**Власовец А. И. ТИ 3 Лабораторная работа 1 вариант  
1. Пример работы алгоритма быстрого возведения в степень**

a1 = 7, z = 17 (10001), n = 41

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | z(степень) | х(результат) | Шаги выполнения |
| 7 | 17 | 1 | 0 |
| 7 | 16 | (1 \* 7) mod 41 = 7 | 1 |
| (7 \* 7) mod 41 = 8 | 8 | 7 (16 – четное) | 2 |
| (8 \* 8) mod 41 = 23 | 4 | 7 (8 – четное) | 3 |
| (23 \* 23) mod 41 = 25 | 2 | 7 (4 – четное) | 4 |
| (25 \* 25) mod 41 = 10 | 1 | 7 (2 – четное) | 5 |
| 10 | 0 | (7 \* 10) mod 41 = 29 | 6 |

7^17 mod 41 = 29

**2.** **Пример поиска случайного первообразного корня**

p = 17, p – 1 = 16 = 2 \* 2 \* 2 \* 2

|  |  |  |
| --- | --- | --- |
| g | g^16/2 mod 17 | Первообразный |
| 2 | 16 | + |
| 3 | 16 | + |
| 4 | 1 | - |
| 5 | 16 | + |
| 6 | 16 | + |
| 7 | 16 | + |
| 8 | 1 | - |
| 9 | 1 | - |
| 10 | 16 | + |
| 11 | 16 | - |
| 12 | 1 | - |
| 13 | 16 | + |
| 14 | 16 | + |
| 15 | 1 | - |
| 16 | 1 | - |

2, 3, 5, 6, 7 10, 13, 14 – первообразные корни

**3.** **Пример работы расширенного алгоритма Евклида**

a = 17, b = 43

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **d0** | **d1** | **x0** | **x1** | **y0** | **y1** |
| 0 | – | 17 | 43 | 1 | 0 | 0 | 1 |
| 1 | 0 | 43 | 17 | 0 | 1 | 1 | 0 |
| 2 | 2 | 17 | 9 | 1 | -2 | 0 | 1 |
| 3 | 1 | 9 | 8 | -2 | 3 | 1 | -1 |
| 4 | 1 | 8 | 1 | 3 | -5 | -1 | 2 |

x = −5, y = 2

17 \* (−5) + 43 \* 2=−85 + 86 = 1

**Проверка работоспособности программы**

**Тест 1**

Тестовая ситуация:

Шифрование и дешифрование текстового файла.

Исходные данные:

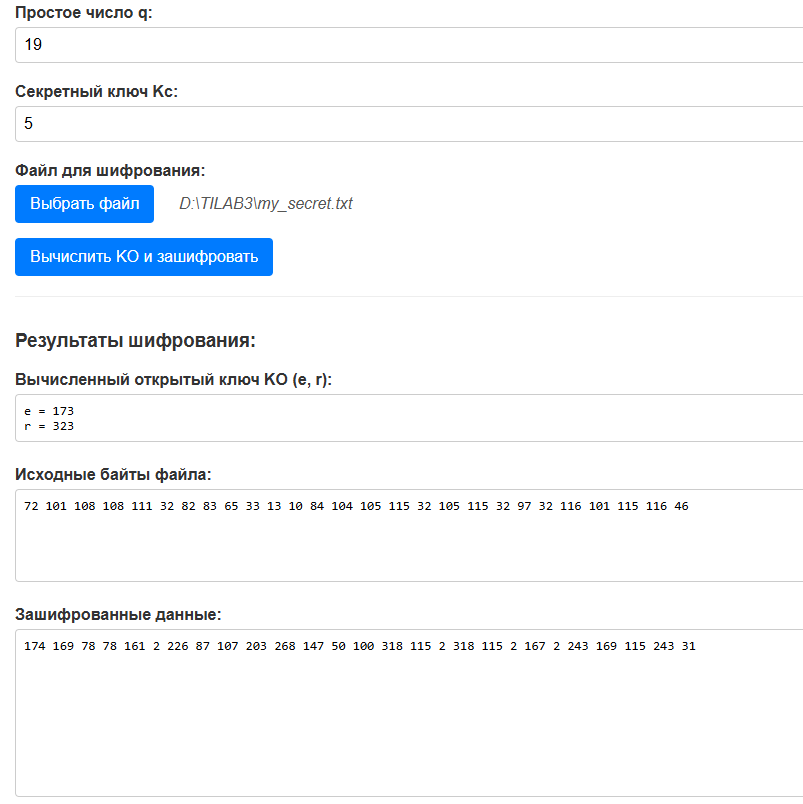
p: 17;

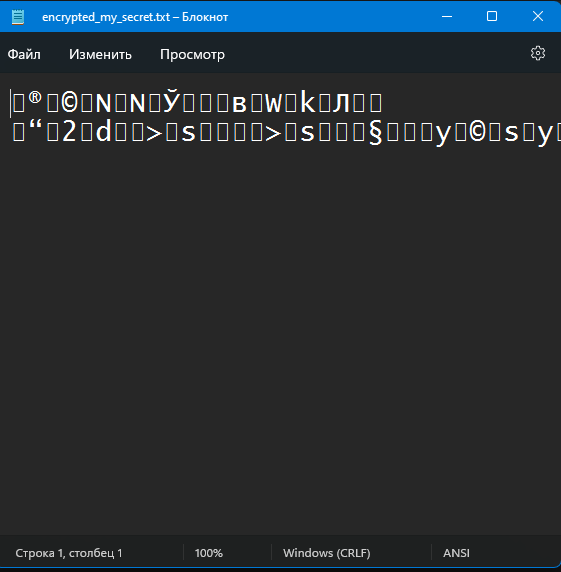
q: 19;

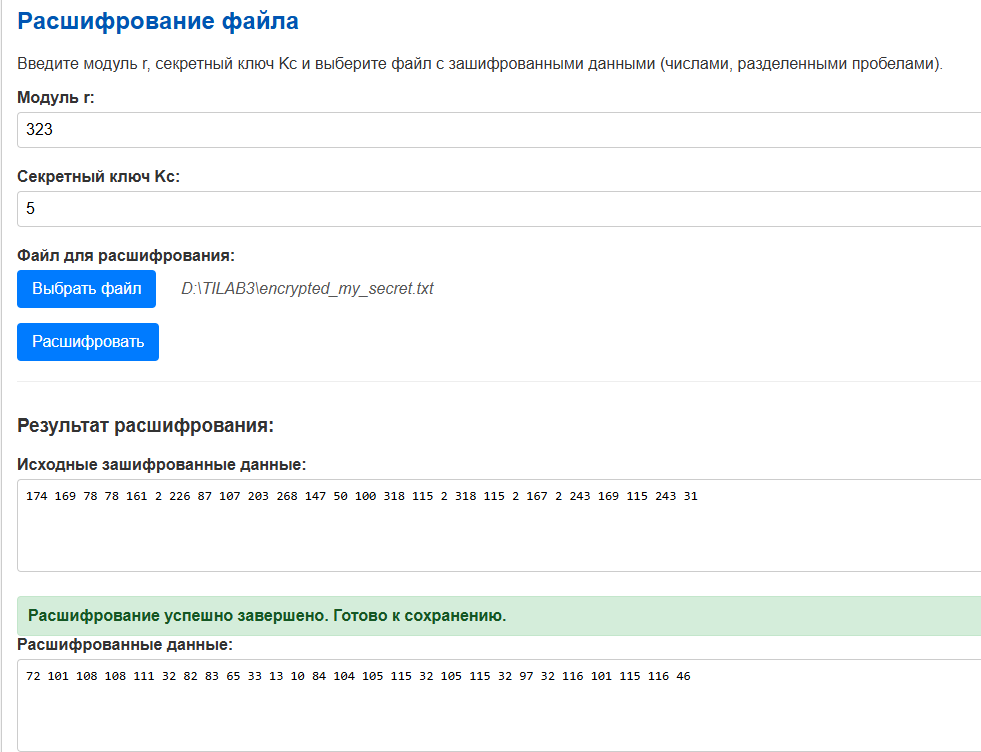
Kc: 5;

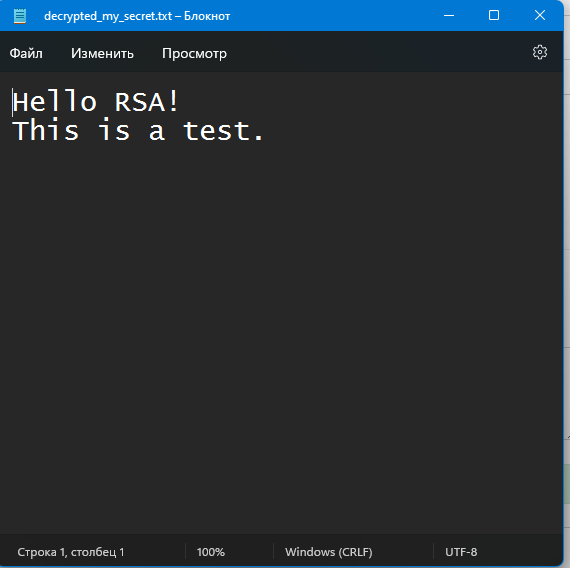
my\_secret.txt (исходный файл):  
Hello RSA!

This is a test.

Полученный результат шифрования:  


encrypted\_my\_secret.txt:  


Полученный результат дешифрования:  


decrypted\_my\_secret.txt:  


**Тест 1**

Тестовая ситуация:

Шифрование и дешифрование изображения.

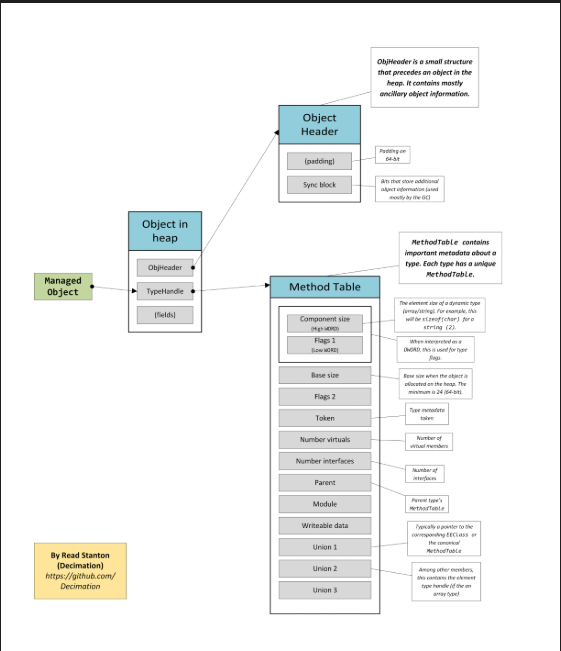
Исходные данные:

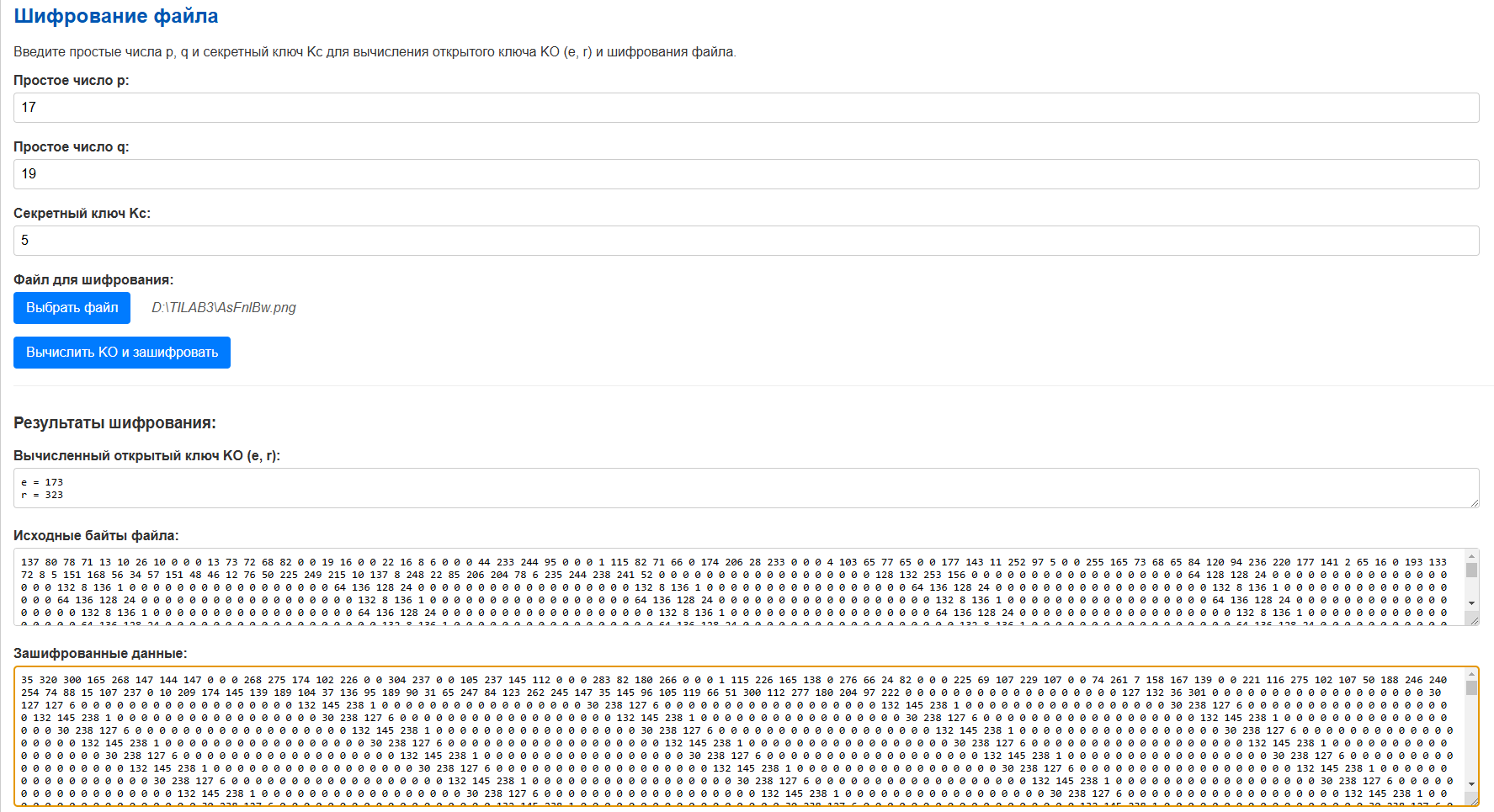
p: 17;

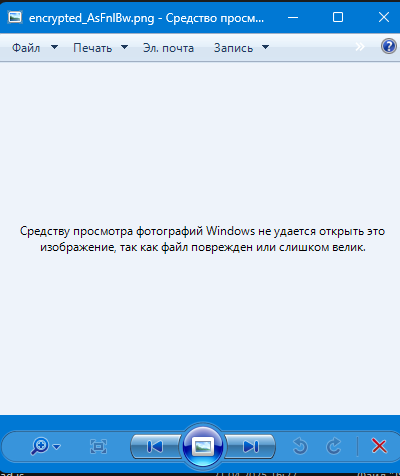
q: 19;

Kc: 5;

AsFnlBw.png (исходный файл):



Результат шифрования:  




Результат дешифрования:  