Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Теория информации

ОТЧЕТ

по лабораторной работе 2

Вариант 2

Выполнил Семашко И. А.
Студент гр. 351001

Проверил Болтак С. В.

Минск 2025

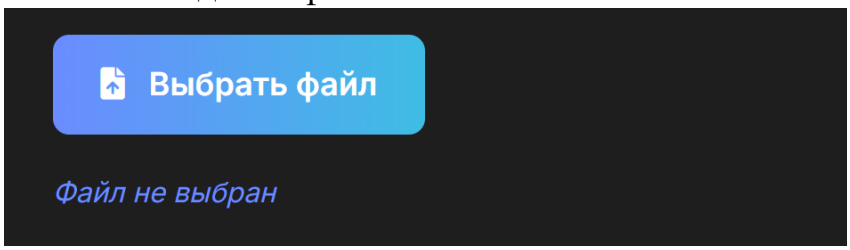
Задание

Реализовать систему потокового шифрования и дешифрования для файла с любым содержимым с помощью генератора ключевой последовательности на основе линейного сдвигового регистра с обратной связью $LFSR_1$ (размерность регистра приведена в таблице №1). Начальное состояние регистра ввести с клавиатуры. Поле для ввода состояния регистра должно игнорировать любые символы кроме 0 и 1. Вывести на экран сгенерированный ключ (последовательность из 0 и 1), исходный файл и зашифрованный файл в двоичном виде. Программа не должна быть написана в консольном режиме. Результат работы программы – зашифрованный/расшифрованный файл.

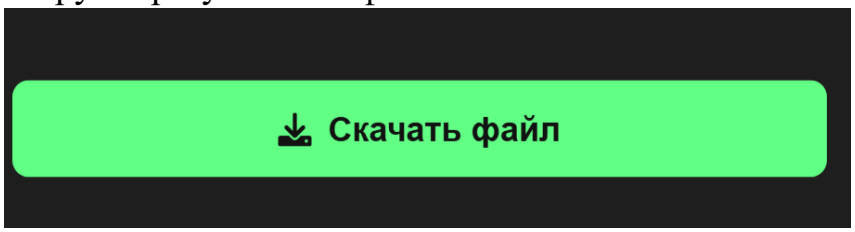
Примитивный многочлен: $x^{24} + x^4 + x^3 + x + 1$.

Работа с файлами

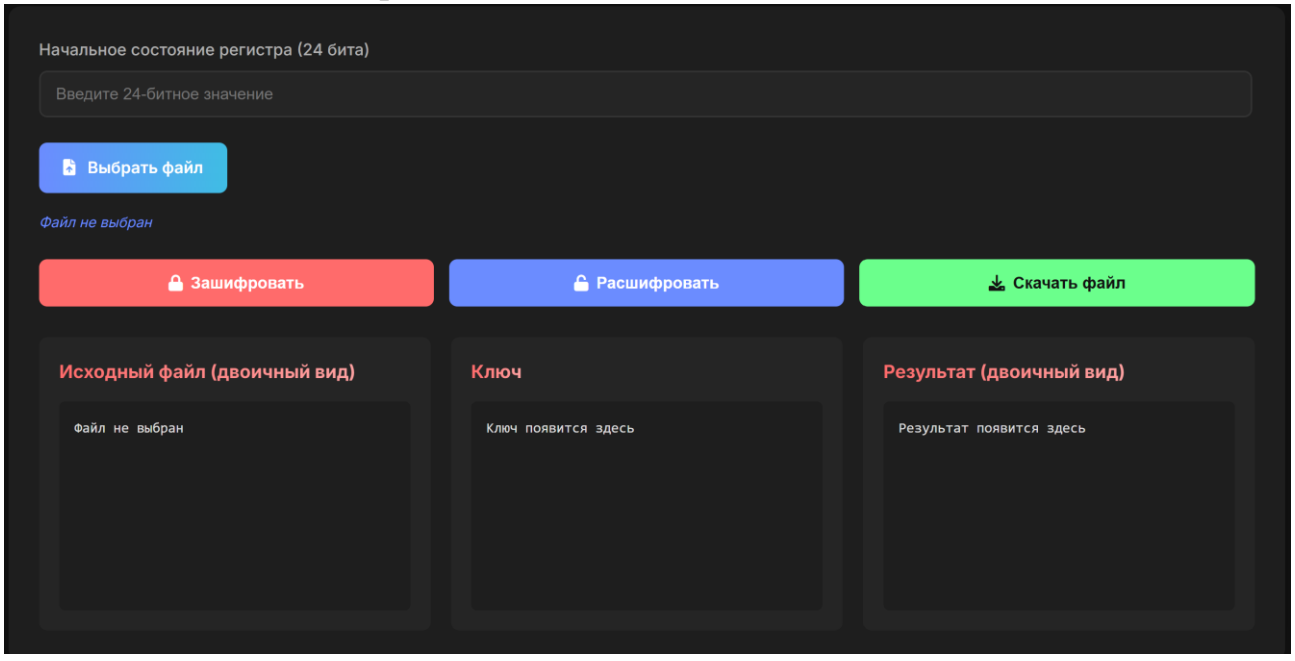
Взятие исходного файла:



Загрузка результата в файл:



Общий внешний вид страницы:



Тесты

Тест 1

Ситуация: простой ключ, небольшой текст
Состояние регистра: 111111111111111111111111
Ключ: 1111111111111111
Исходный текст: 0110100001101001
Зашифрованный текст: 1001011110010110

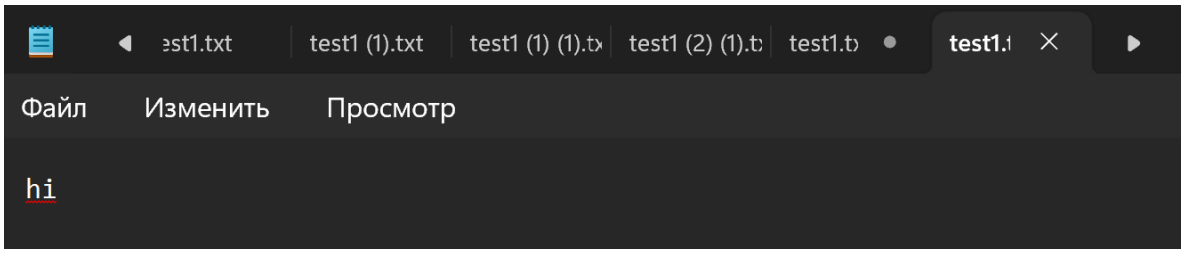
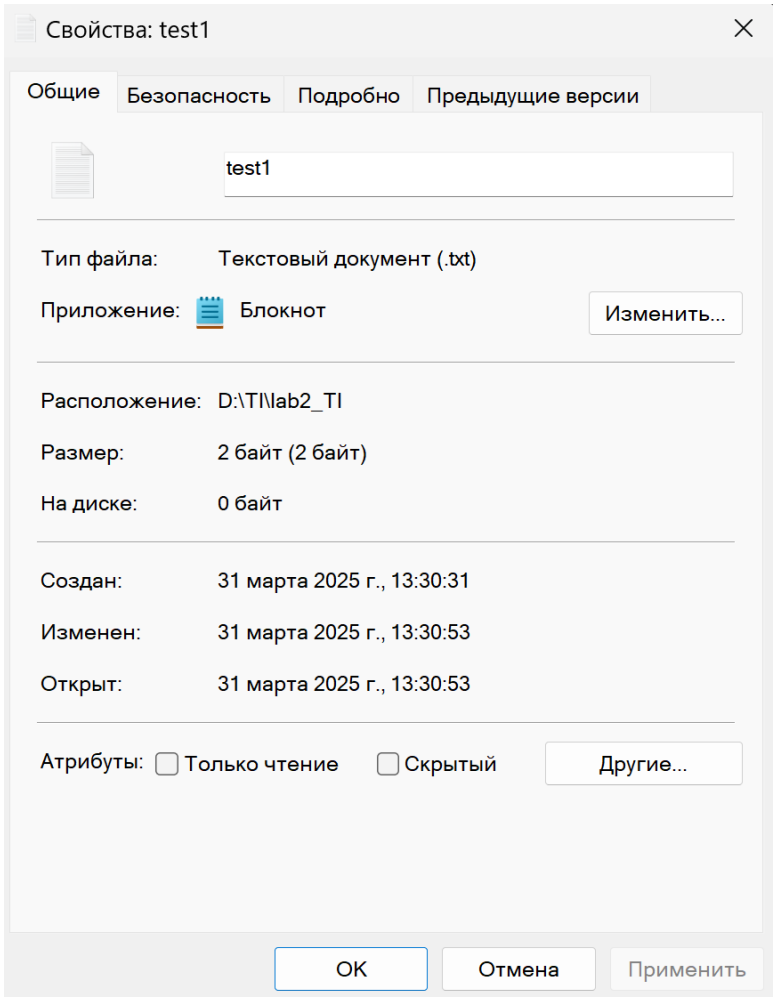
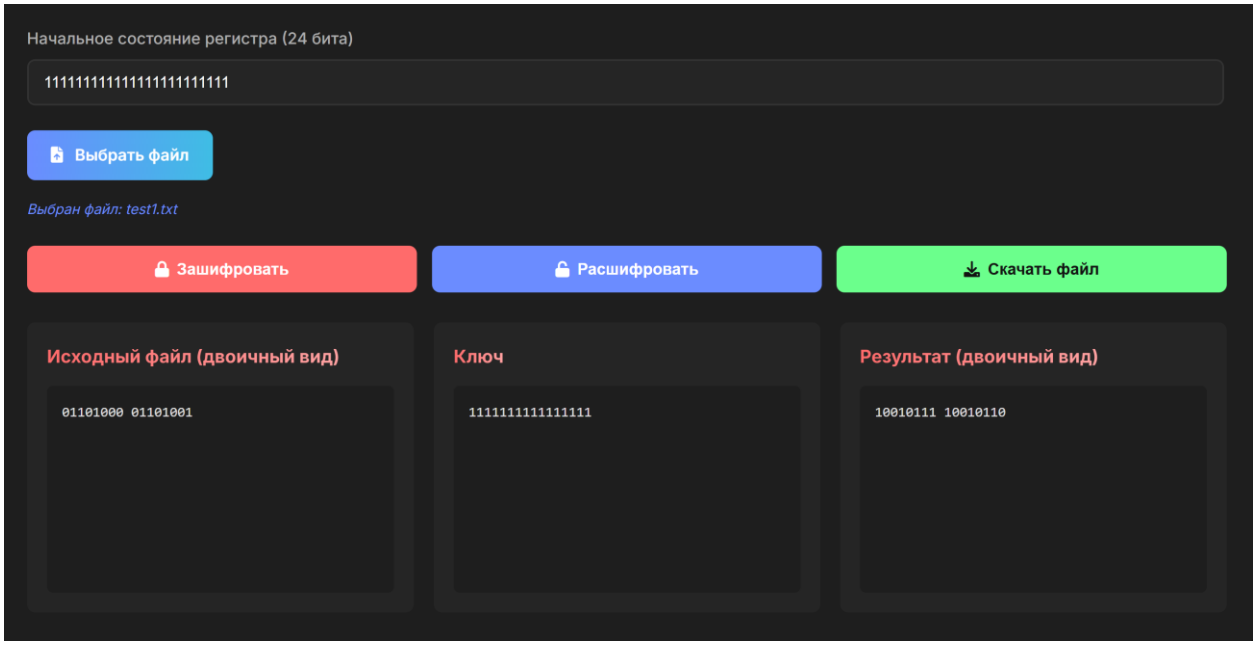


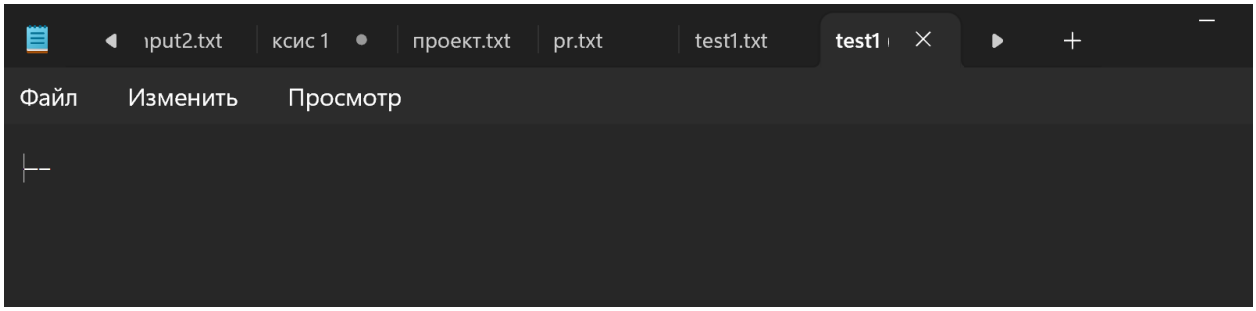
Рисунок 1 – Исходный текст



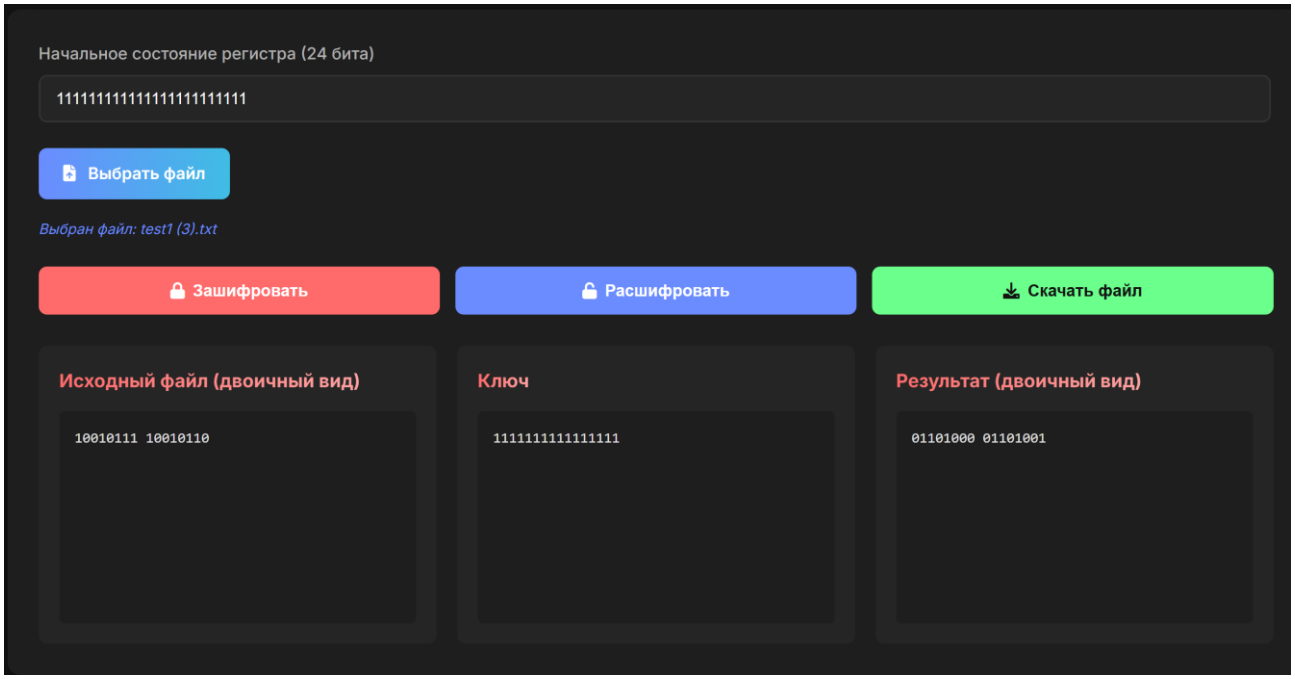
Работа программы (шифрование):

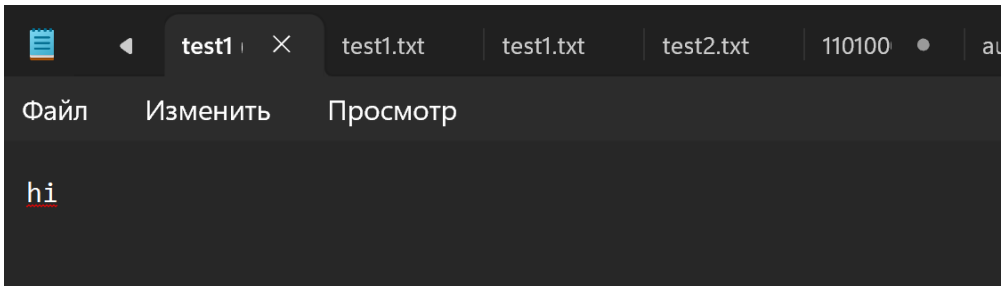


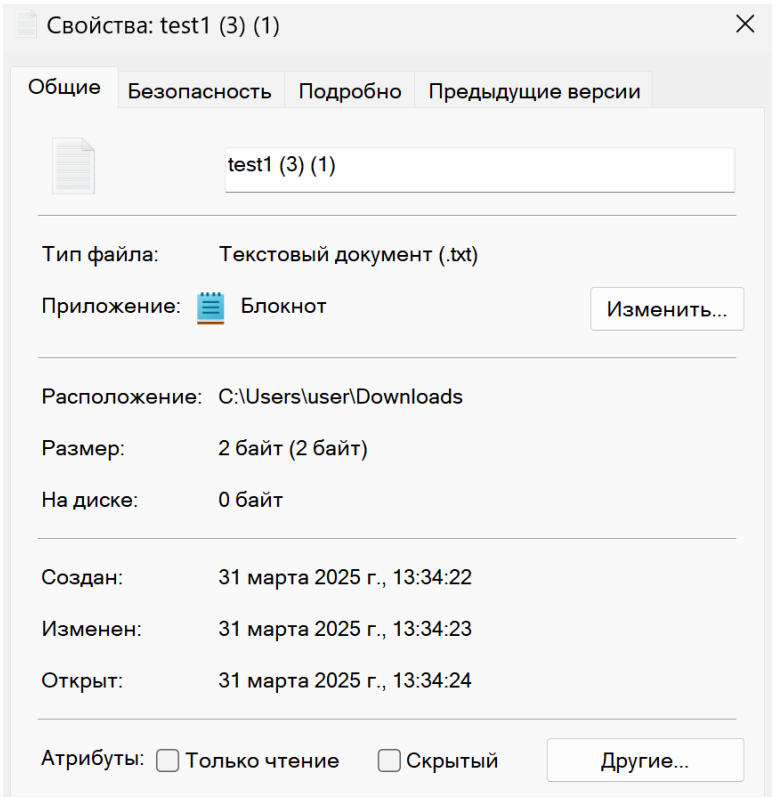
Содержимое зашифрованного скачанного файла test1 (3).txt:



Результат работы программы (дешифрование):







Тест 2

Ситуация: сложный ключ, большой текст
Состояние регистра: 101010010100100111111111
Ключ: Первые 6 байт:
101010010100100111111111001010110001001100110011
Последние 6 байт:
100010001110110110011101010110111001111000010000
Исходный текст: Первые 10 байт:
110100001001101011010000101100001101000010111010001000001101000010111111111010001
Последние 10 байт:
101100001101000110000001110100011000001011010000101110001101000110001111001011110
Зашифрованный текст: Первые 10 байт:
011110011101001100101111100110111100001110001001100110100110010000001010110001001
Последние 10 байт:
000100010011010010001001111010000000101000111101001001011000101001000000000100110

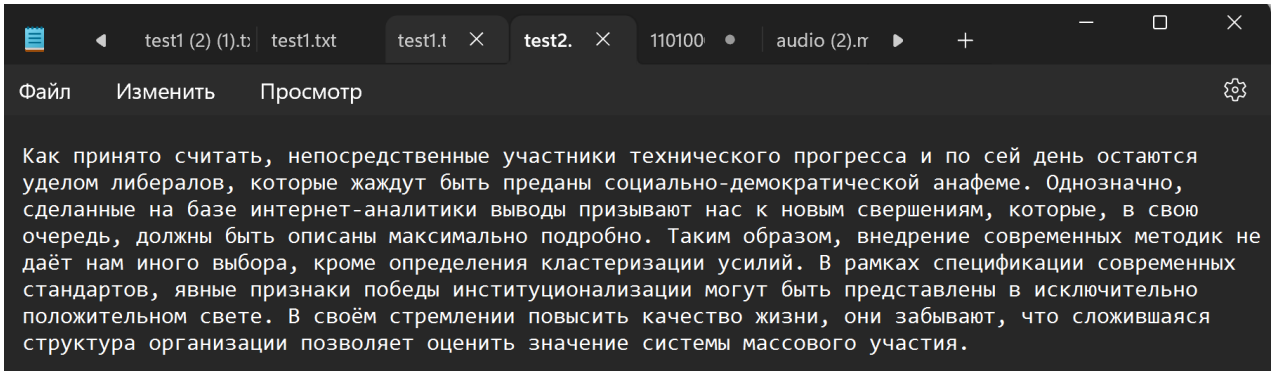
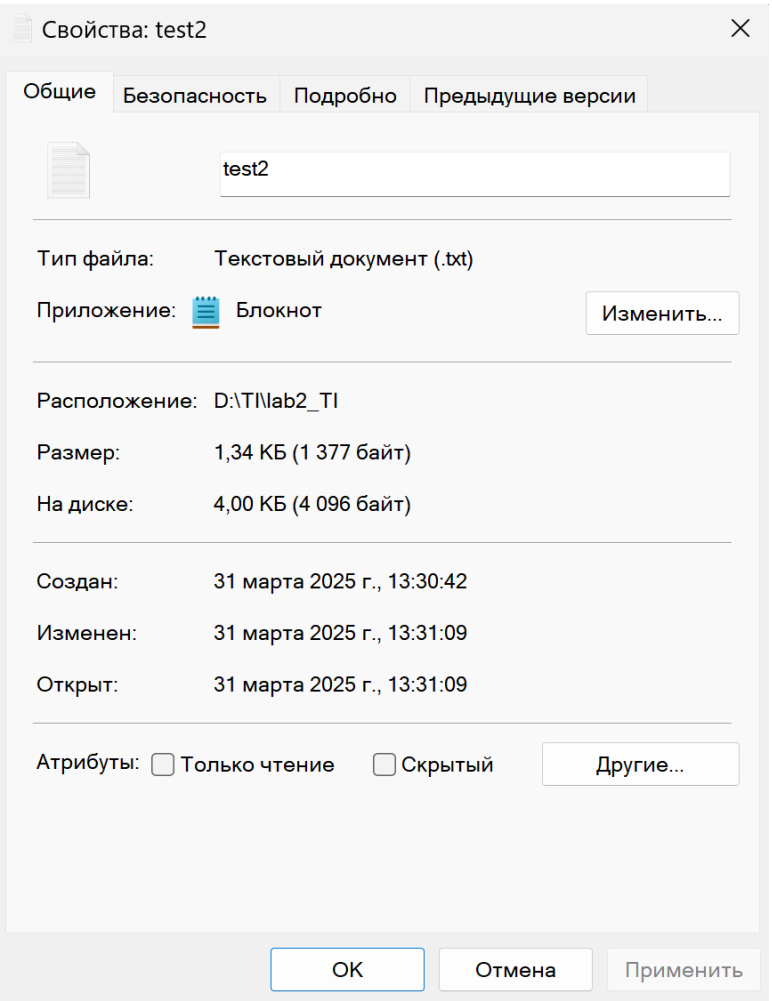
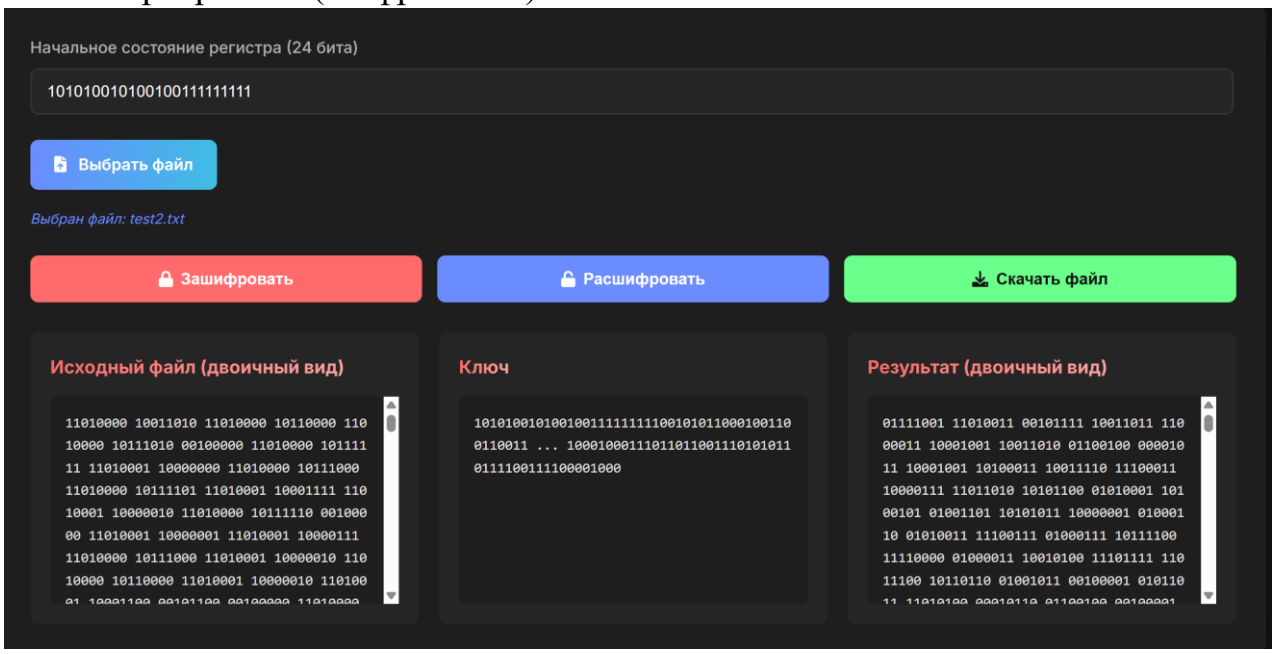


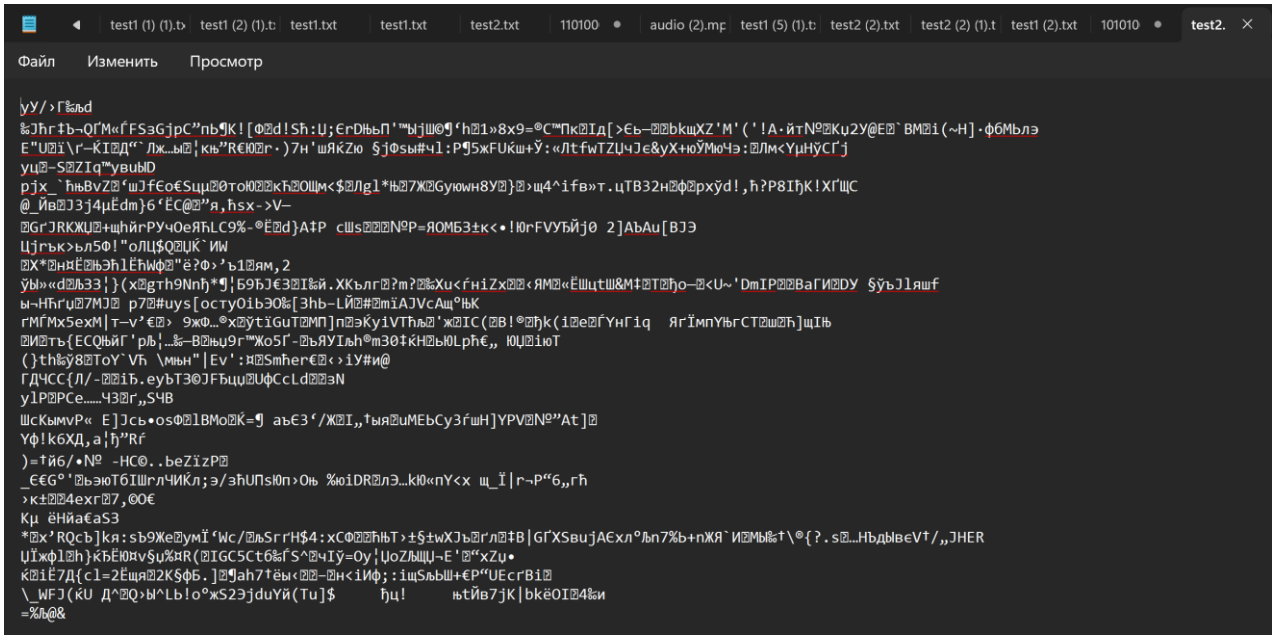
Рисунок 2 – Исходный текст



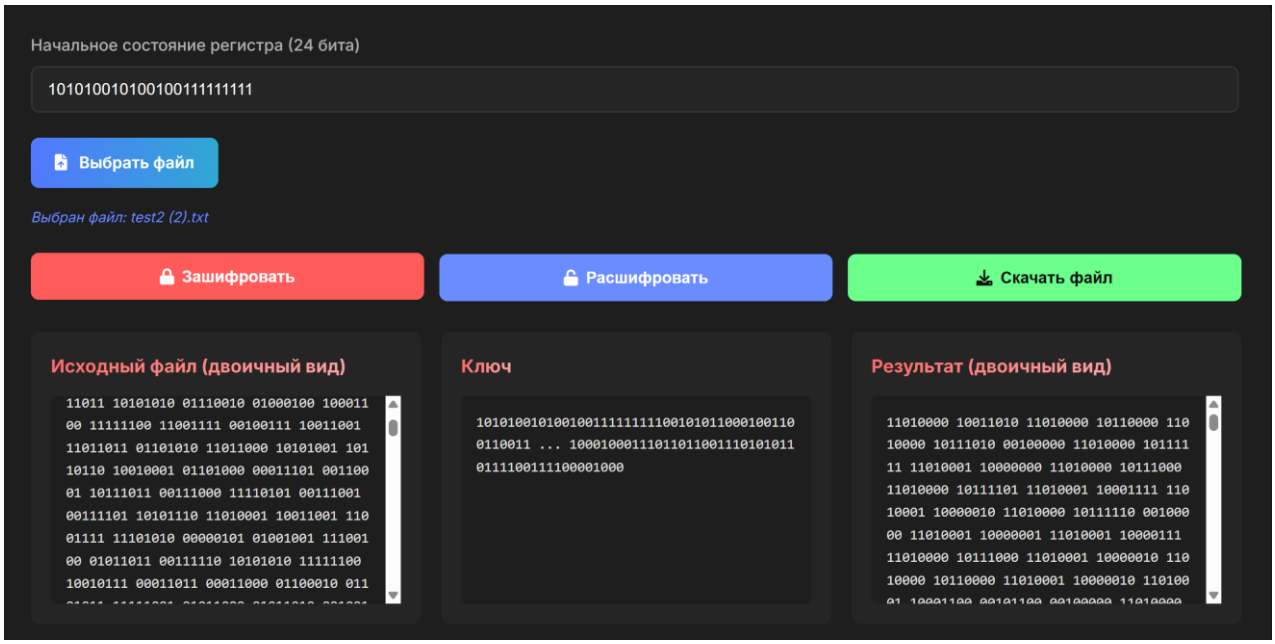
Работа программы (шифрование):

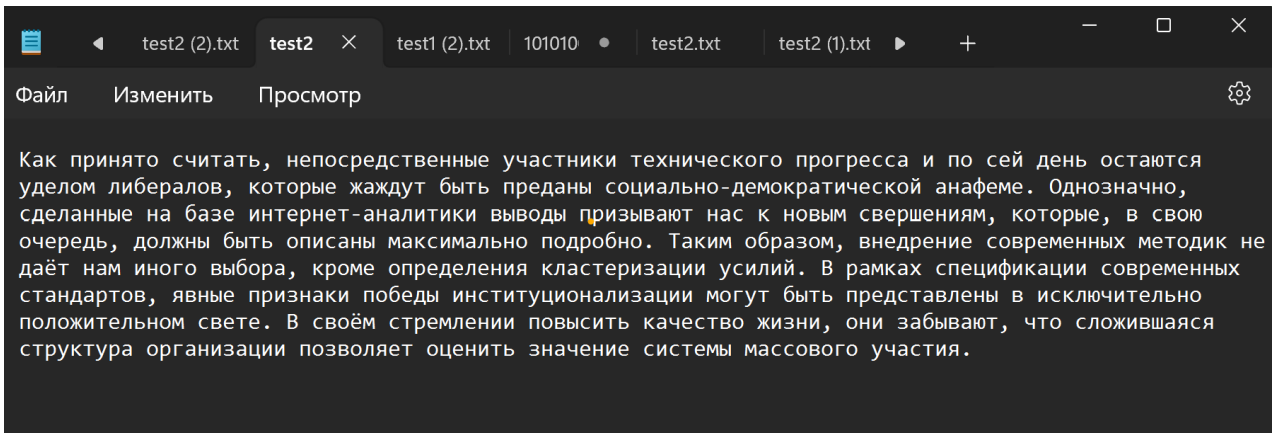


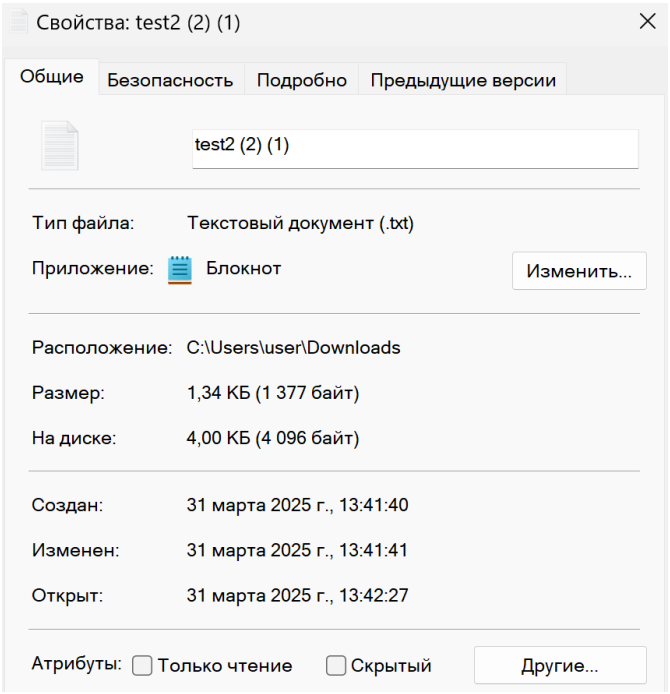
Содержимое зашифрованного скачанного файла test2 (2).txt:



Результат работы программы (дешифрование):





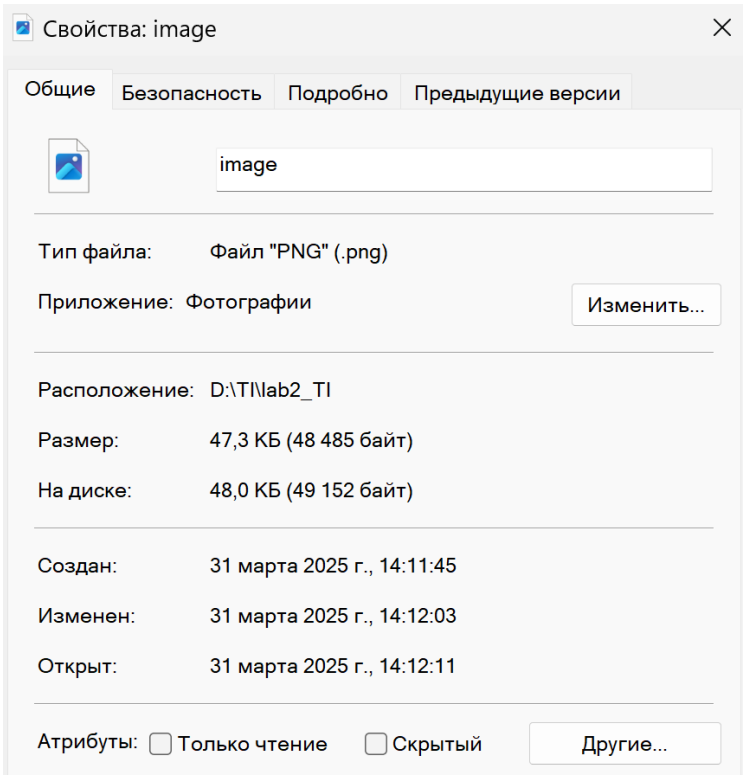


Тест 3

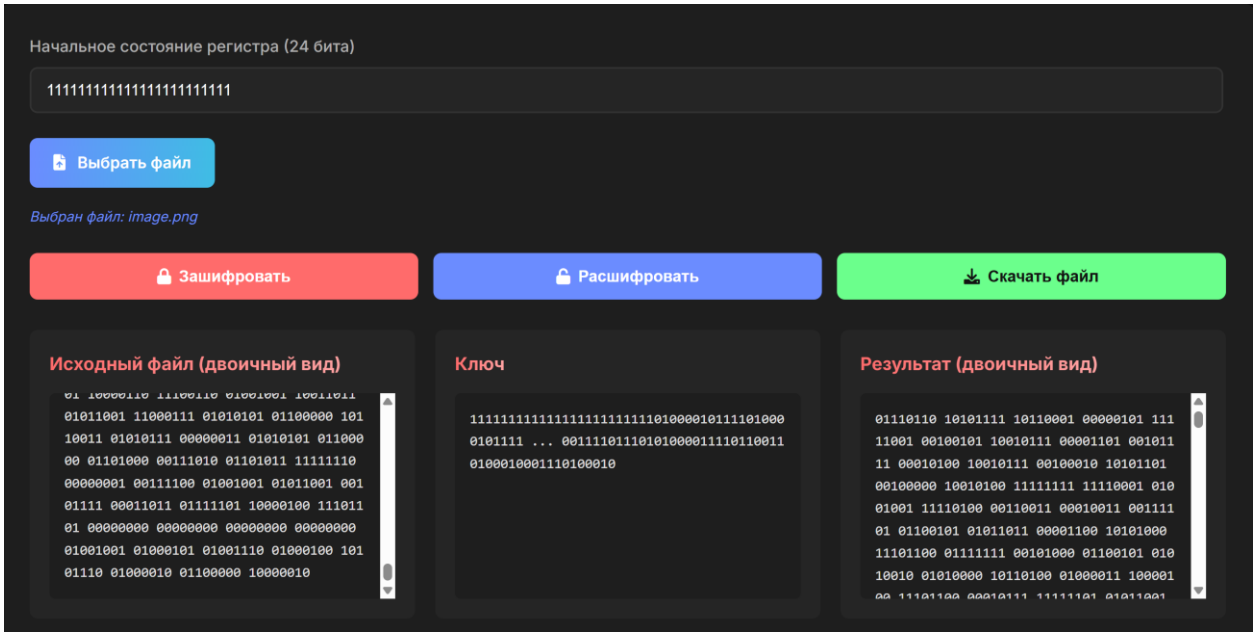
Ситуация: работа с графическим изображением
Состояние регистра: 11111111111111111111111
Ключ: Первые 6 байт:
111111111111111111111111010000101111010000101111
Последние 6 байт:
001111011101010000111101100110100010001110100010
Исходный текст: Первые 10 байт:
1000100101010000010011100100011100001101000010100001101000001010
0000000000000000
Последние 10 байт:
0000000000000000010010010100010101001110010001001010111001000010011
0000010000010

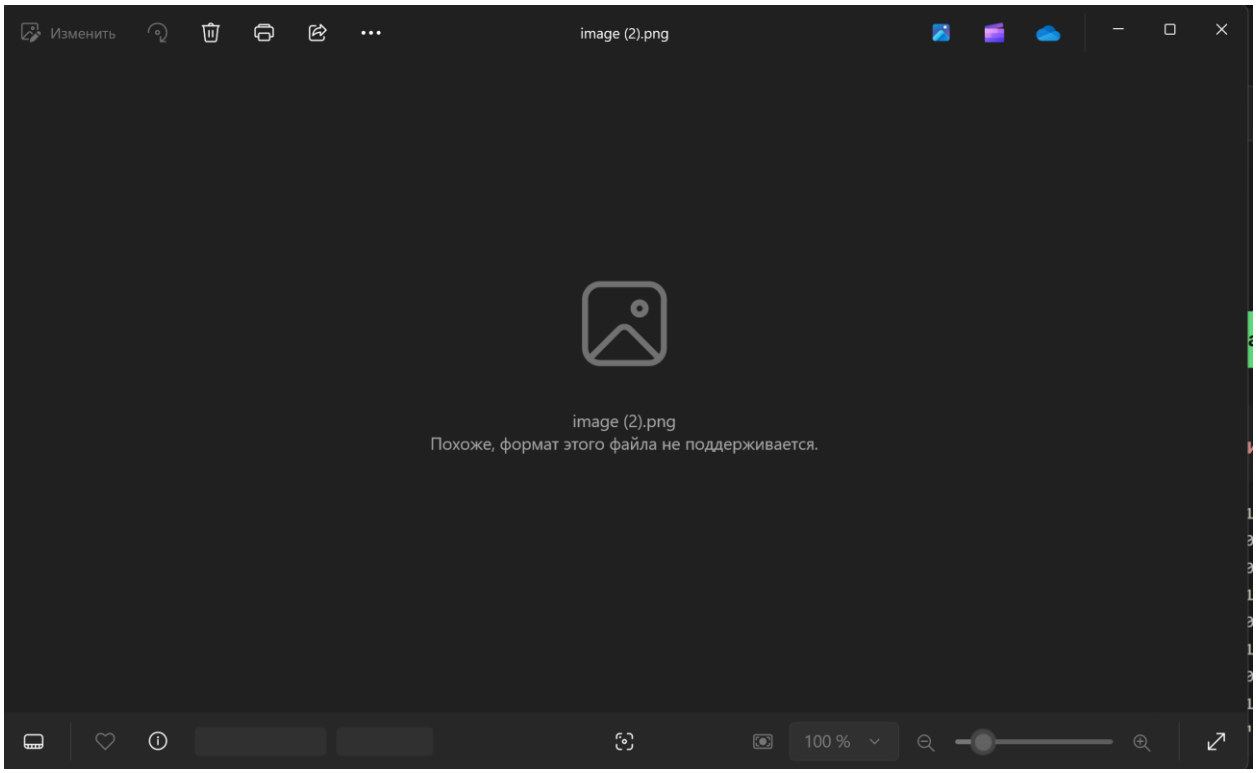
Зашифрованный текст: Первые 10 байт:
01110110 10101111 10110001 00000101 11111001 00100101 10010111 00001101 00101111 00010100
Последние 10 байт:
10110110 00110111 00010000 10100010 01110011 10010000 10010011 11011000 01000011 00100000

Рисунок 3 – Исходный рисунок

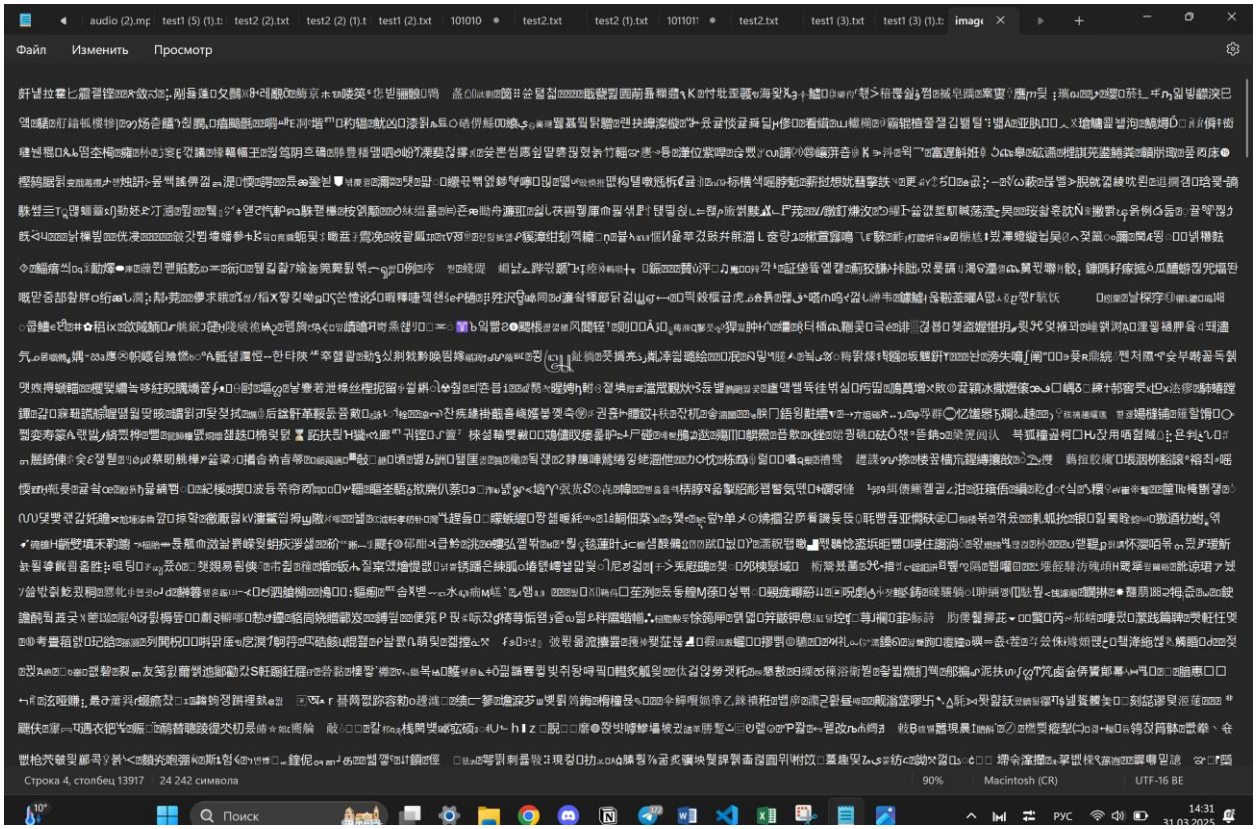


Работа программы (шифрование):

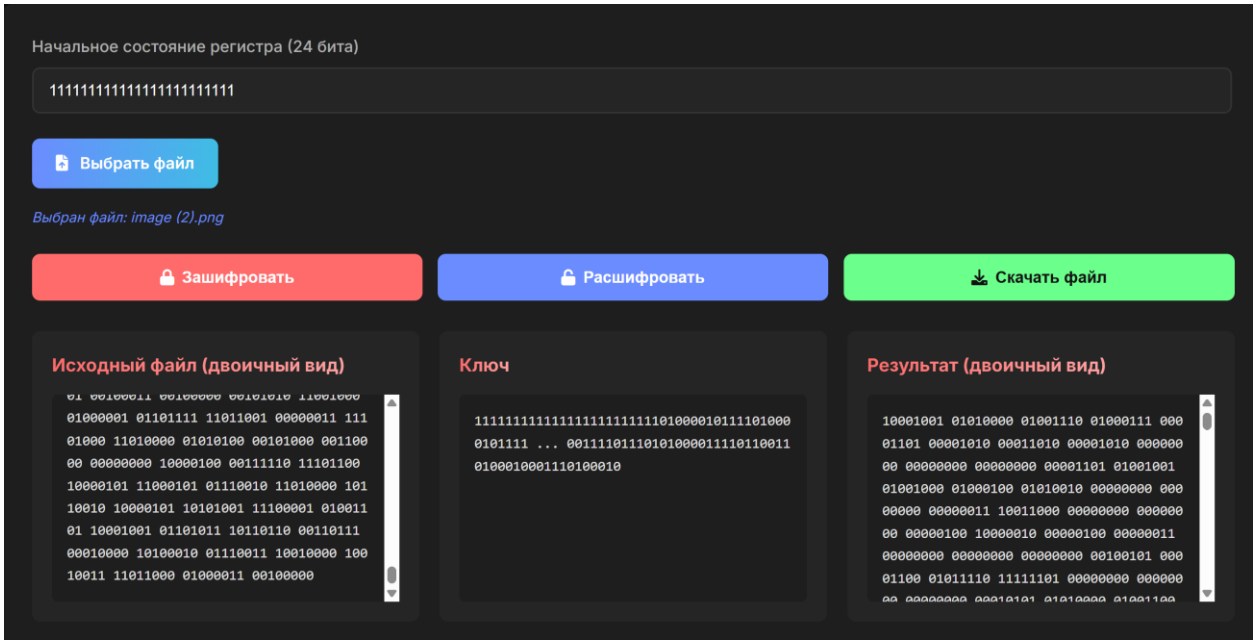




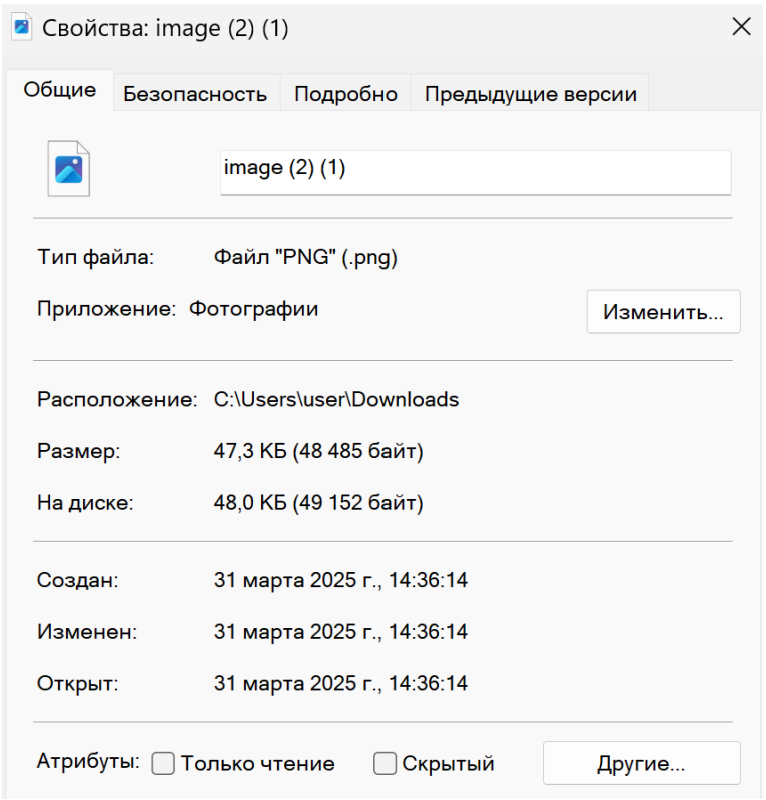
Содержимое зашифрованного скачанного файла image (2).png:



Результат работы программы (дешифрование):




Изменить
image (2) (1).png
920 x 1154
47.3 КБ
100 %


Свойства: image (2) (1)
Общие
Безопасность
Подробно
Предыдущие версии
image (2) (1)
Тип файла: Файл "PNG" (.png)
Приложение: Фотографии
Изменить...
Расположение: C:\Users\user\Downloads
Размер: 47,3 КБ (48 485 байт)
На диске: 48,0 КБ (49 152 байт)
Создан: 31 марта 2025 г., 14:36:14
Изменен: 31 марта 2025 г., 14:36:14
Открыт: 31 марта 2025 г., 14:36:14
Атрибуты: Только чтение Скрытый
Другие...