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

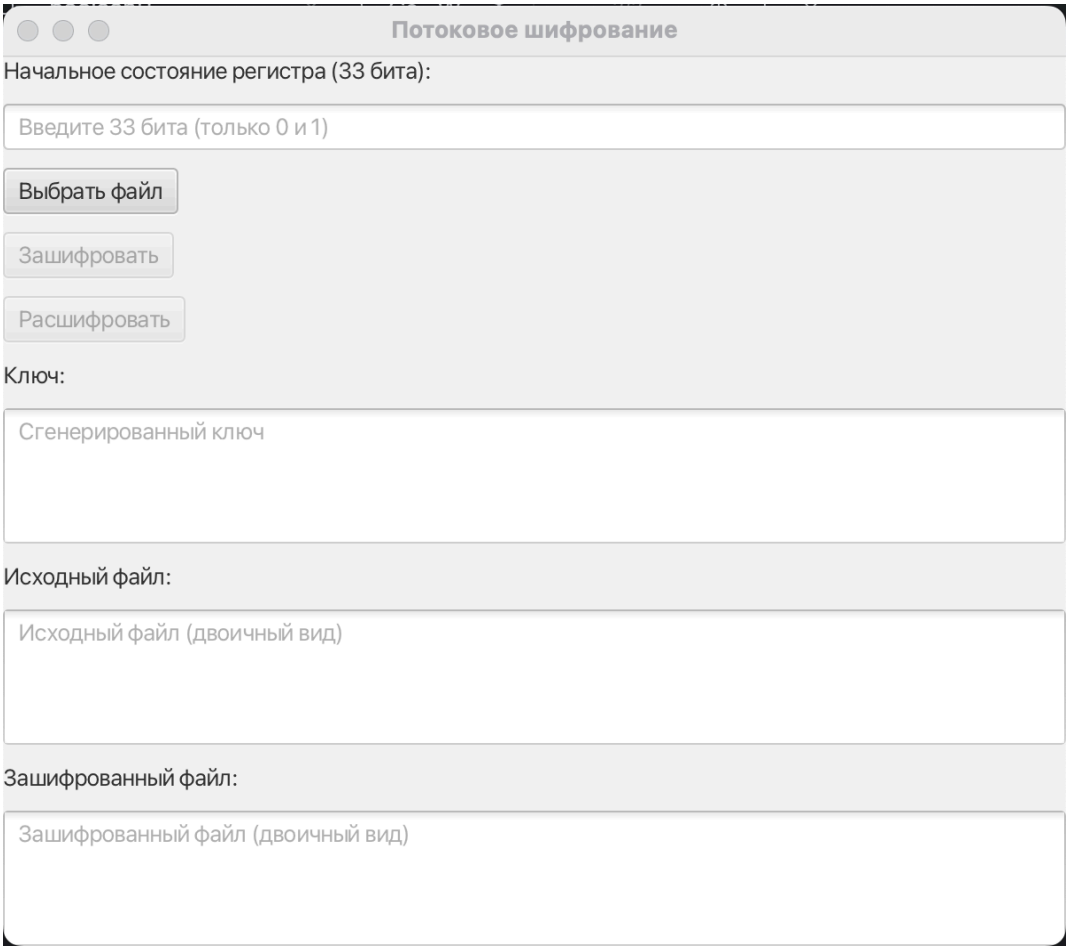
Реализовать систему потокового шифрования и дешифрования для файла с любым содержимым с помощью генератора ключевой последовательности на основе линейного сдвигового регистра с обратной связью $LFSR_1$ (размерность регистра приведена в таблице №1). Начальное состояние регистра ввести с клавиатуры. Поле 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

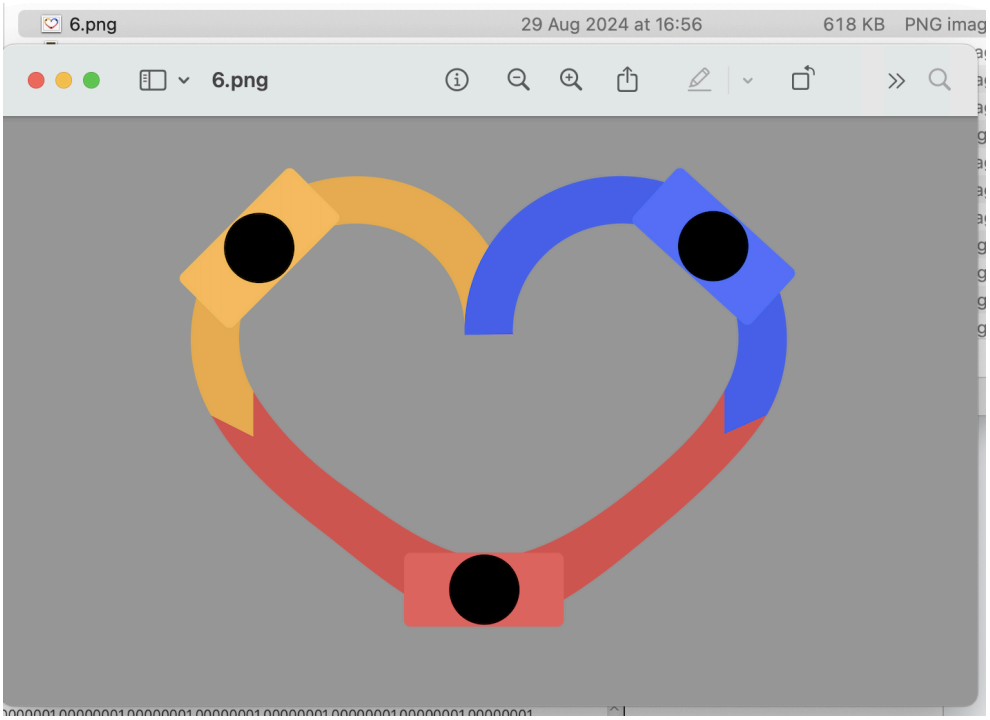
Общий интерфейс:



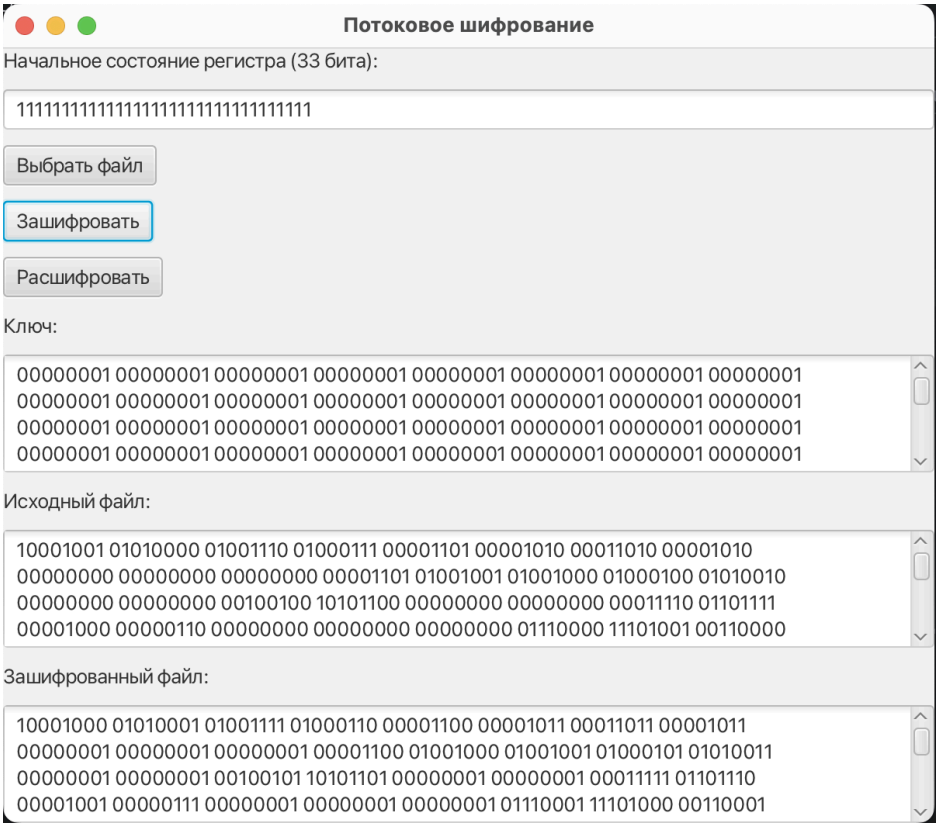
Тесты с разными файлами

1. Изображение

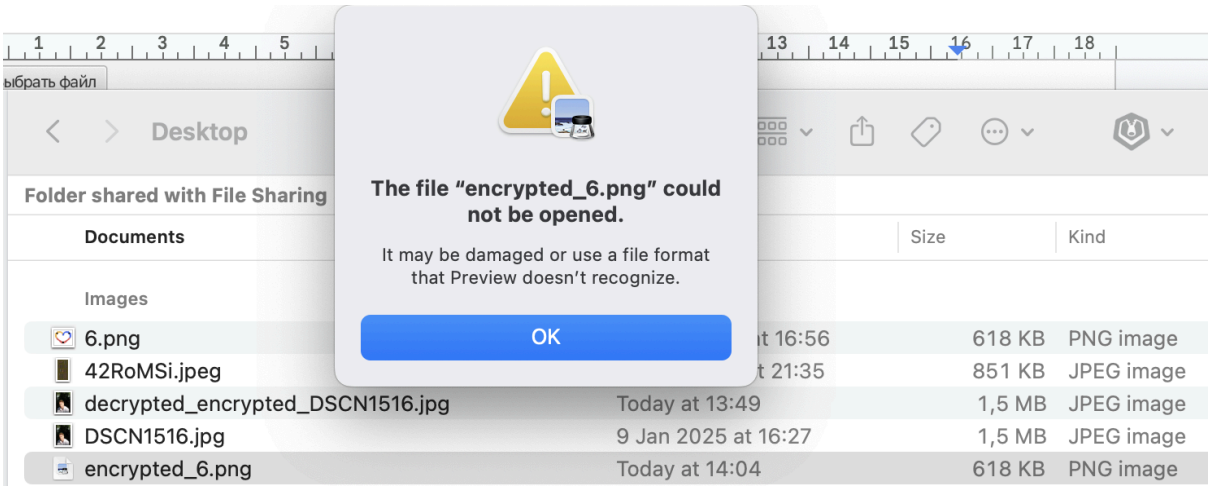
Файл до обработки:



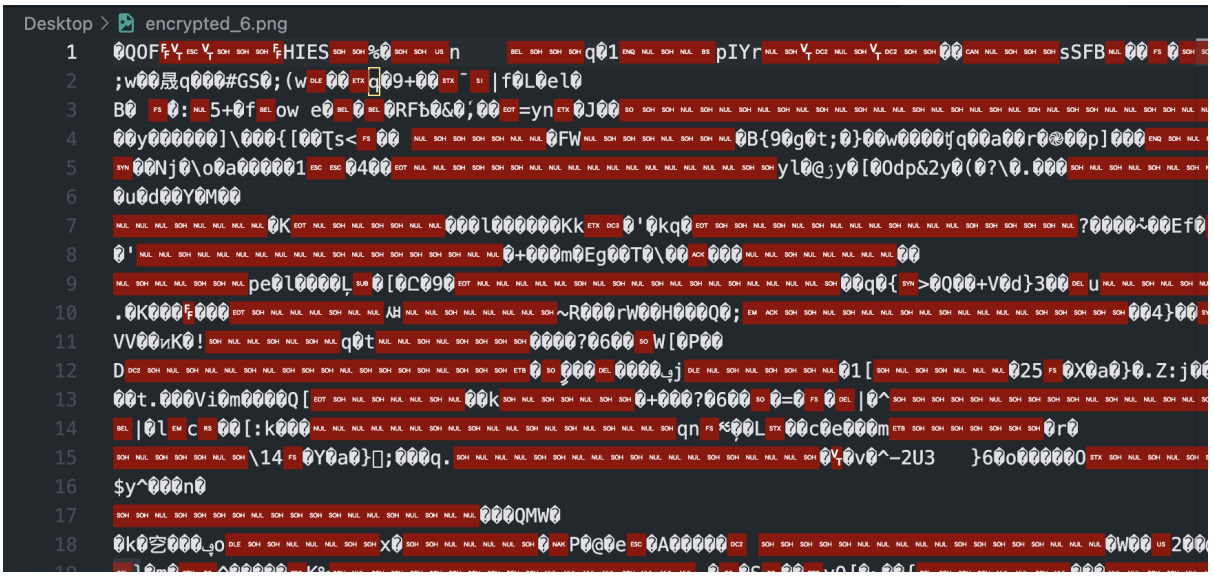
Шифрование:



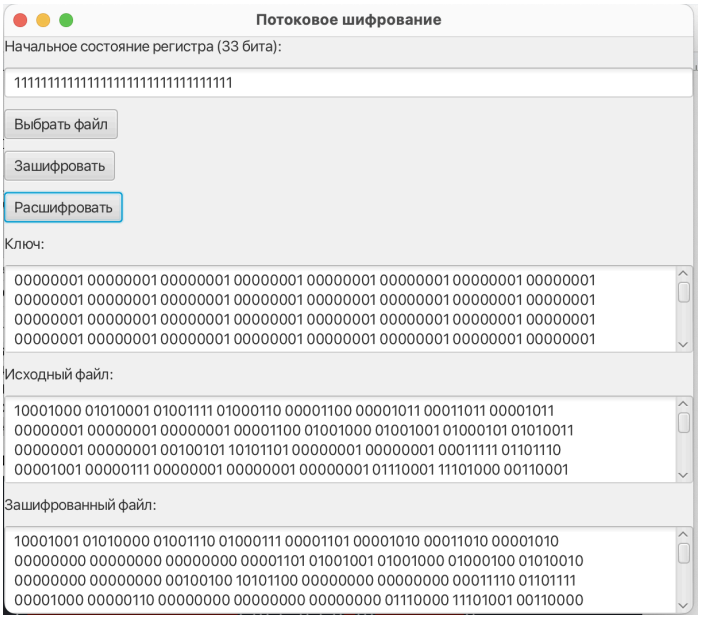
Файл после шифрование(не открывается из-за повреждения содержимого):



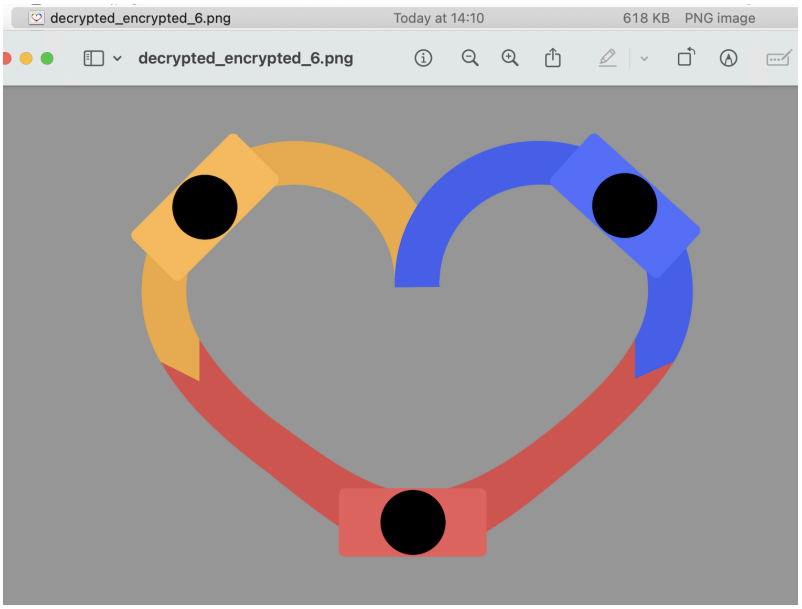
Биты после шифрования были переконвертированы в байты:



Дешифрирование:

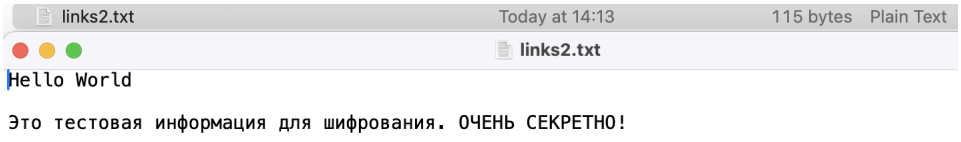


Файл после дешифрирования (фото восстановилось):

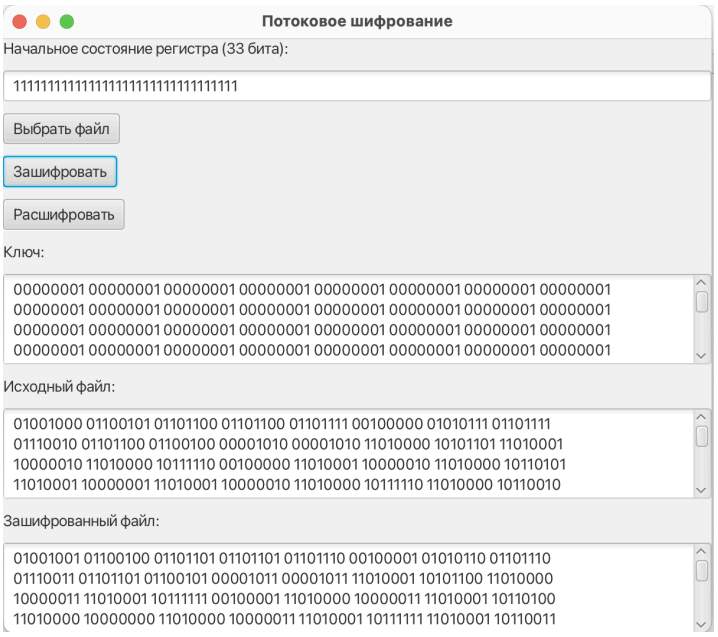


2. Текстовый файл

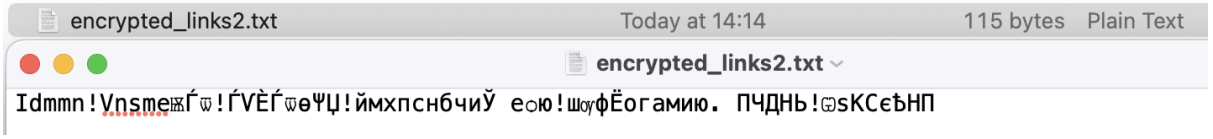
Файл до обработки:



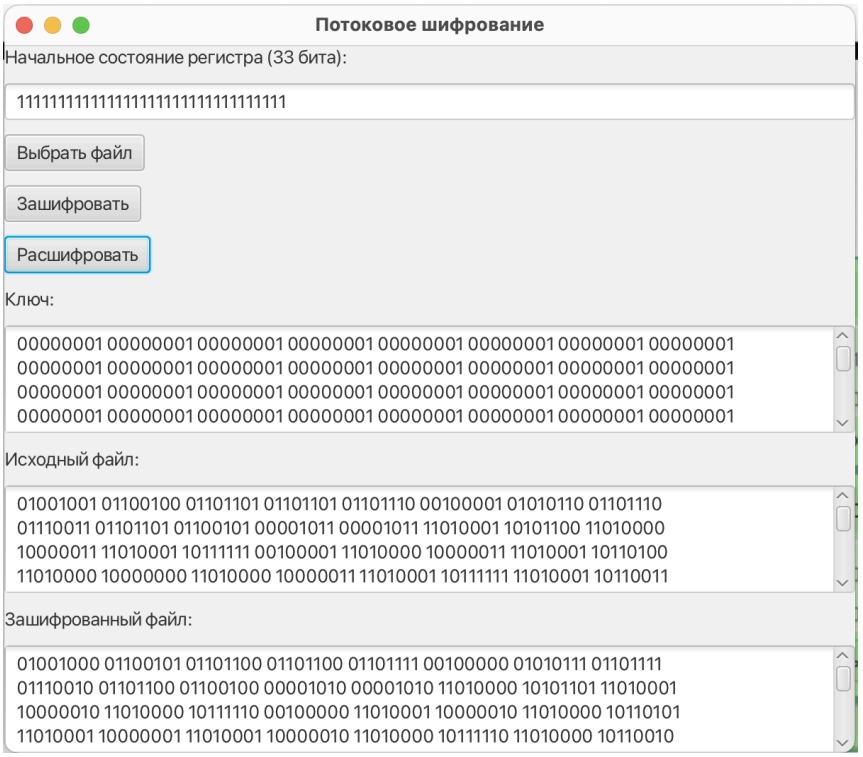
Шифрование:



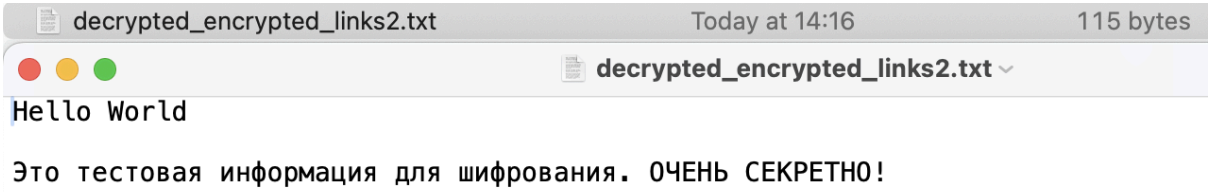
Файл после шифрования:



Дешифрирование:



Файл после дешифрирования:



Тесты с различными ключами

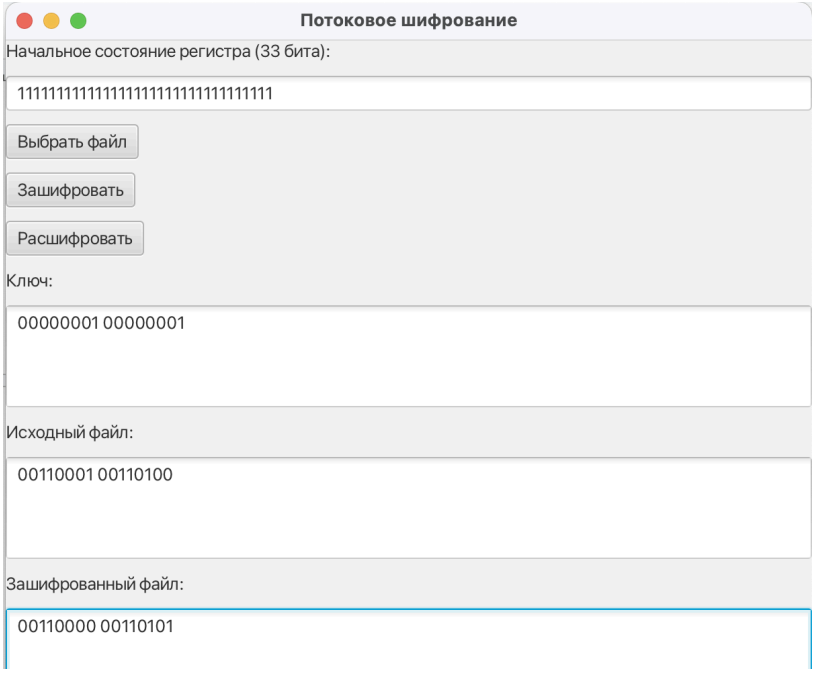
1) Простой ключ, небольшой текст

Ключ: 11111111111111111111111111111111

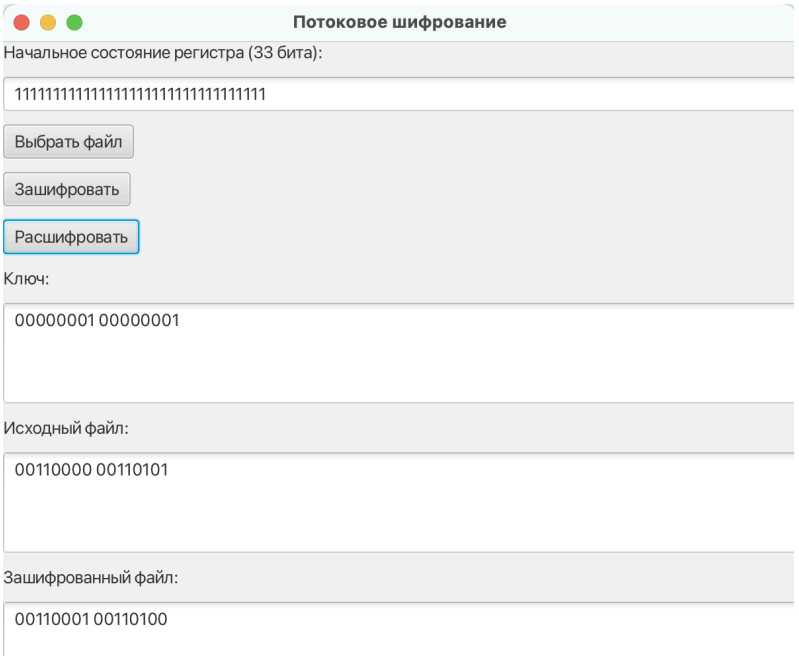
Исходный текст: 0011000100110100

Шифротекст: 00110000 00110101

Шифрование:



Дешифрирование:



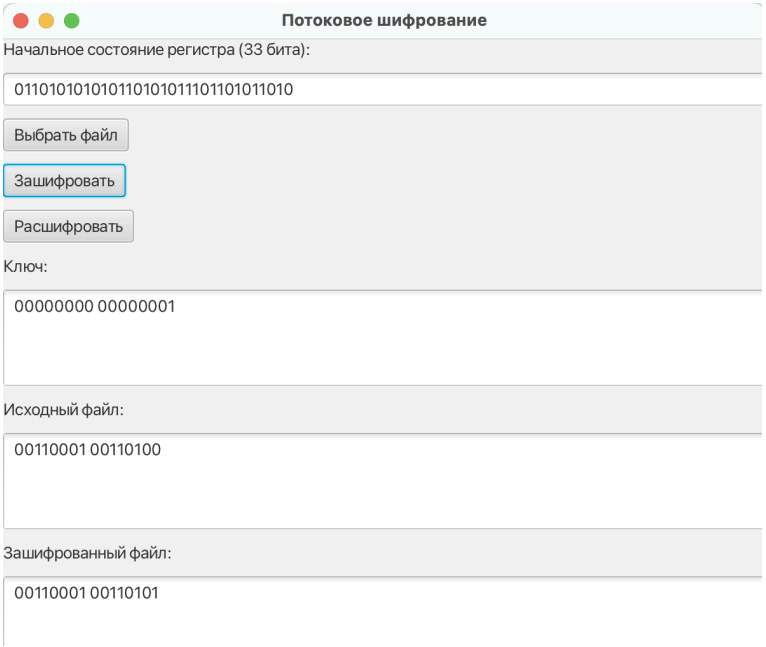
2) Сложный ключ, небольшой текст

Ключ:01101010101011010101111011010110 10

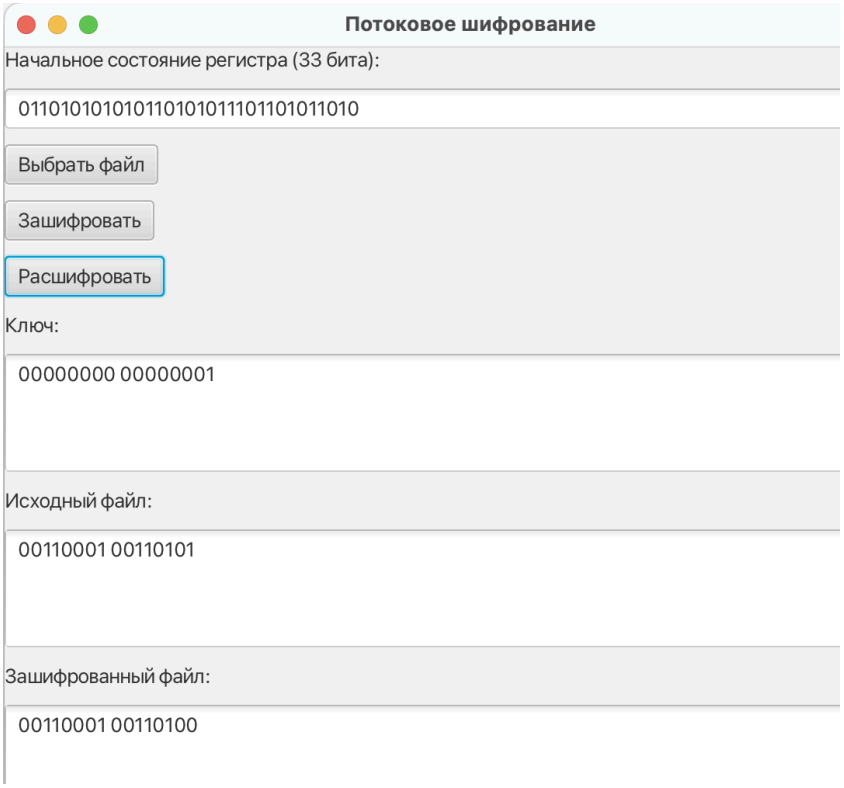
Исходный текст:0011000100110100

Шифротекст:00110001 00110101

Шифрование:



Дешифрирование:



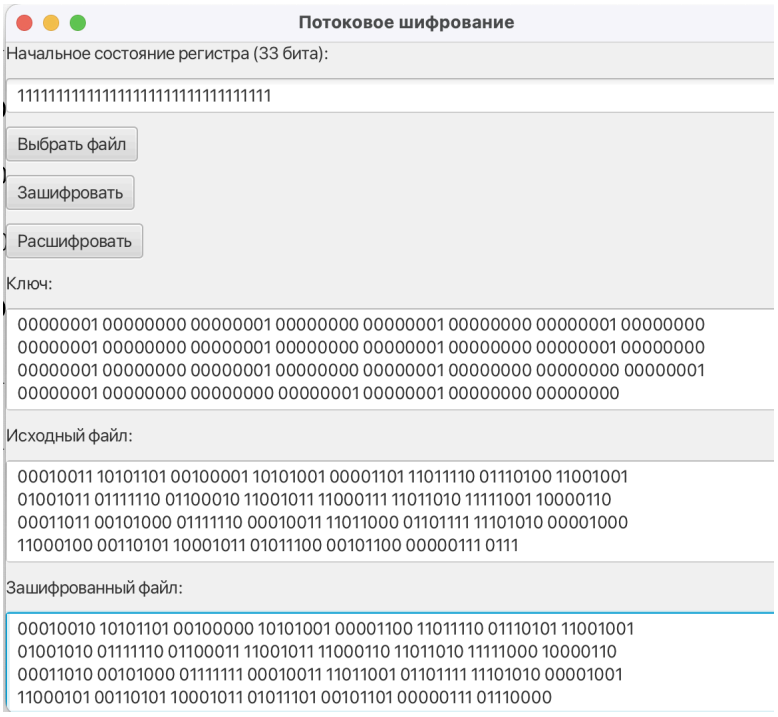
3) Простой ключ, большой текст

Ключ:11111111111111111111111111111111

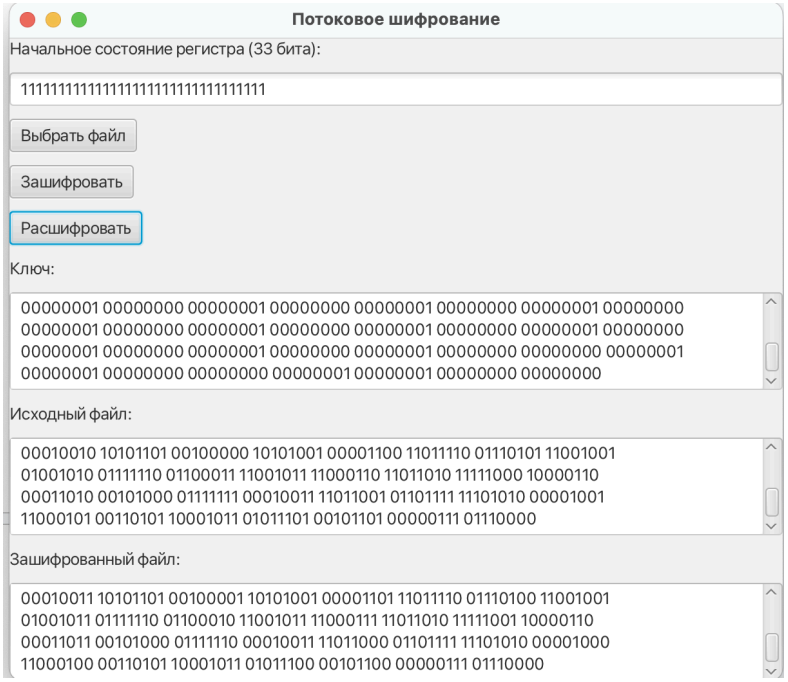
Исходный текст:
0101111111010110000011010001010111110101101110111011111010110111001100110011001111110011001010011000100110101001001000000100001100111111010010000101100111111100100101111110011100011001001100010011011010010111111010100011010001001011110100001100000110010101000001011101011010010000110101001000011010100100001101110111100111010011001001010101101111110011000101100101111000111110110101111110011000001100001101110101110000101101011100001011010111000010110000000011101110001011010111000010111111110101000001000110001000001101011000101101011100001011000000001110111

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:



Дешифрирование:



4) Сложный ключ, большой текст:

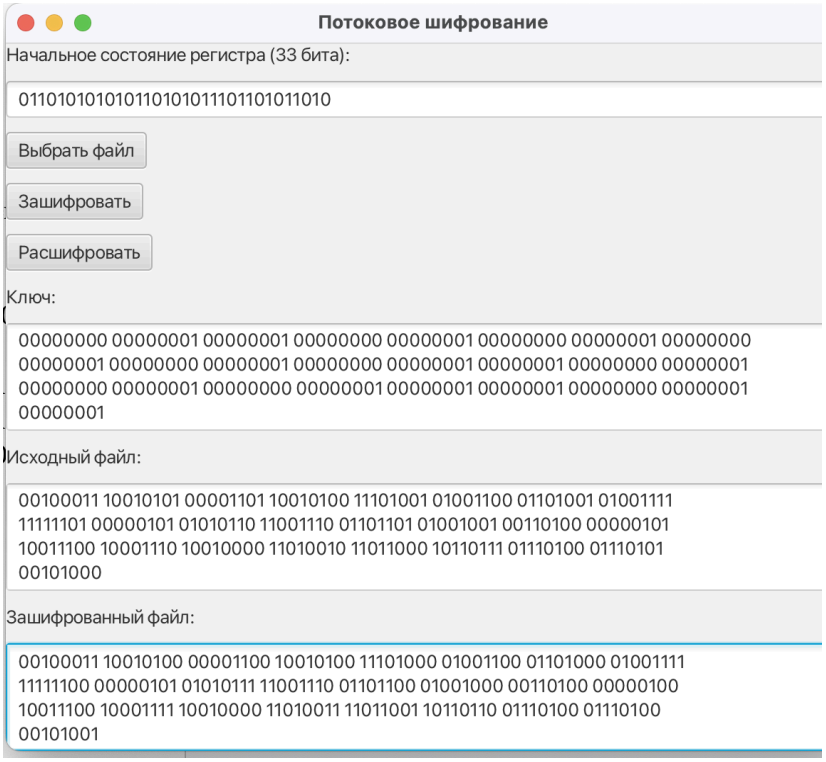
Ключ:01101010101011010101110110101101 0

Исходный текст:

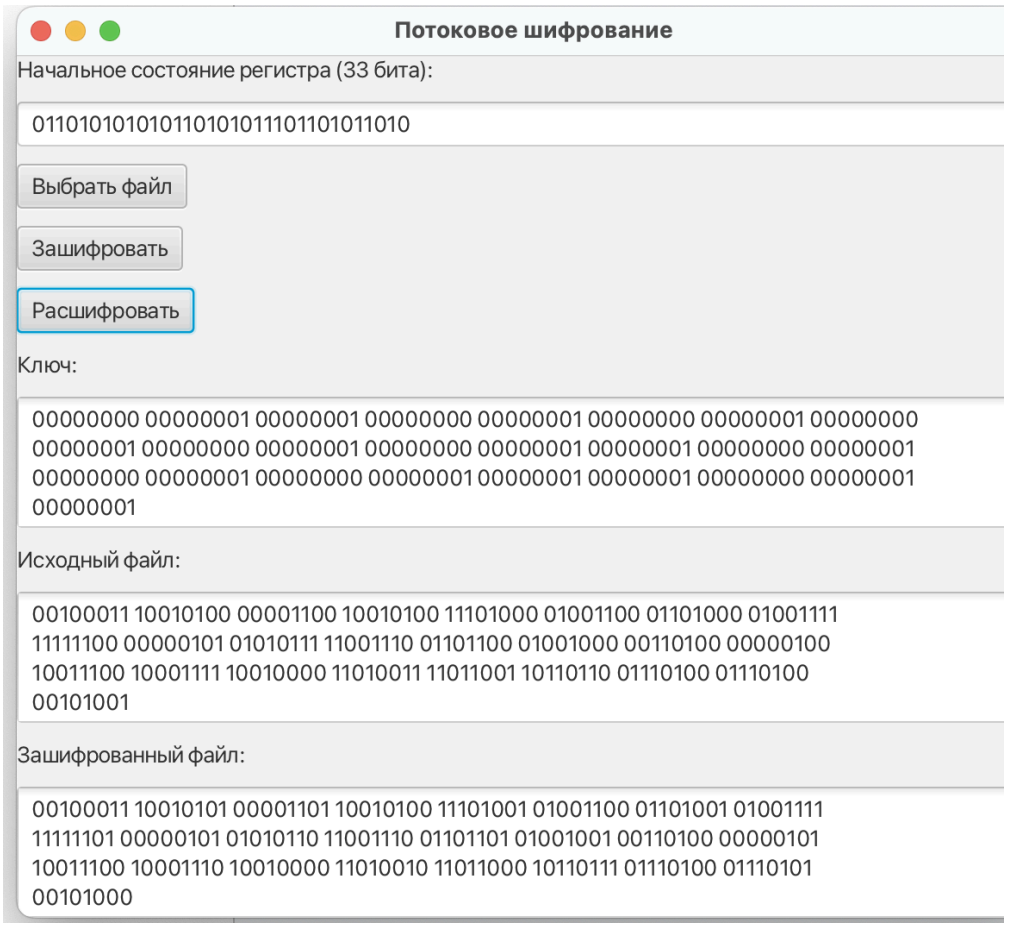
00100011100101010000110110010100111010010100110001101001010011111111101000001010101011011001110011011010100100100110100000001011001110010000111010010000011010010110110001011011101110100011101010010100000

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

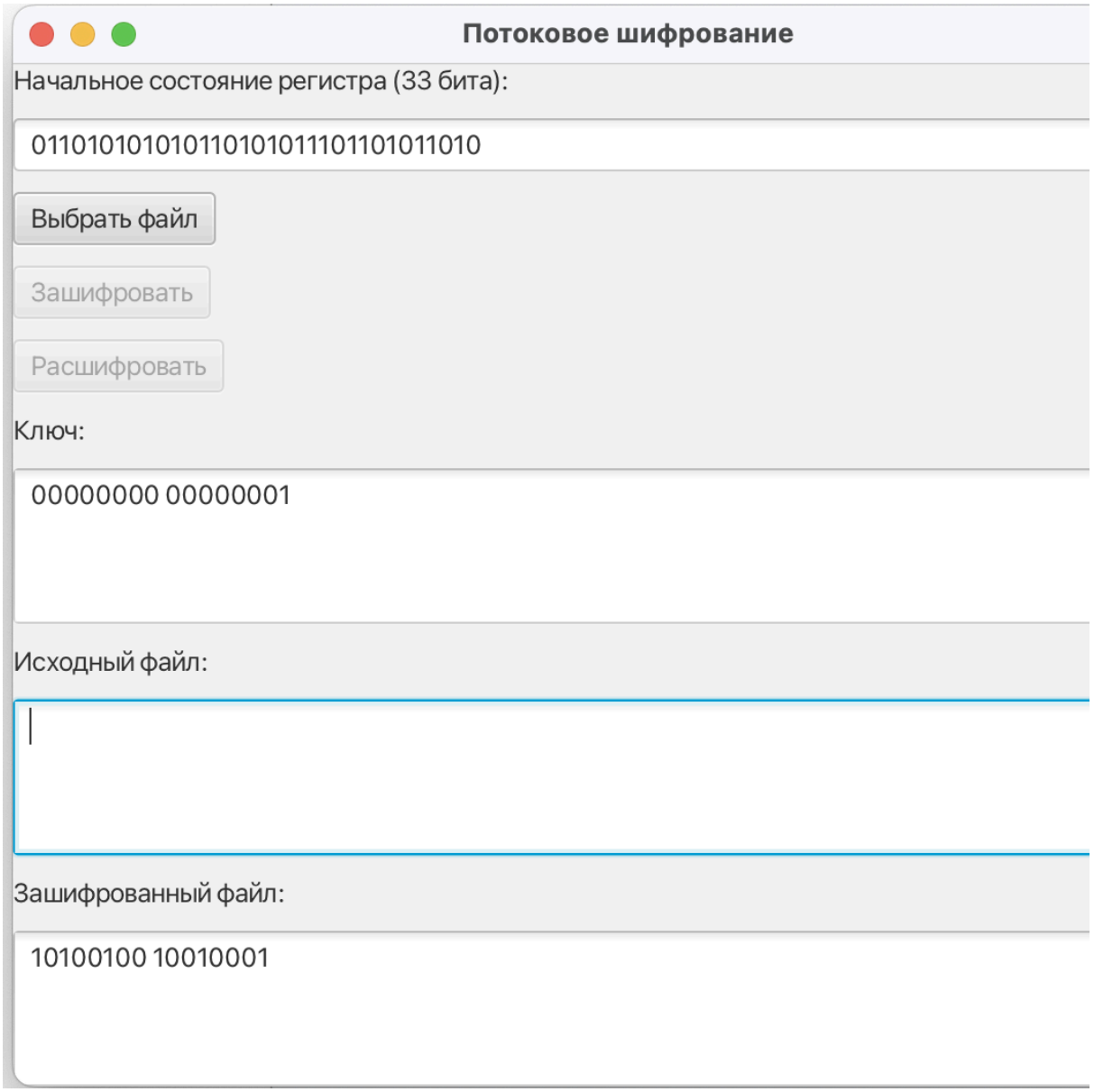
Шифрование:



Дешифрирование:



Валидация:



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