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  Студент гр. 351001 | Семашко И. А. |
| Проверил | Болтак С. В. |

Минск 2025

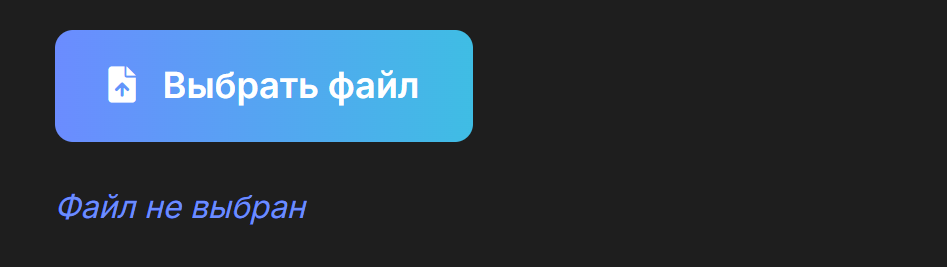
**Задание**

Реализовать систему потокового шифрования и дешифрования для файла с любым содержимым с помощью генератора ключевой последовательности на основе линейного сдвигового регистра с обратной связью LFSR1 (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.

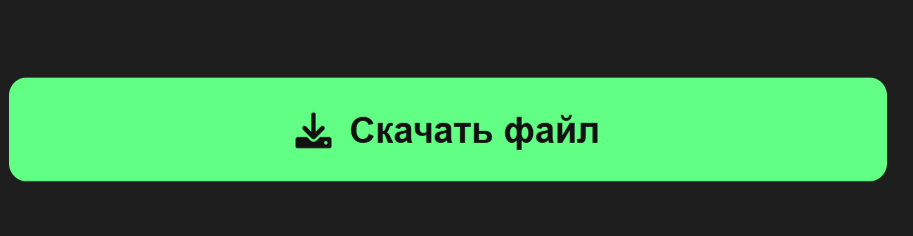
**Примитивный многочлен:** *x*24 + *x*4 + *x*3 + *x* + 1.

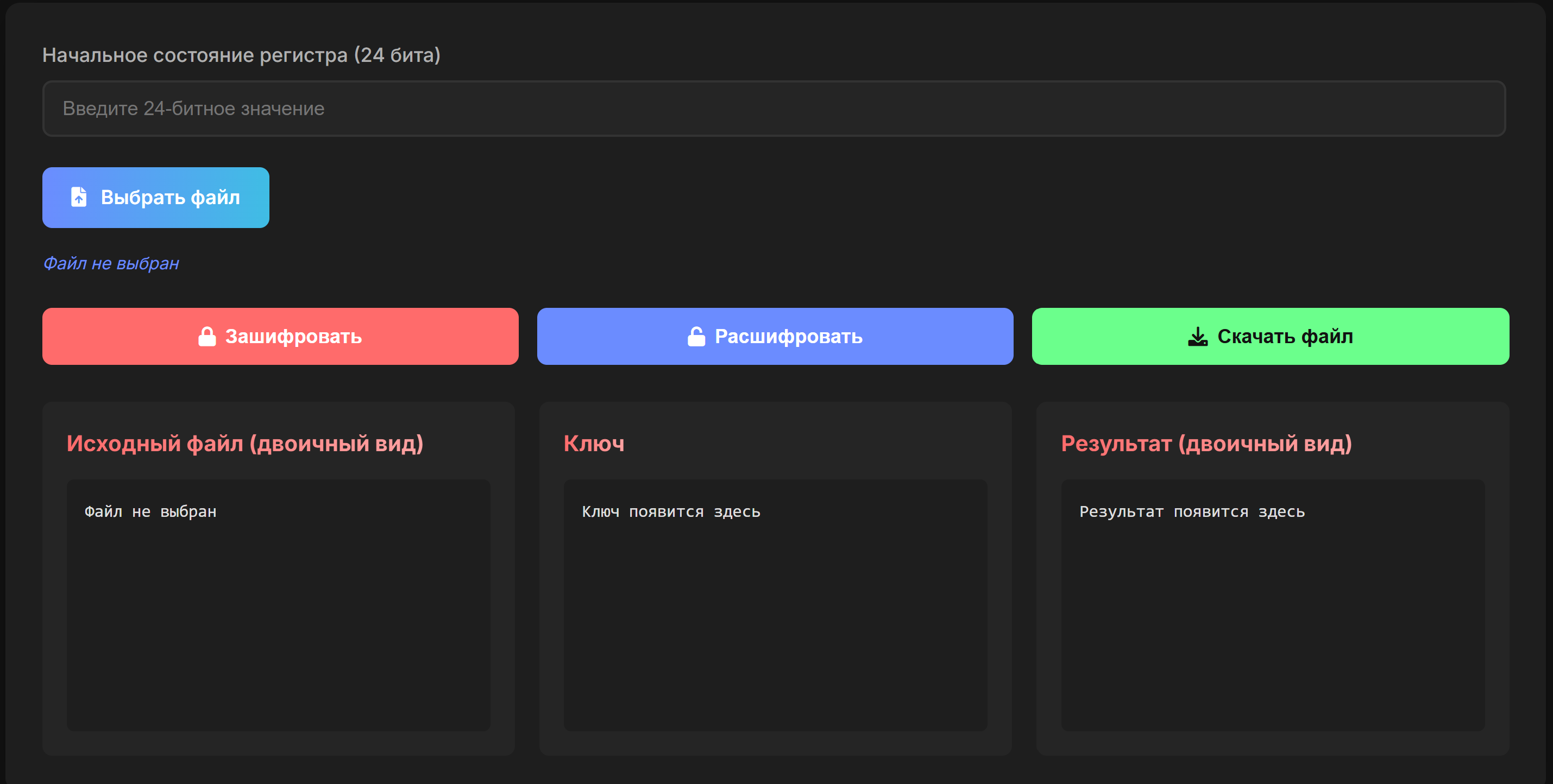
**Работа с файлами**

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

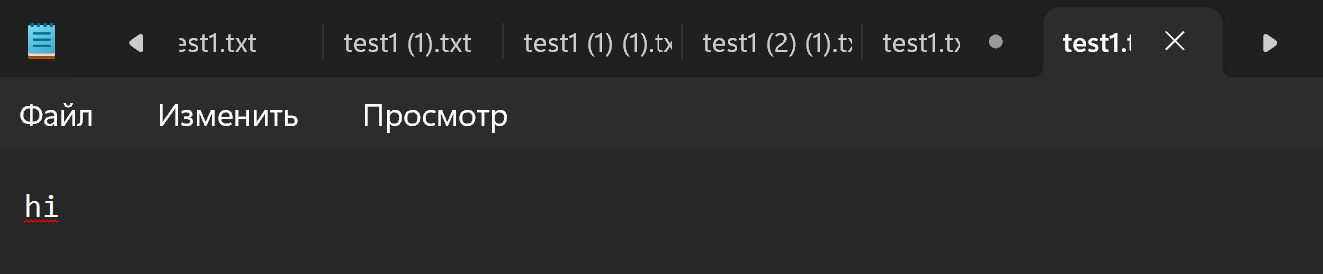
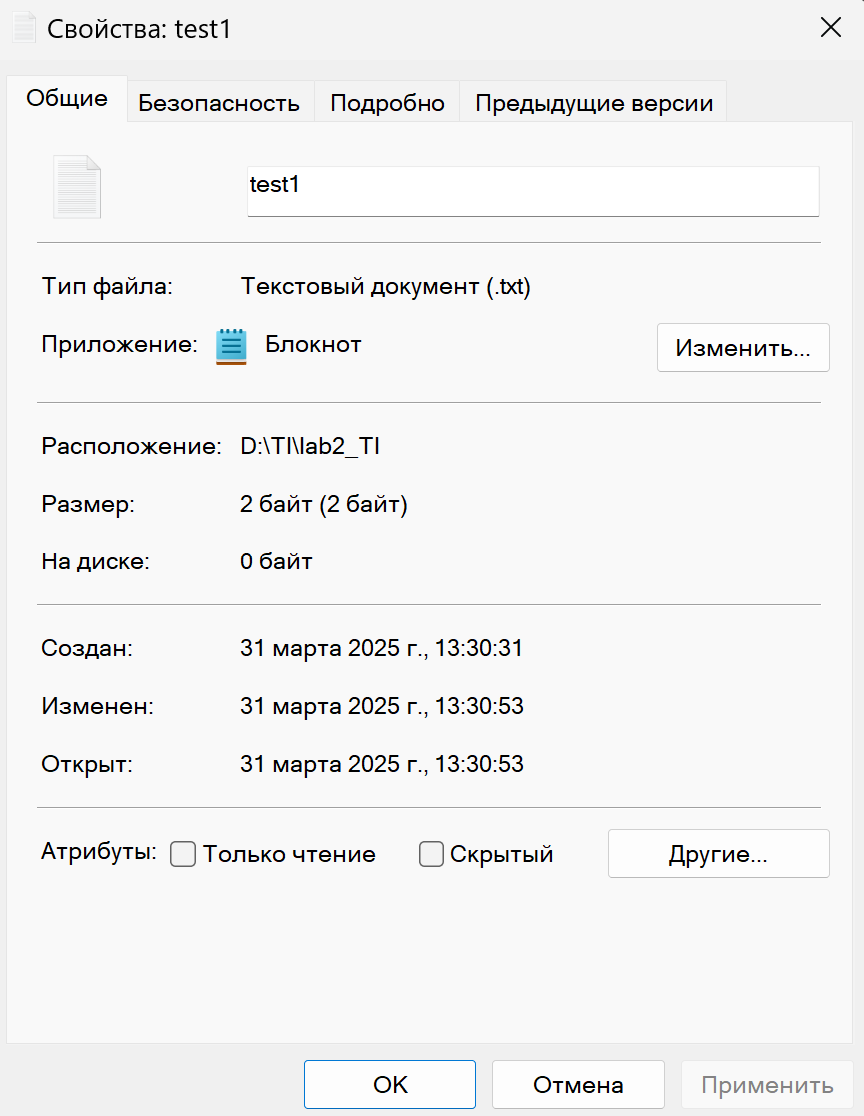
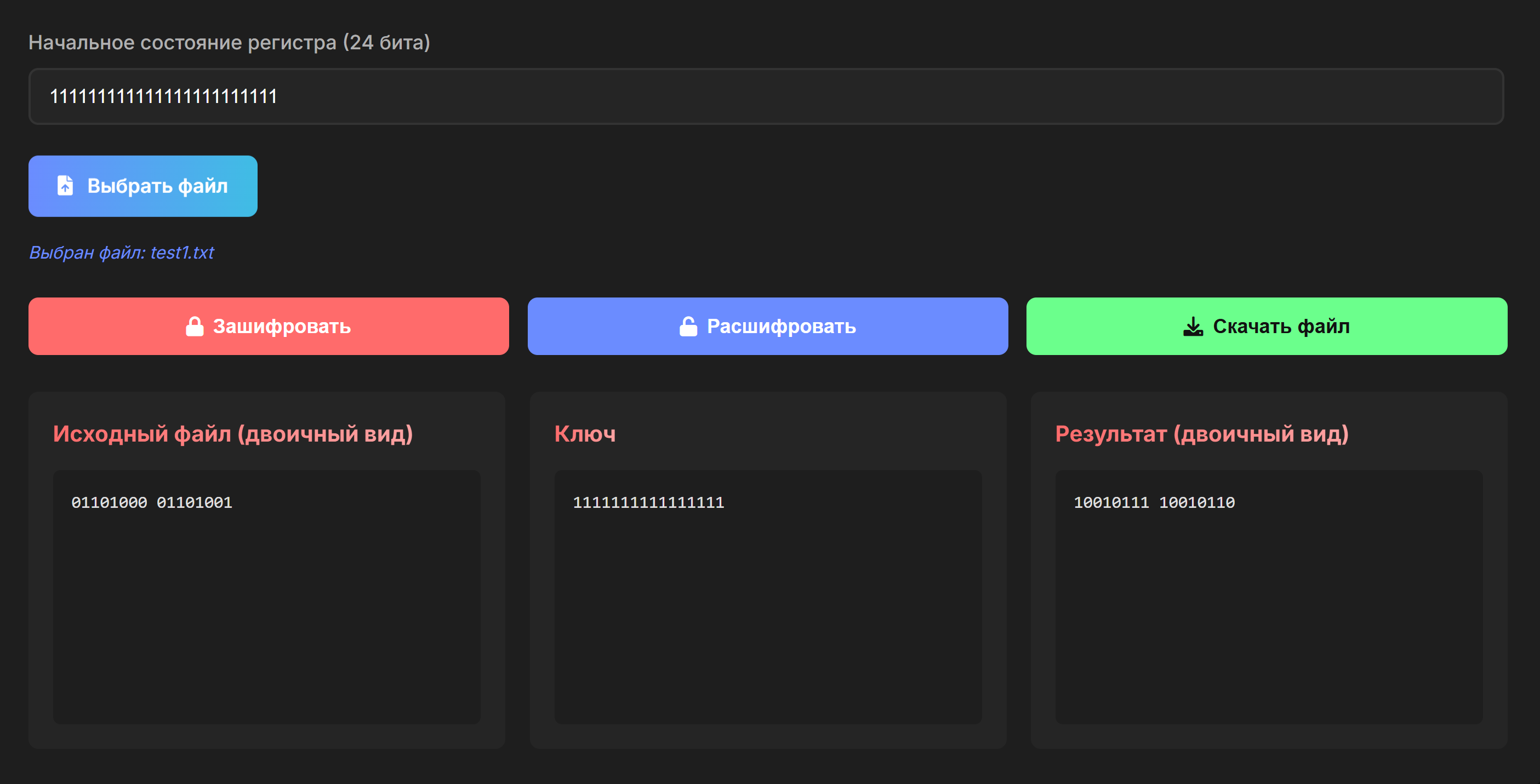


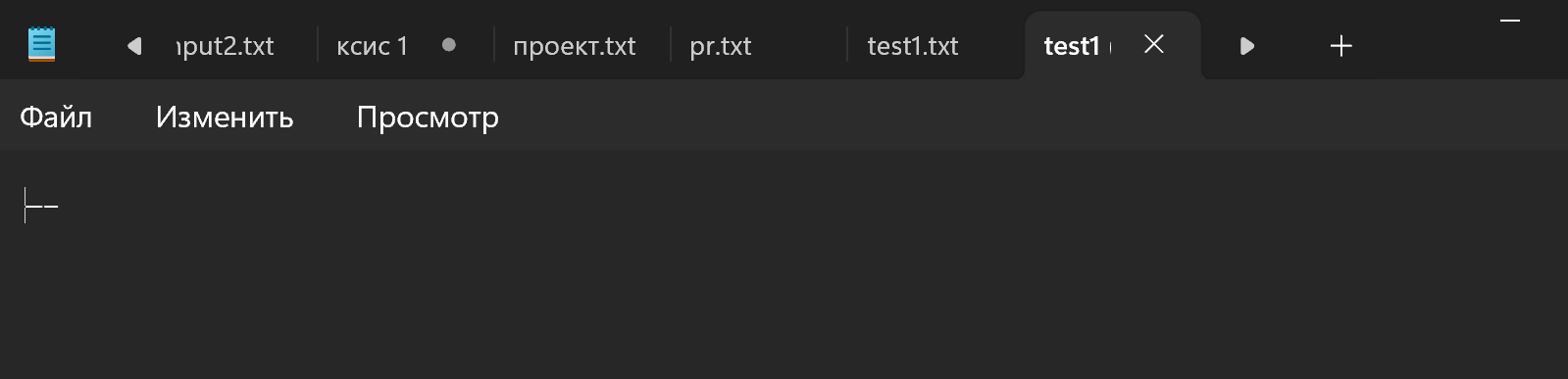
Рисунок 1 – Исходный текст



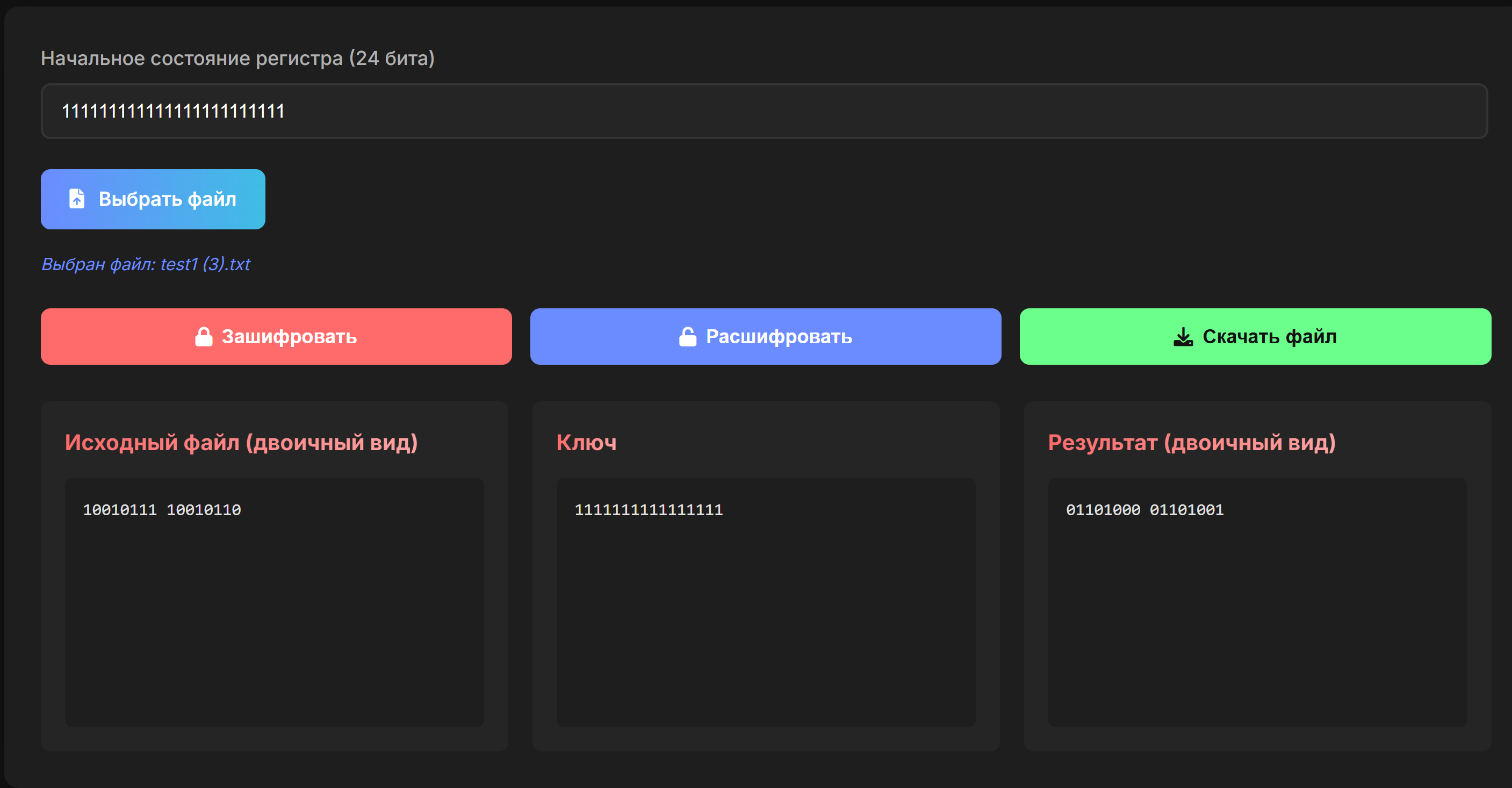
Работа программы (шифрование):

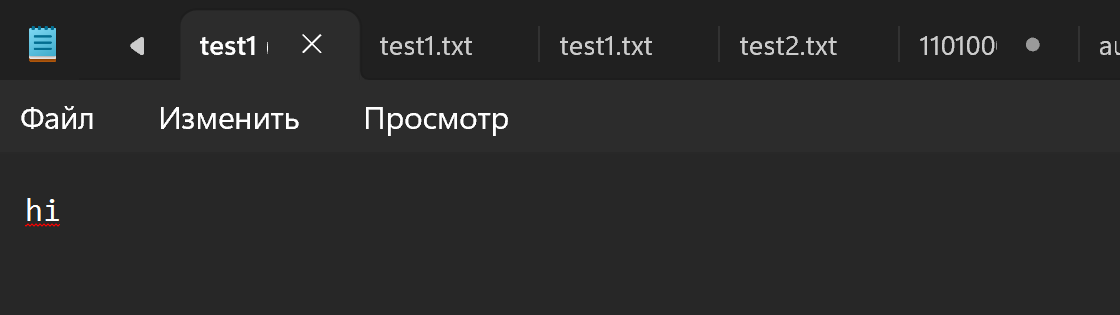
****

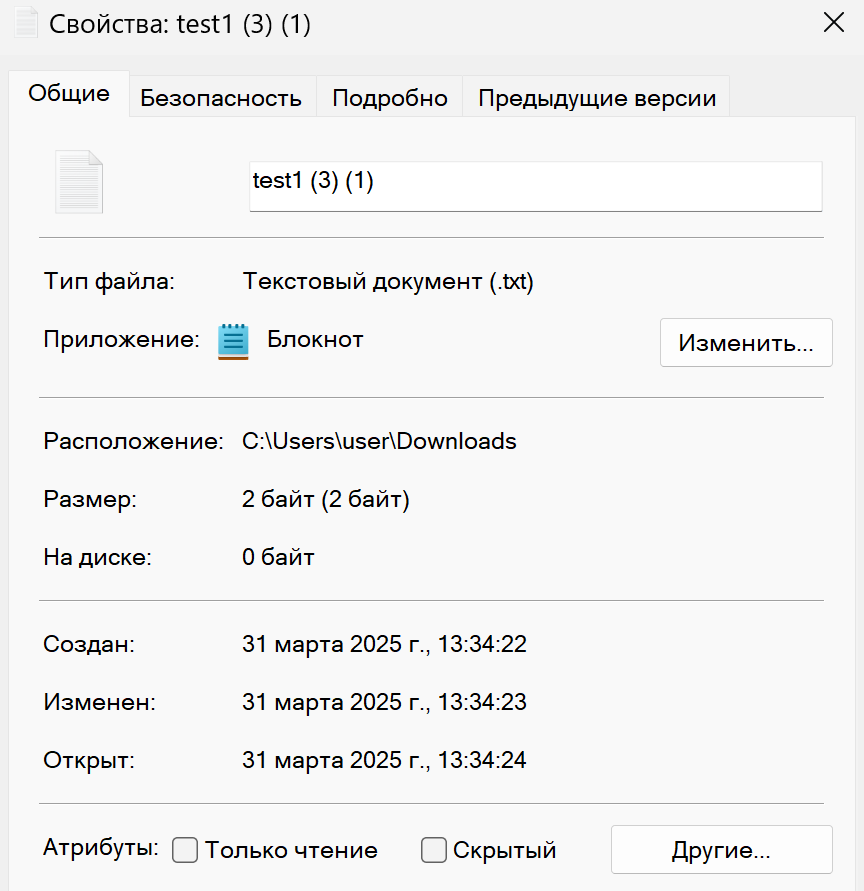
Содержимое зашифрованного скачанного файла test1 (3).txt:

****

Результат работы программы (дешифрование):



****

****

**Тест 2**

**Ситуация:** сложный ключ, большой текст

**Состояние регистра:** 101010010100100111111111

**Ключ:** Первые 6 байт:

101010010100100111111111001010110001001100110011

Последние 6 байт:

100010001110110110011101010110111100111100001000

**Исходный текст:** Первые 10 байт:

11010000100110101101000010110000110100001011101000100000110100001011111111010001

Последние 10 байт:

10110000110100011000000111010001100000101101000010111000110100011000111100101110

**Зашифрованный текст:** Первые 10 байт:

01111001110100110010111110011011110000111000100110011010011001000000101110001001

Последние 10 байт:

00010001001101001000100111101000000010100011110100100101100010100100000000100110

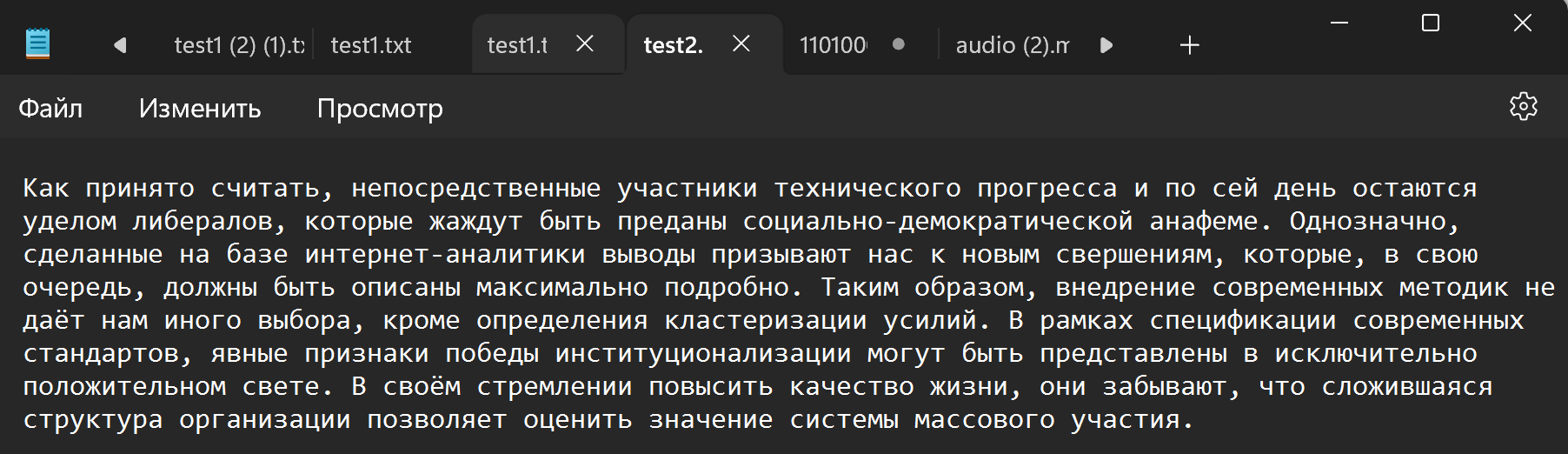
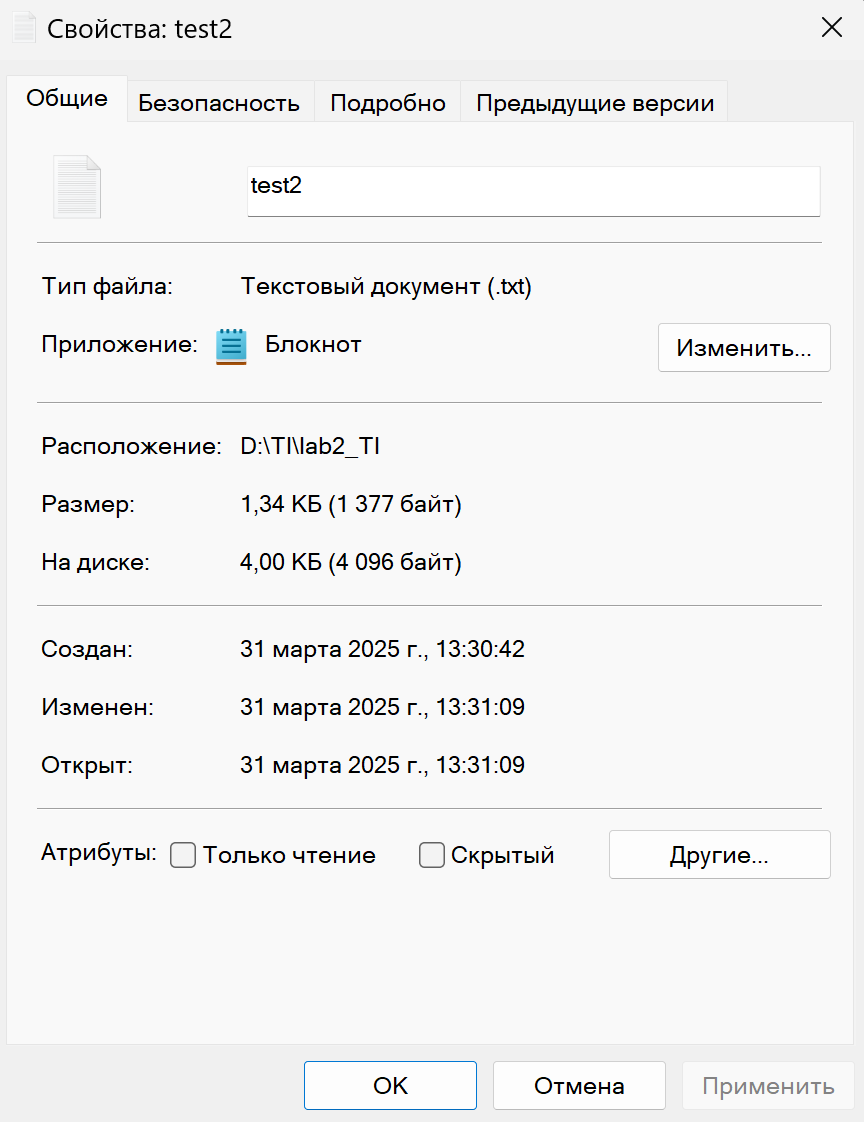
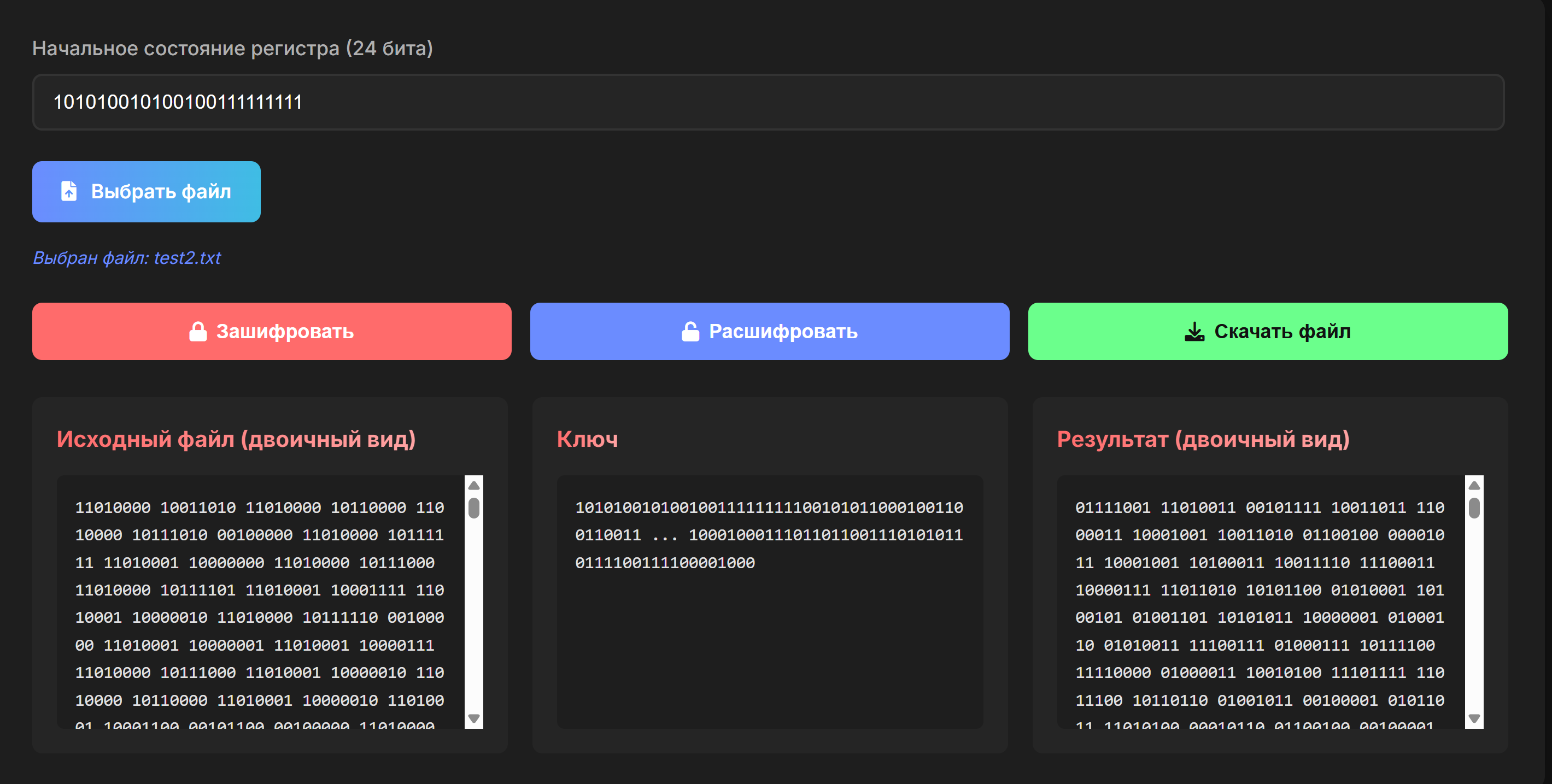


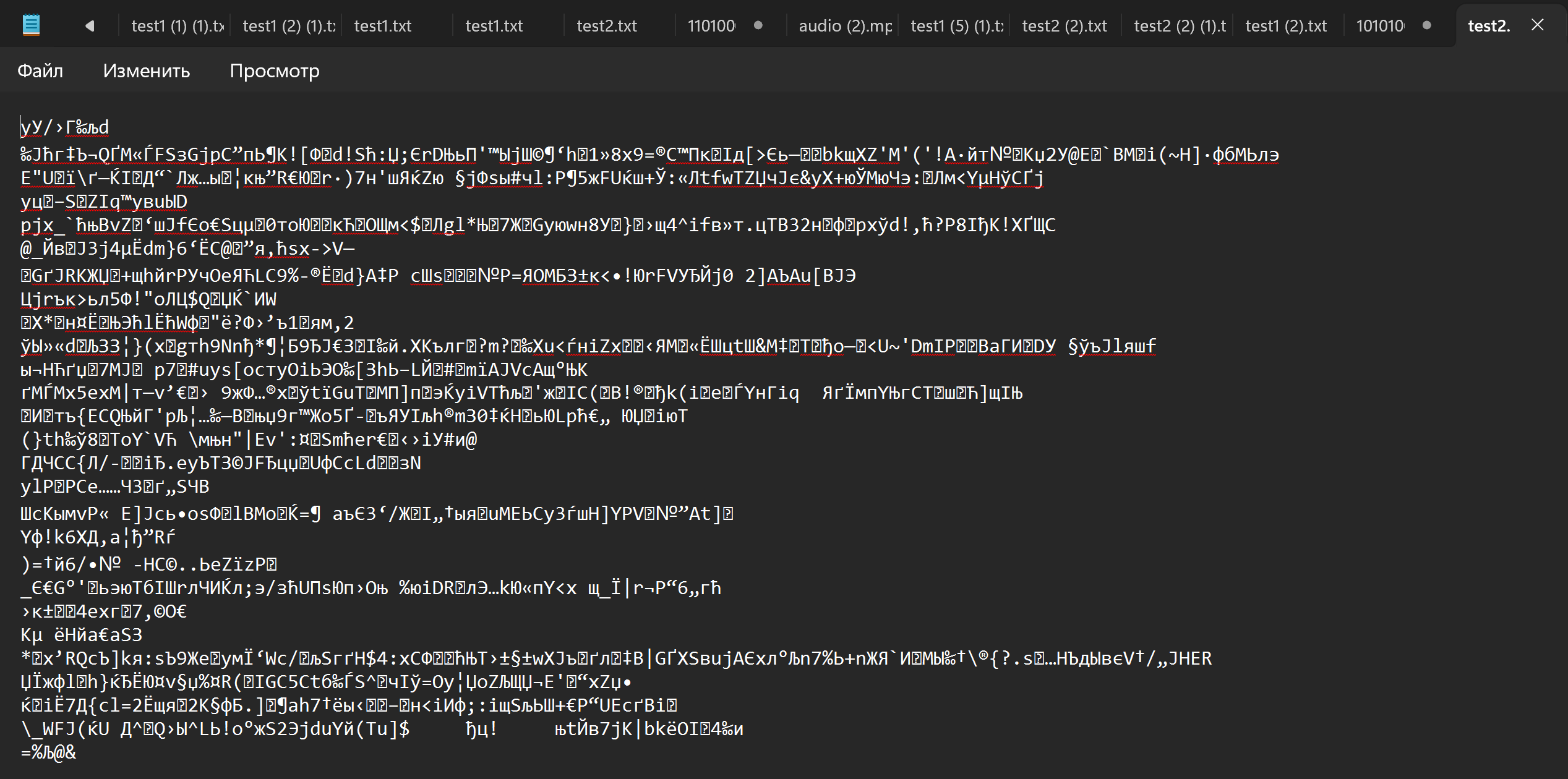
Рисунок 2 – Исходный текст



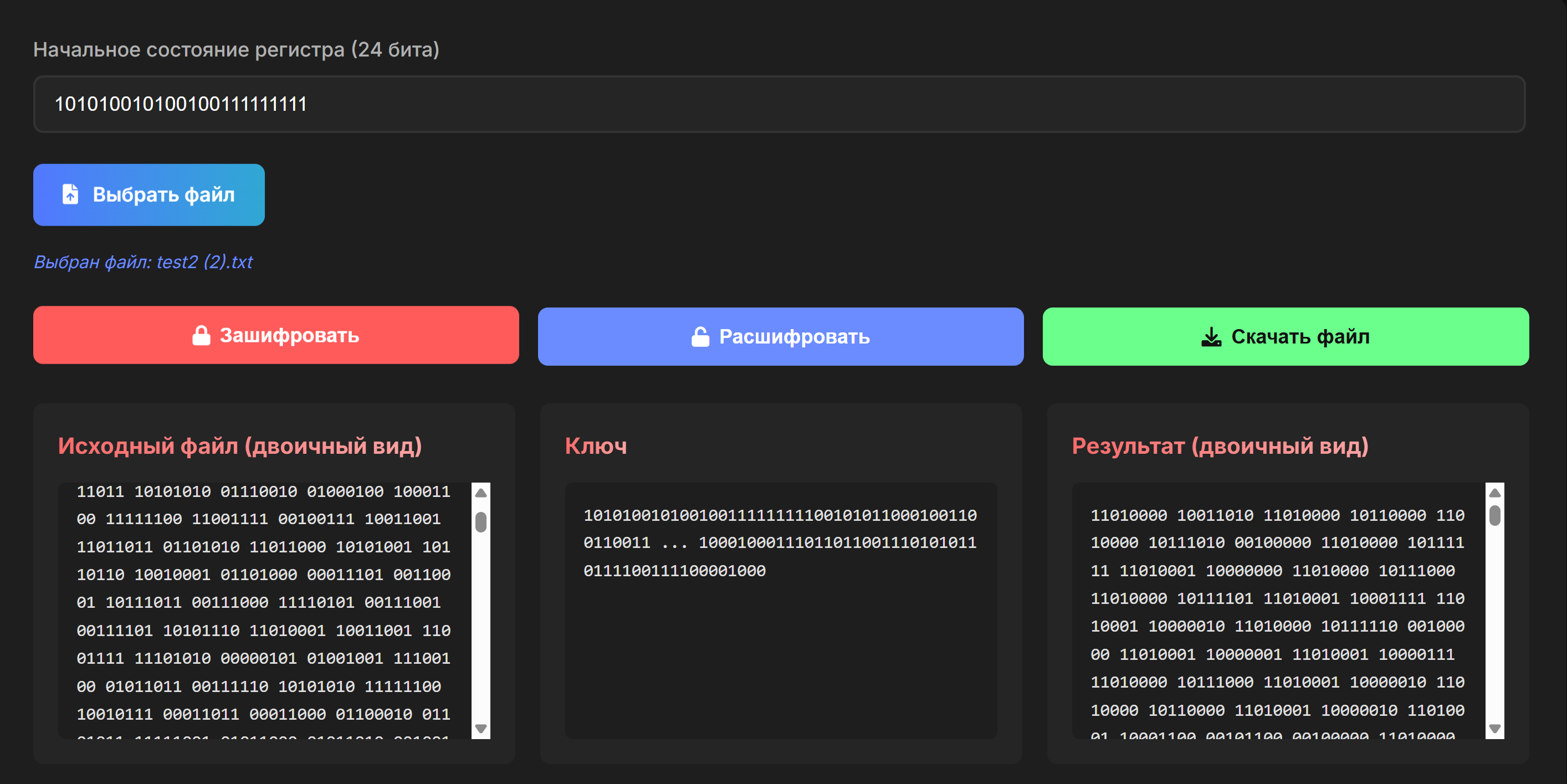
Работа программы (шифрование):

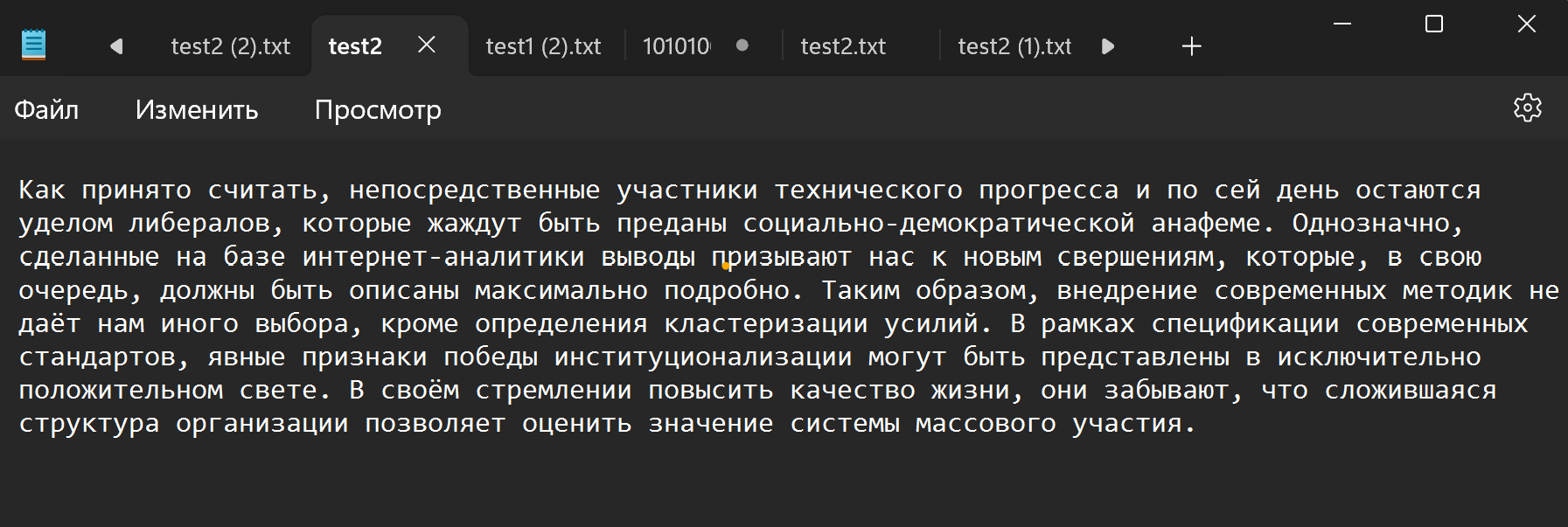
****

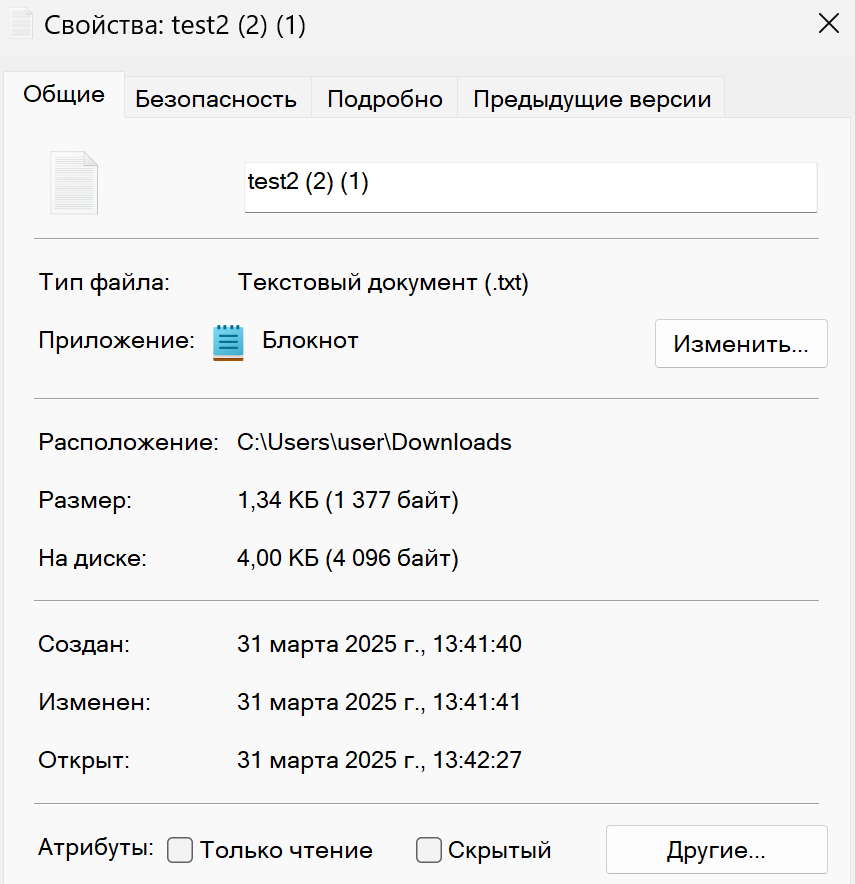
Содержимое зашифрованного скачанного файла test2 (2).txt:

****

Результат работы программы (дешифрование):



****

****

**Тест 3**

**Ситуация:** работа с графическим изображением

**Состояние регистра:** 111111111111111111111111

**Ключ:** Первые 6 байт:

111111111111111111111111010000101111010000101111

Последние 6 байт:

001111011101010000111101100110100010001110100010

**Исходный текст:** Первые 10 байт:

1000100101010000010011100100011100001101000010100001101000001010 0000000000000000

Последние 10 байт:

00000000000000000100100101000101010011100100010010101110010000100110000010000010

**Зашифрованный текст:** Первые 10 байт:

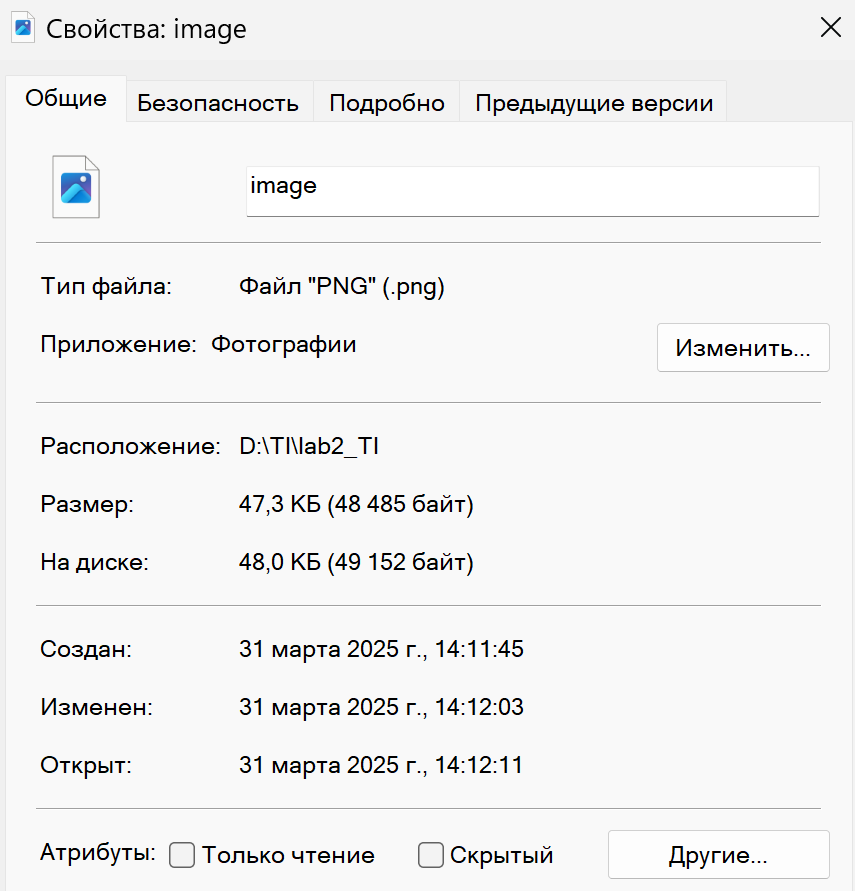
01110110 10101111 10110001 00000101 11111001 00100101 10010111 00001101 00101111 00010100

Последние 10 байт:

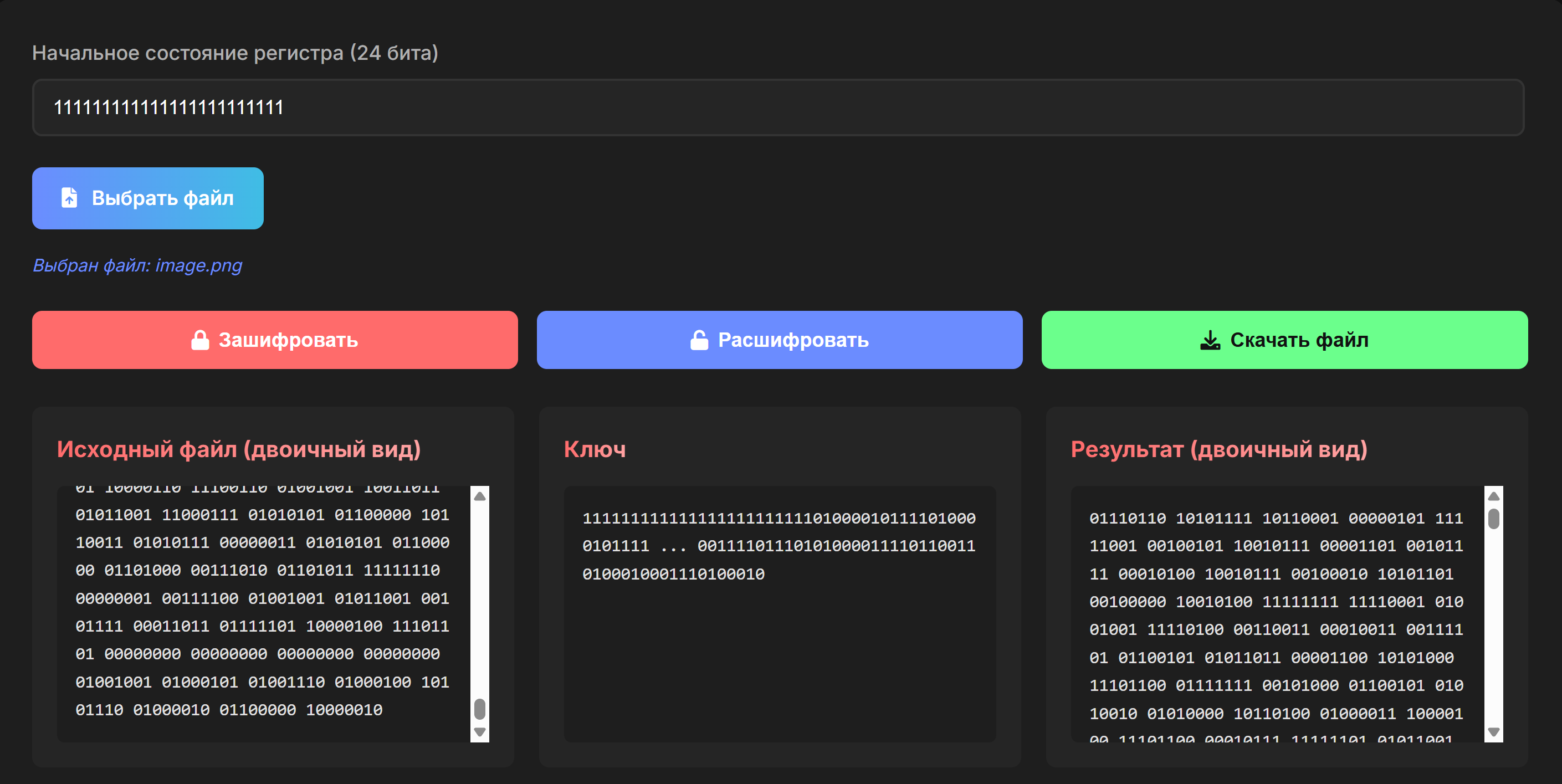
10110110 00110111 00010000 10100010 01110011 10010000 10010011 11011000 01000011 00100000

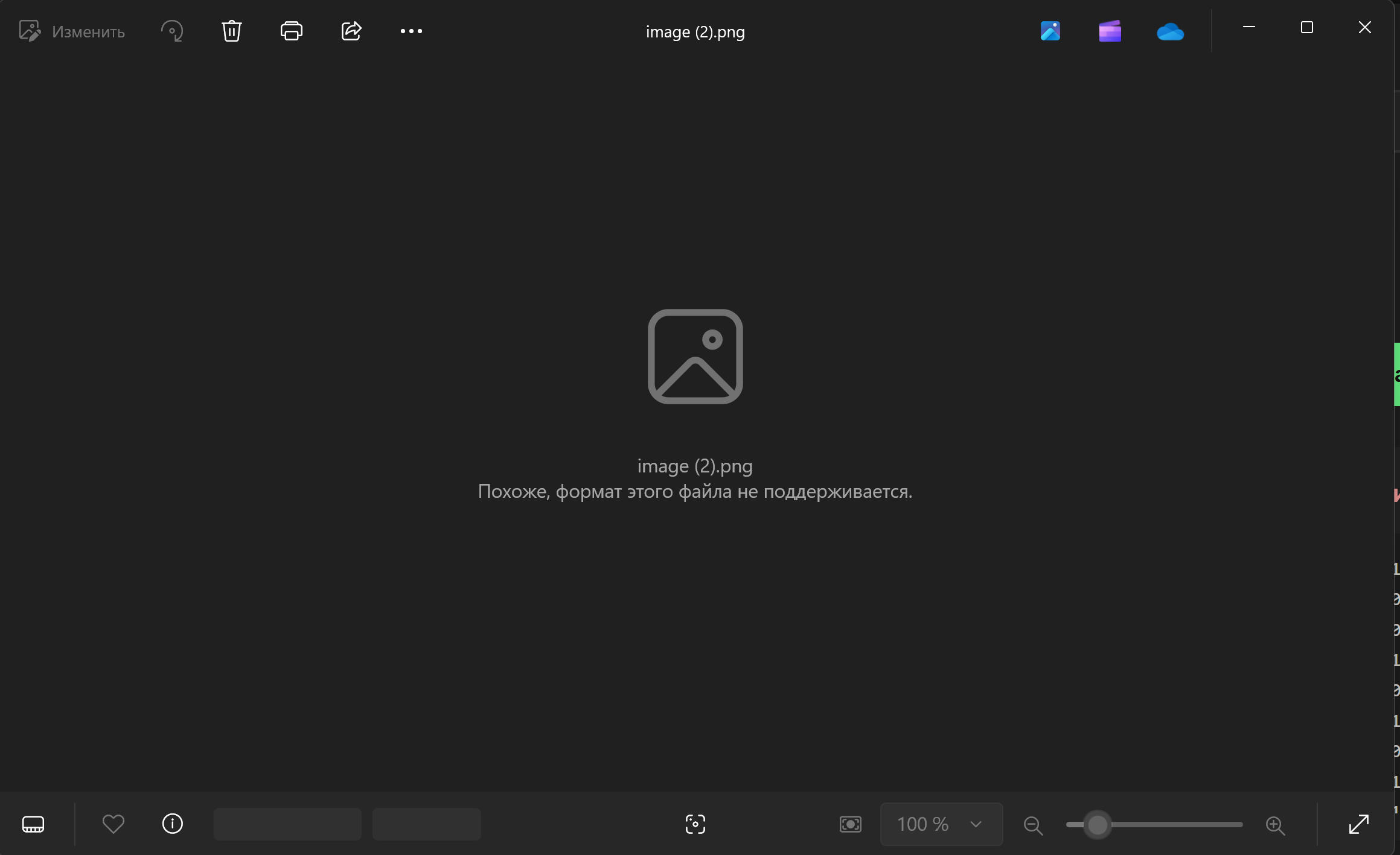


Рисунок 3 – Исходный рисунок

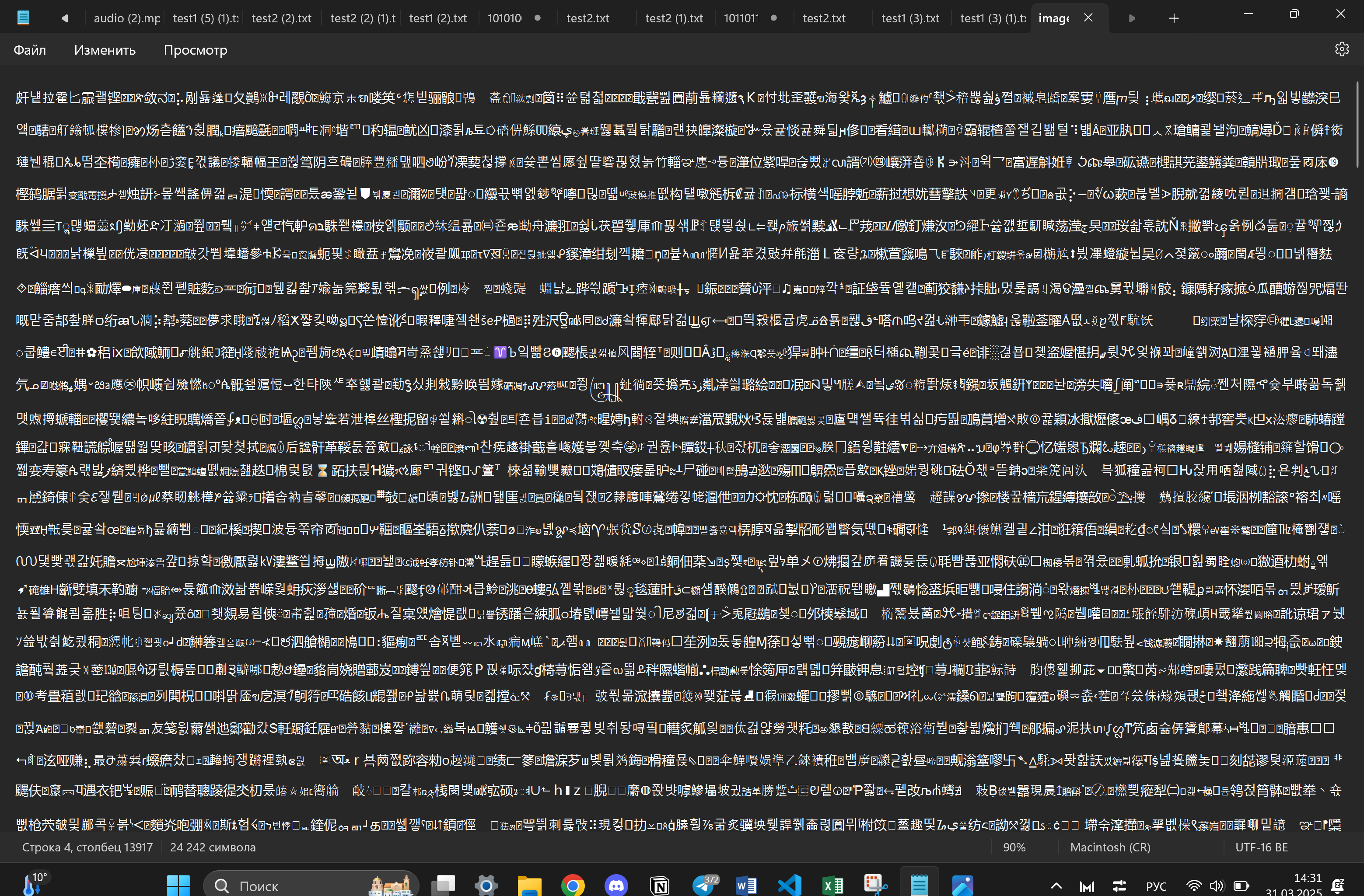


Работа программы (шифрование):

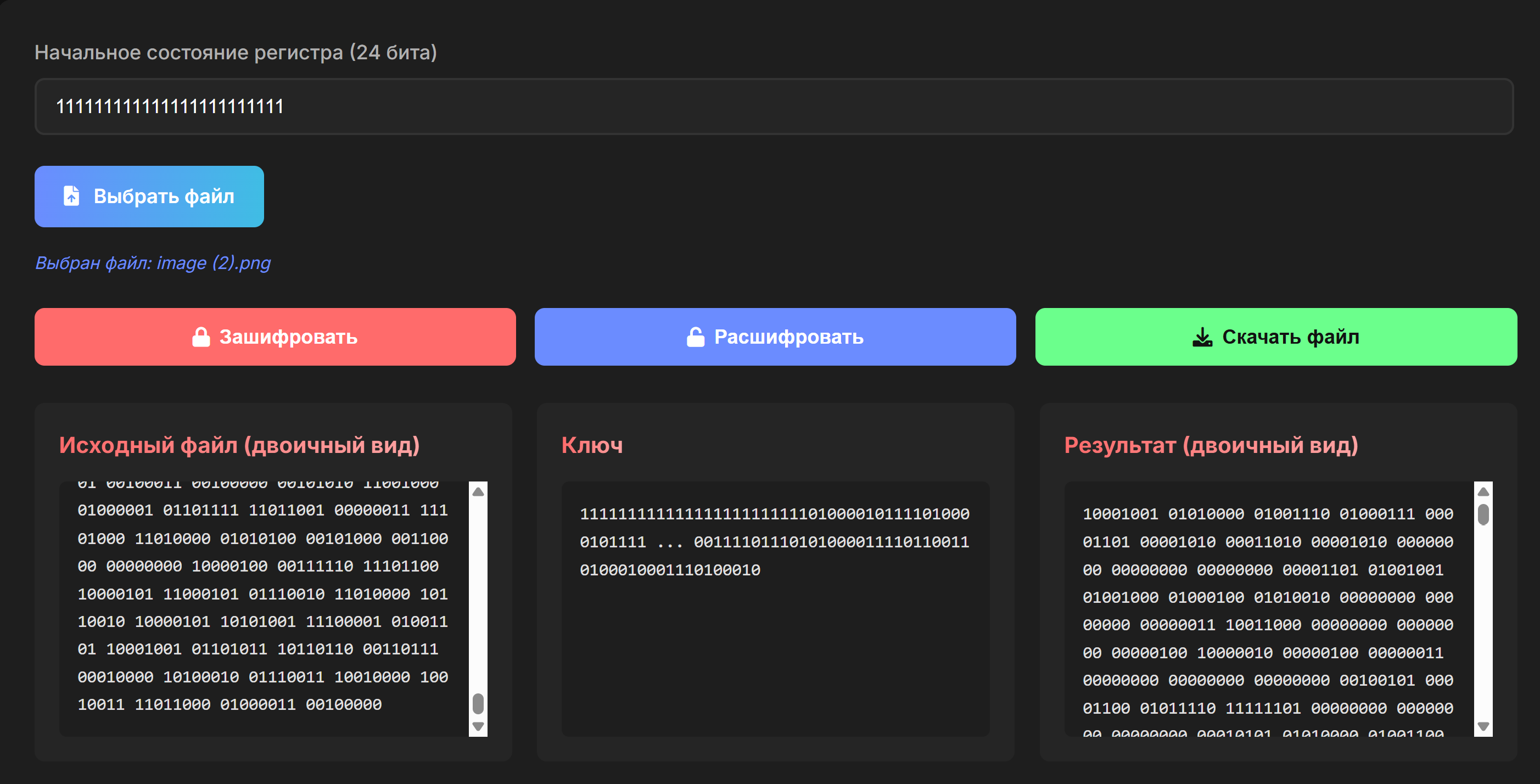
****



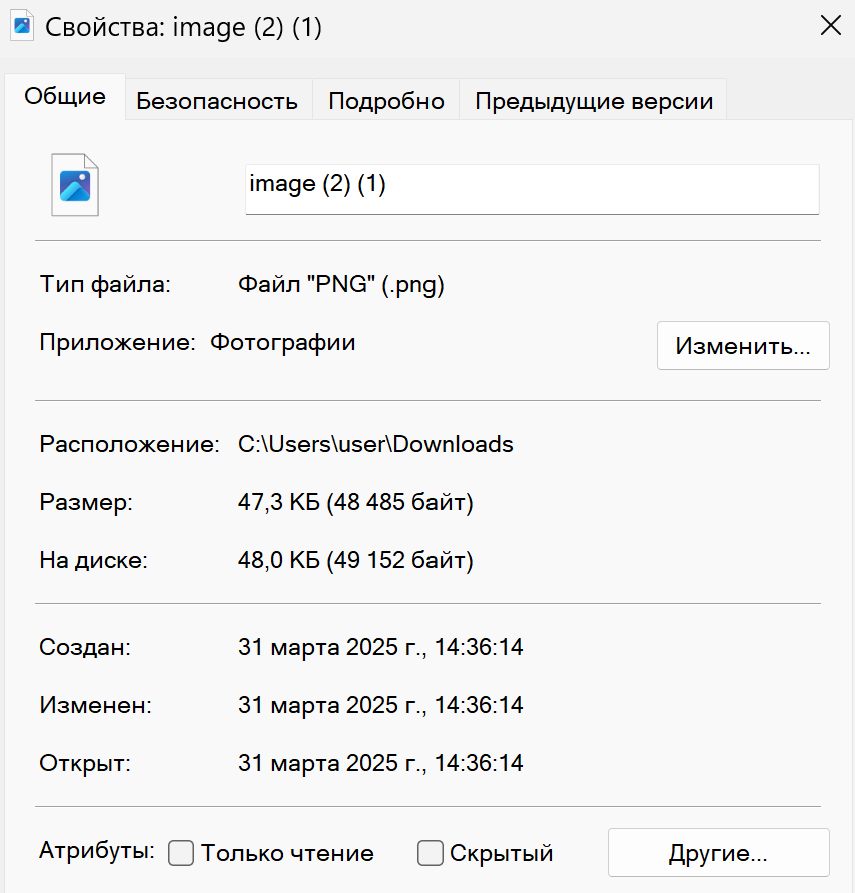
Содержимое зашифрованного скачанного файла image (2).png:

****

Результат работы программы (дешифрование):



****

****