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 №2

Тема работы:

Потоковое шифрование

Выполнила

студент: гр. 351002 Яночкин И.Л.

Проверил: Болтак С.В.

Минск 2025

Тестовые наборы для метода потокового шифрования с помощью LFSR

Тест 1

Тестовая ситуация: проверка на корректность длины ключа.

Полученный результат: предупреждение о том, что регистр не заполнен.

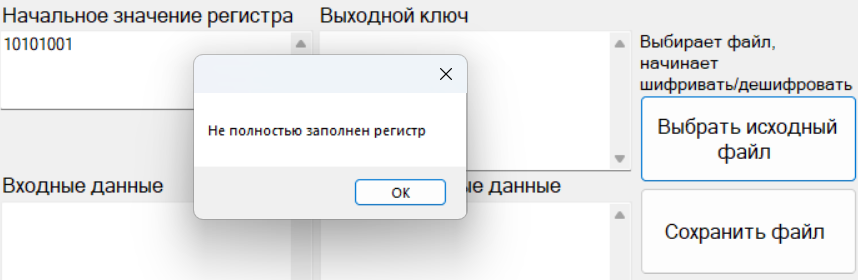


Рисунок 1 – Полученный результат. Тест 1

Тест 2

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

Полученный результат: пустой ключ, пустые входные и выходные данные.

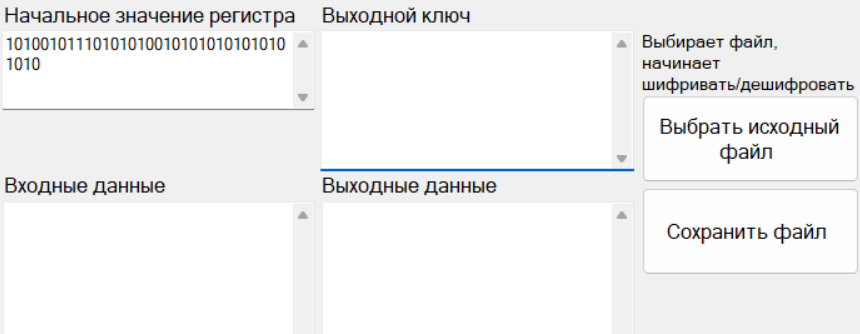


Рисунок 2 – Полученный результат. Тест 2

Тест 3

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

Исходные данные:

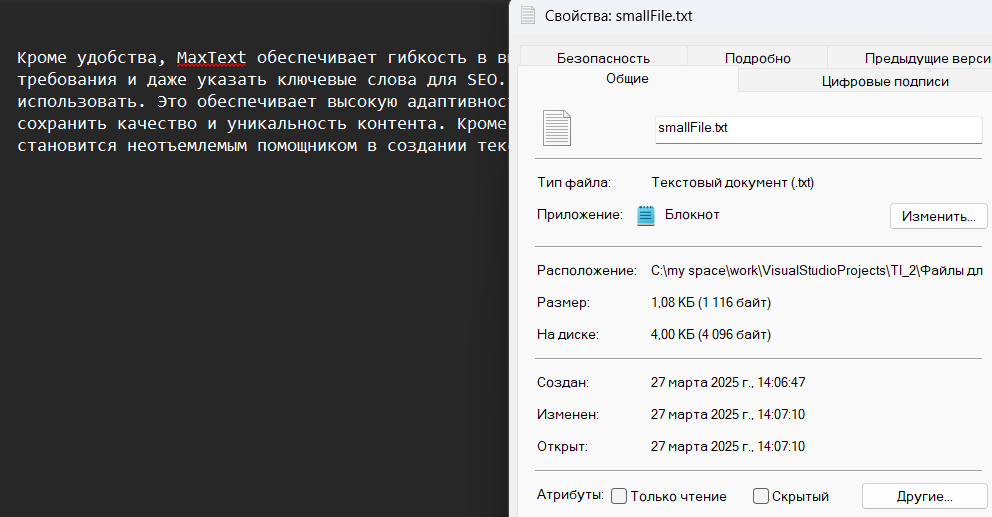


Рисунок 3 – Свойства и содержимое исходного файла. Тест 3

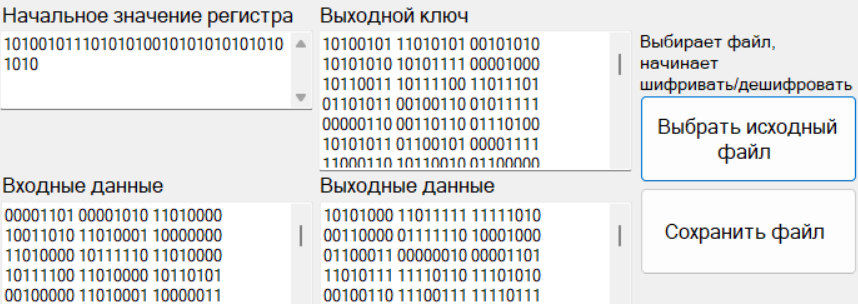


Рисунок 4 – Шифрация. Тест 3

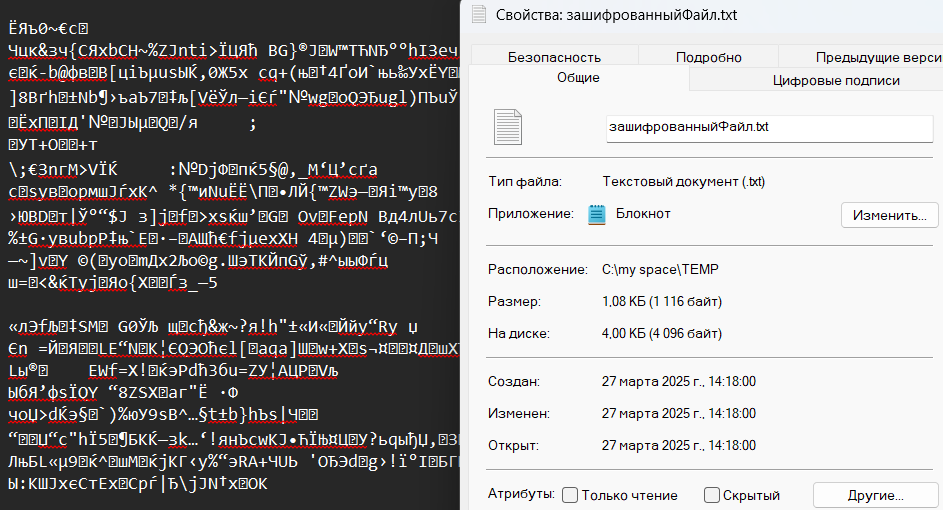


Рисунок 5 – Свойства и содержимое зашифрованного файла. Тест 3

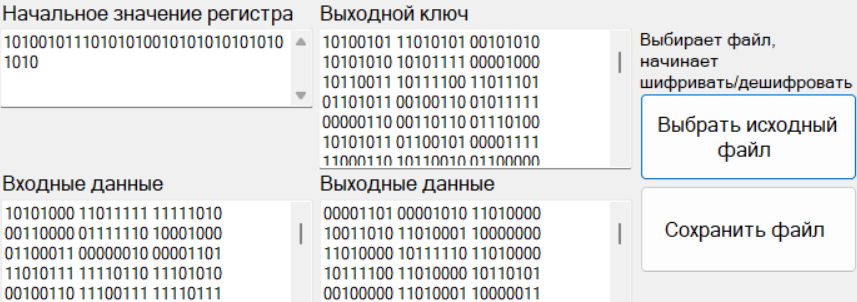


Рисунок 6 – Дешифрация. Тест 3

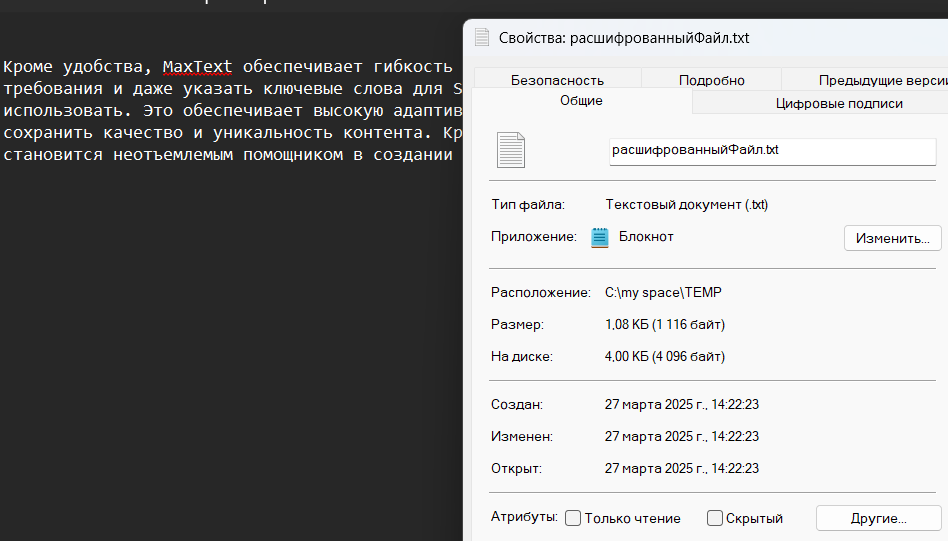


Рисунок 7 – Свойства и содержимое расшифрованного файла. Тест 3

Тест 4

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

Исходные данные:

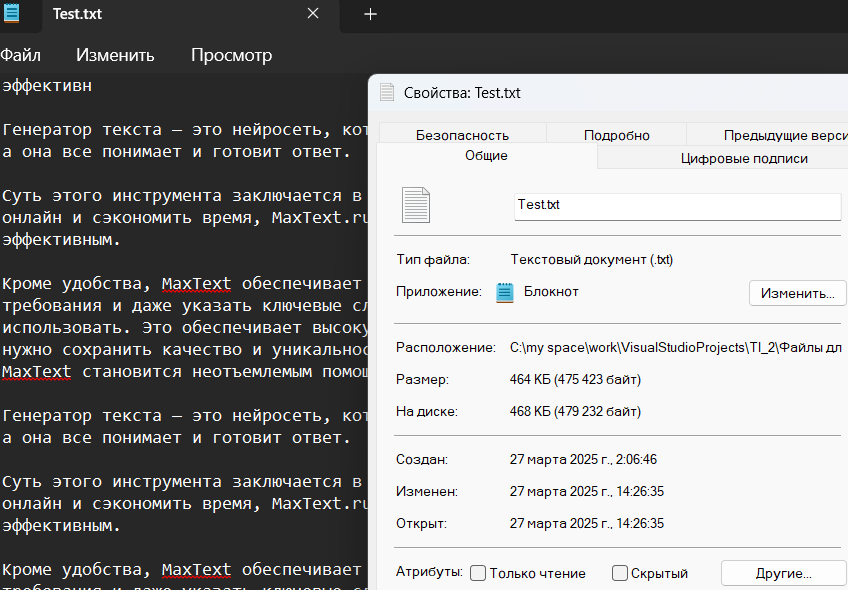


Рисунок 8 – Свойства и содержимое исходного файла. Тест 4

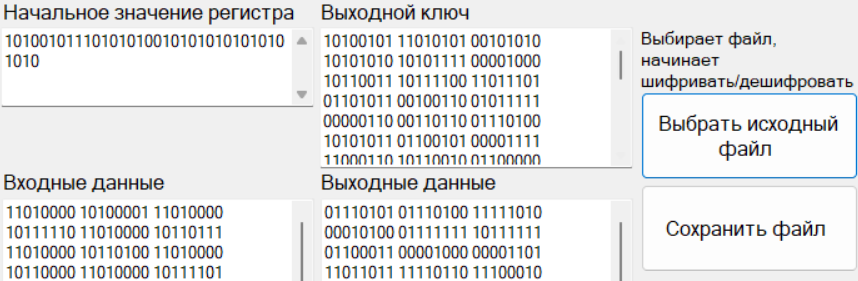


Рисунок 9 – Шифрация. Тест 4

Сохраним файл в формат txt для просмотра результата зашифрованных байтов. В файле будут только первые 30 и последние 30 байтов для ускорения работы, так как файл считается большим.

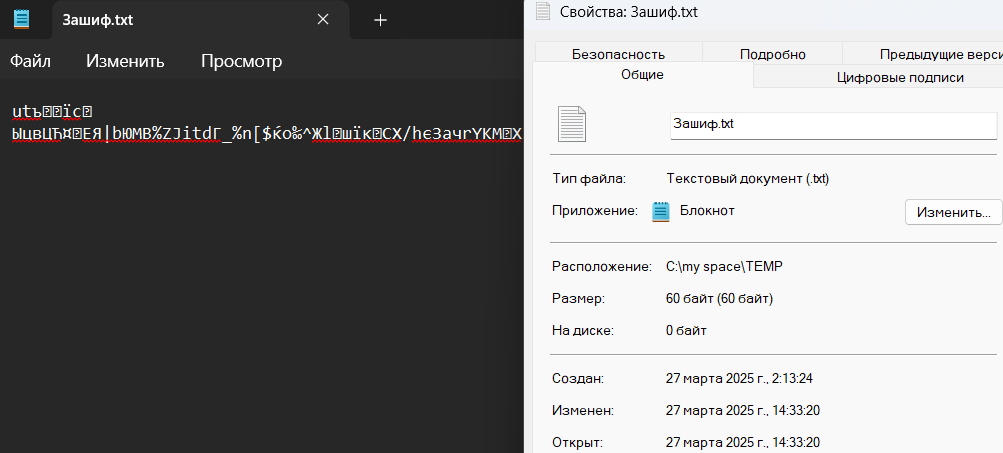


Рисунок 10 – Свойства и содержимое зашифрованного файла. Тест 4

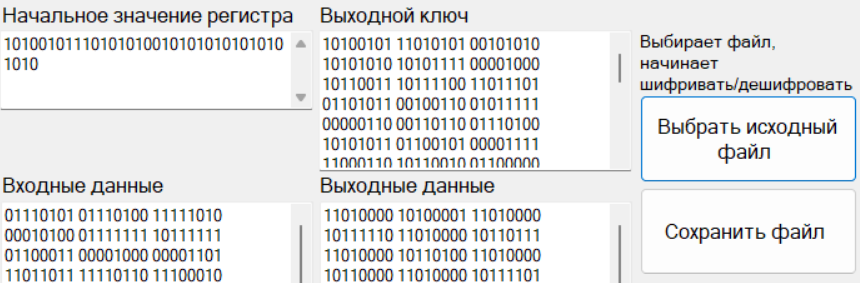


Рисунок 11 – Дешифрация. Тест 4

Тест 5

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

Исходные данные:

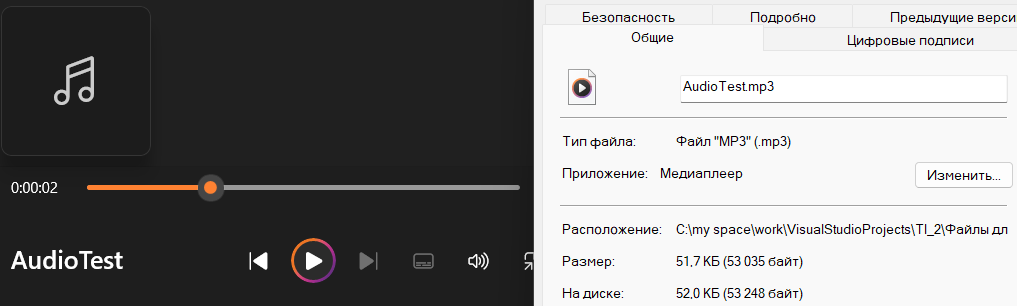


Рисунок 12 – Свойства и содержимое зашифрованного файла. Тест 5

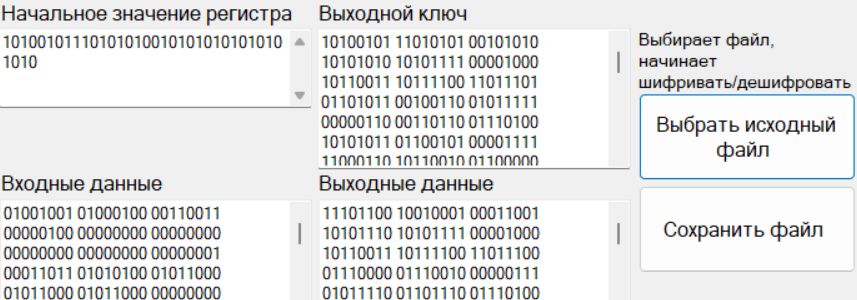


Рисунок 13 – Шифрация. Тест 5

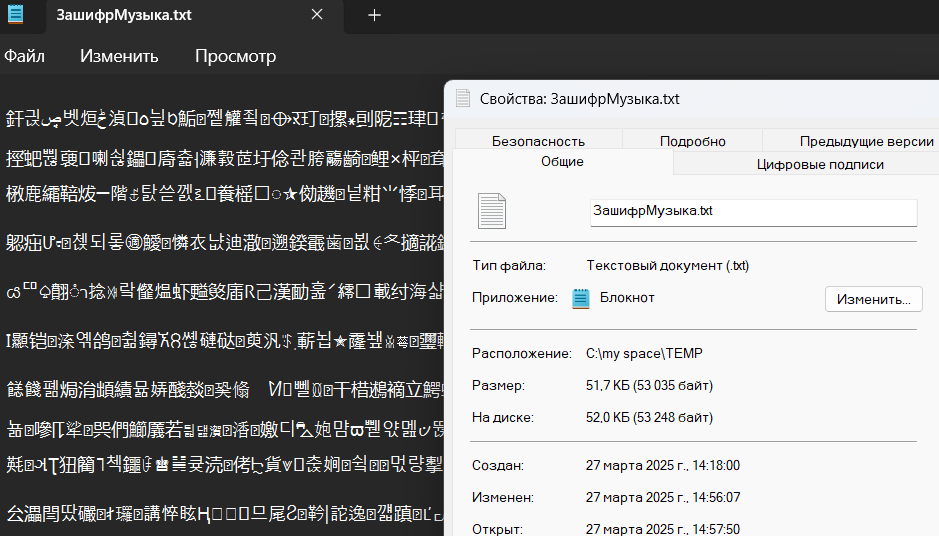


Рисунок 14 – Содержимое и свойства зашифрованного файла. Тест 5

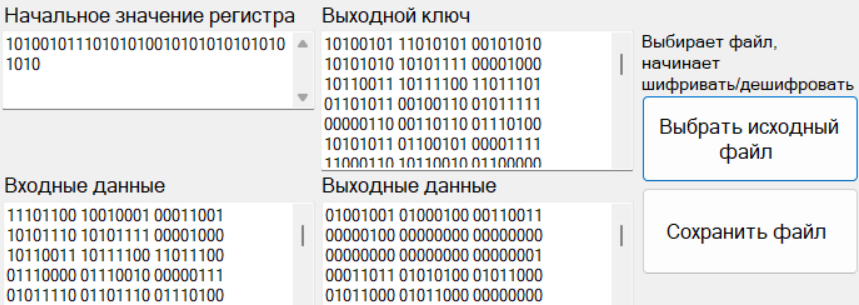


Рисунок 15 – Дешифрация. Тест 5

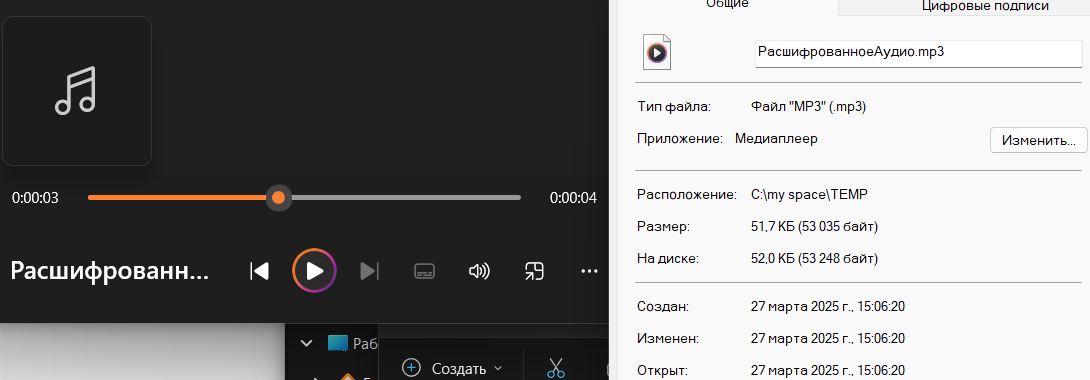


Рисунок 16 – Содержимое и свойства расшифрованного файла. Тест 5

Тест 6

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

Исходные данные:

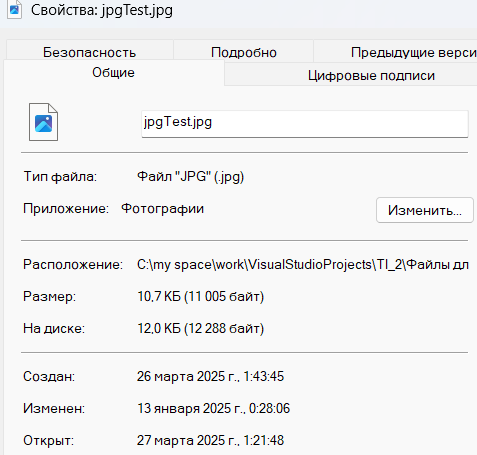
 

Рисунок 17 – Свойства и содержимое исходного файла. Тест 6

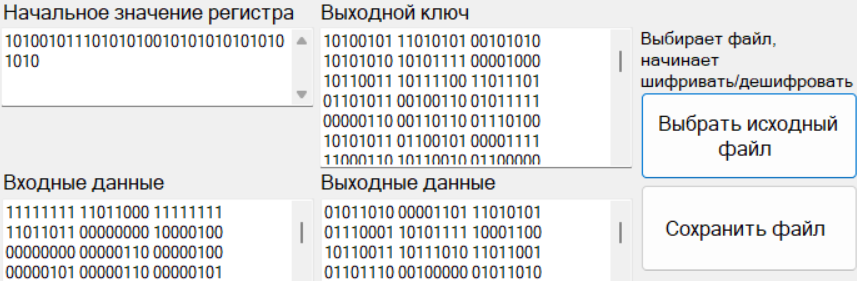


Рисунок 18 – Шифрация. Тест 6

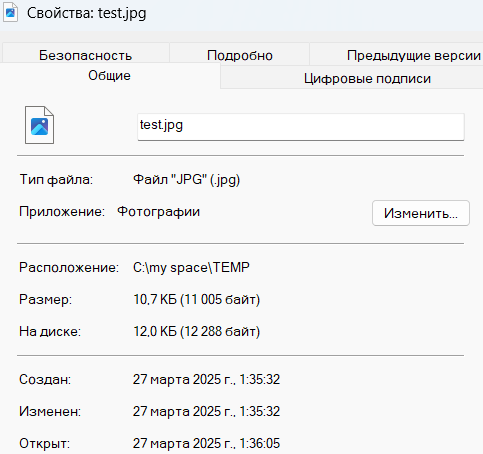
**Содержимое не открывается**

Рисунок 19 – Свойства и содержимое зашифрованного файла. Тест 6

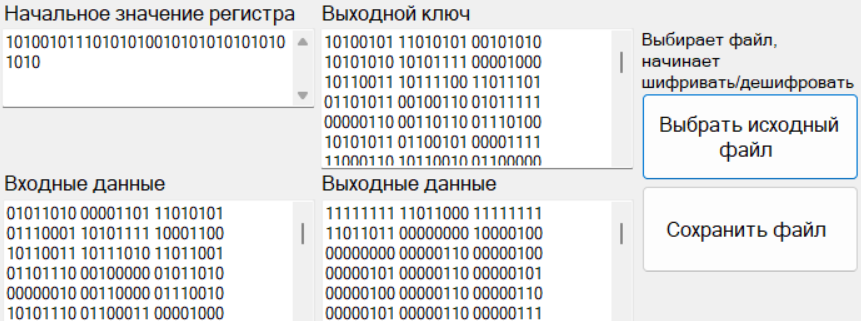


Рисунок 20 – Дешифрация. Тест 6

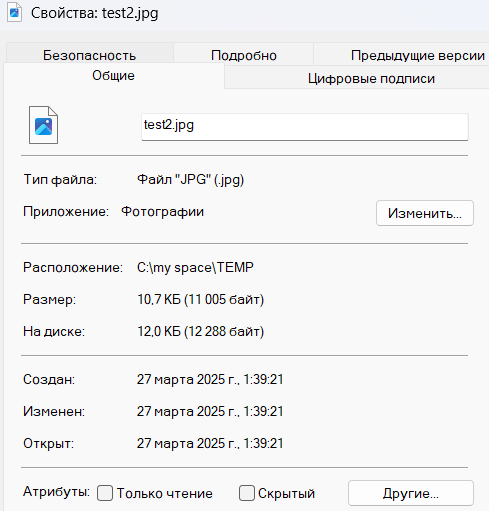


Рисунок 21 – Свойства и содержимое файла после дешифрации. Тест 6

Тест 7

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

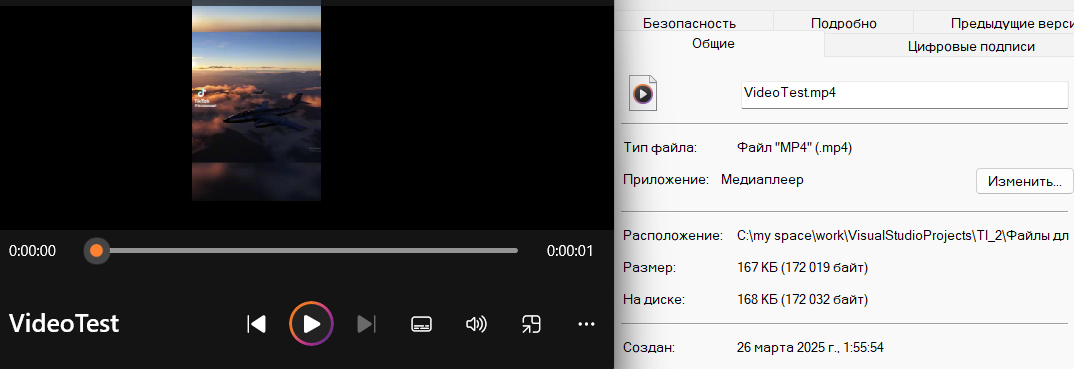
Исходные данные:

Рисунок 22 – Свойства и содержимое исходного файла. Тест 7

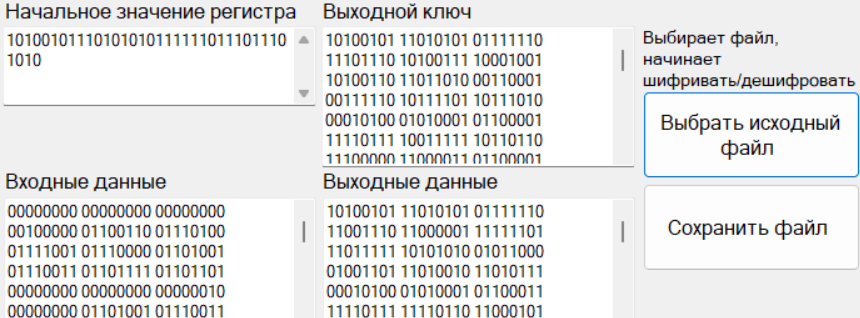


Рисунок 23 – Шифрация. Тест 7

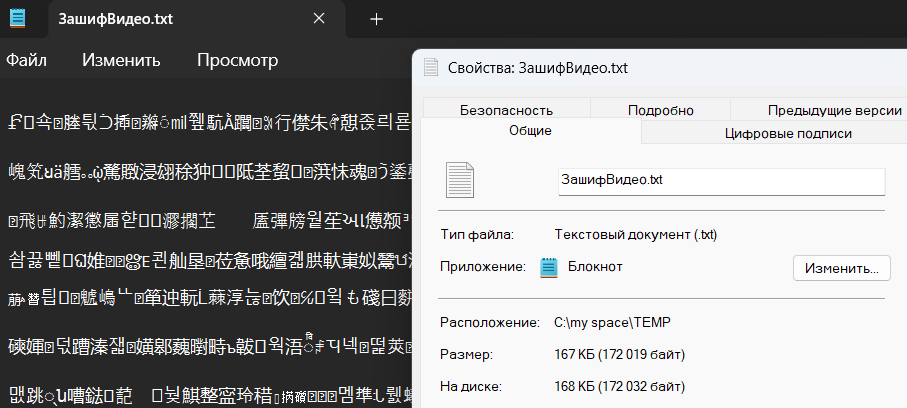


Рисунок 24 – Содержимое зашифрованного файла. Тест 7

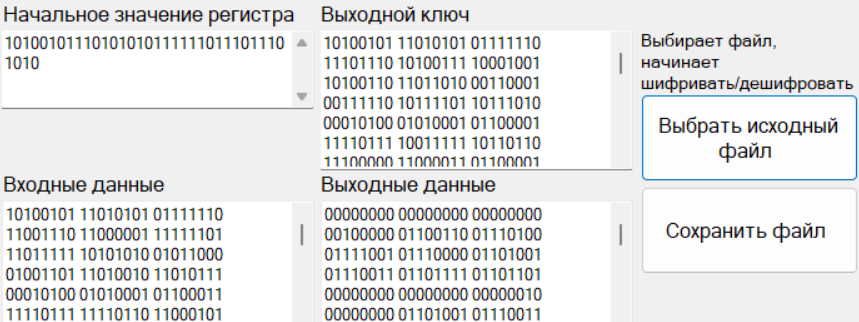
****

Рисунок 25 – Дешифрация. Тест 7

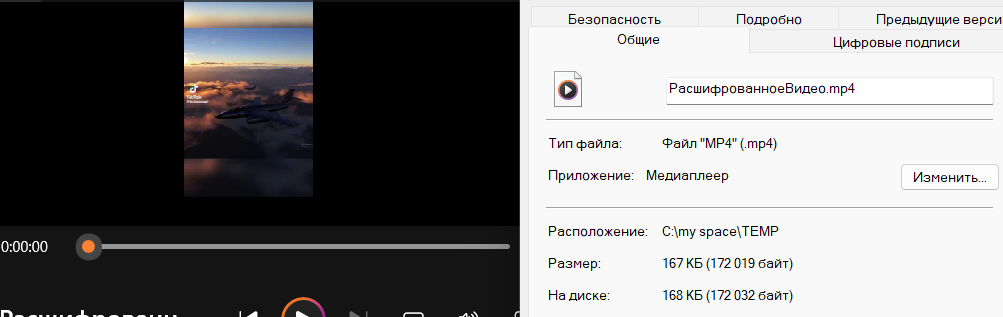
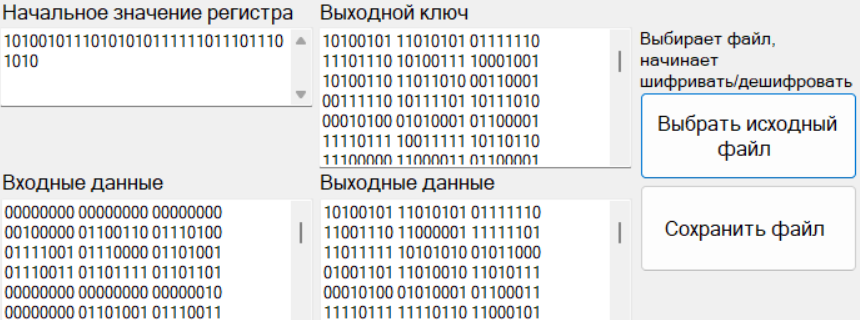
****

Рисунок 26 – Свойства и содержание полученного результата. Тест 7

Тест 8

Тестовая ситуация: проверка на корректность работы программы для файла формата видео, сохранение зашифрованного файла в формате видео.

Исходные данные: см. Тест 7

****

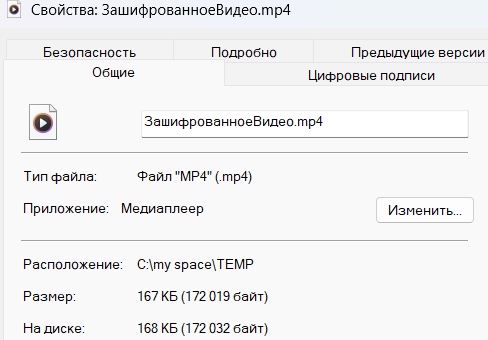
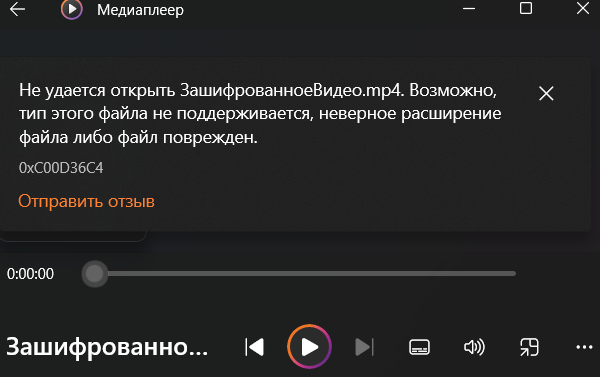
****

Рисунок 27 –Полученный результат. Тест 8

Тест 9

Тестовая ситуация: проверка на корректность работы программы для

относительно большоого файла, содержащего только нули.

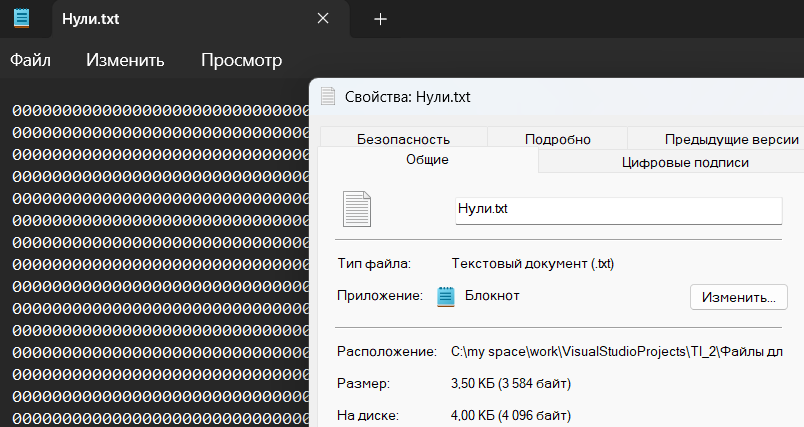


Рисунок 28 – Содержимое исходного файла. Тест 9

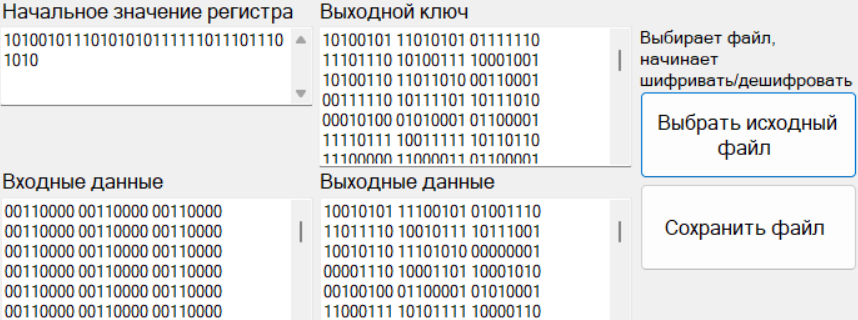


Рисунок 29 – Шифрация. Тест 9

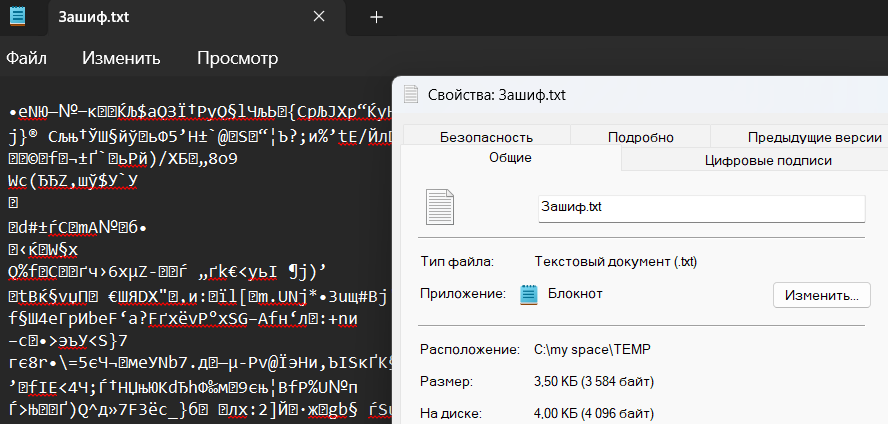


Рисунок 30 – Содержимое зашифрованного файла. Тест 9

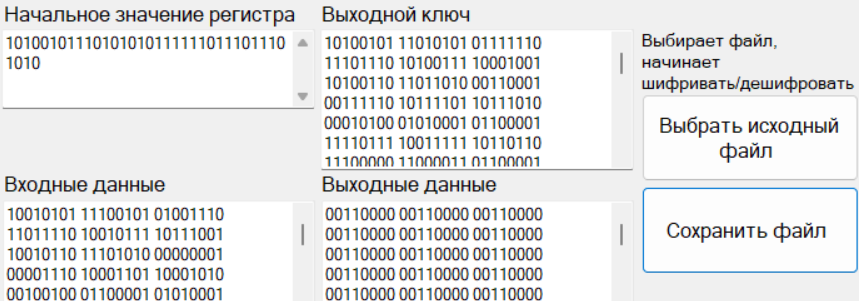


Рисунок 29 – Дешифрация. Тест 9

Тест 10

Тестовая ситуация: проверка на корректность работы программы для

относительно большоого файла, содержащего только нули и регистра содержащего только нули.

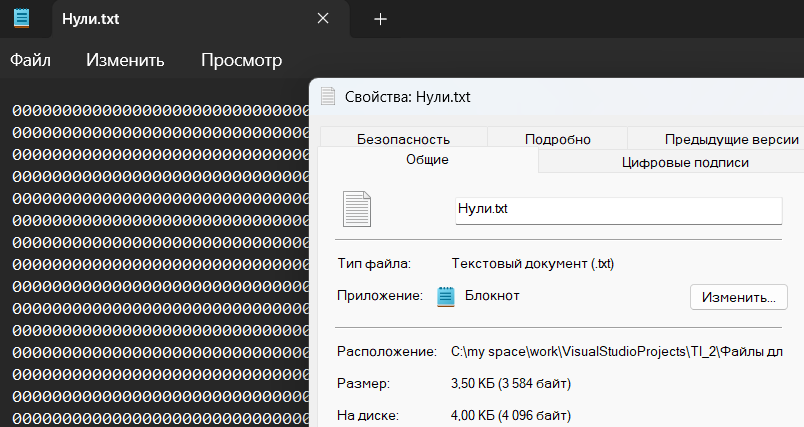


Рисунок 28 – Содержимое и свойства исходного файла. Тест 10

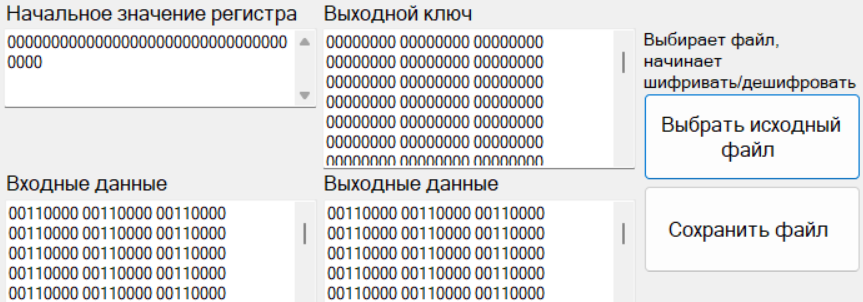


Рисунок 29 – Шифрация. Тест 10

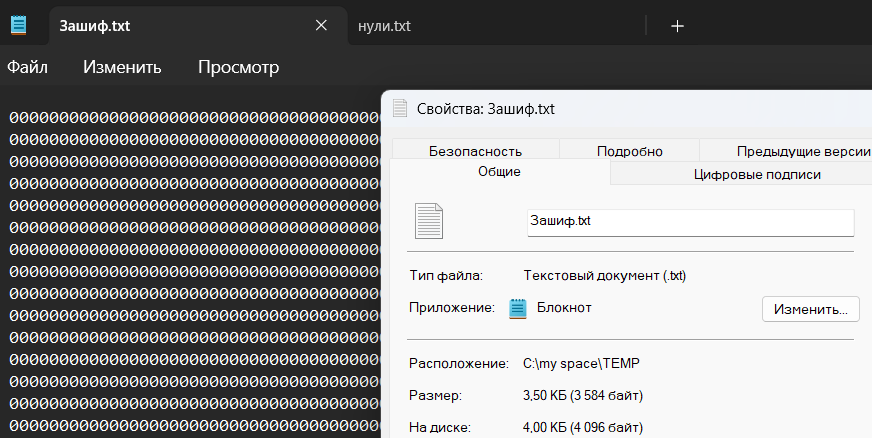


Рисунок 30 – Содержимое зашифрованного файла. Тест 10

Тест 11

Тестовая ситуация: проверка на корректность работы программы для файла, содержащего только единицы и регистра содержащего только единицы.

Исходные данные:

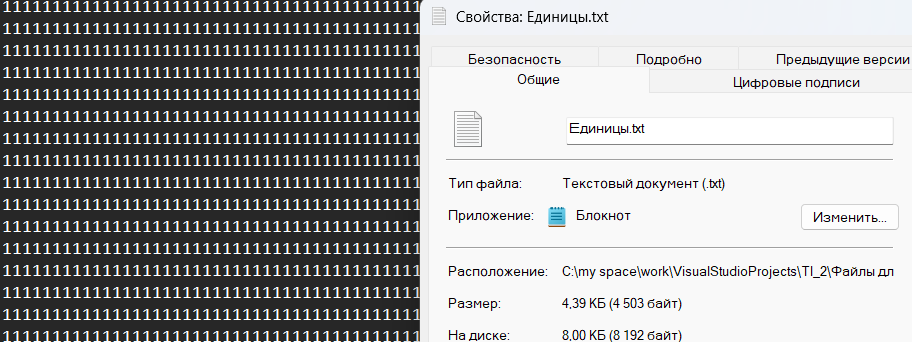


Рисунок 31 – Содержимое и свойства исходного файла. Тест 11

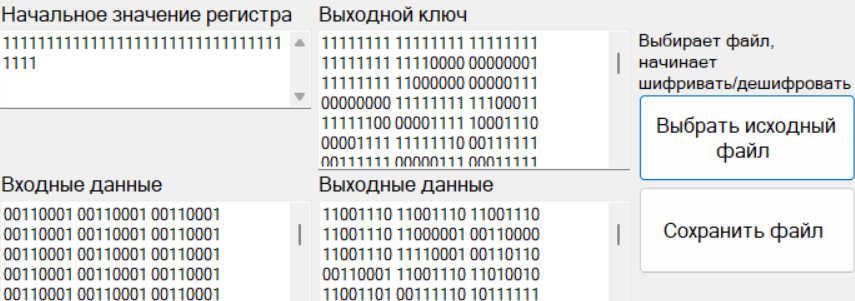


Рисунок 32 – Шифрация. Тест 11

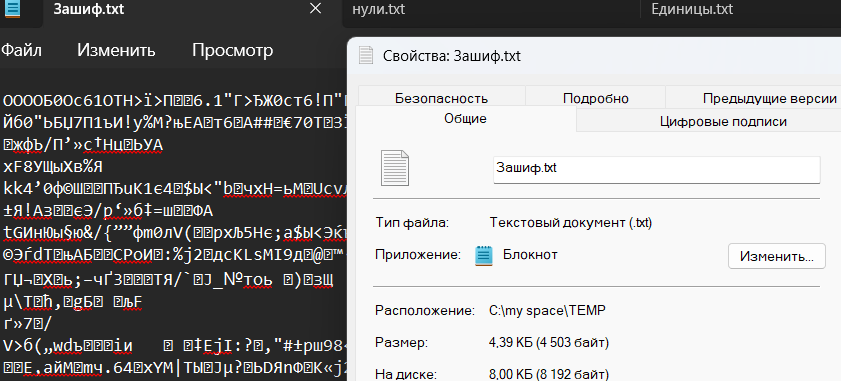


Рисунок 33 – Содержимое и свойства зашифрованного файла. Тест 11

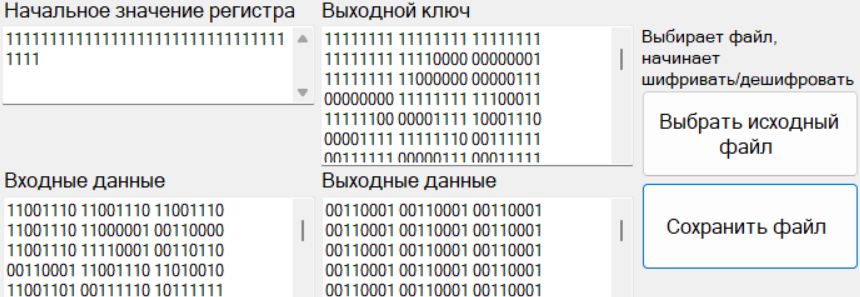
****

Рисунок 34 – Дешифрация. Тест 11

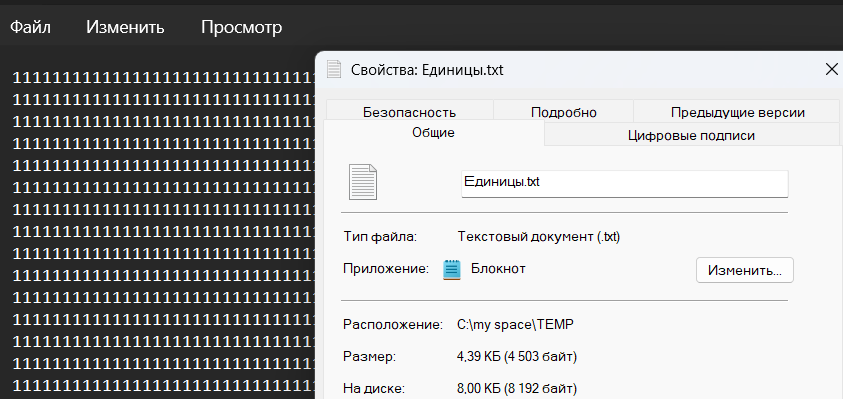
****

Рисунок 33 – Содержимое и свойства расшифрованного файла. Тест 11

**Таблица состояний регистра на каждом шаге**

**Начальное состояние: 101111010101111010101110101101010111**

**Многочлен: X^36+X^11+1**

