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

студентка: гр. 351002 Хмель А.А.

Проверила: Болтак С.В.

Минск 2025

Содержание

[1 Задание 3](#_Toc196655616)

[2 Тестовые наборы 4](#_Toc196655617)

[3 Пример работы алгоритма 15](#_Toc196655618)

# Задание

Вариант 2

Реализовать шифратор и дешифратор *алгоритма* ***Эль-Гамаля*** файла c произвольным содержимым, используя алгоритм быстрого возведения в степень, а также реализовать вычисление открытого ключа ***g*** при данном значении ***p***, используя алгоритм нахождения первообразного корня по модулю. Значения параметров ***p*, *x*** и ***k***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-й системе счисления. Вывести значение ***g*** на экран. Результат работы программы – зашифрованный/расшифрованный файл/ы.

Используя алгоритм из методички, искать все первообразные корни по модулю ***p.*** Все найденные корни вывести на экран и предложить для шифрования ввести на выбор любой из найденных.

При использовании длинной арифметики для определения простоты числа использовать один из вероятностных тестов: тест Ферма или тест Миллера-Рабина.

2 Тестовые наборы

Тест 1

Тестовая ситуация: проверка на корректность вводимого числа 𝑝.

Исходные данные: 𝑝 = 35 (не простое число).

Полученный результат: ошибка о том, что число не простое.



Рисунок 1 – Полученный результат. Тест 1

Тест 2

Тестовая ситуация: проверка на корректность вводимого числа 𝑘.

Исходные данные: 𝑝 = 31, 𝑘 =26 (𝑝−1 не взаимно просто с 𝑘).

Полученный результат: ошибка о том, числа не взаимно просты.



Рисунок 2 – Полученный результат. Тест 2

Тест 3

Тестовая ситуация: проверка на корректность выбора 𝑔.

Исходные данные: 𝑝 = 41, 𝑘 =2. Неверный 𝑔 (не первообразный корень).

Полученный результат: ошибка о том, не находится в списке.



Рисунок 3 – Полученный результат. Тест 3

Тест 4

Тестовая ситуация: проверка на корректность работы программы для пустого (имеет нулевую длину) файла или файл не существует.

Полученный результат: ошибка о том, что файл пуст.



Рисунок 4 – Полученный результат. Тест 4

Тест 5

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

Исходные данные:

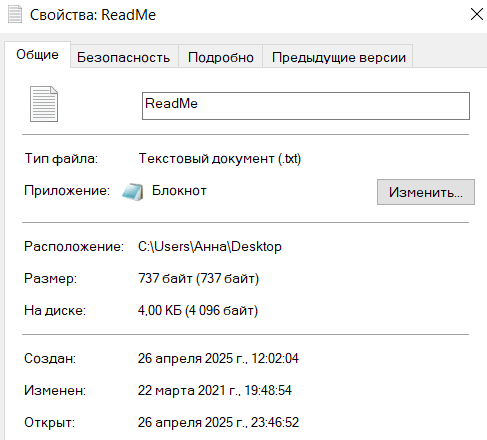
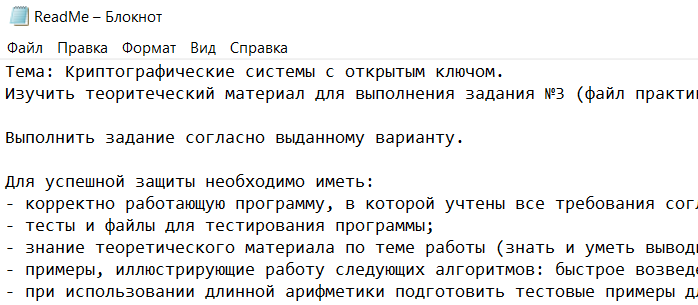
 

Рисунок 5 – Свойства и содержимое исходного файла. Тест 5

**Математическое ограничение криптосистемы Эль-Гамаля - использование простого числа p, которое больше 255 (максимальное значение байта).**

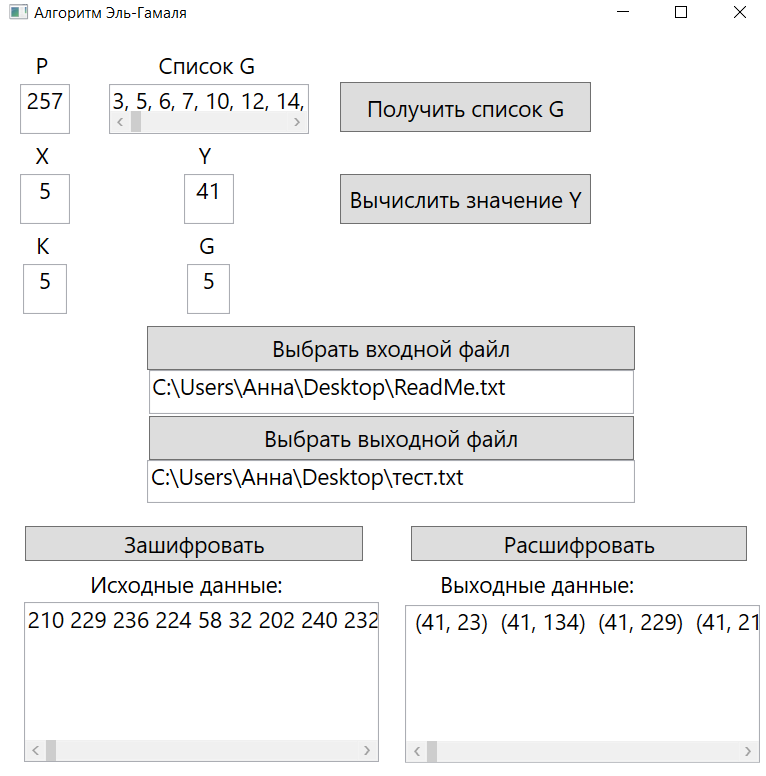


Рисунок 6 – Шифрация. Тест 5

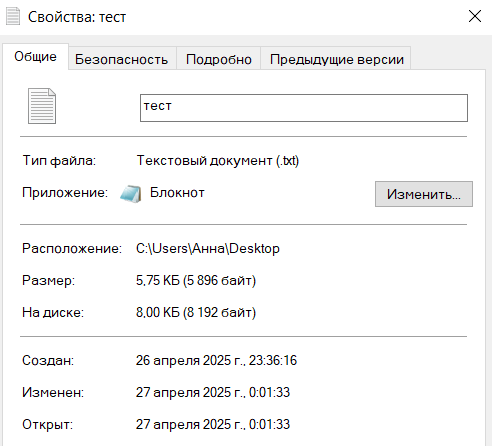
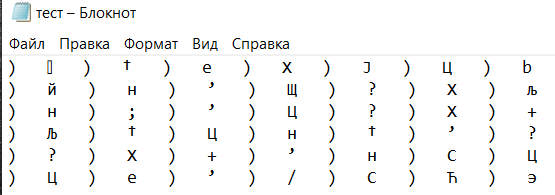
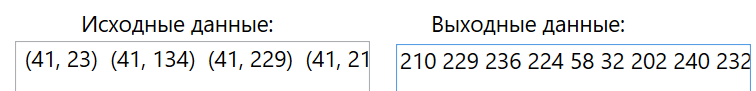
 

Рисунок 7 – Свойства и содержимое зашифрованного файла. Тест 5

**Для шифрования каждый байт преобразуется в два целых числа (a, b), зашифрованный файл должен быть примерно в 8 раз больше исходного (поскольку каждый исходный байт становится двумя 4-байтовыми целыми числами).**



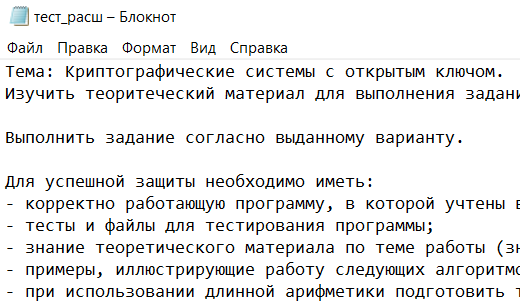


Рисунок 8 – Дешифрация. Тест 5

Тест 6

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

Исходные данные:

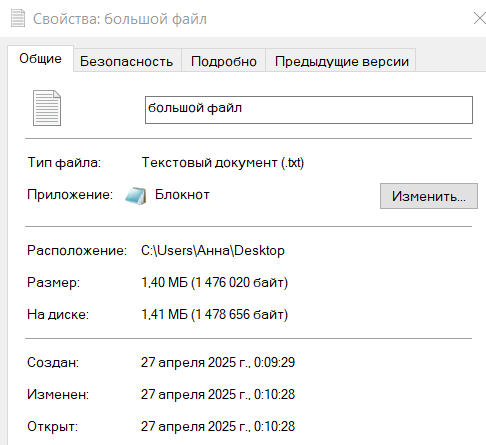
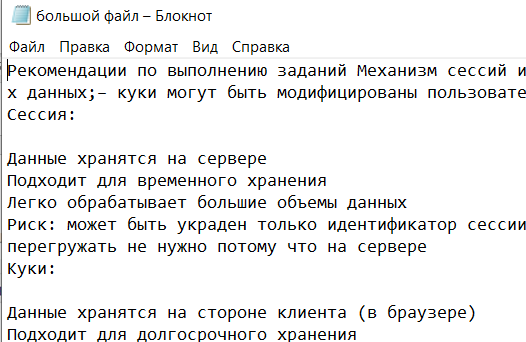
 

Рисунок 9 – Свойства и содержимое исходного файла. Тест 6

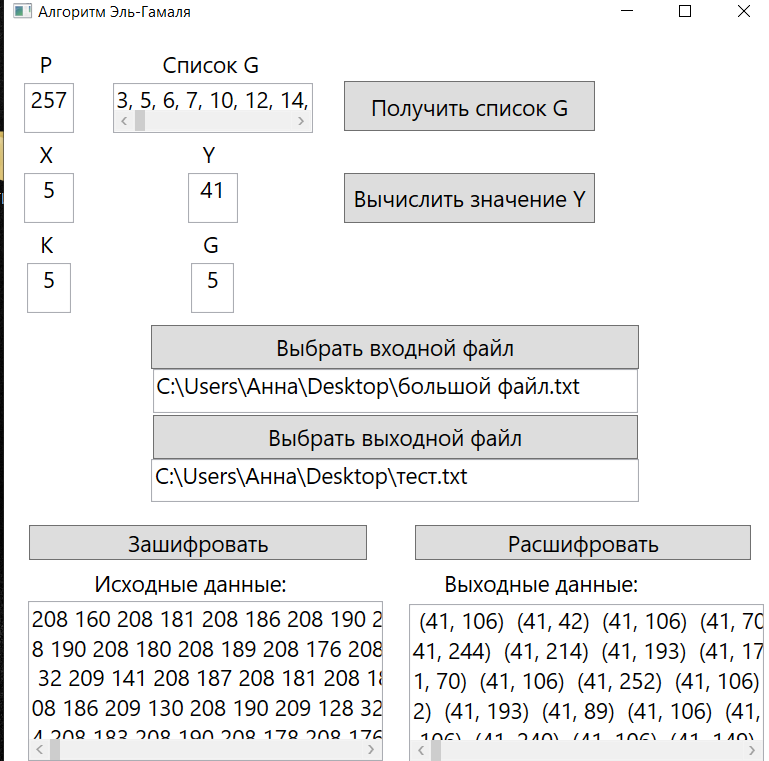


Рисунок 10 – Шифрация. Тест 6

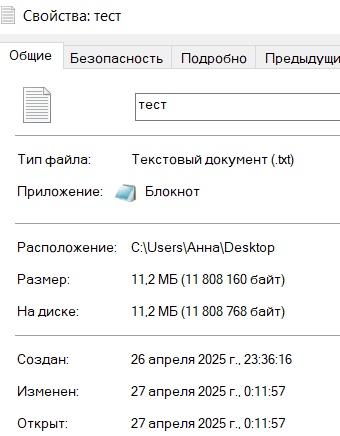
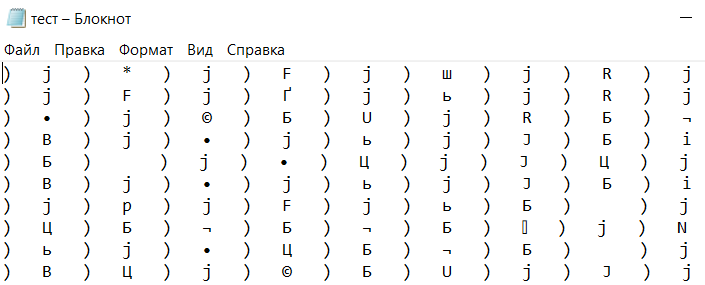
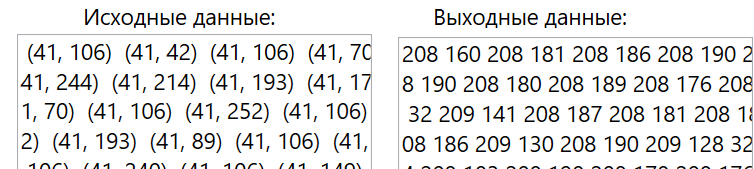
 

Рисунок 11 – Свойства и содержимое зашифрованного файла. Тест 6



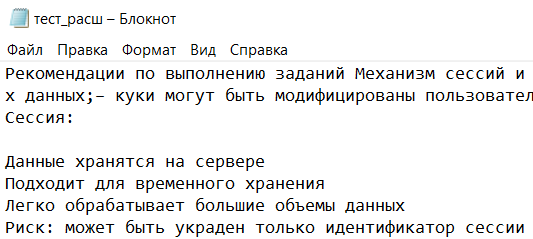


Рисунок 12 – Дешифрация. Тест 6

Тест 7

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



Рисунок 13 – Свойства исходного файла. Тест 7

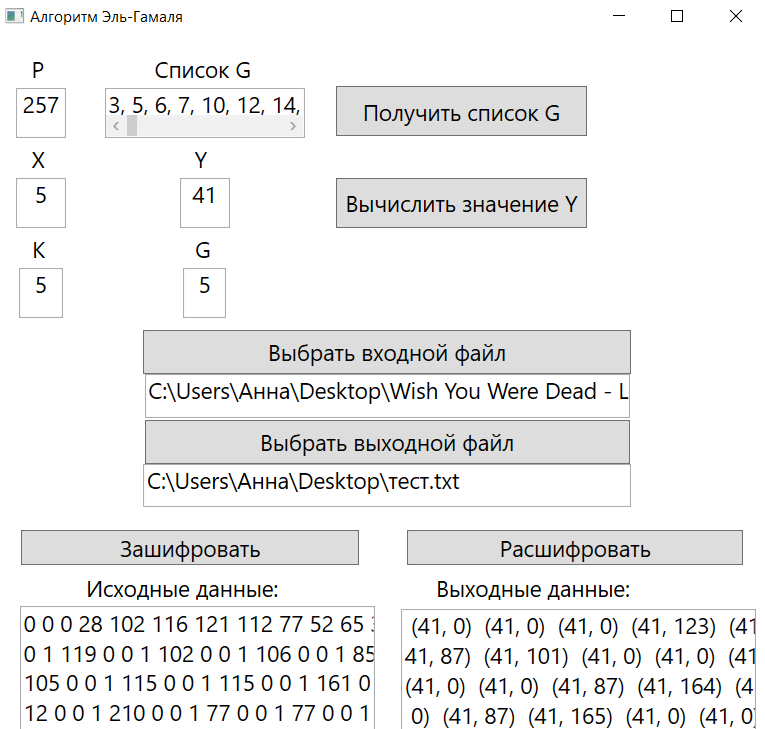


Рисунок 14 – Шифрация. Тест 7

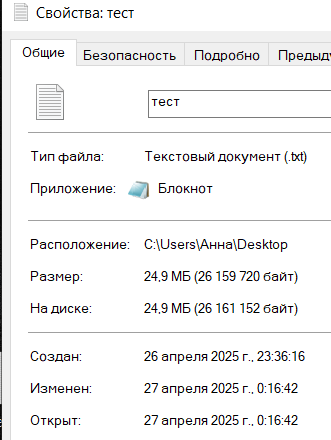
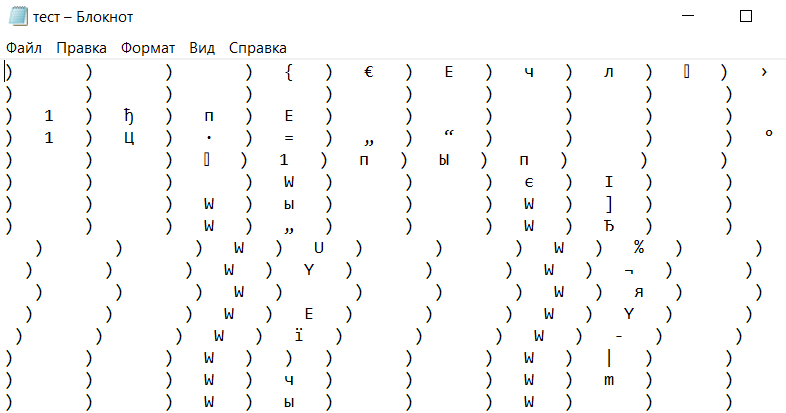
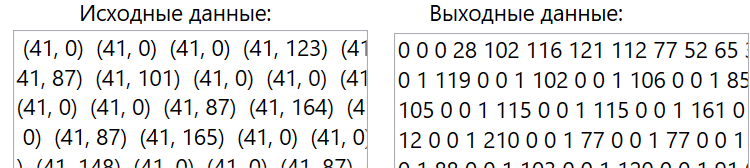
 

Рисунок 15 – Свойства и содержимое зашифрованного файла. Тест 7



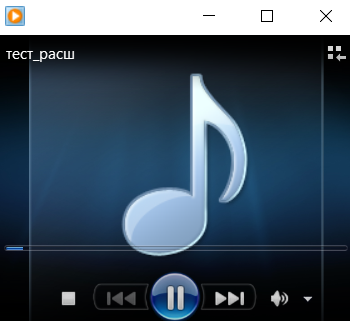


Рисунок 16 – Дешифрация. Тест 7

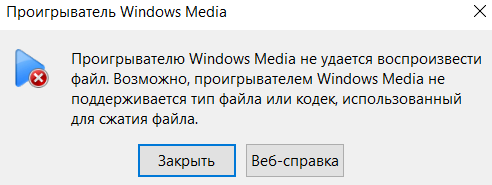


Рисунок 17 – Дешифрация при неправильных вводимых данных. Тест 7

Тест 8

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

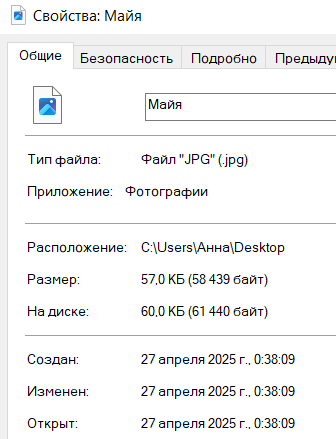
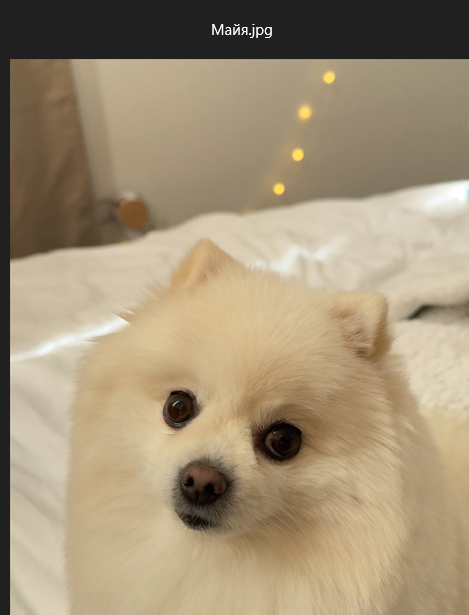
 

Рисунок 18 – Свойства и содержимое исходного файла. Тест 8

Вводимые данные такие же, как и в предыдущих тестах.

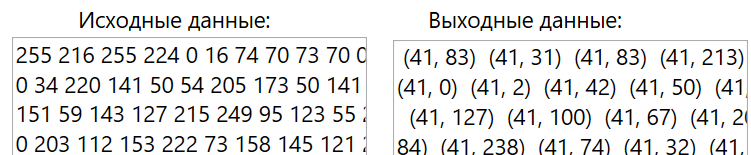


Рисунок 19 – Шифрация. Тест 8

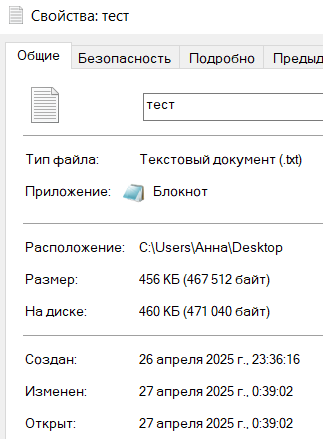
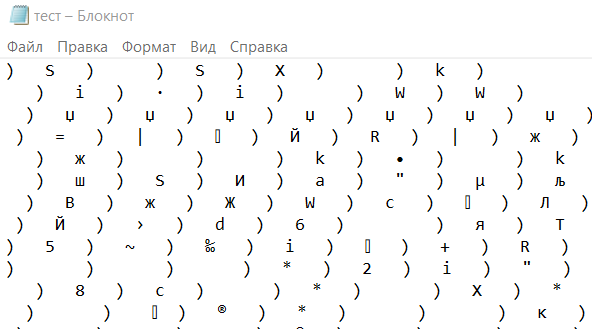
 

Рисунок 20 – Свойства и содержимое зашифрованного файла. Тест 8

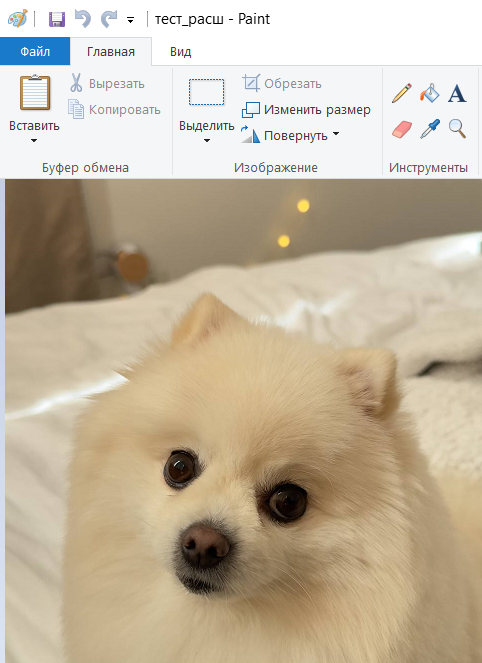
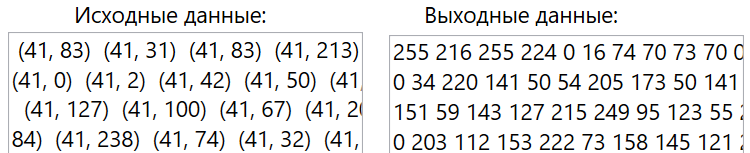


Рисунок 21 – Дешифрация. Тест 8

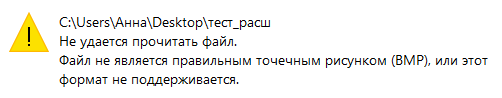


Рисунок 22 – Дешифрация при неправильных вводимых данных. Тест 8

Тест 9

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

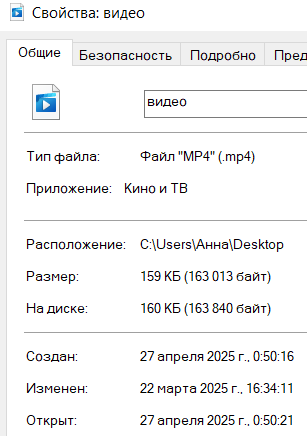
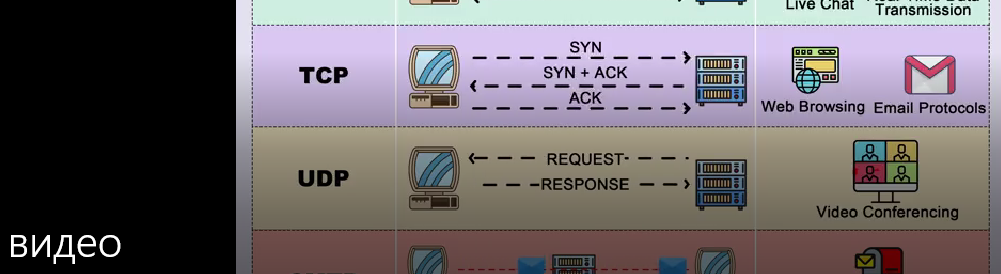
 

Рисунок 23 – Свойства и содержимое исходного файла. Тест 9

Вводимые данные такие же, как и в предыдущих тестах.

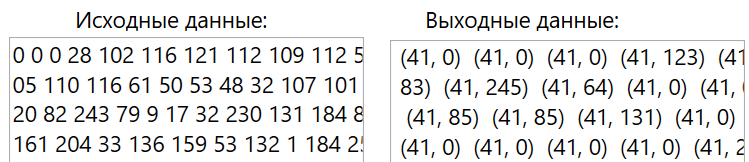


Рисунок 24 – Шифрация. Тест 9

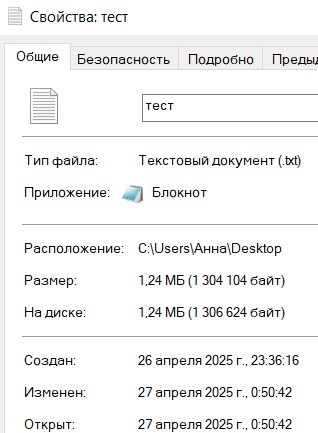
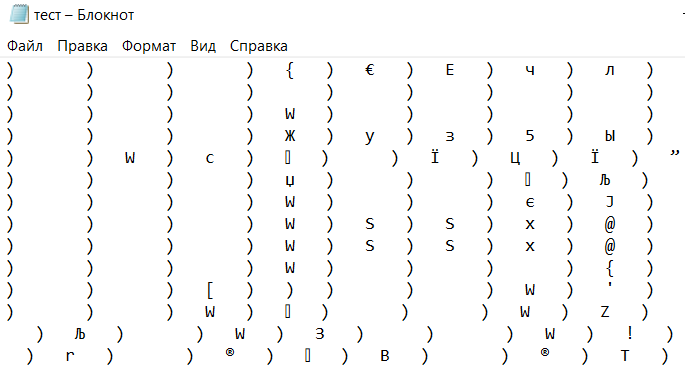
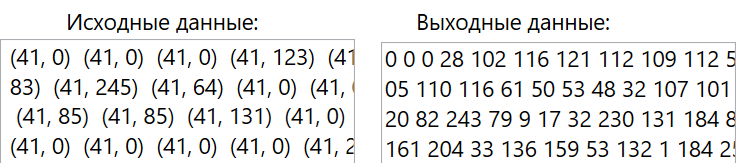
 

Рисунок 25 – Содержимое зашифрованного файла. Тест 9

****

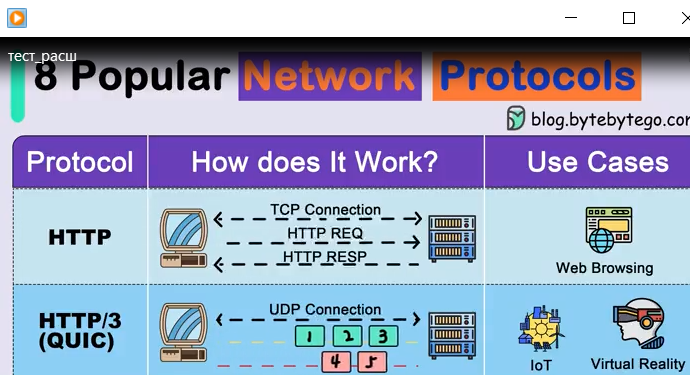
****

Рисунок 26 – Дешифрация. Тест 9

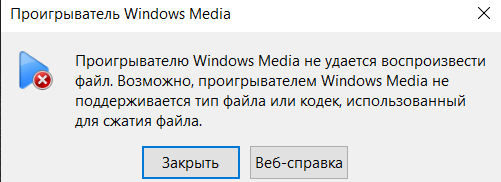
****

Рисунок 27 – Дешифрация при неправильных вводимых данных. Тест 9

3 Пример работы алгоритма

1. **Работа алгоритма быстрого возведения в степень**

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

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | ***i*** |
| 17 | 45 | 1 | 0 |
| 17 | 44 | 1×17=17 | 1 |
|  | 22 | 17 | 2 |
|  | 11 | 17 | 3 |
| 46 | 10 |  | 4 |
|  | 5 | 40 | 5 |
| 49 | 4 |  | 6 |
|  | 2 | 52 | 7 |
|  | 1 | 52 | 8 |
| 44 | 0 |  | 9 |

1. **Поиска всех первообразных корней при 𝑝 = 61**

Условие для первообразного корня:

(

Пусть Простые делители

**Проверка на первообразность**

|  |  |  |  |
| --- | --- | --- | --- |
| gi |  |  |  |
| 1 | *–* | *–* | *–* |
| **2** | **60** | **47** | **9** |
| 3 | 1 | *–* | *–* |
| 4 | 1 | *–* | *–* |
| 5 | 1 | *–* | *–* |
| **6** | **60** | **47** | **20** |
| **7** | **60** | **47** | **34** |
| 8 | 60 | 1 | *–* |
| 9 | 1 | *–* | *–* |
| **10** | **60** | **13** | **58** |
| 11 | 60 | 1 | *–* |
| 12 | 1 | *–* | *–* |
| 13 | 1 | *–* | *–* |
| 14 | 1 | *–* | *–* |
| 15 | 1 | *–* | *–* |
| 16 | 1 | *–* | *–* |
| **17** | **60** | **13** | **20** |
| **18** | **60** | **47** | **58** |
| 19 | 1 | *–* | *–* |
| 20 | 1 | *–* | *–* |
| 21 | 60 | 47 | 1 |
| 22 | 1 | *–* | *–* |
| 23 | 60 | 1 | *–* |
| 24 | 60 | 1 | *–* |
| 25 | 1 | *–* | *–* |
| **26** | **60** | **13** | **9** |
| 27 | 1 | *–* | *–* |
| 28 | 60 | 1 | *–* |
| 29 | 60 | 13 | 1 |
| **30** | **60** | **13** | **34** |
| **31** | **60** | **13** | **34** |
| 32 | 60 | 13 | 1 |
| 33 | 60 | 1 | *–* |
| 34 | 1 | *–* | *–* |
| **35** | **60** | **13** | **9** |
| 36 | 1 | *–* | *–* |
| 37 | 60 | 1 | *–* |
| 38 | 60 | 1 | *–* |
| 39 | 1 | *–* | *–* |
| 40 | 60 | 47 | 1 |
| 41 | 1 | *–* | *–* |
| 42 | 1 | *–* | *–* |
| **43** | **60** | **47** | **58** |
| **44** | **60** | **13** | **20** |
| 45 | 1 | *–* | *–* |
| 46 | 1 | *–* | *–* |
| 47 | 1 | *–* | *–* |
| 48 | 1 | *–* | *–* |
| 49 | 1 | *–* | *–* |
| 50 | 60 | 1 | *–* |
| **51** | **60** | **13** | **58** |
| 52 | 1 | *–* | *–* |
| 53 | 60 | 1 | *–* |
| **54** | **60** | **47** | **34** |
| **55** | **60** | **47** | **20** |
| 56 | 1 | *–* | *–* |
| 57 | 1 | *–* | *–* |
| 58 | 1 | *–* | *–* |
| **59** | **60** | **47** | **9** |
| 60 | 1 | *–* | *–* |

Количество первообразных корней должно равняться .

**Множество первообразных корней для**

1. **Работа расширенного алгоритма Евклида**

Пусть

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **i** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 256 | 713 | 1 | 0 | 0 | 1 |
| 1 | 0 | 713 | 256 | 0 | 1 | 1 | 0 |
| 2 | 2 | 256 | 201 | 1 | -2 | 0 | 1 |
| 3 | 1 | 201 | 55 | -2 | 3 | 1 | -1 |
| 4 | 3 | 55 | 36 | 3 | -11 | -1 | 4 |
| 5 | 1 | 36 | 19 | -11 | 14 | 4 | -5 |
| 6 | 1 | 19 | 17 | 14 | -25 | -5 | 9 |
| 7 | 1 | 17 | 2 | -25 | 39 | 9 | -14 |
| 8 | 8 | 2 | 1 | 39 | -337 | -14 | 121 |
| 9 | 2 | 1 | 0 | -337 | 713 | 121 | -256 |

**x1 = -337, y1 = 121**

**-337 \* 256+ 121\* 713= 1**