УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №3

по предмету «Теория информации»

Вариант 2

Выполнил:

Романовский М.И.

гр. 351004

Проверила:

Болтак С.В.

Минск 2024

1. **Пример работы алгоритма быстрого возведения в степень с использованием модульной арифметики.**

**519mod13=?**

**a–основание=5  
n – показатель степени = 19**

**e – четное n или нет(да/нет)**

**r – результат(вначале равен 1)**

**x – значение = mod 13**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шаг | a | n | e | Действие | r mod x |
| 1 | 5 | 19 | нет | r=1×5mod13=5  n=19−1=18 | 5 |
| 2 | 5 | 18 | да | a=5^2mod13=12  n=18/2=9 | 5 |
| 3 | 12 | 9 | нет | r=5×12mod13=8  n=9−1=8 | 8 |
| 4 | 12 | 8 | да | a=12^2mod13=1  n=8/2=4 | 8 |
| 5 | 1 | 4 | да | a=1^2mod13=1  n=4/2=2 | 8 |
| 6 | 1 | 2 | да | a=1^2mod13=1  n=2/2=1 | 8 |
| 7 | 1 | 1 | нет | r=8×1mod13=8  n=1−1=0 (конец) | 8 |

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

Задано простое p = 17

Ищем простые делители p - 1 = 16 = 2 \* 2 \* 2 \* 2

Проверяем является ли число 2 первообразным корнем по модулю 17:

216/2 mod 17 = 1. Число 2 не является первообразным по модулю 17.

Проверяем является ли число 3 первообразным корнем по модулю 11:

316/2 mod 17 = 16. Число 3 является первообразным по модулю 17.

Если найден один первообразный корень g по модулю p, остальные корни имеют вид g^k, где НОД(k, p-1) = 1. Для p = 17, допустимые k: 1, 3, 5, 7, 9, 11, 13, 15:

1. 3^1 mod 17 = 3 – является первообразным
2. 3^3 mod 17 = 10 – является первообразным
3. 3^5 mod 17 = 5 – является первообразным
4. 3^7 mod 17 = 11 – является первообразным
5. 3^9 mod 17 = 14 – является первообразным
6. 3^11 mod 17 = 7 – является первообразным
7. 3^13 mod 17 = 12 – является первообразным
8. 3^5 mod 17 = 6 – является первообразным

Тогда все первообразные корни для модуля p = 17: 3, 5, 6, 7, 10, 11, 12, 14.

**3.Пример работы расширенного алгоритма Евклида с взаимно простыми числами**

**x1\*a + y1\*b = НОД(a,b), a = 725, b = 318, НОД(a,b) = 1, т.к a и b взаимно простые.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **итерация** | **Делимое** | **Делитель** | **Частное** | **Остаток** |
| 1 | 725 | 318 | 2 | 89 |
| 2 | 318 | 89 | 3 | 51 |
| 3 | 89 | 51 | 1 | 38 |
| 4 | 51 | 38 | 1 | 13 |
| 5 | 38 | 13 | 2 | 12 |
| 6 | 13 | 12 | 1 | 1 |
| 7 | 12 | 1 | 12 | 0 |

Начинаем обратный ход с предпоследней операции(13/12):  
1=13−12×1  
1=13−(38−13×2)×1=13×3−38×1

1 = (51 – 38 \* 1) \* 3 - 38 \* 1

1=51×3−(89−51×1)×4=51×7−89×4

1=(318−89×3)×7−89×4=318×7−89×25

1=318×7−(725−318×2)×25=318×57−725×25

1=(−25)×725+57×318  
Получаем ответ: x = -25,y = 57

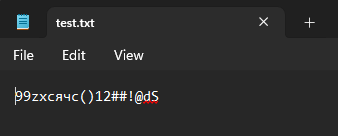
Проверка:

(−25)×725+57×318=−18125+18126=1

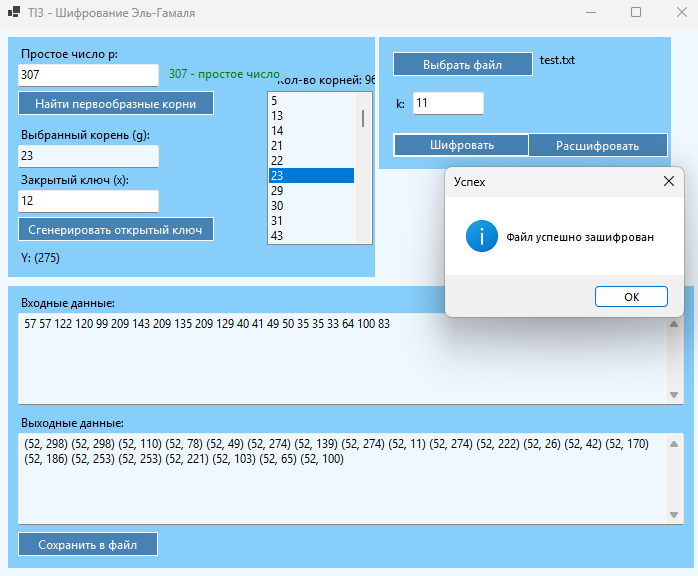
**Проверка работоспособности программы**

**Исходный текст:**

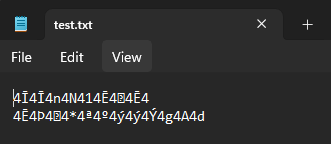
99zxcячс()12##!@dS



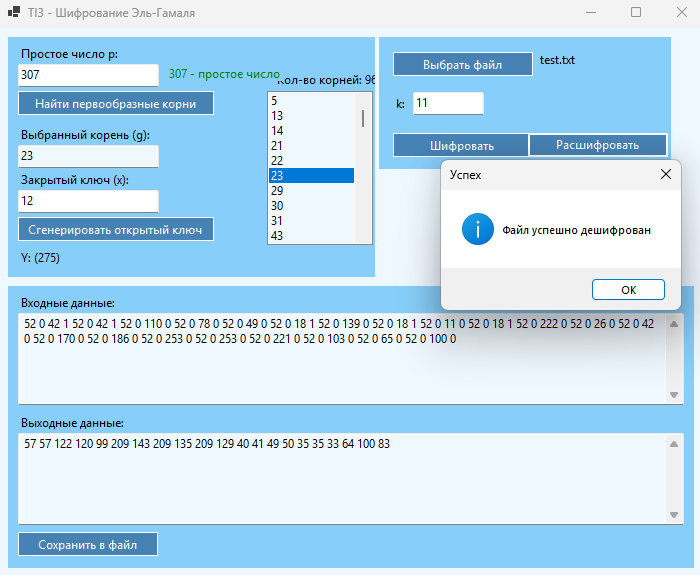
**Шифрование:**

****

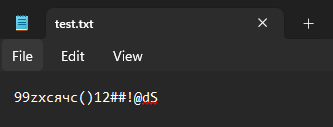
**Результат шифрования:**

****

**Дешифрование:**

****

**Значение файла после дешифрования:**

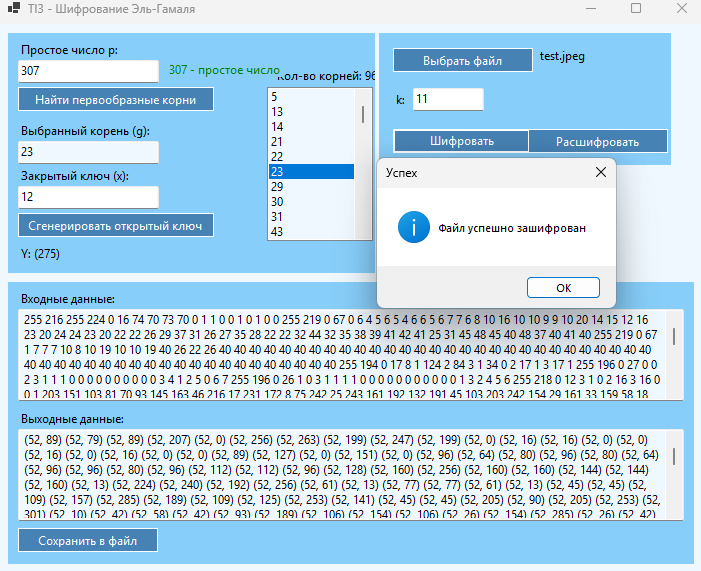
****

**Шифрование картинки:**

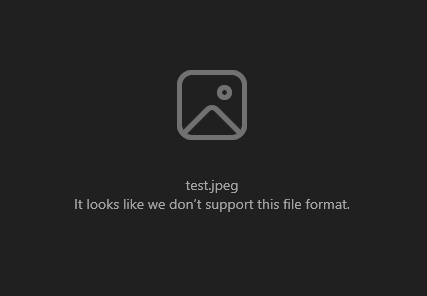
**Исходное изображение:**

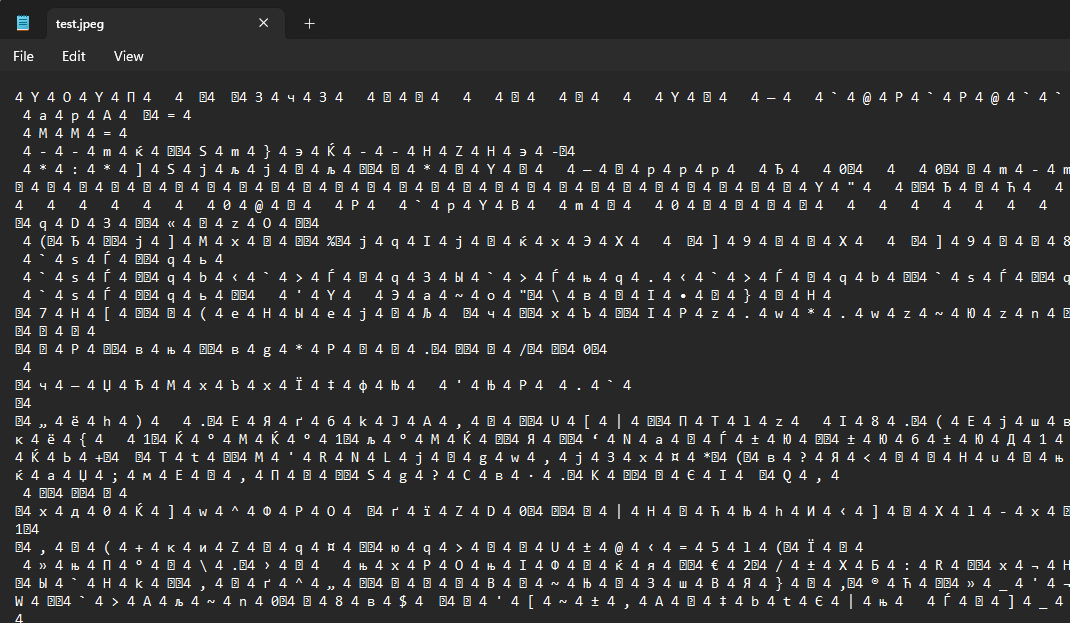


**Шифрование:**

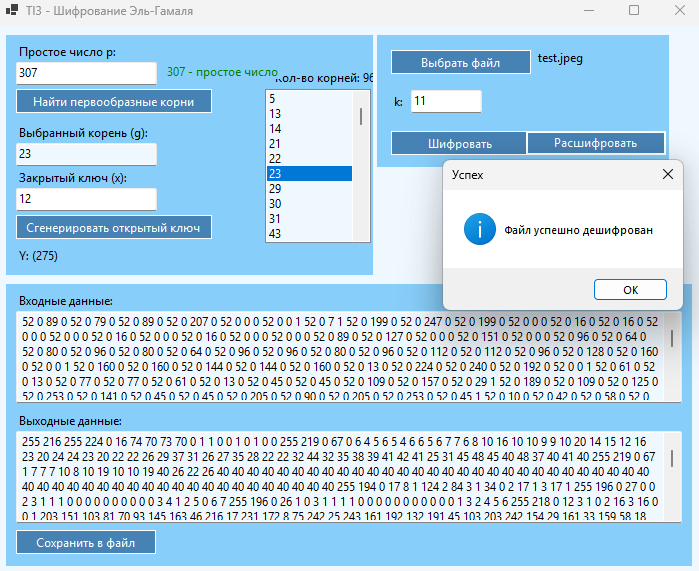
****

**Содержимое зашифрованного файла:**

****



**Дешифрование:**



**Файл после дешифрования:**

