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)

**y = 210 mod 131 = 45 mod 131 = 4\*44 mod 131 = 4 \* 162 mod 131 = 4 \* 2561 mod 131 = 1024 mod 131 = 107**

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 2 | 10 | 1 | 0 |
| 4 | 5 | 1 | 1 |
| 4 | 4 | 1\*4 mod 131 = 4 | 2 |
| 16 | 2 | 4 | 3 |
| 256 | 1 | 4\*256 mod 131 = 107 | 4 |
|  | 0 | Результат: 107 | 5 |

210 mod 131 = 107

1. **Пример поиска случайного первообразного корня** (студент должен привести пример поиска всех первообразных корней по заданному модулю)

Задано простое p = 11

Ищем простые делители p-1 = 10 = 2\*5

Проверяем является ли число 2 первообразным корнем по модулю 11:

210/2 mod 11 = 10; 210/5 mod 11 = 4. Число 2 является первообразным по модулю 11.

Проверяем является ли число 3 первообразным корнем по модулю 11:

310/2 mod 11 = 1; 310/5 mod 11 = 9. Число 3 не является первообразным по модулю 11.

Если найден один первообразный корень g по модулю p, остальные корни имеют вид g^k, где НОД(k, p-1) = 1. Для p = 11, допустимые k: 1, 3, 7, 9:

1. 2^1 mod 11 = 2
2. 2^3 mod 11 = 8
3. 2^7 mod 11 = 7
4. 2^9 mod 11 = 6

Тогда все первообразные корни для модуля p = 11: 2,6,7,8.

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 143 | 89 | 1 | 0 | 0 | 1 |
| 1 | 3 | 89 | 54 | 0 | 1 | 1 | -1 |
| 2 | 1 | 54 | 35 | 1 | -1 | -1 | 2 |
| 3 | 2 | 35 | 19 | -1 | 2 | 2 | -3 |
| 4 | 1 | 19 | 16 | 2 | -3 | -3 | 5 |
| 5 | 2 | 16 | 3 | -3 | 5 | 5 | -8 |
| 6 | 5 | 3 | 1 | 5 | -28 | -8 | 45 |
| 7 | 3 | 1 | 0 | -28 | 89 | 45 | -143 |

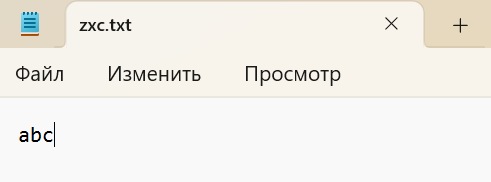
**x1 = -89 y1 = -143**

**89 \* 143 + (-143) \* 89 = 1**

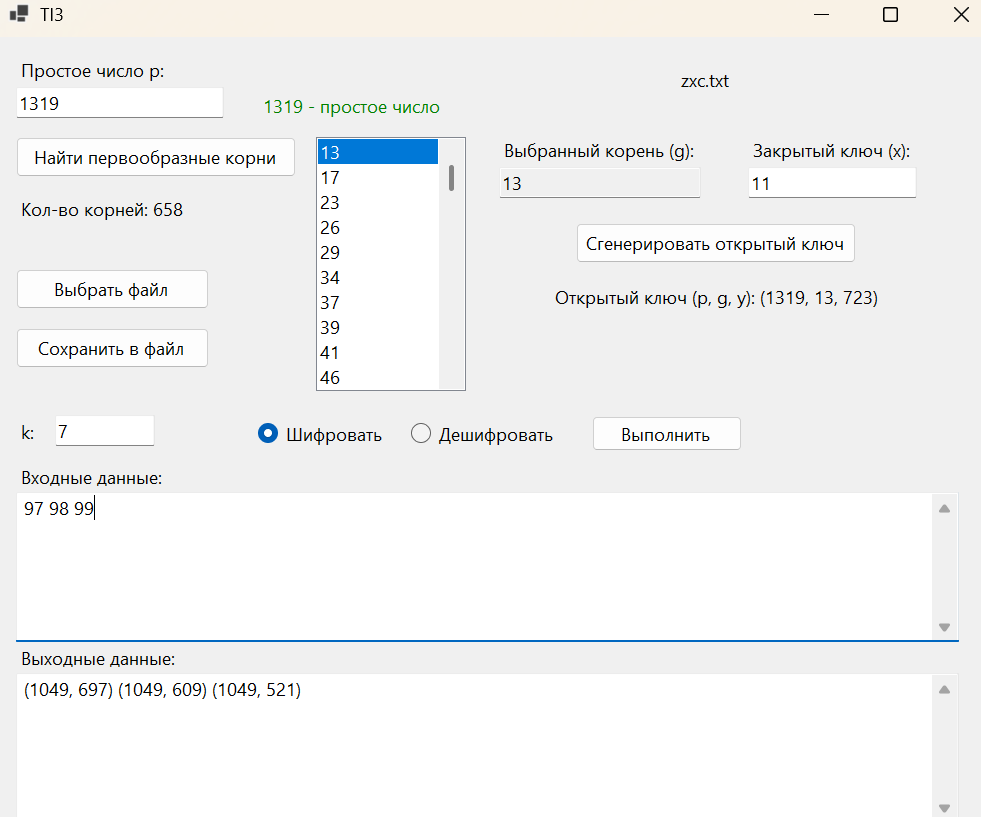
**ТЕСТЫ**

* + - 1. **Текстовый файл**

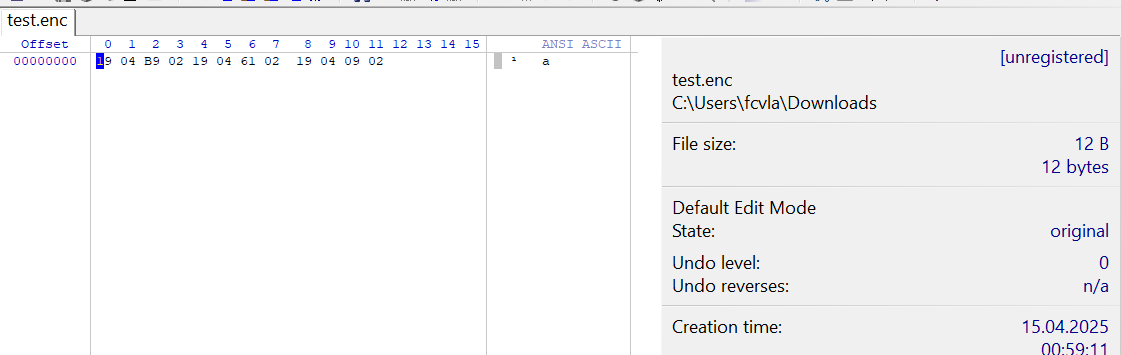
Содержимое файла:



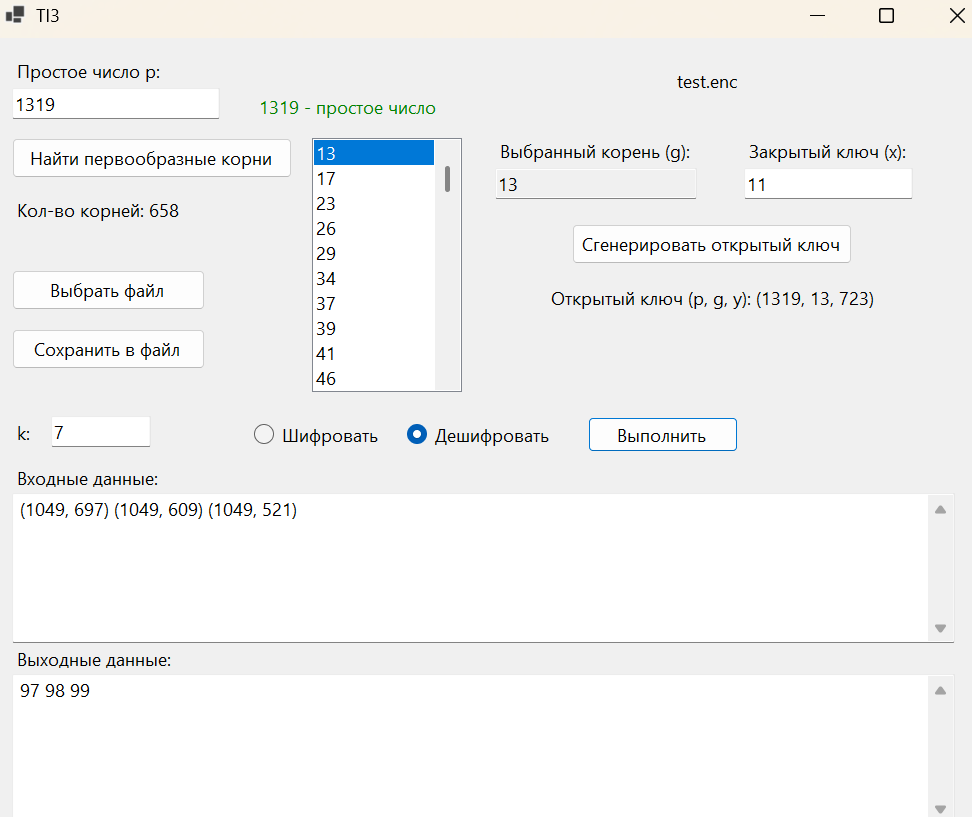
Результат шифрования файла:



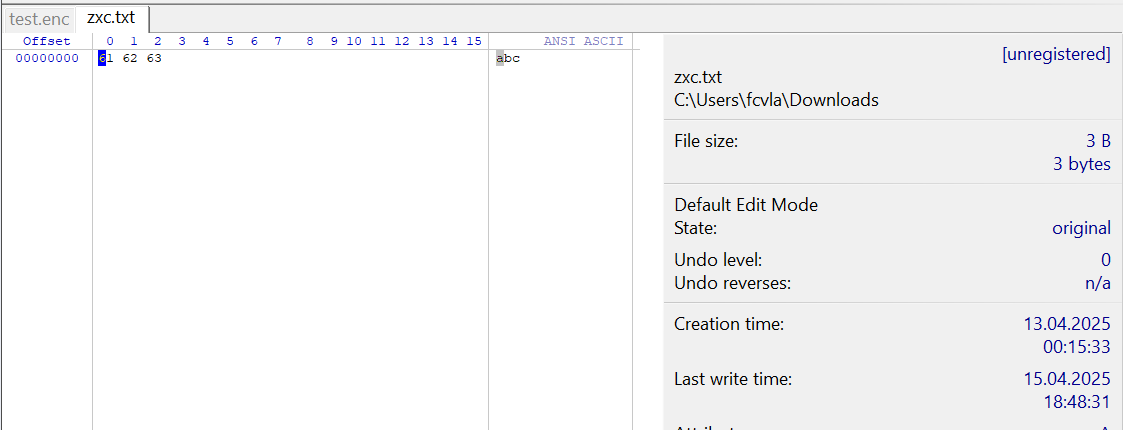
Содержимое сохраненного зашифрованного файла:



Результат дешифрования зашифрованного файла:

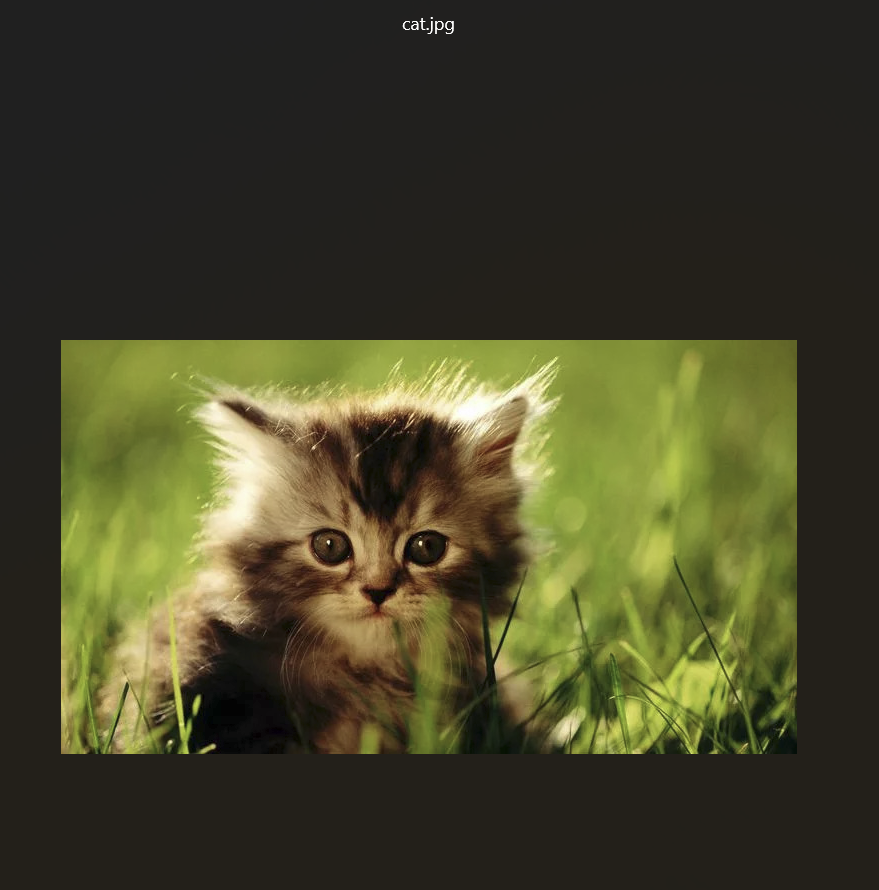


Содержимое сохраненного дешифрированного файла:

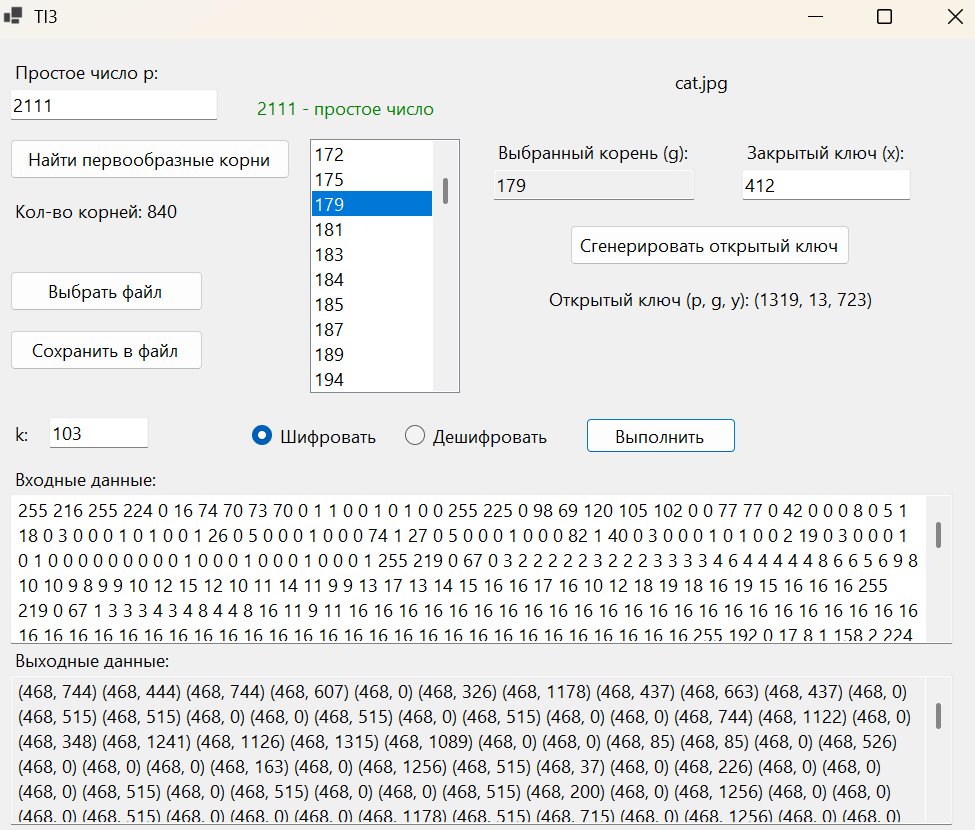


* + - 1. **Изображение**

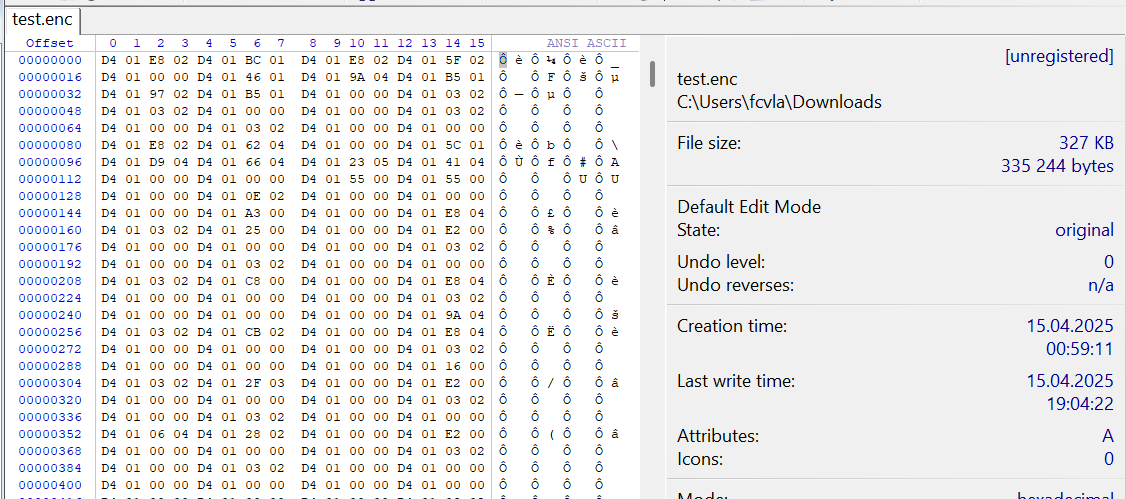
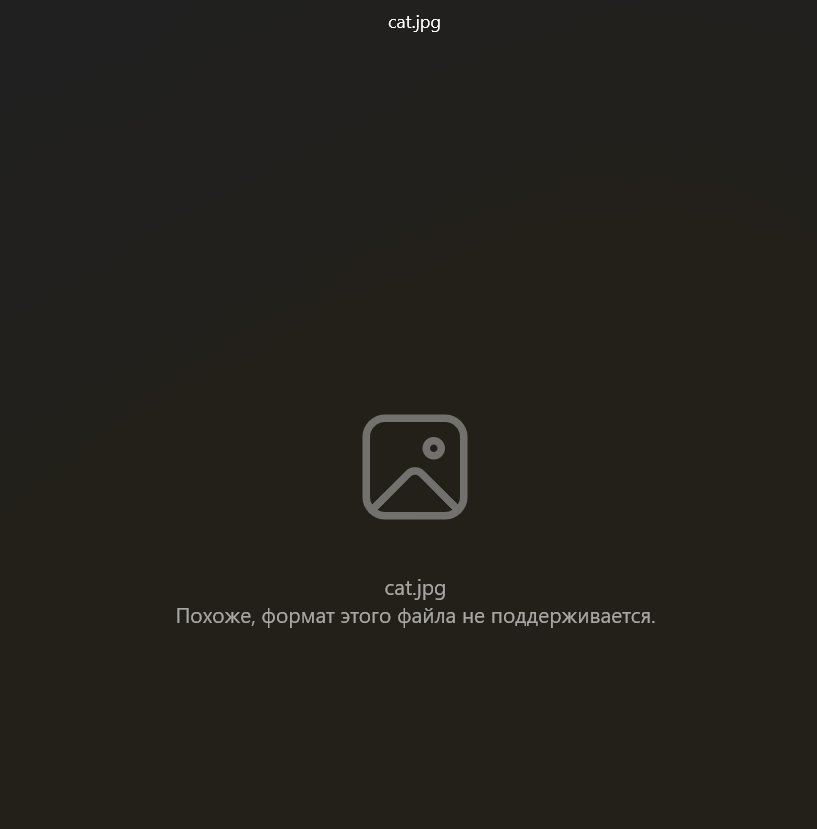
Изображение:

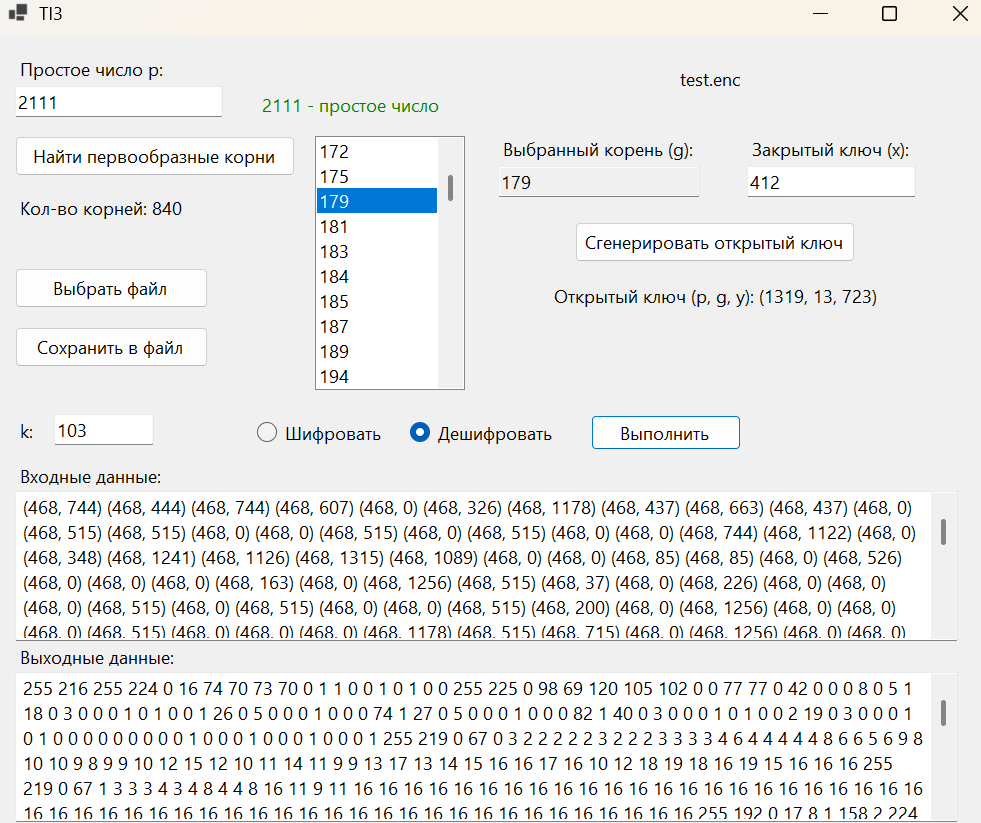


Результат шифрования изображения:



Содержимое сохраненного зашифрованного файла:

Результат дешифрования зашифрованнаого изображения:  
  
Содержимое дешифрованного файла:  
