

УО “Белорусский государственный университет информатики и
радиоэлектроники”
Кафедра ПОИТ

Отчёт по лабораторной работе №2
по предмету
Теория Информации
Вариант 11

Выполнил:
студент гр.351001
Орсик С.П.

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:

$$x^{33} + x^{13} + 1$$

Работа программы

Общий интерфейс:

Потоковое шифрование

Начальное состояние регистра (33 бита):

Введите 33 бита (только 0 и 1)

Выбрать файл

Зашифровать

Расшифровать

Ключ:

Сгенерированный ключ

Исходный файл:

Исходный файл (двоичный вид)

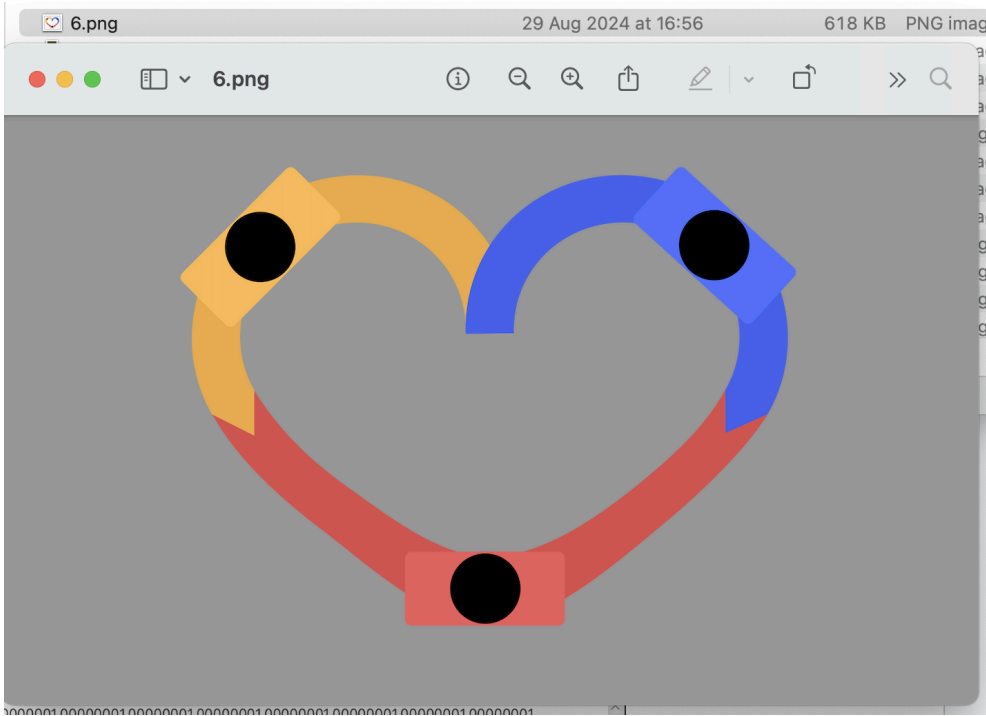
Зашифрованный файл:

Зашифрованный файл (двоичный вид)

Тесты с разными файлами

1. Изображение

Файл до обработки:



Шифрование:

Потоковое шифрование

Начальное состояние регистра (33 бита):

111111111111111111111111111111111

Выбрать файл

Зашифровать

Расшифровать

Ключ:

00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000001
00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000001
00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000001
00000001 00000001 00000001 00000001 00000001 00000001 00000001 00000001

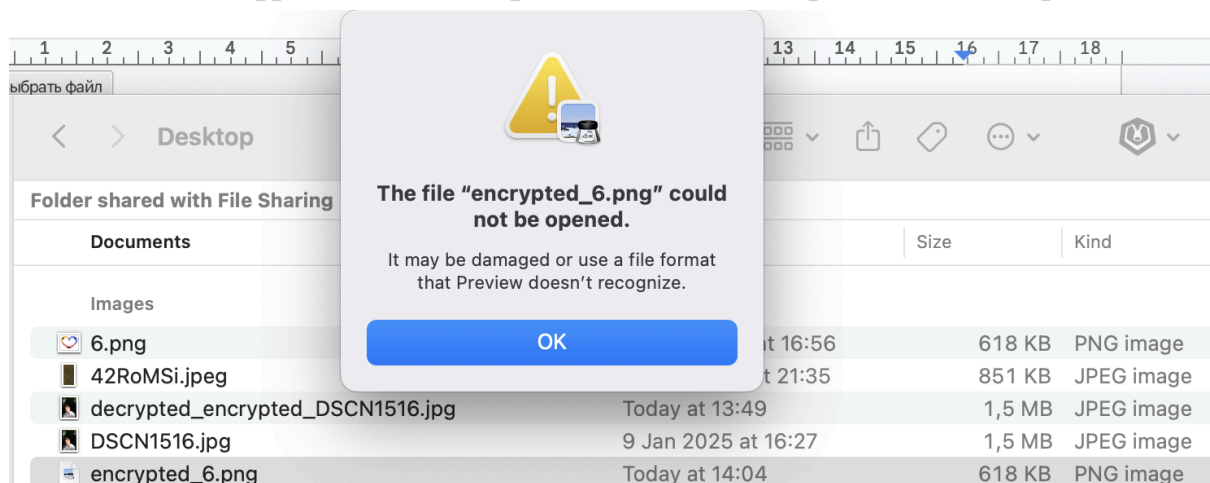
Исходный файл:

10001001 01010000 01001110 01000111 00001101 00001010 00011010 00001010
00000000 00000000 00000000 00001101 01001001 01001000 01000100 01010010
00000000 00000000 00100100 10101100 00000000 00000000 00011110 01101111
00001000 00000110 00000000 00000000 00000000 01110000 11101001 00110000

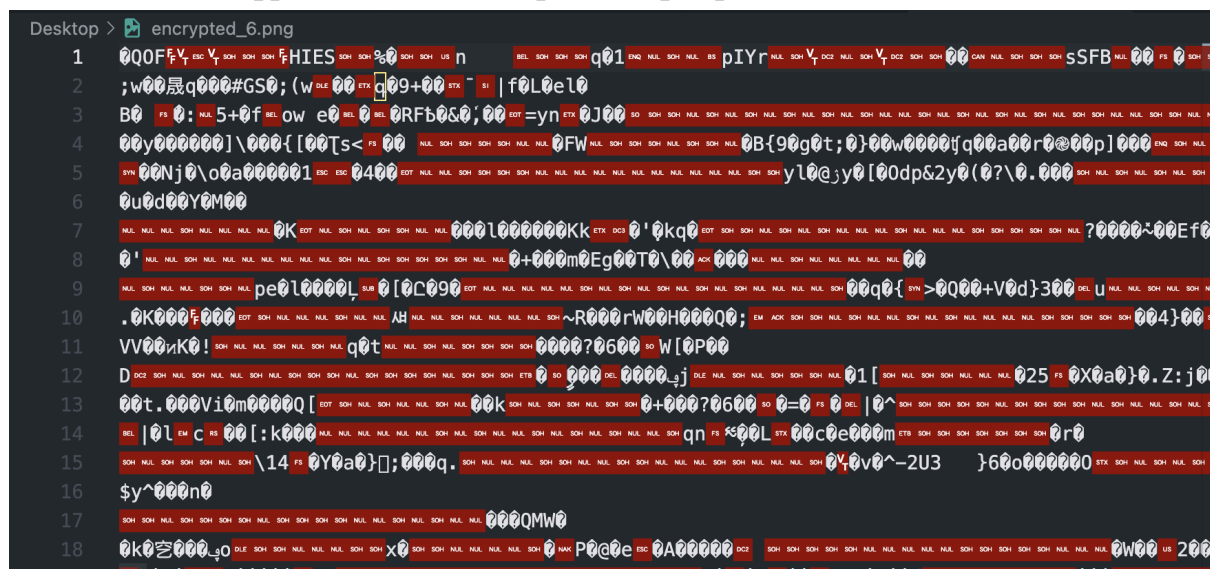
Зашифрованный файл:

10001000 01010001 01001111 01000110 00001100 00001011 00011011 00001011
00000001 00000001 00000001 00001100 01001000 01001001 01000101 01010011
00000001 00000001 00100101 10101101 00000001 00000001 00011111 01101110
00001001 00000111 00000001 00000001 00000001 01110001 11101000 00110001

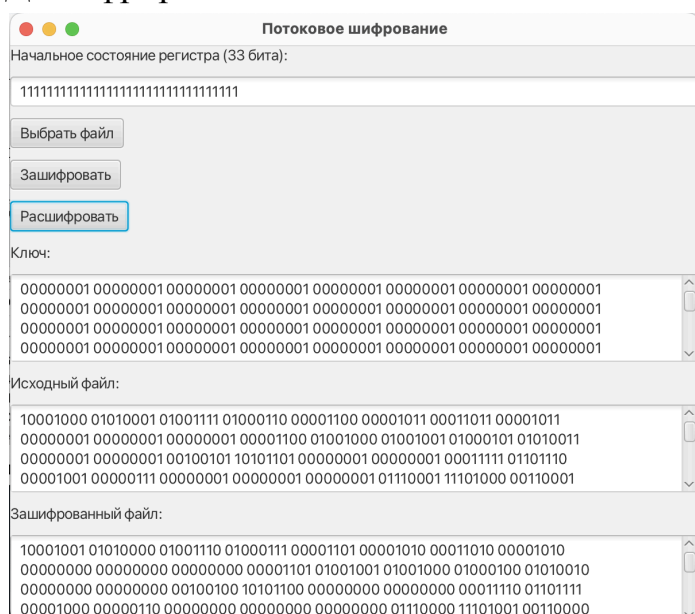
Файл после шифрование(не открывается из-за повреждения содержимого):



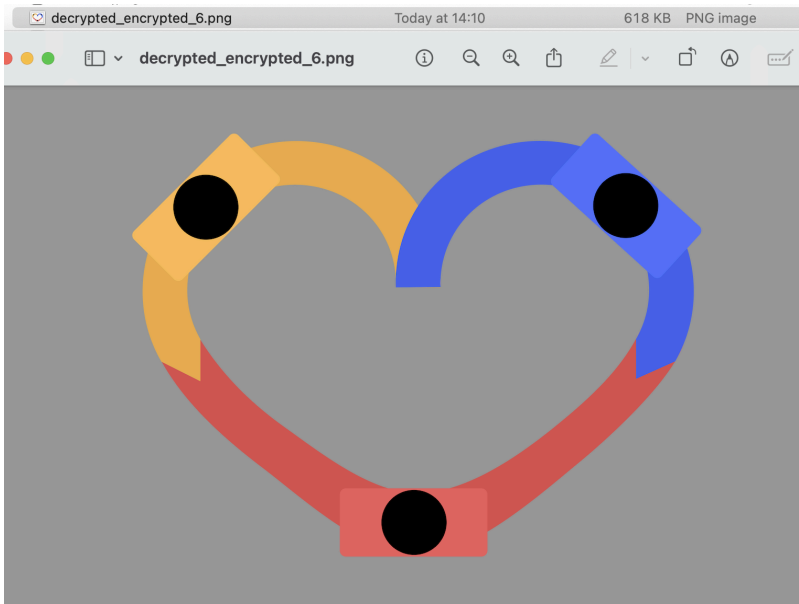
Биты после шифрования были перекодированы в байты:



Дешифрирование:

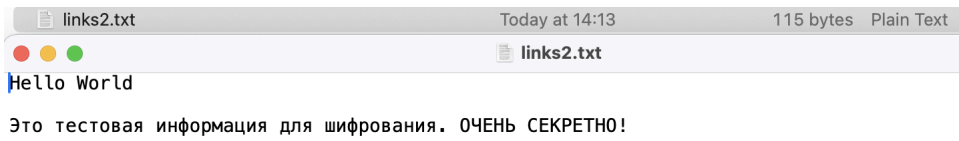


Файл после дешифрования (фото восстановилось):

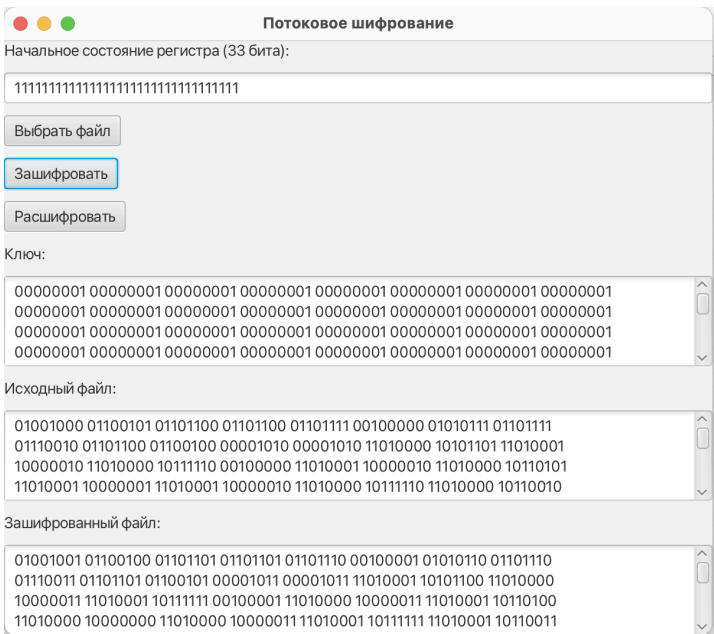


2. Текстовый файл

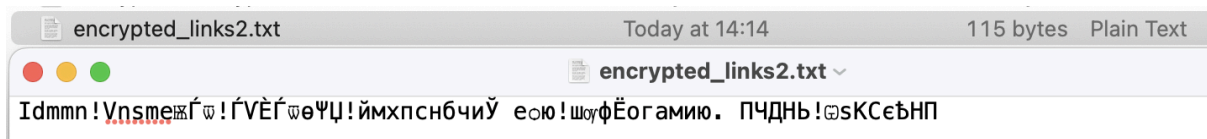
Файл до обработки:



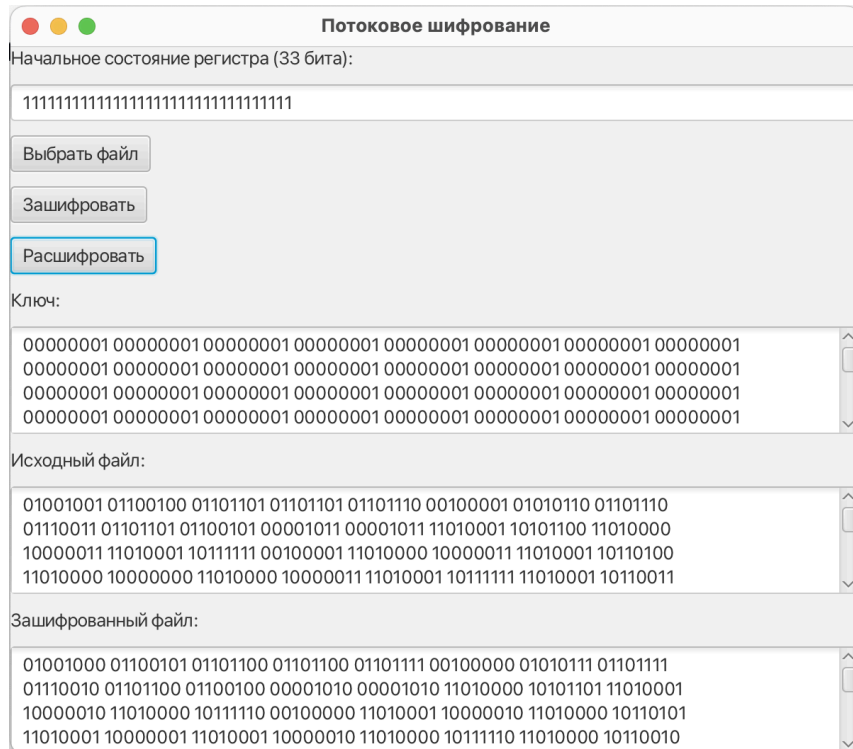
Шифрование:



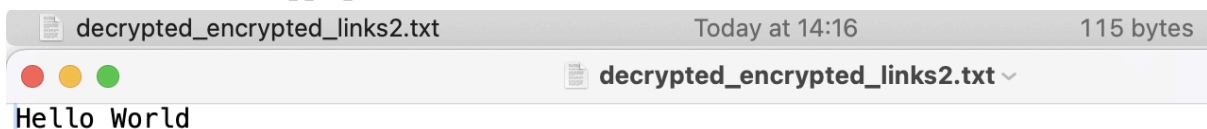
Файл после шифрования:



Дешифрирование:



Файл после дешифрирования:



Это тестовая информация для шифрования. ОЧЕНЬ СЕКРЕТНО!

Тесты с различными ключами

1) Простой ключ, небольшой текст

Ключ: 11111111111111111111111111111111

Исходный текст: 0011000100110100

Шифротекст: 00110000 00110101

Шифрование:

Потоковое шифрование

Начальное состояние регистра (33 бита):
11111111111111111111111111111111

Выбрать файл

Зашифровать

Расшифровать

Ключ:
00000001 00000001

Исходный файл:
00110001 00110100

Зашифрованный файл:
00110000 00110101

Дешифрирование:

Потоковое шифрование

Начальное состояние регистра (33 бита):
11111111111111111111111111111111

Выбрать файл

Зашифровать

Расшифровать

Ключ:
00000001 00000001

Исходный файл:
00110000 00110101

Зашифрованный файл:
00110001 00110100

2) Сложный ключ, небольшой текст

Ключ:011010101010110101011101101011010

Исходный текст:0011000100110100

Шифротекст:00110001 00110101

Шифрование:

Потоковое шифрование

Начальное состояние регистра (33 бита):

011010101010110101011101101011010

Выбрать файл

Зашифровать

Расшифровать

Ключ:

00000000 00000001

Исходный файл:

00110001 00110100

Зашифрованный файл:

00110001 00110101

Дешифрирование:

Потоковое шифрование

Начальное состояние регистра (33 бита):

011010101010110101011101101011010

Выбрать файл

Зашифровать

Расшифровать

Ключ:

00000000 00000001

Исходный файл:

00110001 00110101

Зашифрованный файл:

00110001 00110100

3) Простой ключ, большой текст

Ключ: 11111111111111111111111111111111

Исходный

текст:

```
01011111110101100000110100010101111101011011101111101011011011
11001100110011111001100101001100010011010100100100000010000110011
111101001000010110011111100100101111100111000110010011000100110
11010101111110101000110100010010111101000011000001100101010000010
01110101101001000011010100100001101110111100111010011001001010010
110111111001100010110010111100011111011010111110011000011000011011
0010100001111110000100111101100001101111110101000001000110001000
0110101100010110101110000101100000001110111
```

Шифротекст: 01011110 11010111 00001100 00010100 11110100 10111010
10111111 10110111 11110010 00110010 11100111 01010010 00010010
01010011 01000001 10000111 01111111 10010001 10110010 11111000
00101110 11001111 00110011 01100011 01101100 01011110 10101001
11010000 00101110 01000010 00000111 01010101 00010010 10101101
00100000 10101001 00001100 11011110 01110101 11001001 01001010
01111110 01100011 11001011 11000110 11011010 11111000 10000110
00011010 00101000 01111111 00010011 11011001 01101111 11101010
00001001 11000101 00110101 10001011 01011101 00101101 00000111
01110000

Шифрование:

Потоковое шифрование

Начальное состояние регистра (32 бита):

11111111111111111111111111111111

Выбрать файл

Зашифровать

Расшифровать

Ключ:

00000001 00000000 00000001 00000000 00000001 00000000 00000001 00000000
00000001 00000000 00000001 00000000 00000001 00000000 00000001 00000000
00000001 00000000 00000001 00000000 00000001 00000000 00000001 00000000
00000001 00000000 00000001 00000000 00000001 00000000 00000001 00000000

Исходный файл:

00010011 10101101 00100001 10101001 00001101 11011110 01110100 11001001
01001011 01111110 01100010 11001011 11000111 11011010 11111001 10000110
00011011 00101000 01111110 00010011 11011000 01101111 11101010 00001000
11000100 00110101 10001011 01011100 00101100 00000111 0111

Зашифрованный файл:

00010010 10101101 00100000 10101001 00001100 11011110 01110101 11001001
01001010 01111110 01100011 11001011 11000110 11011010 11111000 10000110
00011010 00101000 01111111 00010011 11011001 01101111 11101010 00001001
11000101 00110101 10001011 01011101 00101101 00000111 01110000

Дешифрирование:

Потоковое шифрование

Начальное состояние регистра (33 бита):

111111111111111111111111111111111111

Выбрать файл

Зашифровать

Расшифровать

Ключ:

00000001 00000000 00000001 00000000 00000001 00000000 00000001 00000000
00000001 00000000 00000001 00000000 00000001 00000000 00000001 00000000
00000001 00000000 00000001 00000000 00000001 00000000 00000001 00000000
00000001 00000000 00000000 00000001 00000001 00000000 00000000 00000001

Исходный файл:

00010010 10101101 00100000 10101001 00001100 11011110 01110101 11001001
01001010 01111110 01100011 11001011 11000110 11011010 11111000 10000110
00011010 00101000 01111111 00010011 11011001 01101111 11101010 00001001
11000101 00110101 10001011 01011101 00101101 00000111 01110000

Зашифрованный файл:

00010011 10101101 00100001 10101001 00001101 11011110 01110100 11001001
01001011 01111110 01100010 11001011 11000111 11011010 11111001 10000110
00011011 00101000 01111110 00010011 11011000 01101111 11101010 00001000
11000100 00110101 10001011 01011100 00101100 00000111 01110000

4) Сложный ключ, большой текст:

Ключ: 011010101010110101011101101011010

Исходный

текст:

00100011100101010000110110010100111010010100110001101001010011111
11111010000010101010110110011100110110101001001001101000000010110
01110010001110100100001101001011011000101101110111010001110101001
01000

Шифротекст: 00100011 10010100 00001100 10010100 11101000 01001100
01101000 01001111 11111100 00000101 01010111 11001110 01101100
01001000 00110100 00000100 10011100 10001111 10010000 11010011
11011001 10110110 01110100 01110100 00101001

Шифрование:

Потоковое шифрование

Начальное состояние регистра (33 бита):

011010101010110101011101101011010

Выбрать файл

Зашифровать

Расшифровать

Ключ:

00000000 00000001 00000001 00000000 00000001 00000000 00000001 00000000
00000001 00000000 00000001 00000000 00000001 00000001 00000000 00000001
00000000 00000001 00000000 00000001 00000001 00000001 00000000 00000001
00000001

Исходный файл:

00100011 10010101 00001101 10010100 11101001 01001100 01101001 01001111
11111101 00000101 01010110 11001110 01101101 01001001 00110100 00000101
10011100 10001110 10010000 11010010 11011000 10110111 01110100 01110101
00101000

Зашифрованный файл:

00100011 10010100 00001100 10010100 11101000 01001100 01101000 01001111
11111100 00000101 01010111 11001110 01101100 01001000 00110100 00000100
10011100 10001111 10010000 11010011 11011001 10110110 01110100 01110100
00101001

Дешифрирование:

Потоковое шифрование

Начальное состояние регистра (33 бита):

011010101010110101011101101011010

Выбрать файл

Зашифровать

Расшифровать

Ключ:

00000000 00000001 00000001 00000000 00000001 00000000 00000001 00000000
00000001 00000000 00000001 00000000 00000001 00000001 00000000 00000001
00000000 00000001 00000000 00000001 00000001 00000001 00000000 00000001
00000001

Исходный файл:

00100011 10010100 00001100 10010100 11101000 01001100 01101000 01001111
11111100 00000101 01010111 11001110 01101100 01001000 00110100 00000100
10011100 10001111 10010000 11010011 11011001 10110110 01110100 01110100
00101001

Зашифрованный файл:

00100011 10010101 00001101 10010100 11101001 01001100 01101001 01001111
11111101 00000101 01010110 11001110 01101101 01001001 00110100 00000101
10011100 10001110 10010000 11010010 11011000 10110111 01110100 01110101
00101000

Валидация:

Потоковое шифрование

Начальное состояние регистра (33 бита):

011010101010110101011101101011010

Выбрать файл

Зашифровать

Расшифровать

Ключ:

00000000 00000001

Исходный файл:

Зашифрованный файл:

10100100 10010001

Пока не введены исходные данные (или не выбран файл), а также начальное состояние регистра, зашифровать/расшифровать нельзя