Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Теория информации (ТИ)

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

Тема работы:

КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

Выполнила

студент: гр. 351002 Яночкин И.Л.

Проверила: Болтак С.В.

Минск 2025

# Задание

Вариант 1

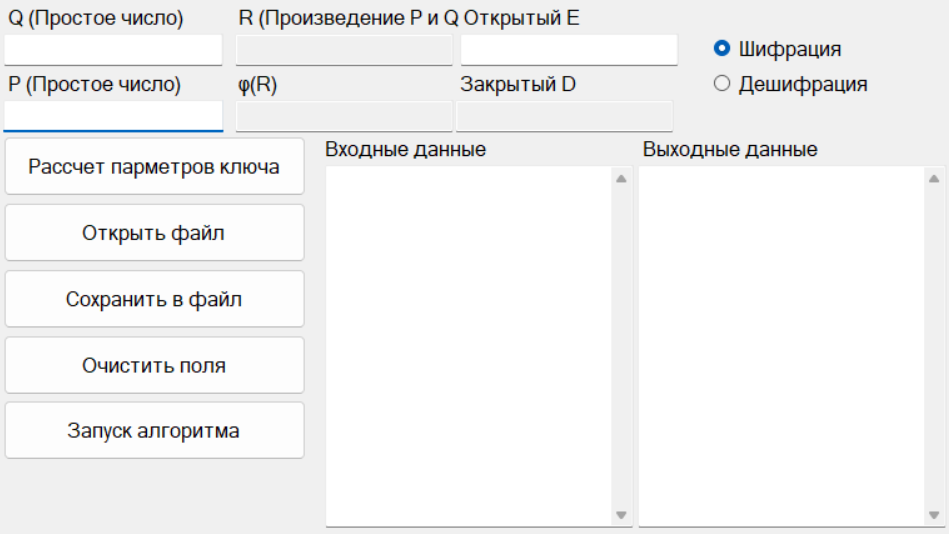
Разработать программное средство, выполняющее вычисление открытого ключа **(*KO*)** алгоритма ***RSA*** и побайтовое шифрование данным ключом по алгоритму ***RSA*** произвольного файла. Значения параметров ***p,*** ***q*** и ***KС*,** а также имя входного файла задаются пользователем. Программа должна осуществлять проверку ограничений на вводимые пользователем значения параметров алгоритма. Организовать вывод содержимого зашифрованного файла на экран в виде чисел в 10 системе счисления.

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

Использовать алгоритм быстрого возведения в степень и расширенный алгоритм Евклида.

Результат работы программы – зашифрованный/расшифрованный файл/ы.

2 Тестовые наборы



Тест 1

Тестовая ситуация: проверка на корректность вводимого числа P.

Исходные данные: 𝑝 = 75 (не простое число).

Полученный результат: Вывод ошибочного сообщения.

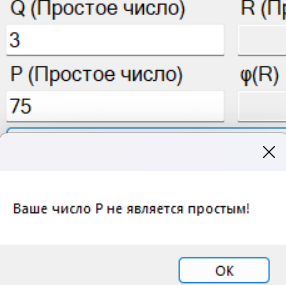


Рисунок 1 – Полученный результат. Тест 1

Тест 2

Тестовая ситуация: проверка на корректность вводимого числа Q.

Исходные данные: Q = 10 (не простое число).

Полученный результат: Вывод ошибочного сообщения.

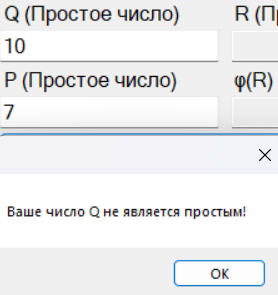


Рисунок 2 – Полученный результат. Тест 2

Тест 3

Тестовая ситуация: проверка на диапазон произведения P и Q.

Исходные данные: P = 17, Q =11. Полученные параметры ключа не подходят для шифрования в два байта.

Полученный результат: Вывод ошибочного сообщения.

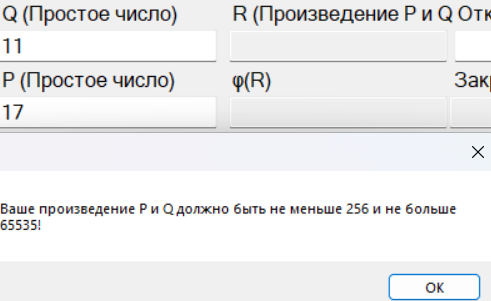


Рисунок 3 – Полученный результат. Тест 3

Тест 4

Тестовая ситуация: проверка на диапазон произведения P и Q.

Исходные данные: P = 197, Q = 941. Полученные параметры ключа не подходят для шифрования в два байта.

Полученный результат: Вывод ошибочного сообщения.

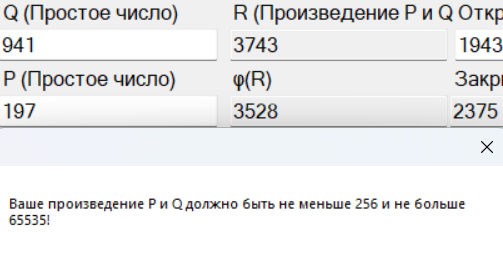


Рисунок 4 – Полученный результат. Тест 4

Тест 5

Тестовая ситуация: Ввод пустого поля P или Q.

Исходные данные: Пустое поле.

Полученный результат: Вывод ошибочного сообщения.

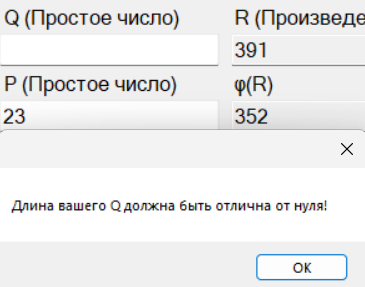


Рисунок 5 – Полученный результат. Тест 5

Тест 6

Тестовая ситуация: проверка на корректность работы программы для маленького размера текстового файла.

Исходные данные:

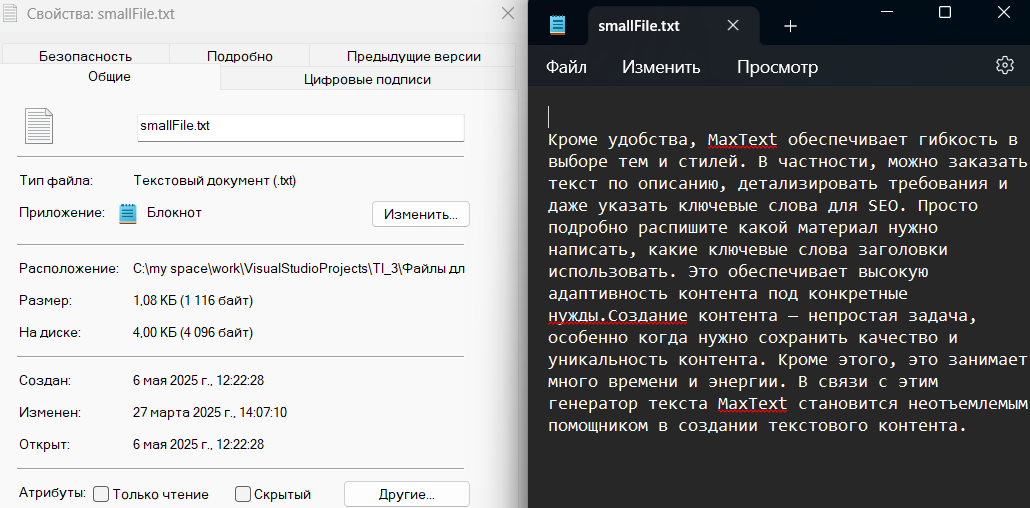


Рисунок 6 – Свойства и содержимое исходного файла. Тест 6

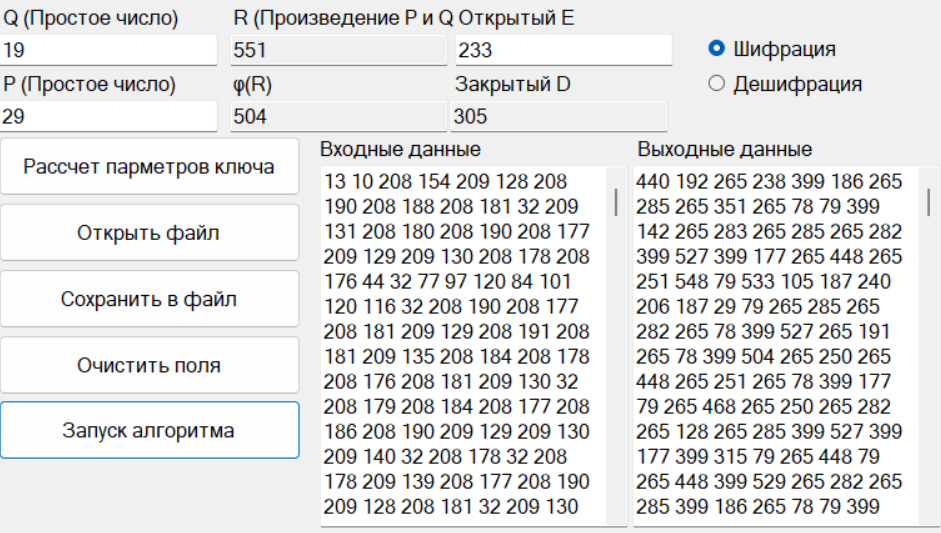


Рисунок 6 – Шифрация. Тест 6

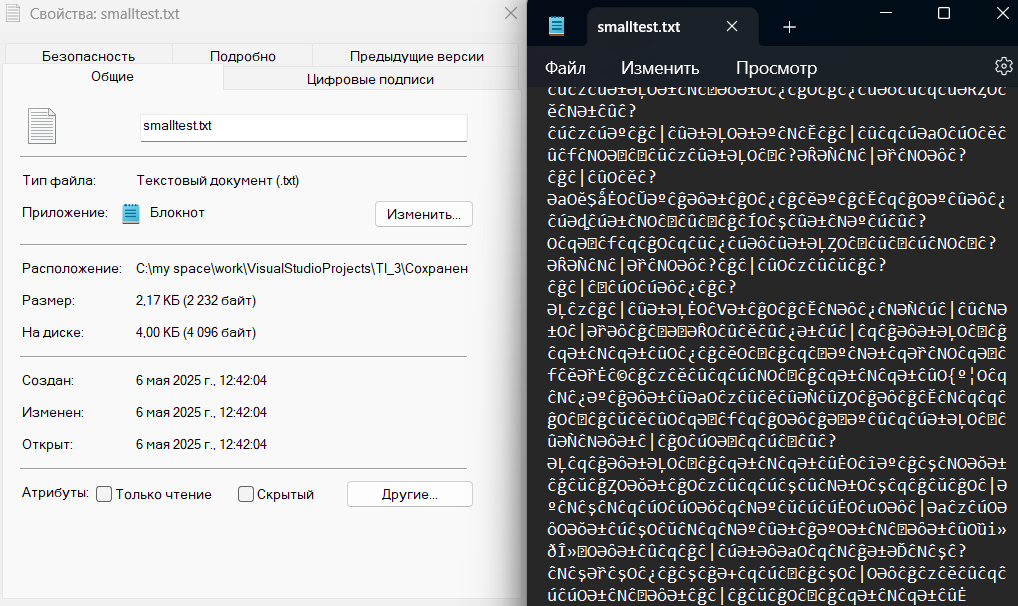
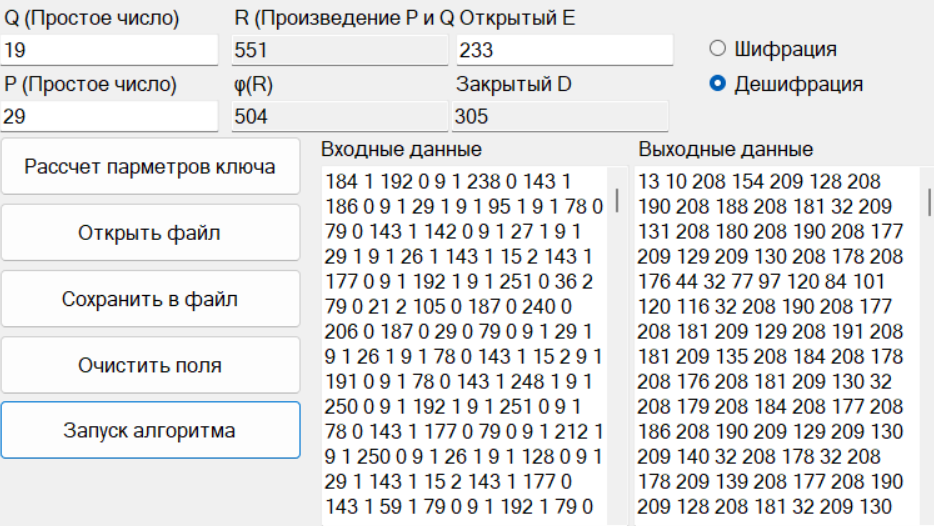


Рисунок 7 – Свойства и содержимое зашифрованного файла. Тест 6

****

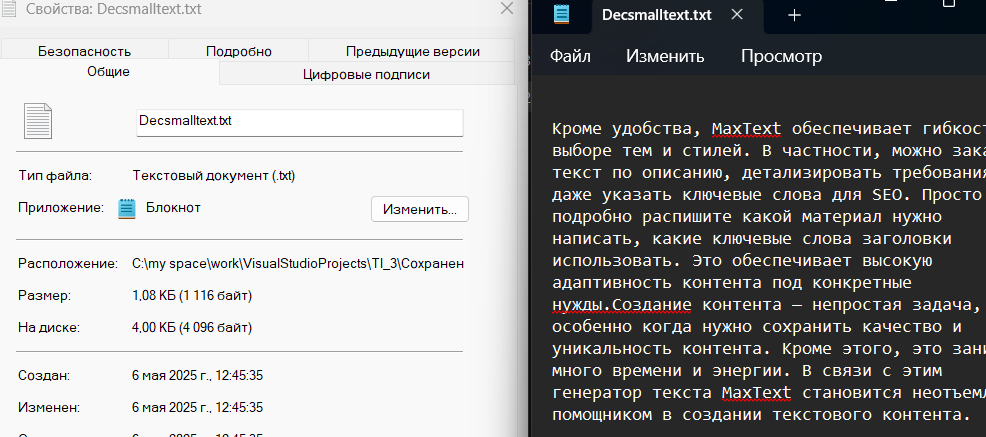


Рисунок 8 – Дешифрация. Тест 6

Тест 7

Тестовая ситуация: проверка на корректность работы программы для большого размера текстового файла.

Исходные данные:

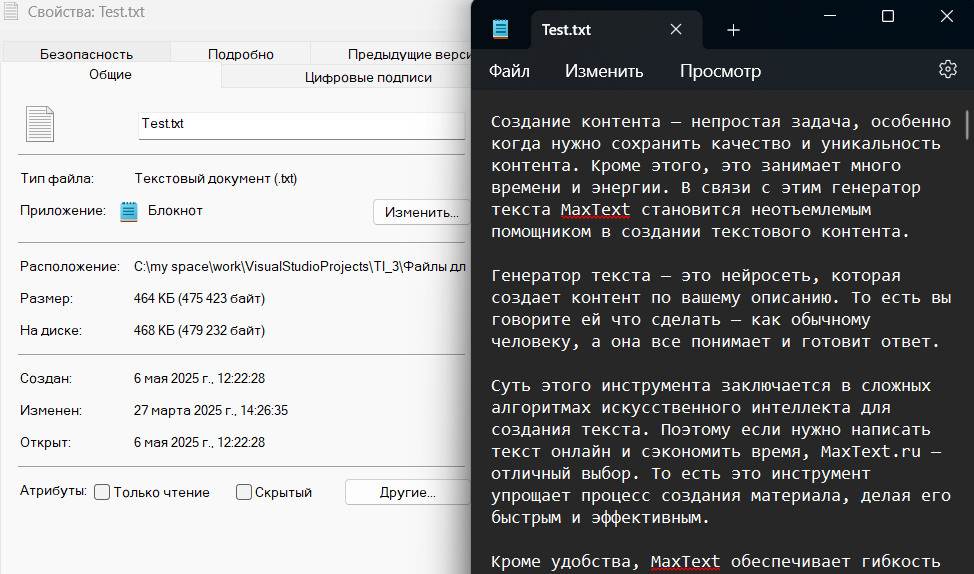


Рисунок 9 – Свойства и содержимое исходного файла. Тест 7

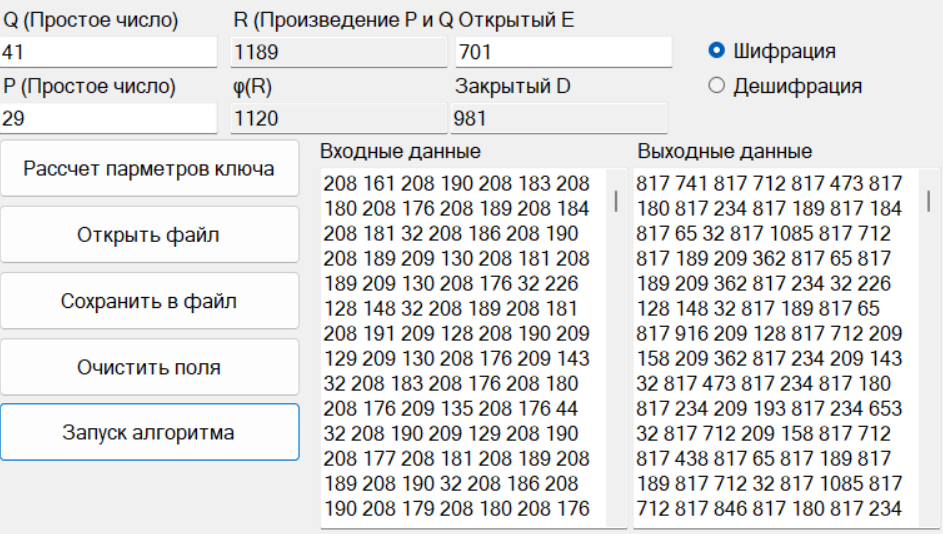


Рисунок 10 – Шифрация. Тест 7

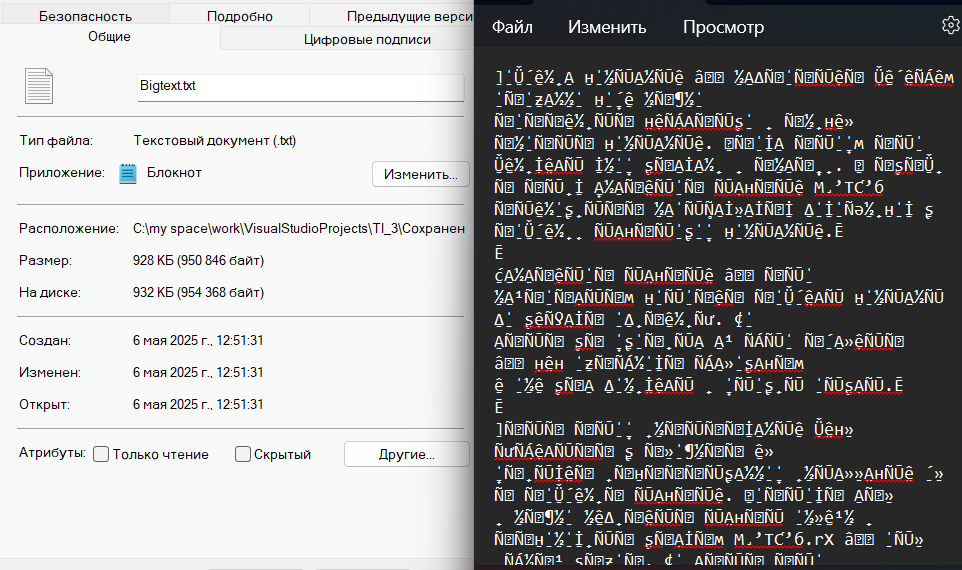
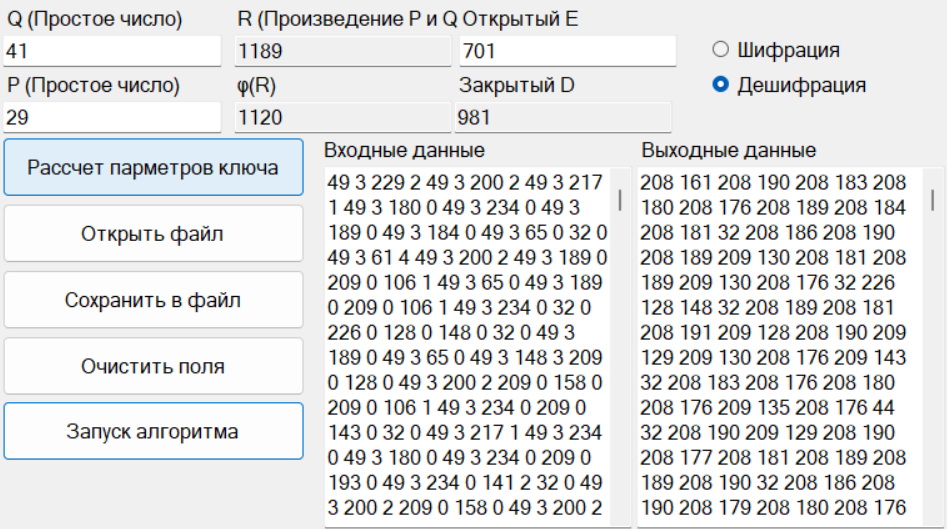


Рисунок 11 – Свойства и содержимое зашифрованного файла. Тест 7



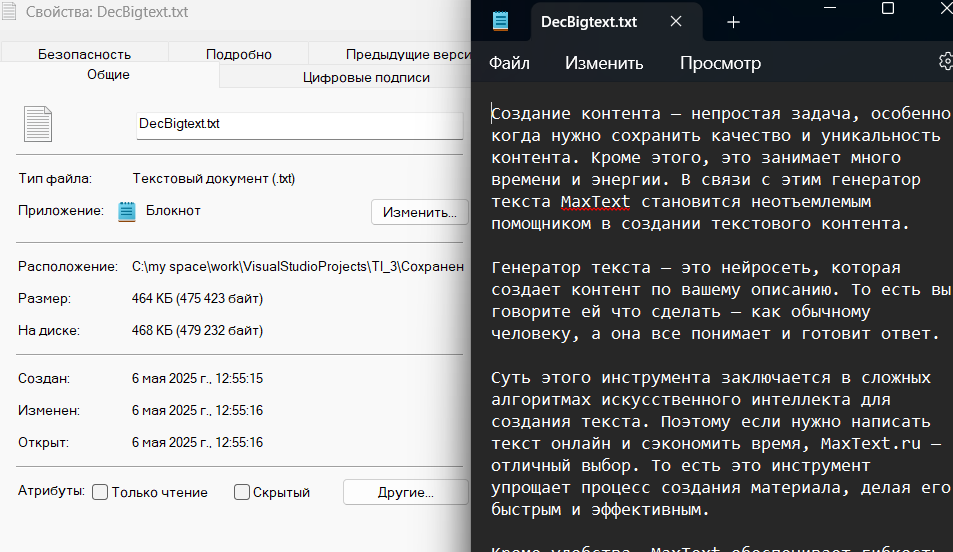


Рисунок 12 – Дешифрация. Тест 7

Тест 8

Тестовая ситуация: проверка на корректность работы программы для файла музыки.

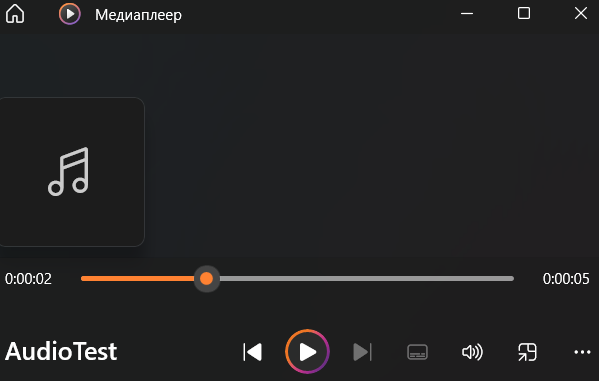
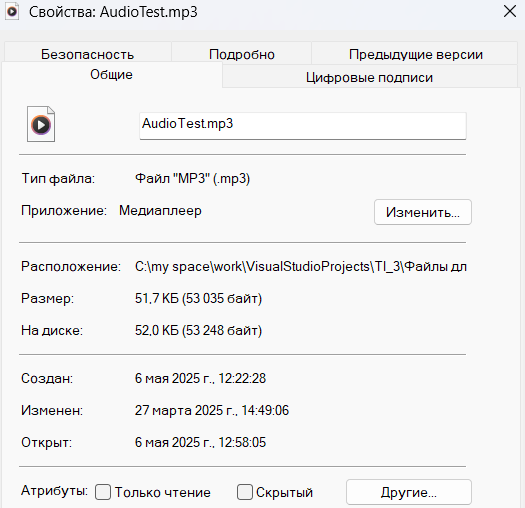


Рисунок 13 – Свойства исходного файла. Тест 8

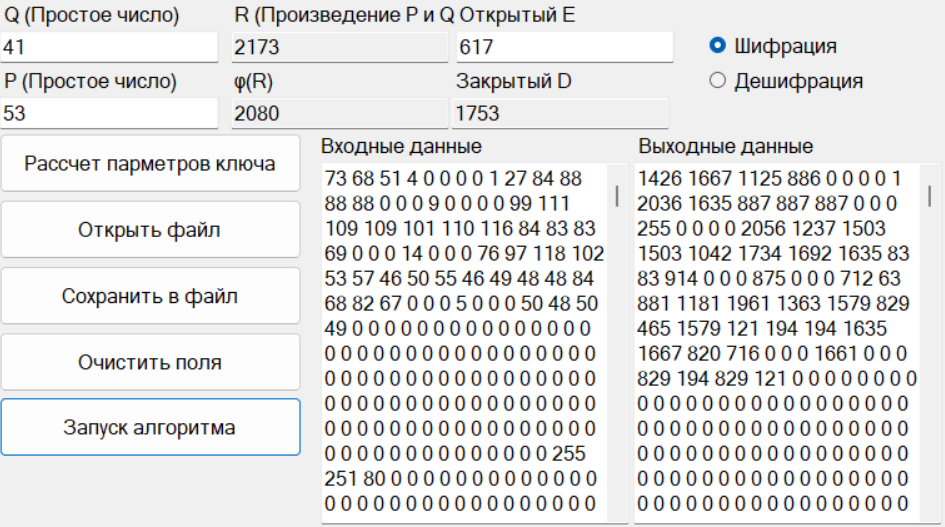


Рисунок 14 – Шифрация. Тест 8

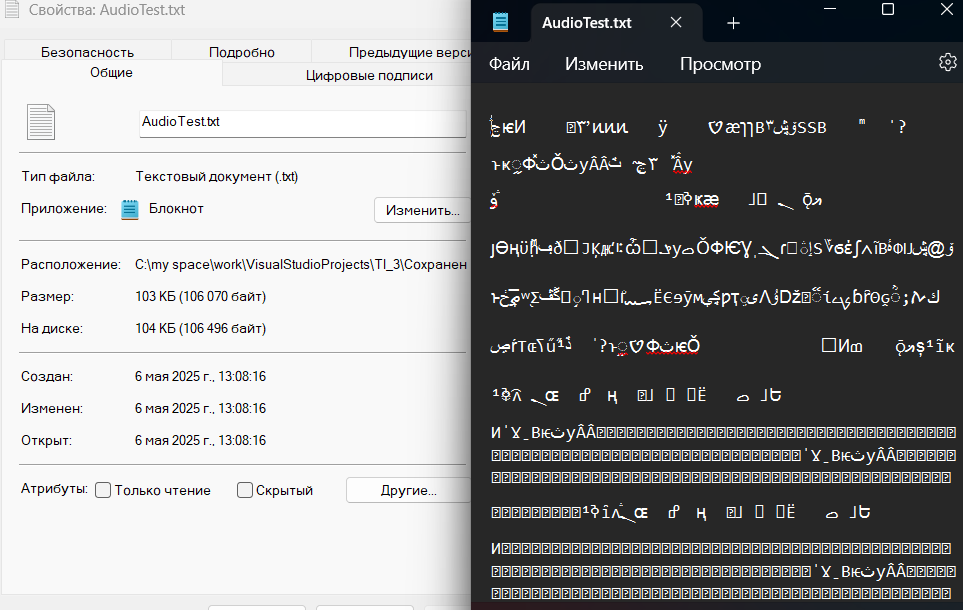


Рисунок 15 – Свойства и содержимое зашифрованного файла. Тест 8

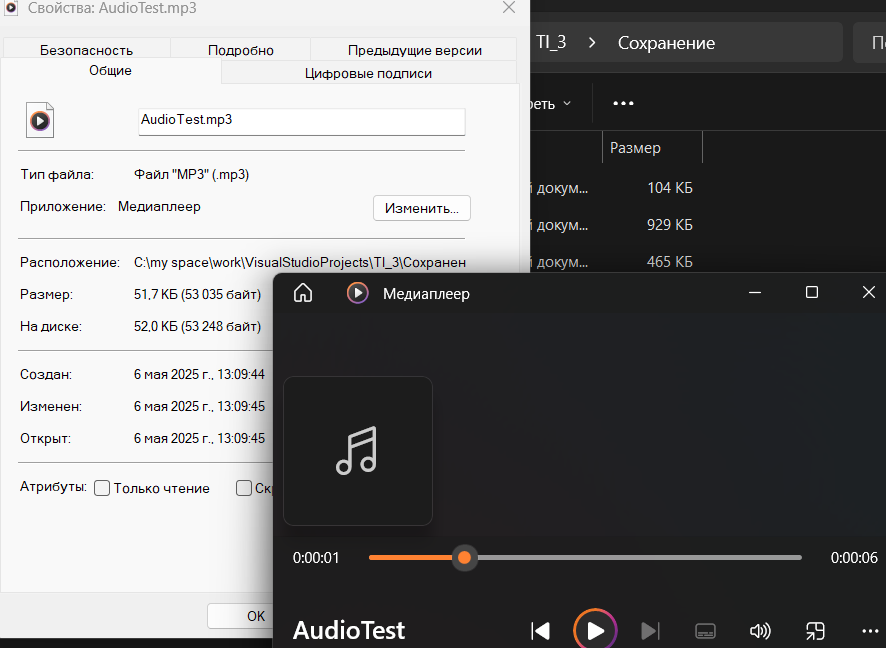


Рисунок 16 – Дешифрация. Тест 8

Тест 9

Тестовая ситуация: Проверка на корректность работы программы для файла формата изображения.

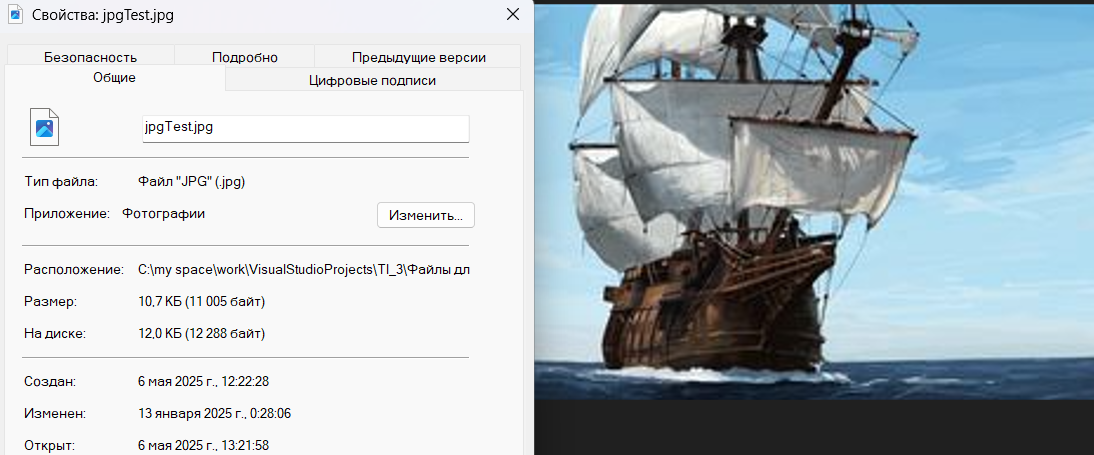
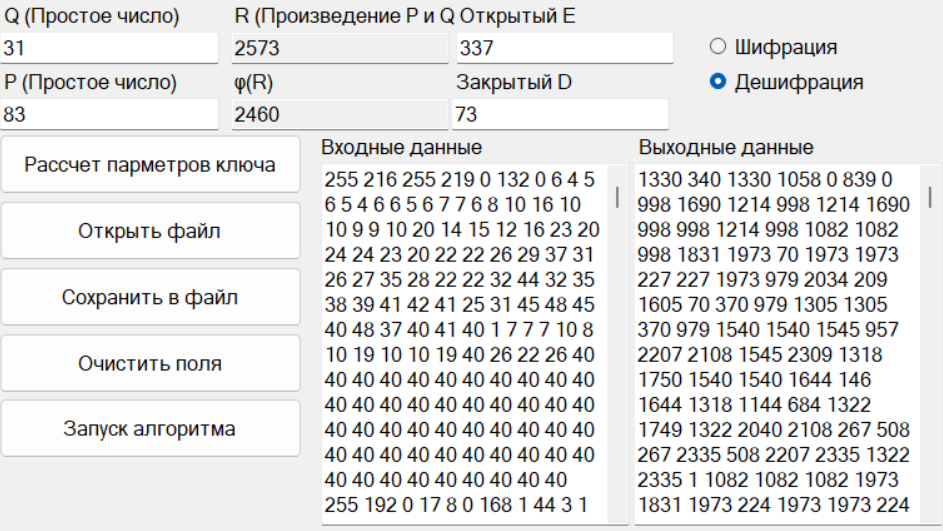


Рисунок 17 – Свойства и содержимое исходного файла. Тест 9



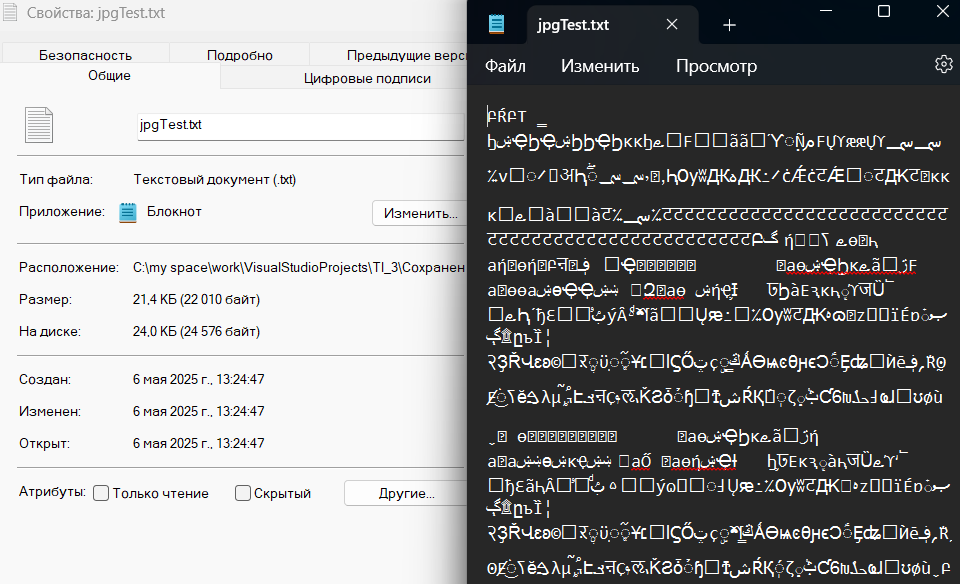


Рисунок 18 – Шифрация. Тест 9

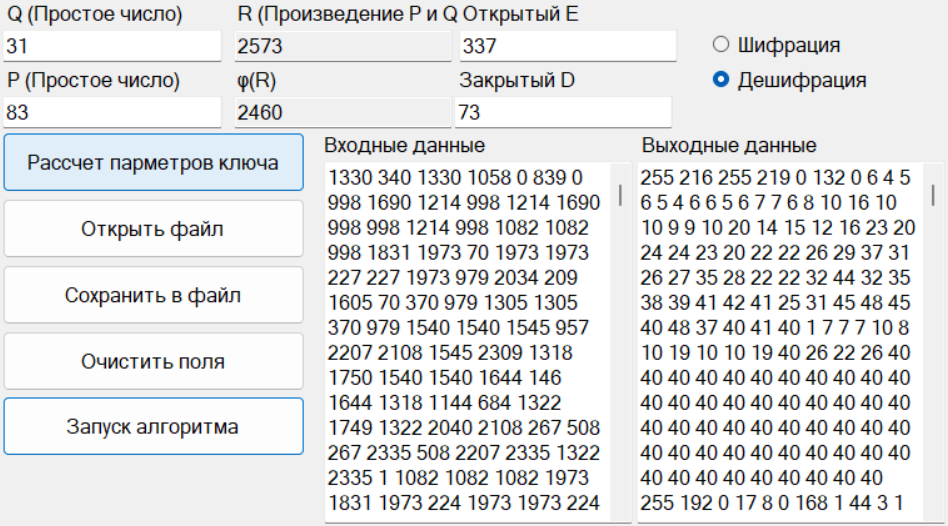


Рисунок 19 – Свойства и содержимое зашифрованного файла. Тест 9

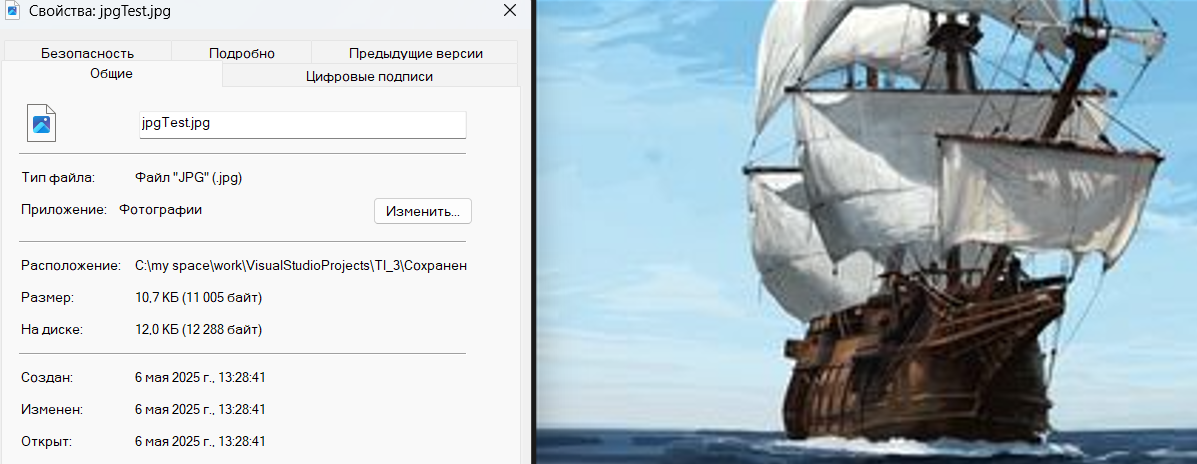


Рисунок 20 – Дешифрация. Тест 9

Тест 10

Тестовая ситуация: проверка на корректность работы программы для файла формата видео.

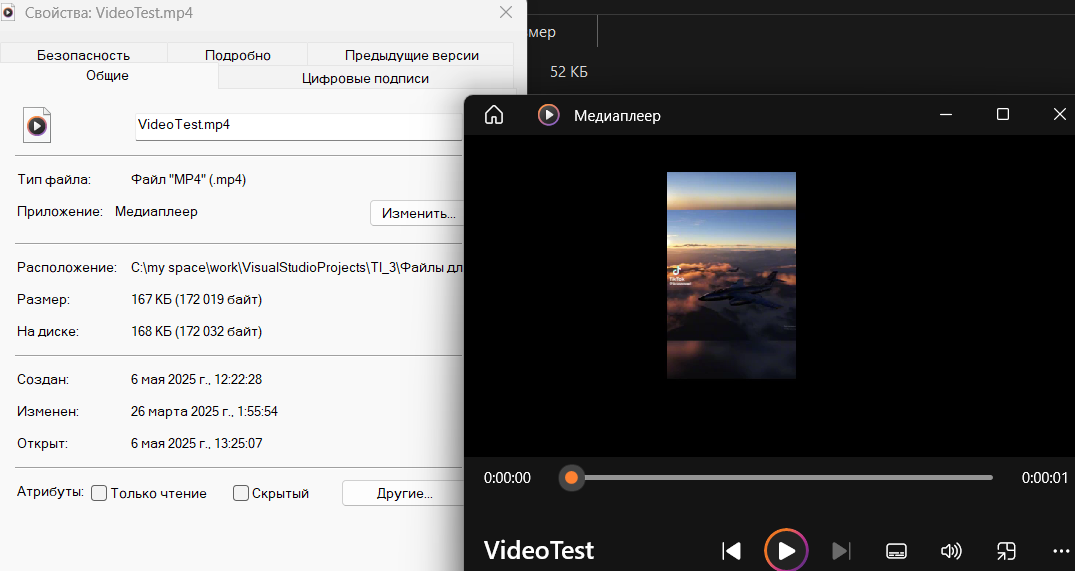
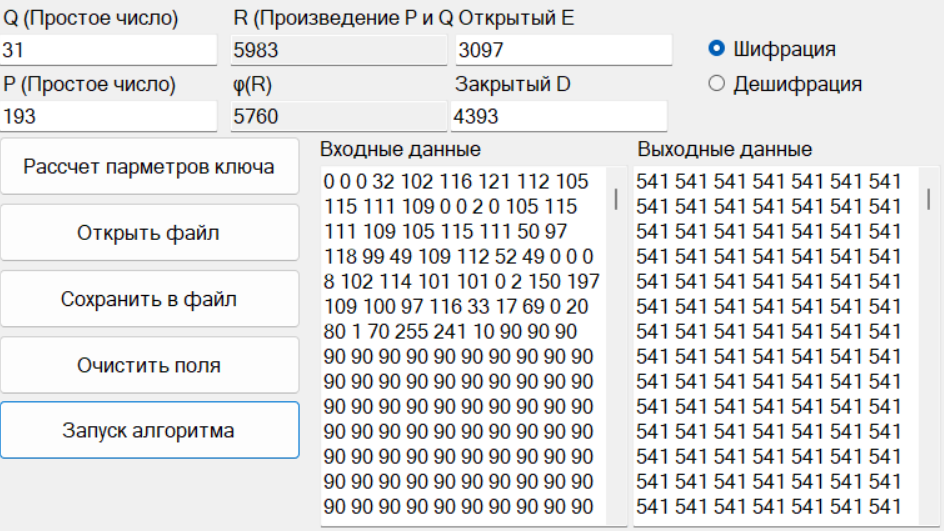


Рисунок 21 – Свойства и содержимое исходного файла. Тест 10



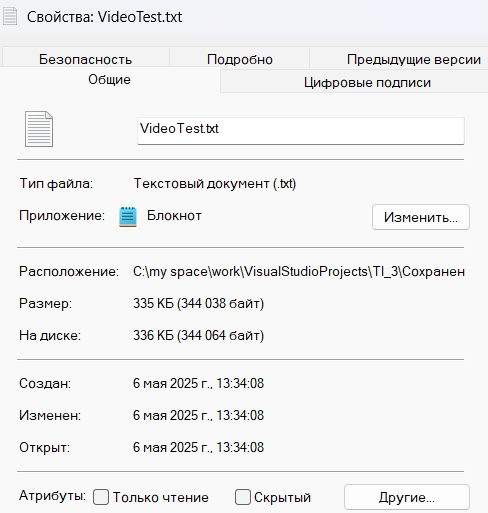
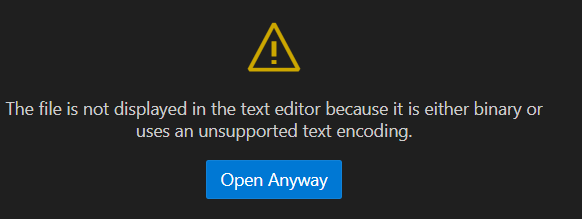


Рисунок 22 – Шифрация. Тест 10



Файл не открывается в текстовом редакторе

Рисунок 23 – Содержимое зашифрованного файла. Тест 10

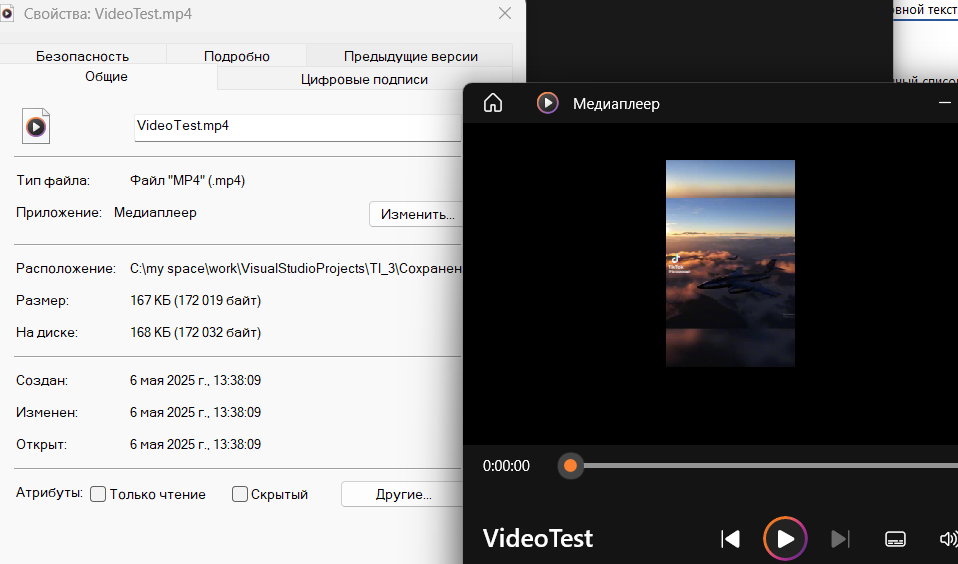
****

Рисунок 26 – Дешифрация. Тест 10

1. Пример работы алгоритма

#### **Работа алгоритма быстрого возведения в степень**

, где – основание степени, – степень, – результат, i – шаги.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | ***i*** |
| 22 | 27 | 1 | 0 |
| 22 | 26 | 1\*22=22 | 1 |
| 22\*22 = 484 mod 47 = 14 | 13 | 22 | 2 |
| 14 | 12 | 14\*22 = 308 mod 47 = 26 | 3 |
| 14\*14 = 196 mod 47 = 8 | 6 | 26 | 4 |
| 8\*8 = 64 mod 47 =17 | 3 | 26 | 5 |
| 17 | 2 | 26 \*17 = 442 mod 47 = 19 | 6 |
| 17\*17 = 289 mod 47 = 7 | 1 | 19 | 7 |
| 7 | 0 | 19\*7 = 133 mod 47 = 39 | 8 |

Ответ:

**Поиска всех первообразных корней при 𝑝 = 43**

Условие для первообразного корня:

(

Пусть Простые делители

**Проверка на первообразность:**

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| gi |  |  |  |
| 1 | - | - | - |
| 2 | 42 | 1 | - |
| 3 | 42 | 36 | 41 |
| 4 | 1 | - | - |
| 5 | 42 | 36 | 16 |
| 6 | 1 | - | - |
| 7 | 42 | 6 | 1 |
| 8 | 42 | 1 | - |
| 9 | 1 | - | - |
| 10 | 1 | - | - |
| 11 | 1 | - | - |
| 12 | 42 | 36 | 21 |
| 13 | 1 | - | - |
| 14 | 1 | - | - |
| 15 | 1 | - | - |

Продолжение таблицы 1

|  |  |  |  |
| --- | --- | --- | --- |
| 16 | 1 | - | - |
| 17 | 1 | - | - |
| 18 | 42 | 6 | 41 |
| 19 | 42 | 36 | 11 |
| 20 | 42 | 36 | 4 |
| 21 | 1 | - | - |
| 22 | 42 | 1 | - |
| 23 | 1 | - | - |
| 24 | 1 | - | - |
| 25 | 1 | - | - |
| 26 | 42 | 6 | 35 |
| 27 | 42 | 1 | - |
| 28 | 42 | 6 | 11 |
| 29 | 42 | 6 | 21 |
| 30 | 42 | 6 | 16 |
| 31 | 1 | - | - |
| 32 | 42 | 1 | - |
| 33 | 42 | 36 | 35 |
| 34 | 42 | 6 | 4 |
| 35 | 1 | - | - |
| 36 | 1 | - | - |
| 37 | 42 | 36 | 1 |
| 38 | 1 | - | - |
| 39 | 42 | 1 | - |
| 40 | 1 | - | - |
| 41 | 1 | - | - |
| 42 | 42 | 1 | - |

Количество первообразных корней должно равняться .

**Множество первообразных: {3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34}**

**Работа расширенного алгоритма Евклида**

Пусть

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| i | q | a0 | a1 | x0 | x1 | y0 | y1 |
| 0 | - | 383 | 647 | 1 | 0 | 0 | 1 |
| 1 | 0 | 647 | 383 | 0 | 1 | 1 | 0 |
| 2 | 1 | 383 | 264 | 1 | -1 | 0 | 1 |
| 3 | 1 | 264 | 119 | -1 | 2 | 1 | -1 |
| 4 | 2 | 119 | 26 | 2 | -5 | -1 | 3 |
| 5 | 4 | 26 | 15 | -5 | 22 | 3 | -13 |
| 6 | 1 | 15 | 11 | 22 | -27 | -13 | 16 |
| 7 | 1 | 11 | 4 | -27 | 49 | 16 | -29 |
| 8 | 2 | 4 | 3 | 49 | -125 | -29 | 74 |
| 9 | 1 | 3 | 1 | -125 | 174 | 74 | -103 |
| 10 | 3 | 1 | 0 | 174 | -647 | -103 | 383 |

**x1 = 174, y1 = -103**

**Ответ: 174 \* 383 + (-103)\* 647= 1**