УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №3

по теории информации

Вариант 1

Выполнил:

Полозков А.Ю.

Группа 351001

Проверила:

Болтак С.В.

Минск 2025

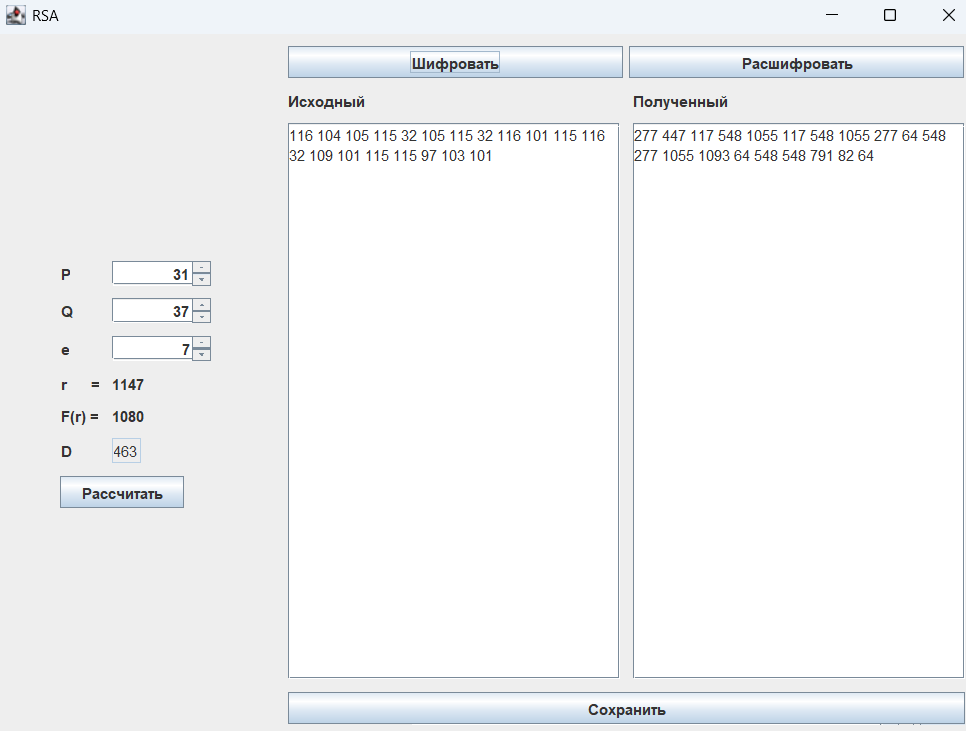
**Задание**

Разработать программное средство, выполняющее вычисление открытого ключа Ko алгоритма RSA и побайтовое шифрование данным ключом по алгоритму RSA произвольного файла. Значения параметров p, q и закрытого ключа Kc, а также имя входного файла задаются пользователем и проходят проверку на корректность. Результат шифрования выводится на экран в виде чисел в 10 системе счисления.

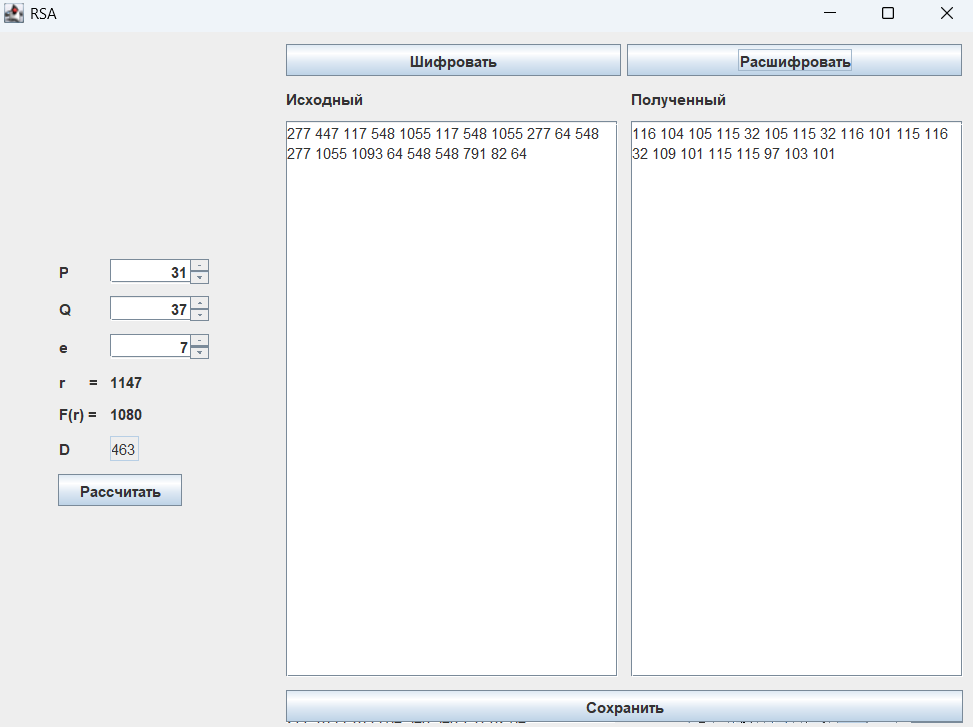
Разработать программное средство, выполняющее расшифровку файла, каждый 16-битный блок которого представляет собой зашифрованное по алгоритму RSA 8-битное значение. Значения модуля r и закрытого ключа Kc задаются пользователем.  
 **Тесты**

1. **Текстовый файл**

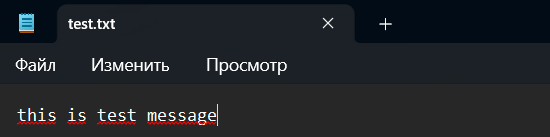
Шифрование:



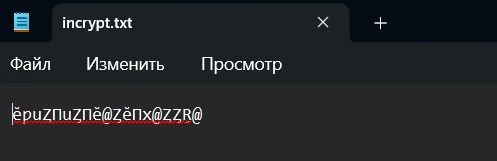
Дешифрование:



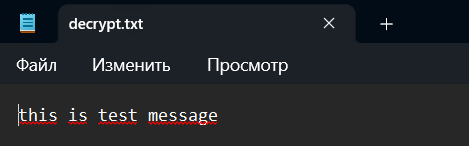
Начальный файл:

****

Зашифрованный файл:

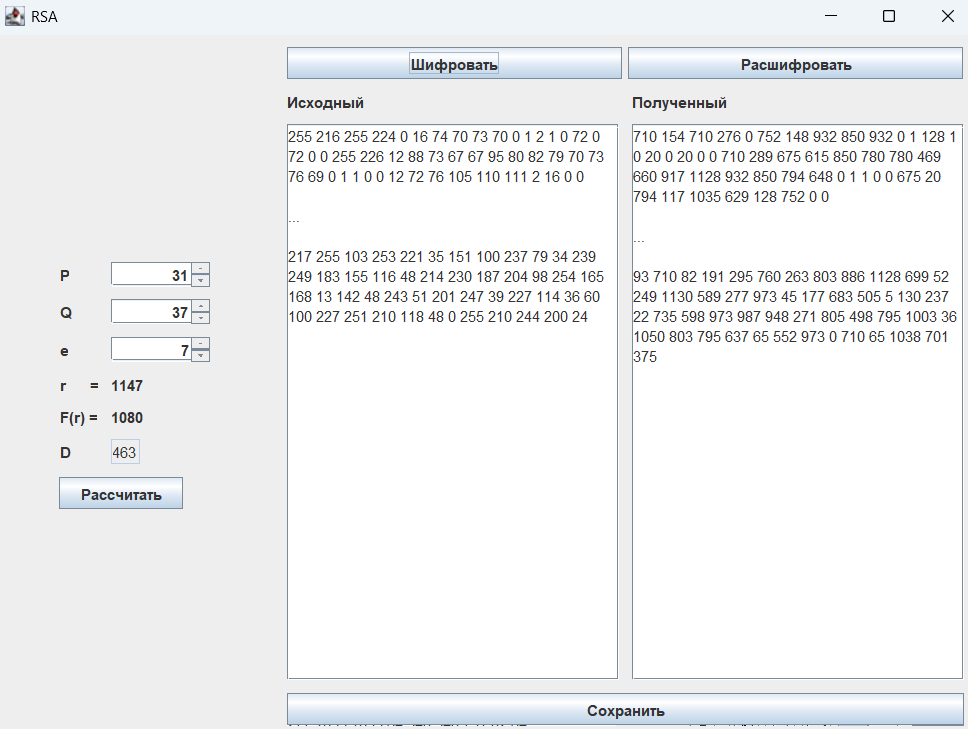
****

Расшифрованный файл:

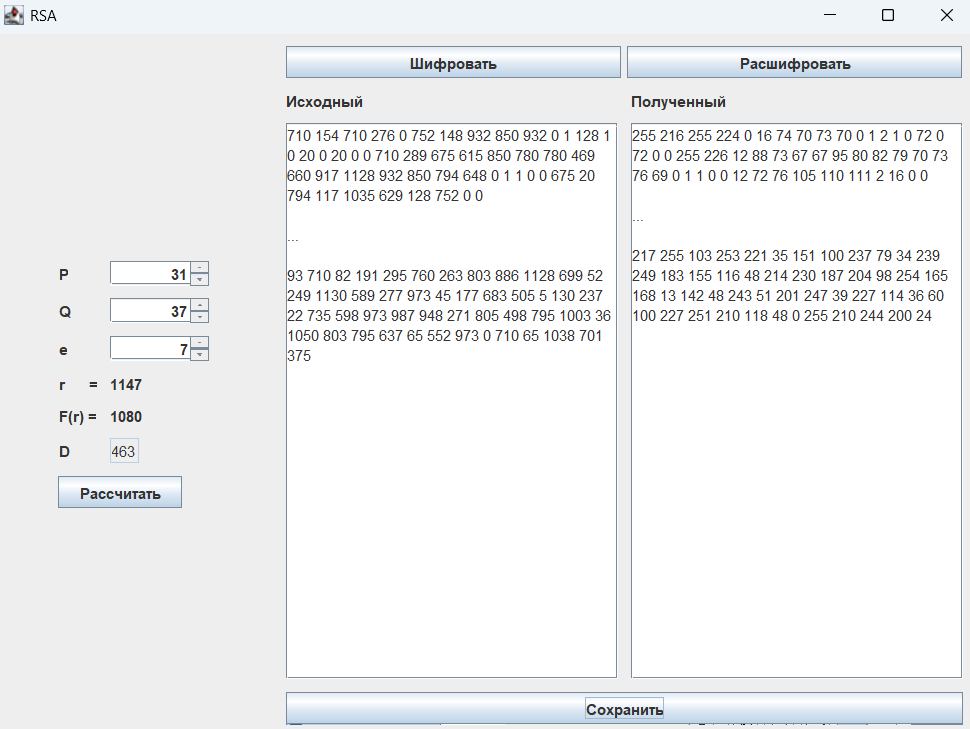
****

1. **JPG-файл**

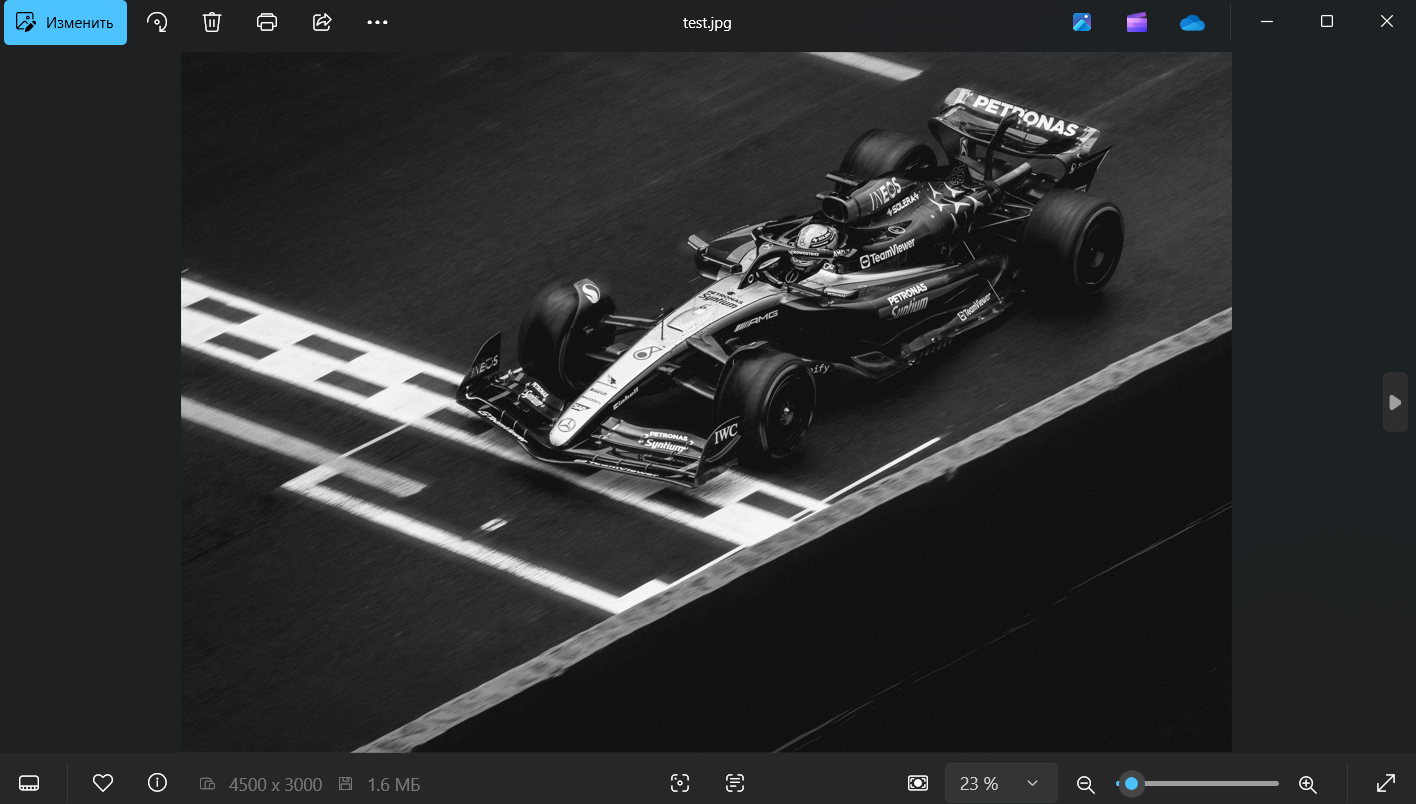
Шифрование:



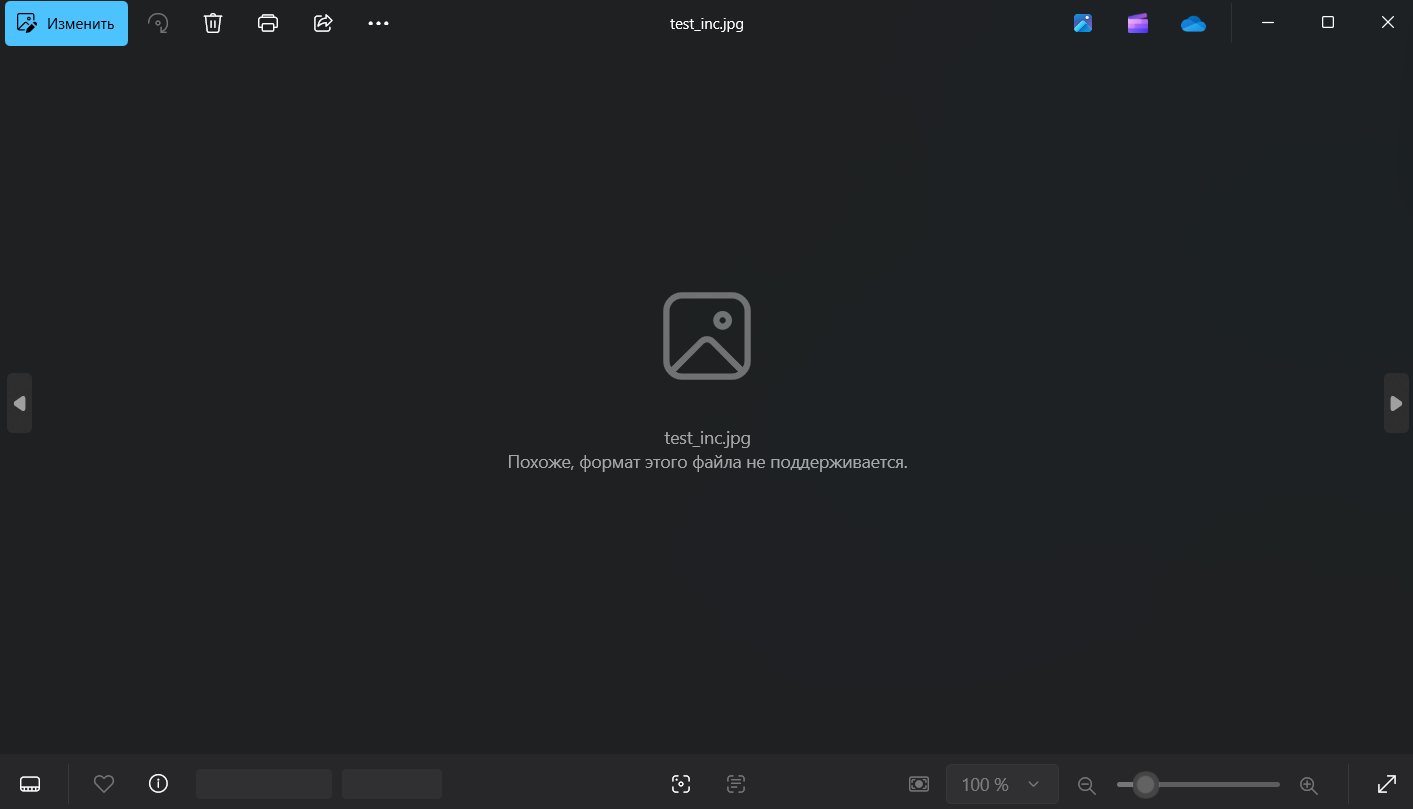
Дешифрование:



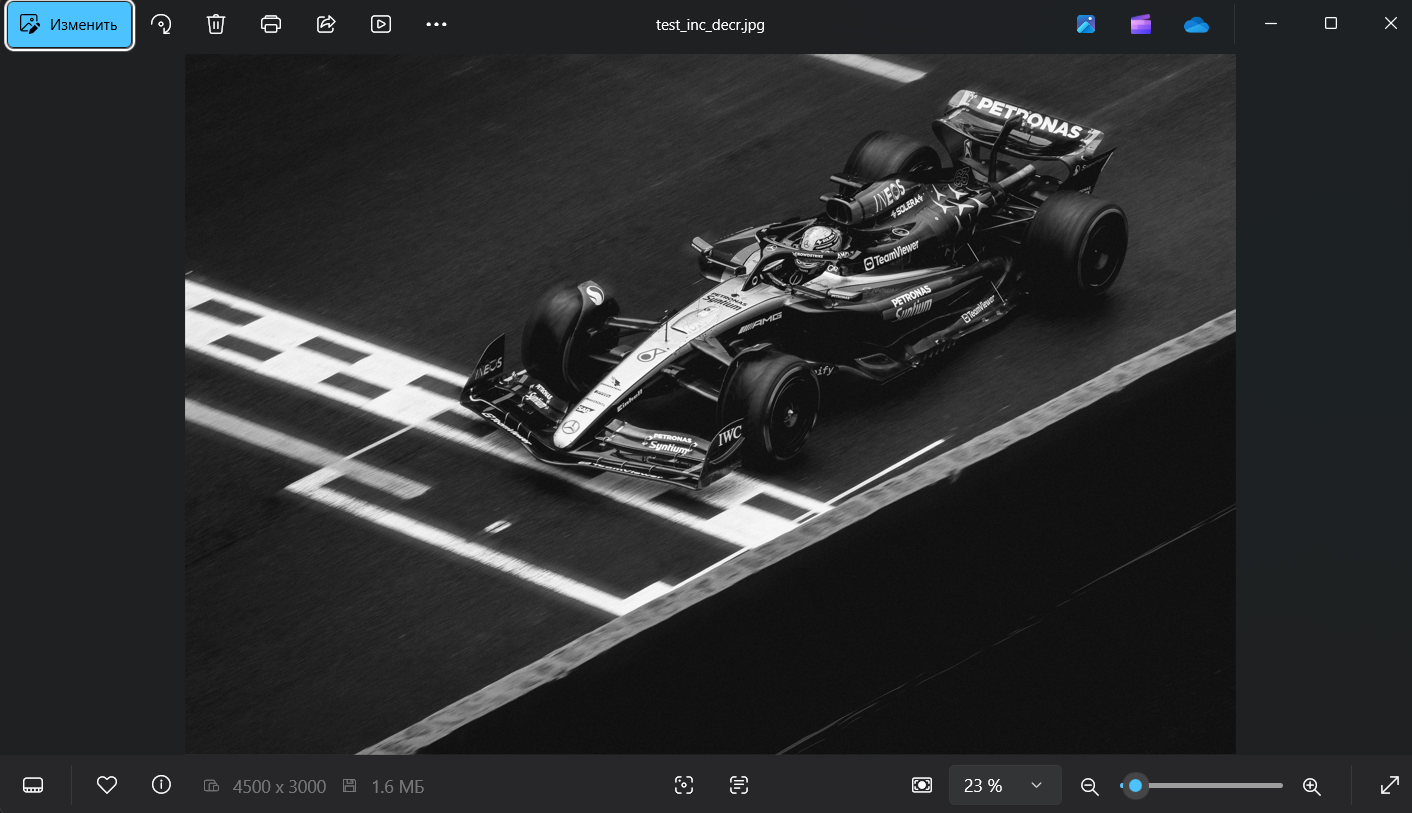
Изначальное:



Зашифрованное:

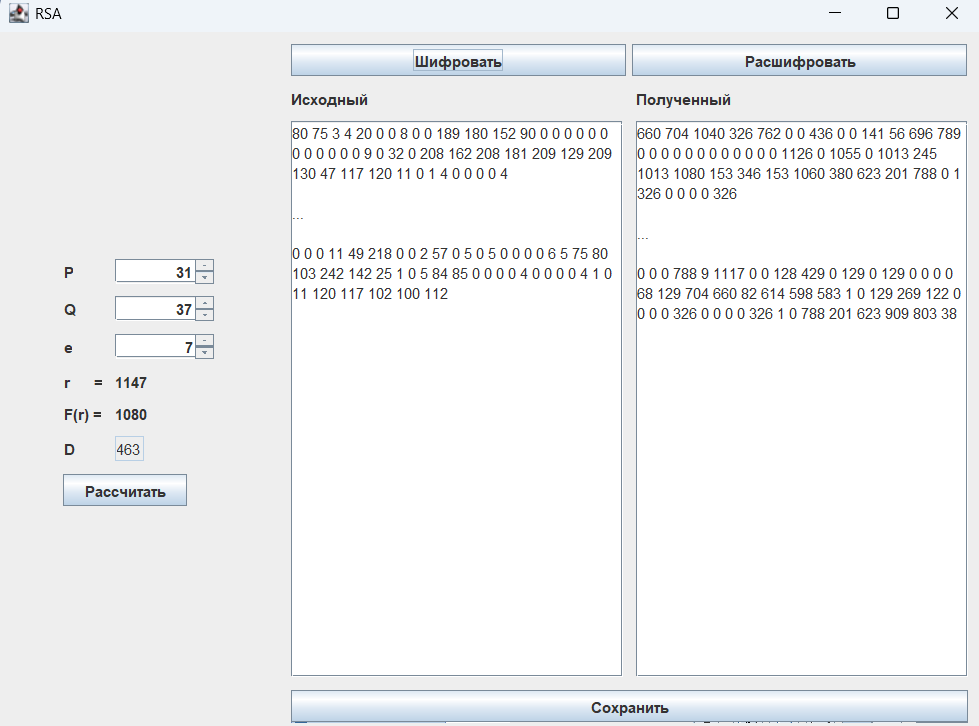


Расшифрованное:

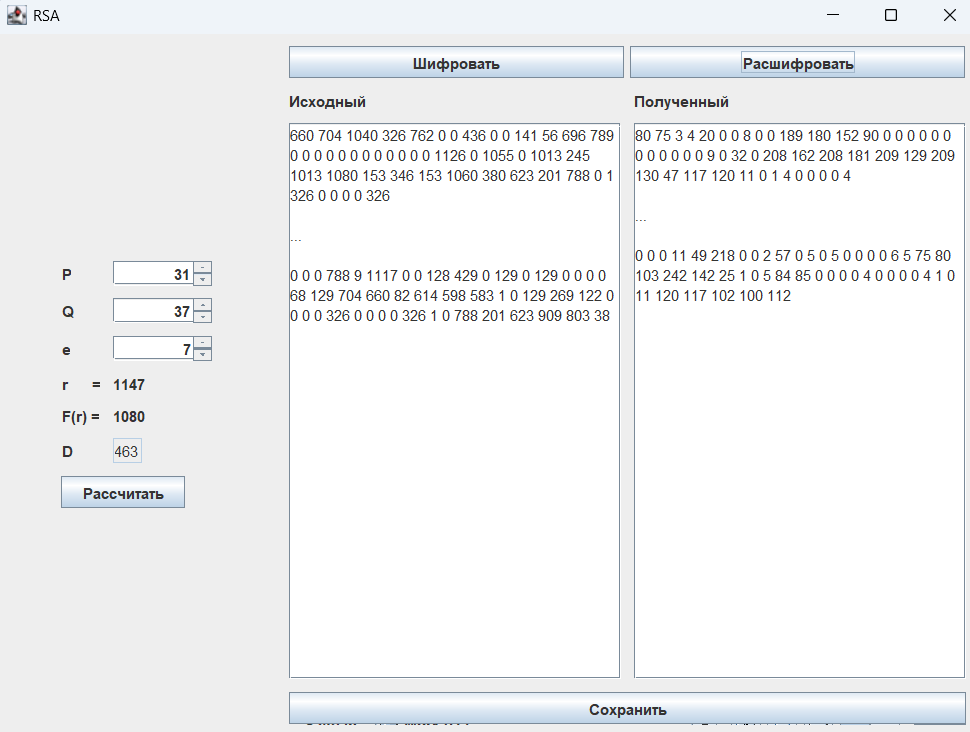


1. **ZIP-файл**

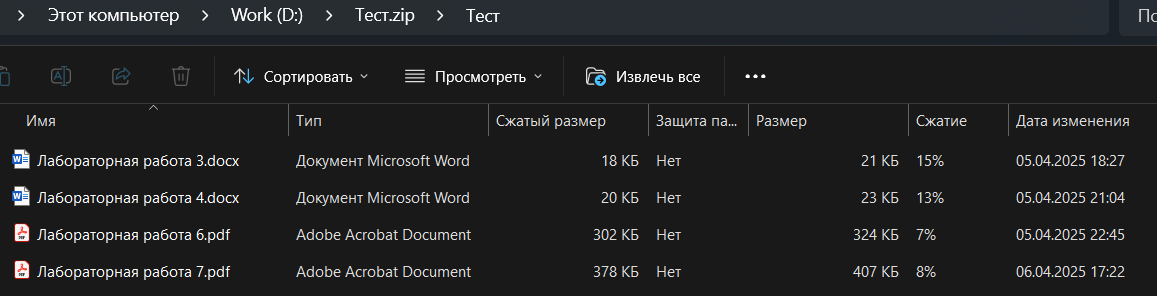
Шифрование:



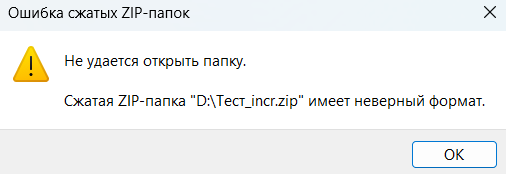
Дешифрование:



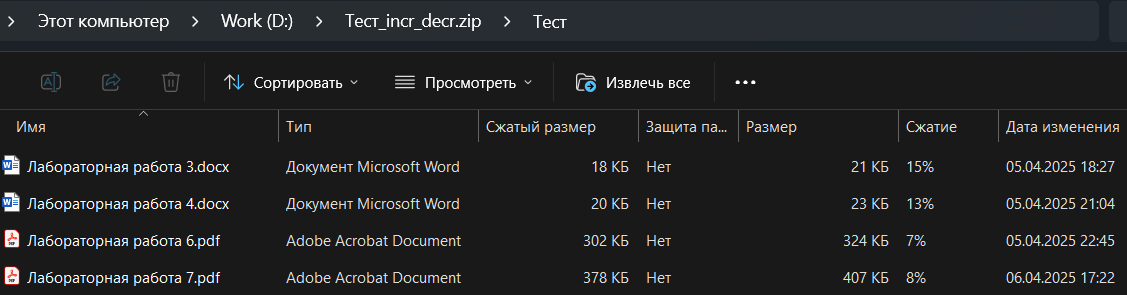
Изначальный:



Зашифрованный:



Расшифрованный:



**Быстрое возведение в степень:**

|  |  |  |  |
| --- | --- | --- | --- |
| Шаг | Степень | Основание | Результат |
| 0 | 37 | 7 | 1 |
| 1 | 37 | (7 \* 7) mod 31 = 18 | (1\*7) mod 31 = 7 |
| 2 | 18 | (18\*18)mod 31 = 14 | 7 |
| 3 | 9 | (14\*14)mod 31 = 10 | (7\*14)mod 31 = 5 |
| 4 | 4 | (10\*10)mod 31 =7 | 5 |
| 5 | 2 | (7\*7)mod 31 = 18 | 5 |
| 6 | 1 | (18\*18) mod 31 = 14 | 5 \* 18 mod 31 = 28 |
| 7 | 0 | - | - |

731 mod 31 = 28.

**Расширенный алгоритм Евклида:**

Для чисел 36 и 21

36x+24y=НОД(36,24)

36 = 1\*36 + 0\*24

24 = 0\*36 + 1\*24

Первая итерация:

36 = 1\*24 + 12

Новое ур-е: 12 = 36 – 24

Вторая итерация:

24 = 2\*12 + 0

Новое ур-е: 0 = 24 – 2 \* 12

Процесс завершается, т.к. остаток 0.

НОД(36, 24) = 12 – последний не нулевой остаток.

Коэф-ты x = 1, y = -1(из предпоследнего уравнения).

**Поиск первообразных корней:**

Для числа 7.

Ф-ция Эйлера = 6 = 2\*3.

q1=2, q2=3.

Для 1: 12 = 1 mod7, 13 = 1 mod 7

Для 2: 22 = 4 mod7, 23 = 1 mod 7

Для 3: 32 = 2 mod7, 33 = 6 mod 7 – первообразный корень

Для 4: 42 = 2 mod7, 43 = 1 mod 7

Для 5: 52 = 4 mod7, 53 = 6 mod 7 – первообразный корень

Для 6: 62 = 1 mod7, 63 = 6 mod 7

Таким образом, первообразные корни по модулю 7: 3 и 5.