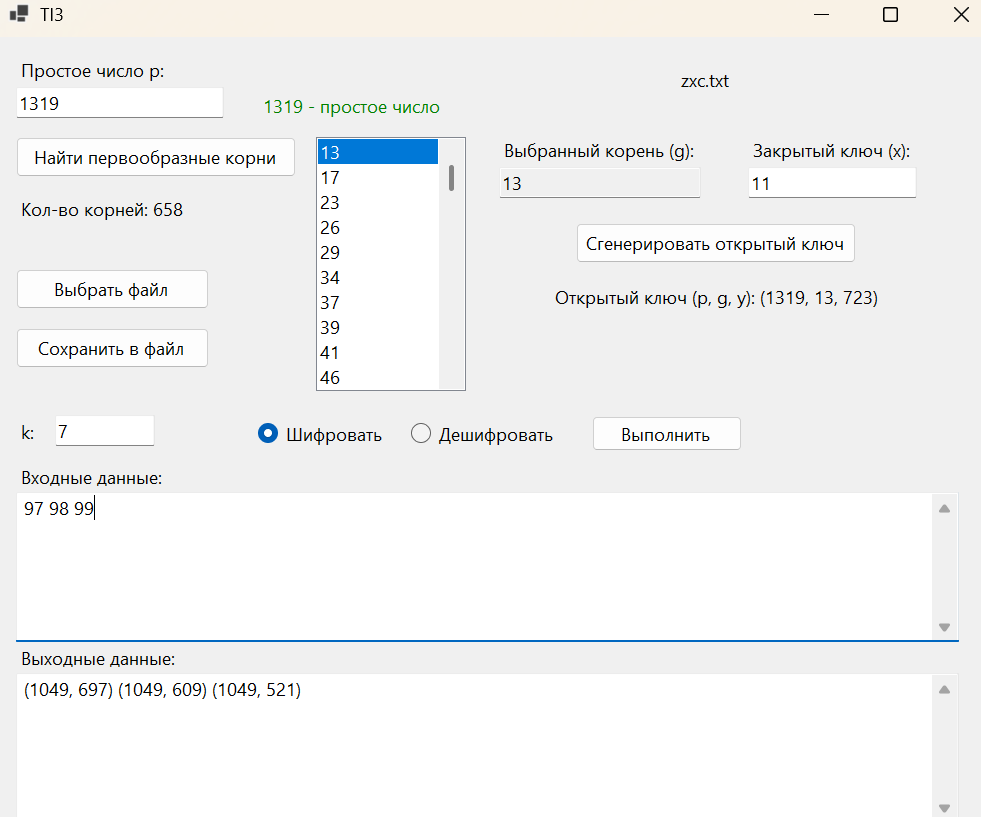
**ТЕСТЫ**

* + - 1. **Текстовый файл**

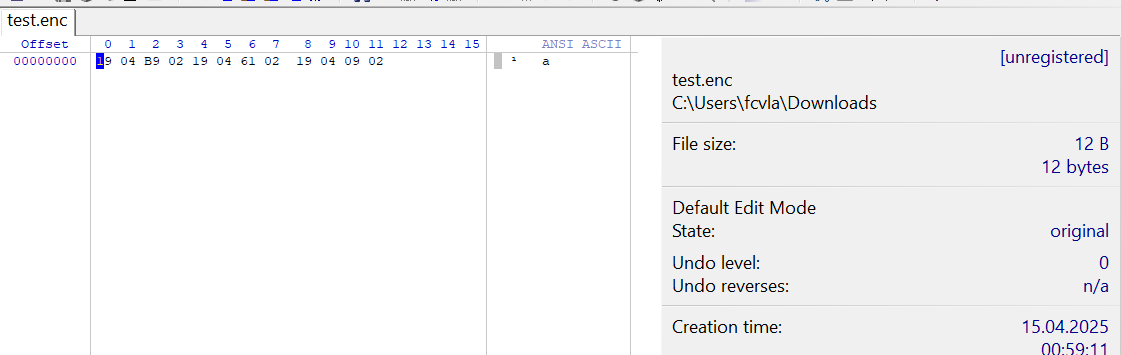
Содержимое файла:



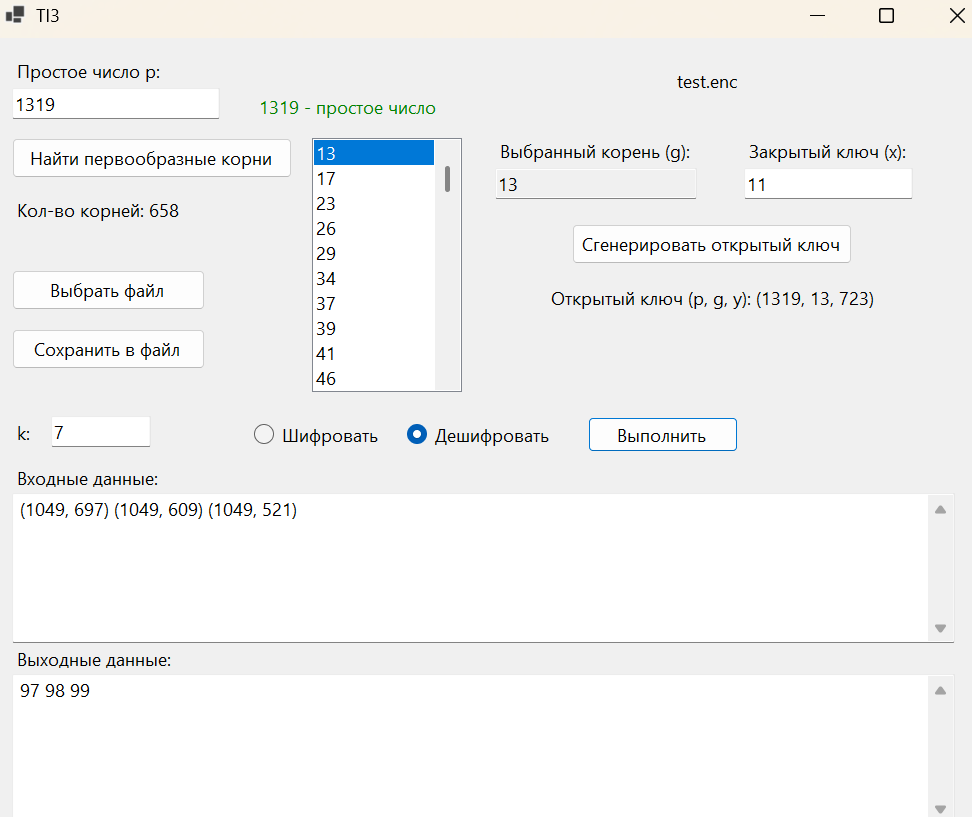
Результат шифрования файла:



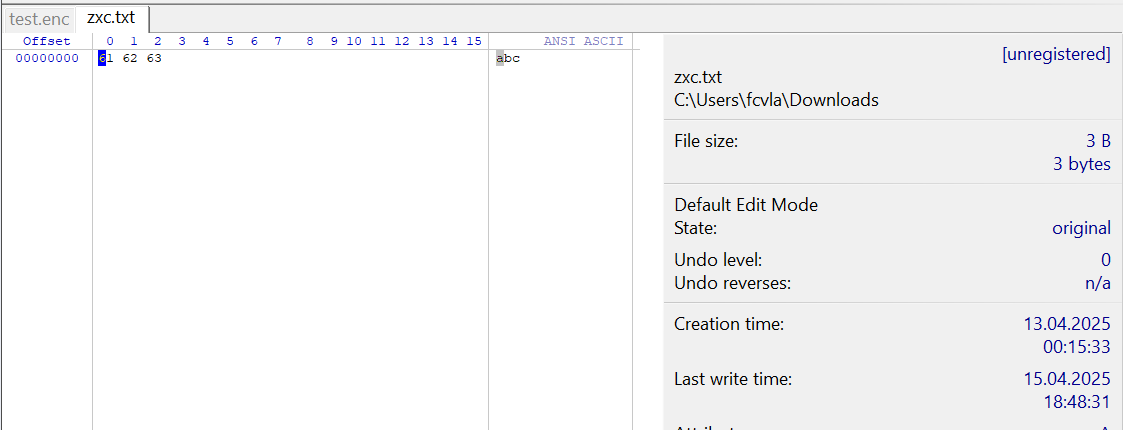
Содержимое сохраненного зашифрованного файла:



Результат дешифрования зашифрованного файла:

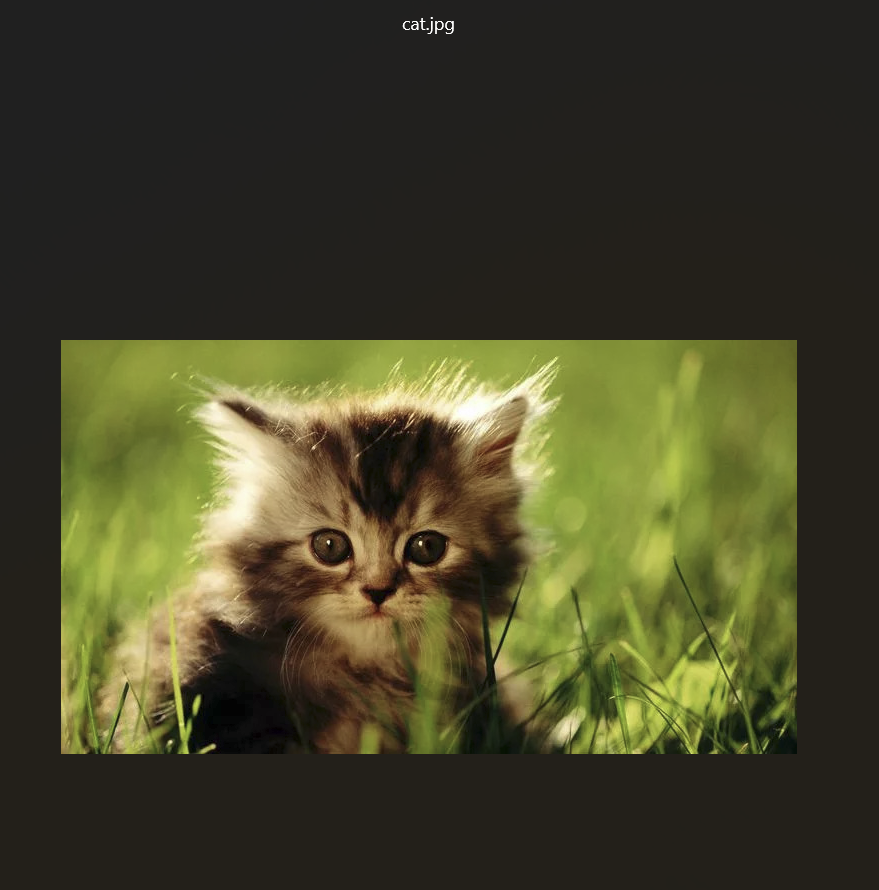


Содержимое сохраненного дешифрированного файла:

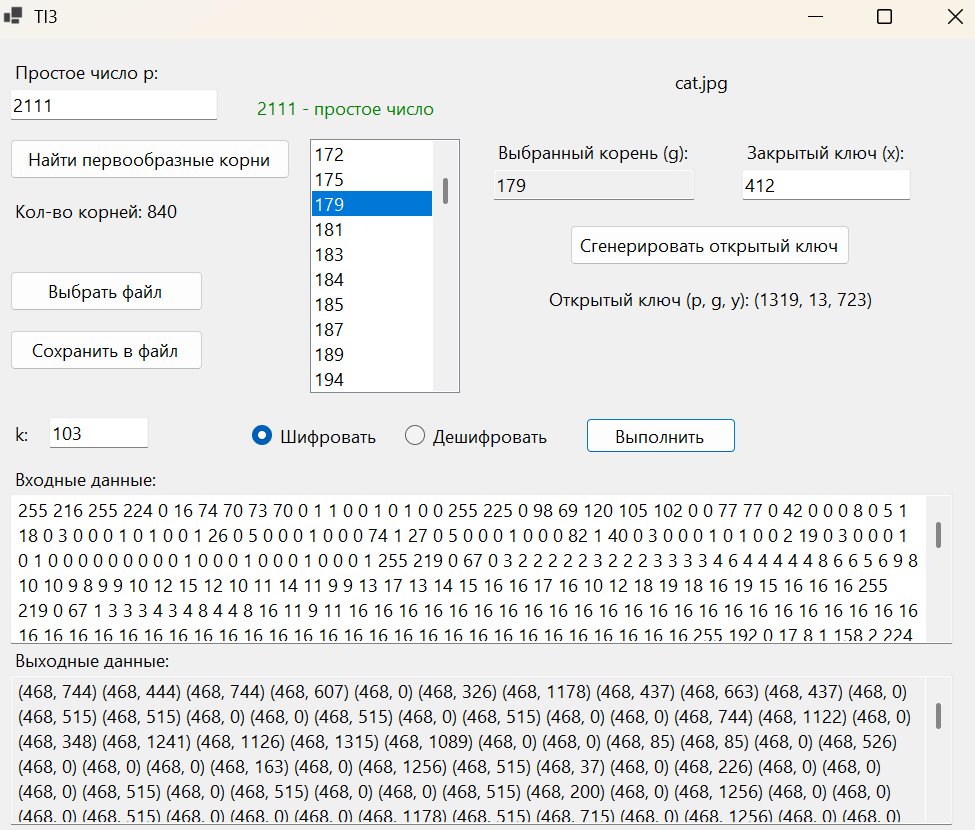


* + - 1. **Изображение**

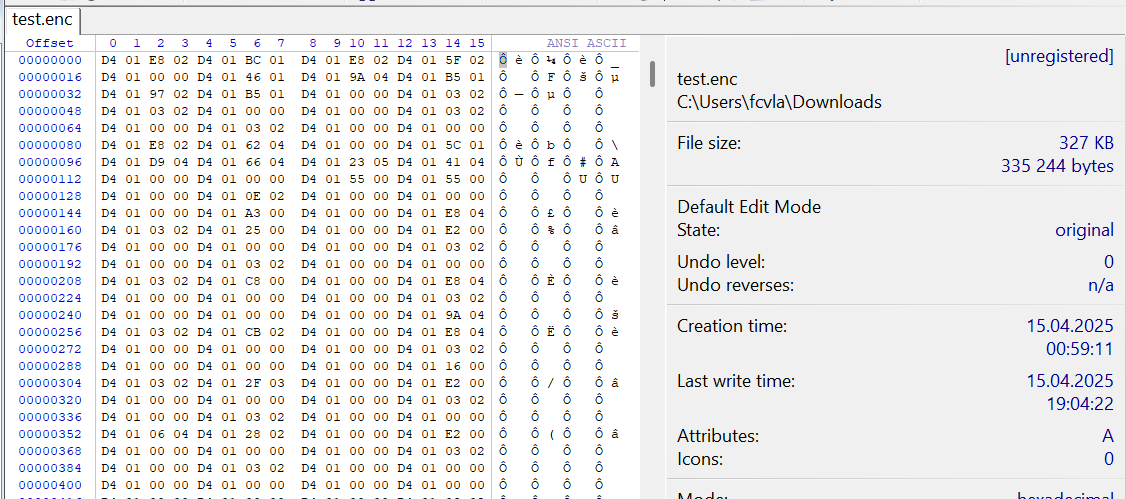
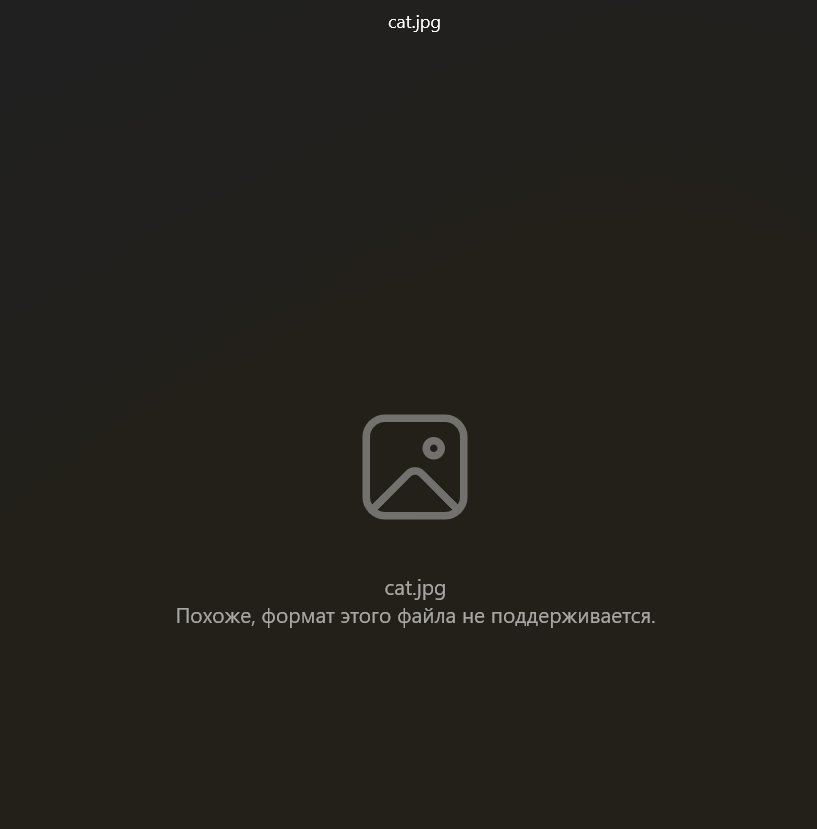
Изображение:

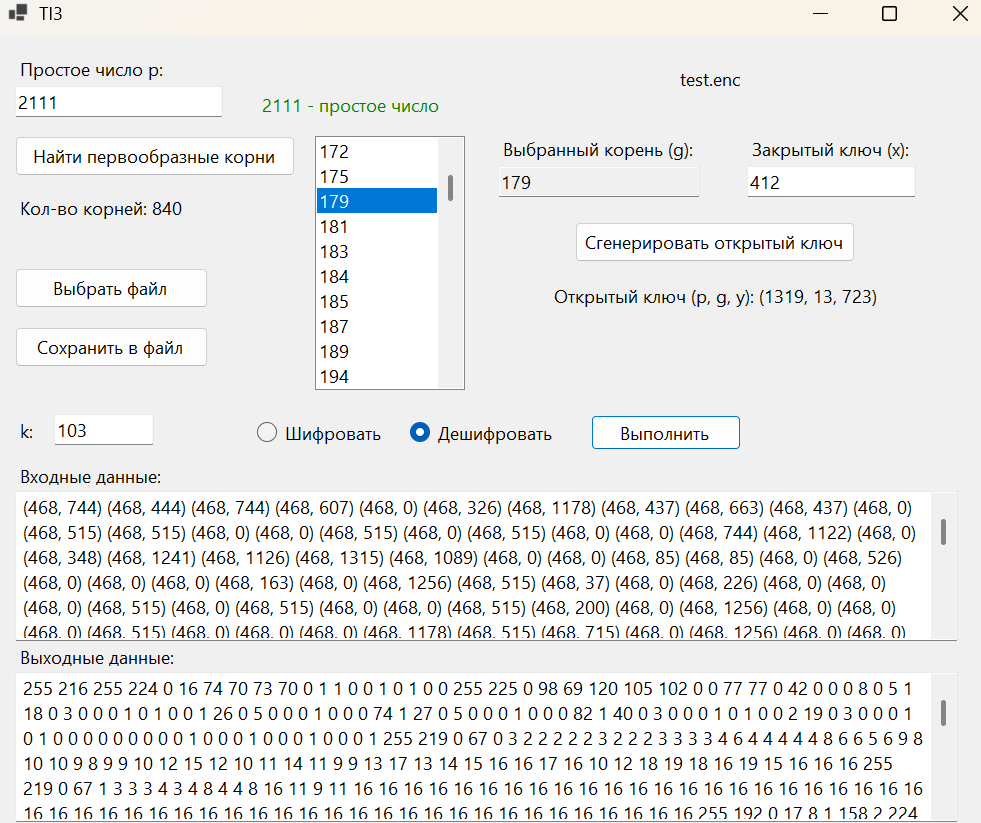


Результат шифрования изображения:



Содержимое сохраненного зашифрованного файла:

Результат дешифрования зашифрованнаого изображения:  
  
Содержимое дешифрованного файла:  
