УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №3

по предмету «Теория информации»

Вариант 2

Выполнила:

Кисель П.А.

гр. 351003

Проверила:

Болтак С.В.

Минск 2025

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

**423 mod 13 = ?**

**a – основание=4  
n – показатель степени = 23**

**e – четное n или нет (четн / нечетн)**

**r – результат (в начале равен 1)**

**x – значение = mod 13**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шаг | a | n | e | Действие | r mod x |
| 1 | 4 | 23 | нечетн | r = 1×4 mod 13 = 4  n = 23−1 = 22 | 4 |
| 2 | 4 | 22 | четн | a = 4^2 mod 13 = 3  n = 22/2 = 11 | 4 |
| 3 | 3 | 11 | нечетн | r = 4×3 mod 13 = 12  n = 11−1 = 10 | 12 |
| 4 | 3 | 10 | четн | a = 3^2 mod 13 = 9  n = 10/2 = 5 | 12 |
| 5 | 9 | 5 | нечетн | r = 12×9 mod 13 = 4  n = 5−1 = 4 | 4 |
| 6 | 9 | 4 | четн | a = 9^2 mod 13 = 3  n = 4/2 = 2 | 4 |
| 7 | 3 | 2 | четн | a = 3^2 mod 13 = 9  n = 2/2 = 1 | 4 |
| 8 | 9 | 1 | нечетн | r = 4×9 mod 13 = 10  n = 1−1 = 0 (Конец) | 10 |

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

Задано простое p = 19

Ищем простые делители p - 1 = 18 = {2,3}

Проверяем является ли число g = 2 первообразным корнем по модулю 19:

218/2 mod 19 = 18 ≠ 1

218/3 mod 19 = 7 ≠ 1. ⇒ 2 - первообразный корень

Проверяем является ли число g = 3 первообразным корнем по модулю 19:  
 3⁹ mod 19 = 18 ≠ 1  
 3⁶ mod 19 = 7 ≠ 1 ⇒ 3 - также первообразный корень

Если найден один первообразный корень g по модулю p, остальные корни имеют вид g^k, где НОД(k, p-1) = 1. Для p = 18, допустимые k (взаимно простые с 18): 1, 5, 7, 11, 13, 17:

1. 2^1 mod 19 = 2 – является первообразным
2. 2^5 mod 19 = 13 – является первообразным
3. 2^7 mod 19 = 14 – является первообразным
4. 2^11 mod 19 = 15 – является первообразным
5. 2^13 mod 19 = 3 – является первообразным
6. 2^17 mod 19 = 10 – является первообразным

Тогда все первообразные корни для модуля p = 19: 2, 3, 10, 13, 14, 15.

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

**x1\*a + y1\*b = НОД(a, b), a = 117, b = 85, НОД(a, b) = 1, т.к a и b взаимно простые.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **итерация** | **Делимое** | **Делитель** | **Частное** | **Остаток** |
| 1 | 117 | 85 | 1 | 32 |
| 2 | 85 | 32 | 2 | 21 |
| 3 | 32 | 21 | 1 | 11 |
| 4 | 21 | 11 | 1 | 10 |
| 5 | 11 | 10 | 1 | 1 |
| 6 | 10 | 1 | 10 | 0 |

1. Начинаем обратный ход с предпоследней операции (шаг 5), где остаток равен 1:  
   **Базовое уравнение:**  
   1 = 11 - 10×1
2. **Выражаем 10 из шага 4:**  
   10 = 21 - 11×1  
   Подставляем:  
   1 = 11 - (21 - 11×1)×1 = 11×2 - 21×1
3. **Выражаем 11 из шага 3:**  
   11 = 32 - 21×1  
   Подставляем:  
   1 = (32 - 21×1)×2 - 21×1 = 32×2 - 21×3
4. **Выражаем 21 из шага 2:**  
   21 = 85 - 32×2  
   Подставляем:  
   1 = 32×2 - (85 - 32×2)×3 = 32×8 - 85×3
5. **Выражаем 32 из шага 1:**  
   32 = 117 - 85×1  
   Подставляем:  
   1 = (117 - 85×1)×8 - 85×3 = **117×8 - 85×11**

**Итоговое решение:**

1=8×117+(−11)×85

Коэффициенты Безу:

x = 8, y= −11

**Проверка:**

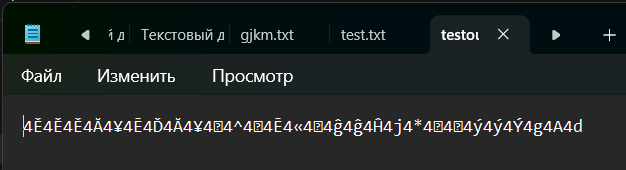
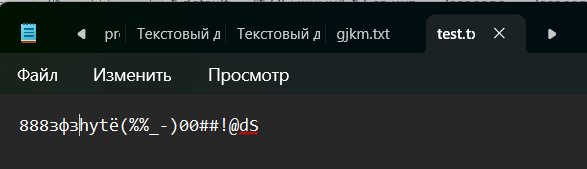
8×117+(−11)×85=936−935=18×117+(−11)×85=936−935=1

Результат верен.

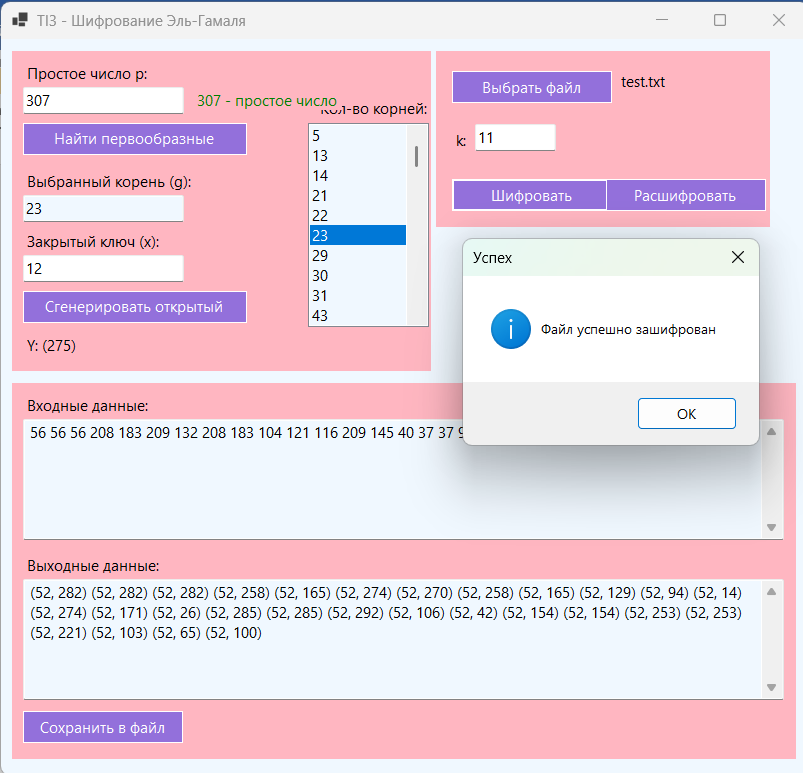
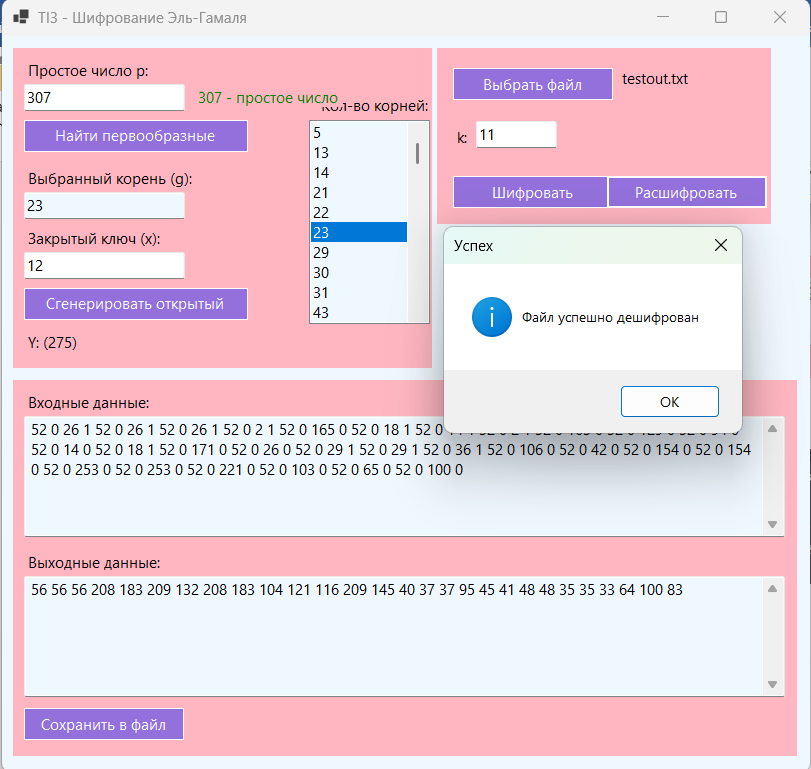
**Проверка работоспособности программы**

**Исходный текст: Результат шифрования:**

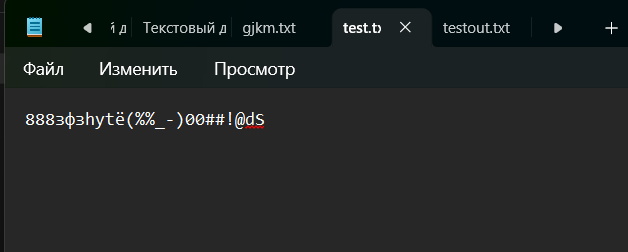
888зфзhytё(%%\_-)00##!@dS

****

**Шифрование: Дешифрование:**

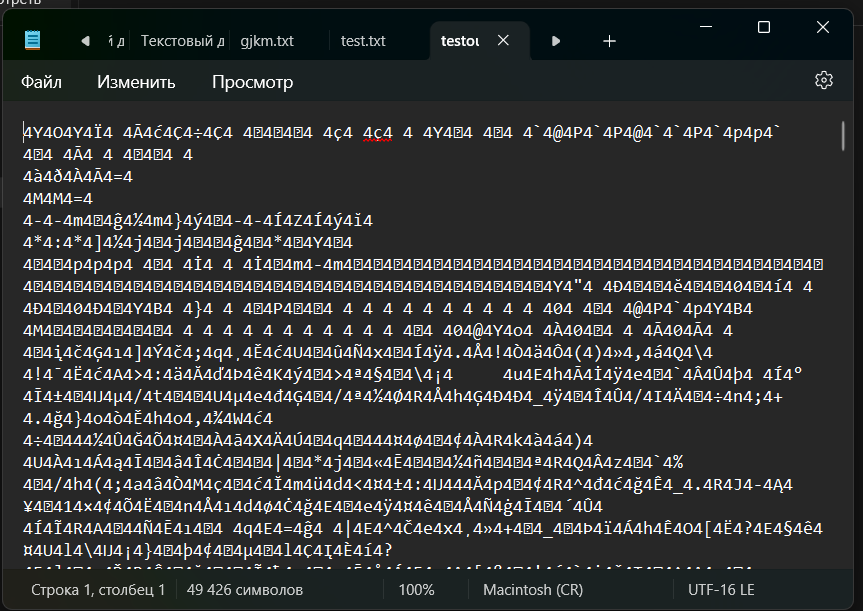
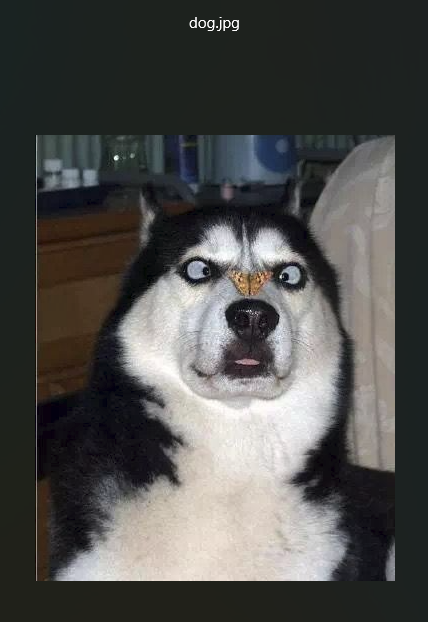
****

**Значение файла после дешифрования:**

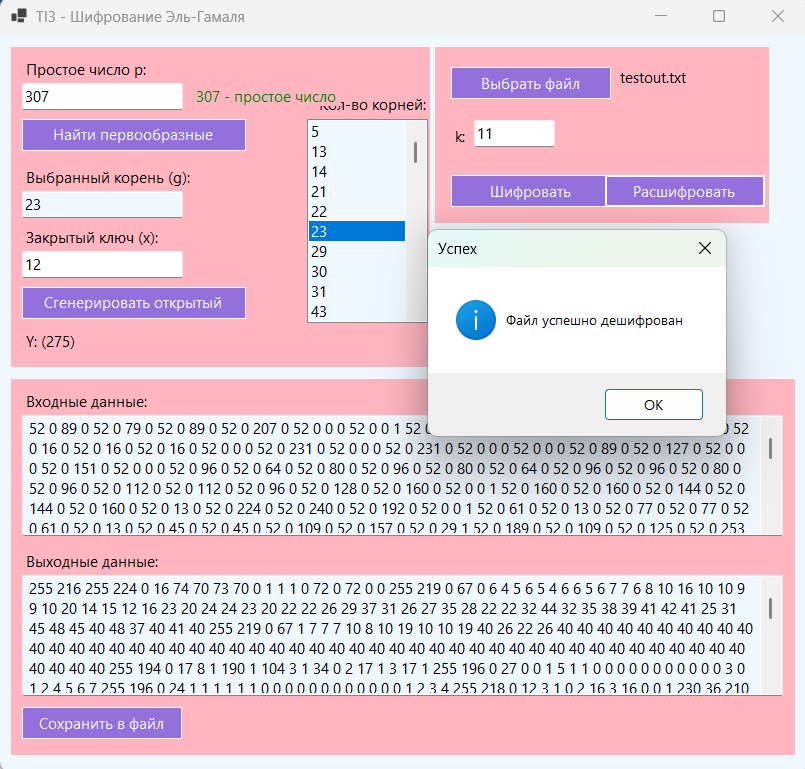
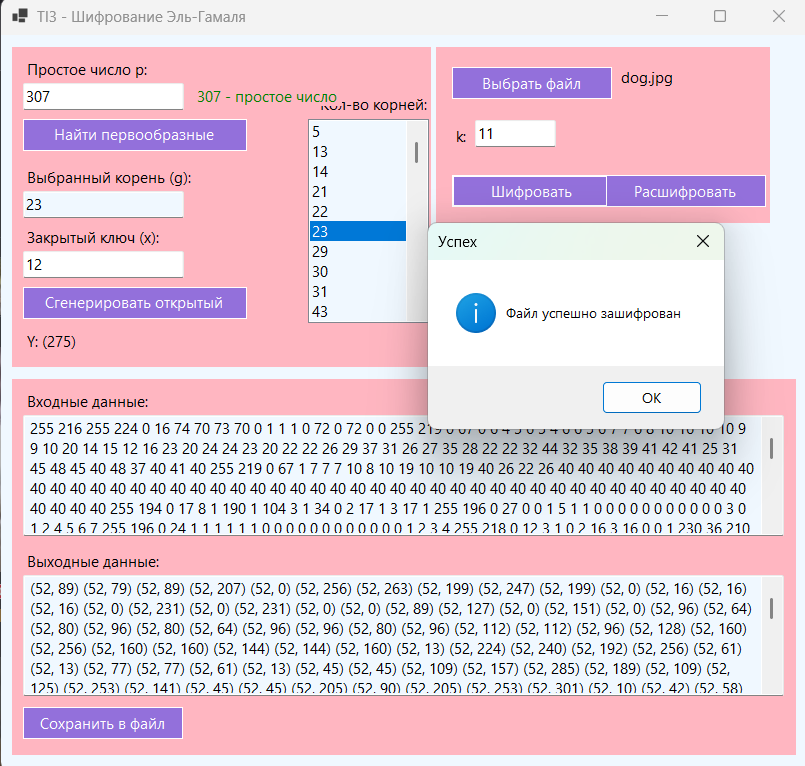
****

**Шифрование картинки:**

**Исходное изображение: Содержимое зашифрованного файла:**

****

**Шифрование: Дешифрование:**

****

**Файл после дешифрования:**

