УО «Белорусский государственный университет информатики и радиоэлектроники»
Кафедра ПОИТ

Отчет по лабораторной работе №2
по предмету
Теория Информации

Вариант 16

Выполнил:
Ушаков А.Д.

Проверил:
Болтак С.В.

Группа 351001

Минск 2025

Задание:

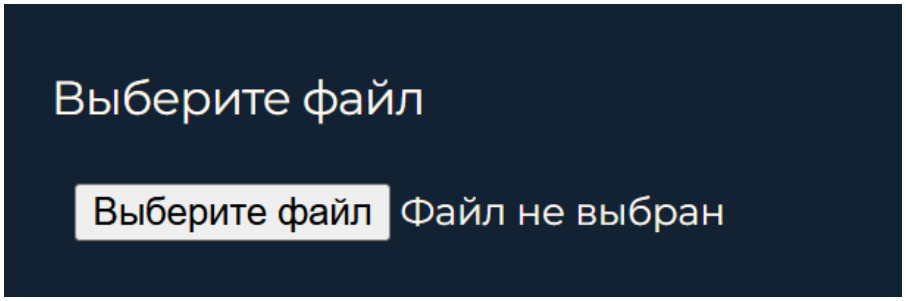
Реализовать систему потокового шифрования и дешифрования для файла с любым содержимым с помощью генератора ключевой последовательности на основе линейного сдвигового регистра с обратной связью LFSR1 (размерность регистра ***38***). Начальное состояние регистра ввести с клавиатуры. Поле для ввода состояния 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

$x^{38} + x^6 + x^5 + x + 1$

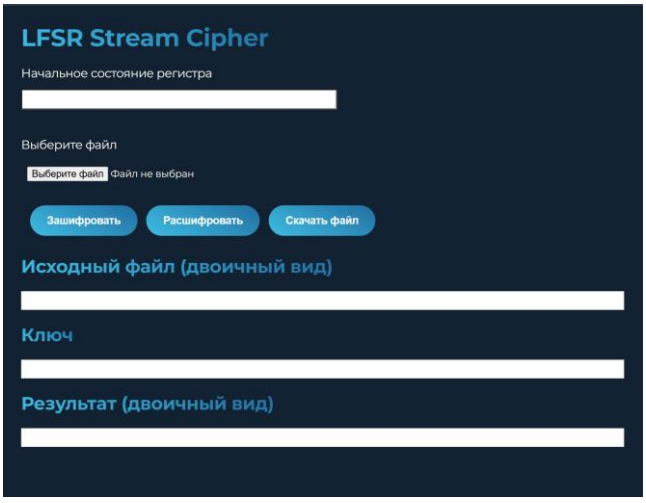
Работа с файлами

Взятие исходного файла:



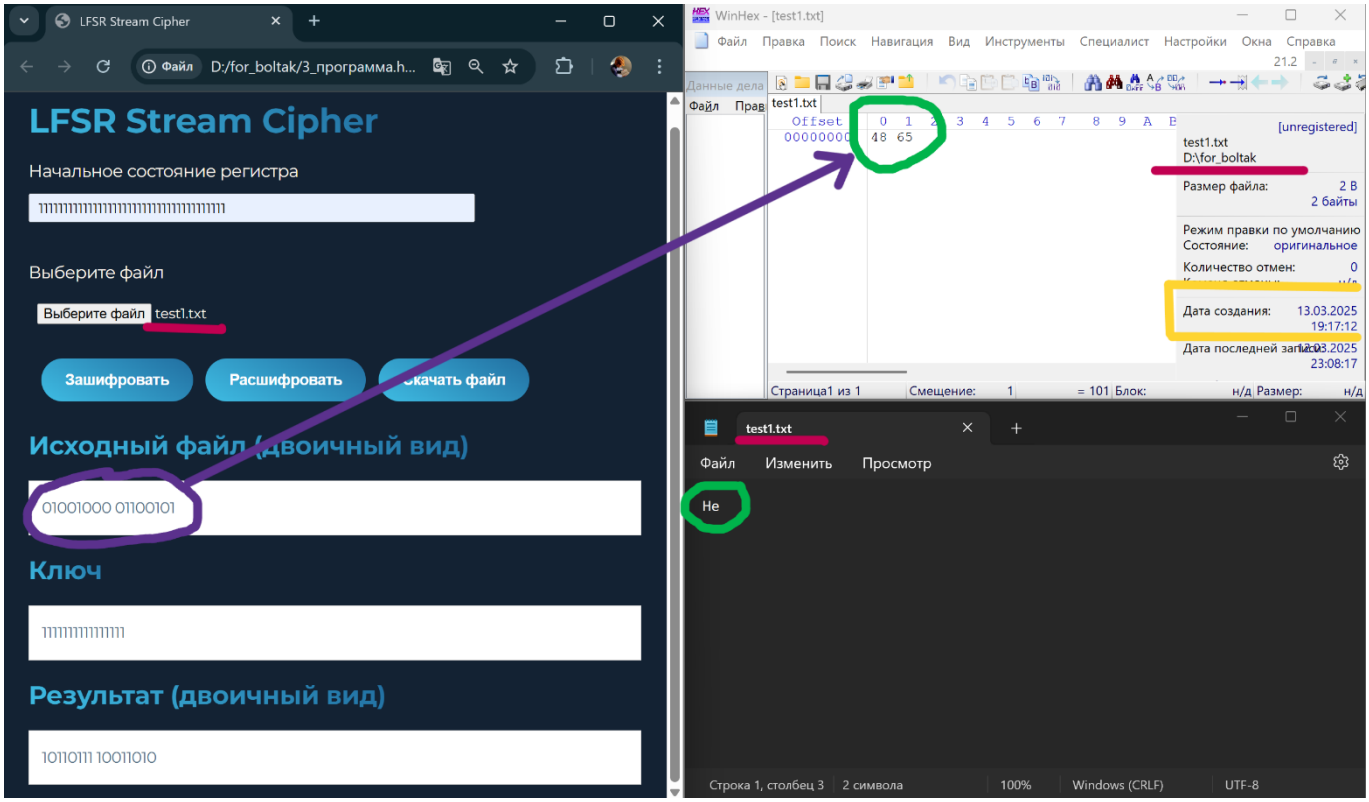
Загрузка результата файла:

Общий внешний вид страницы:

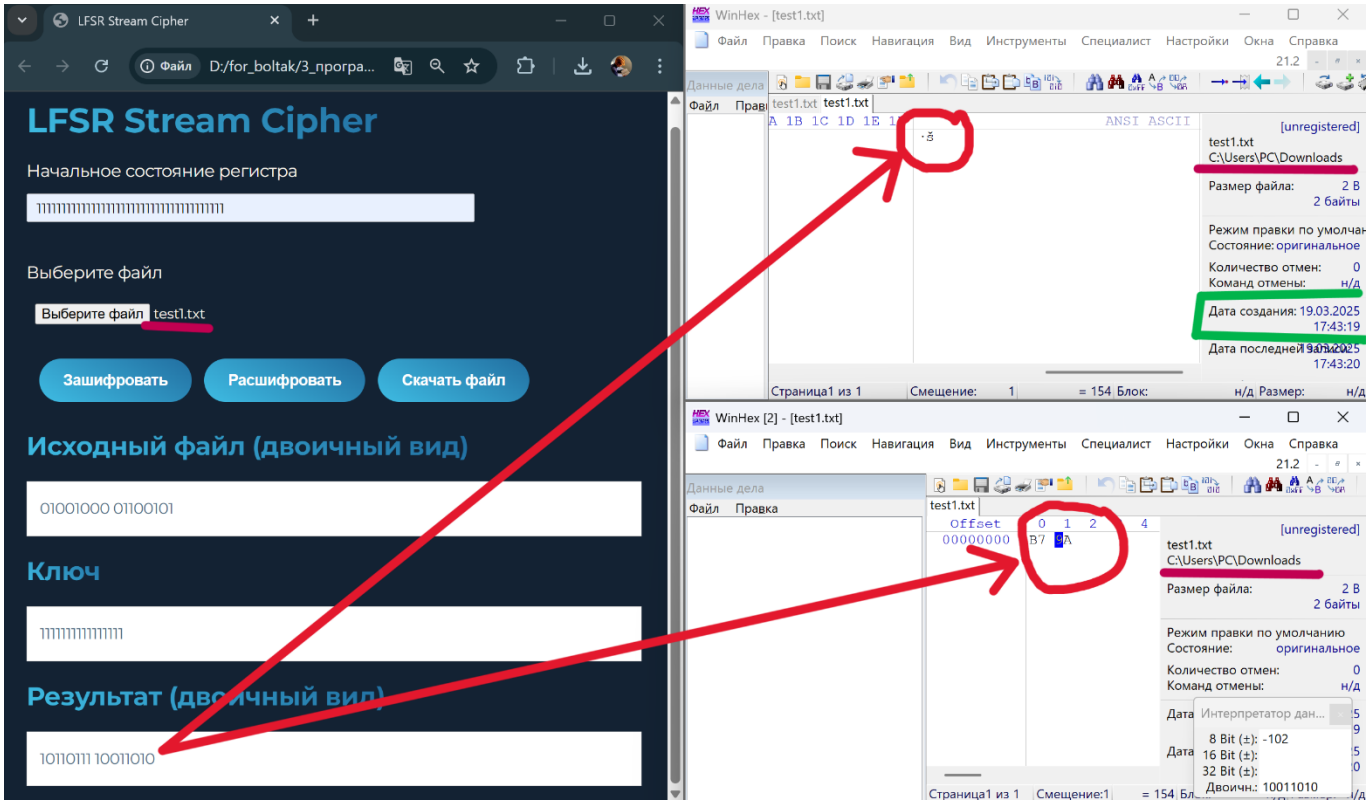


Тесты

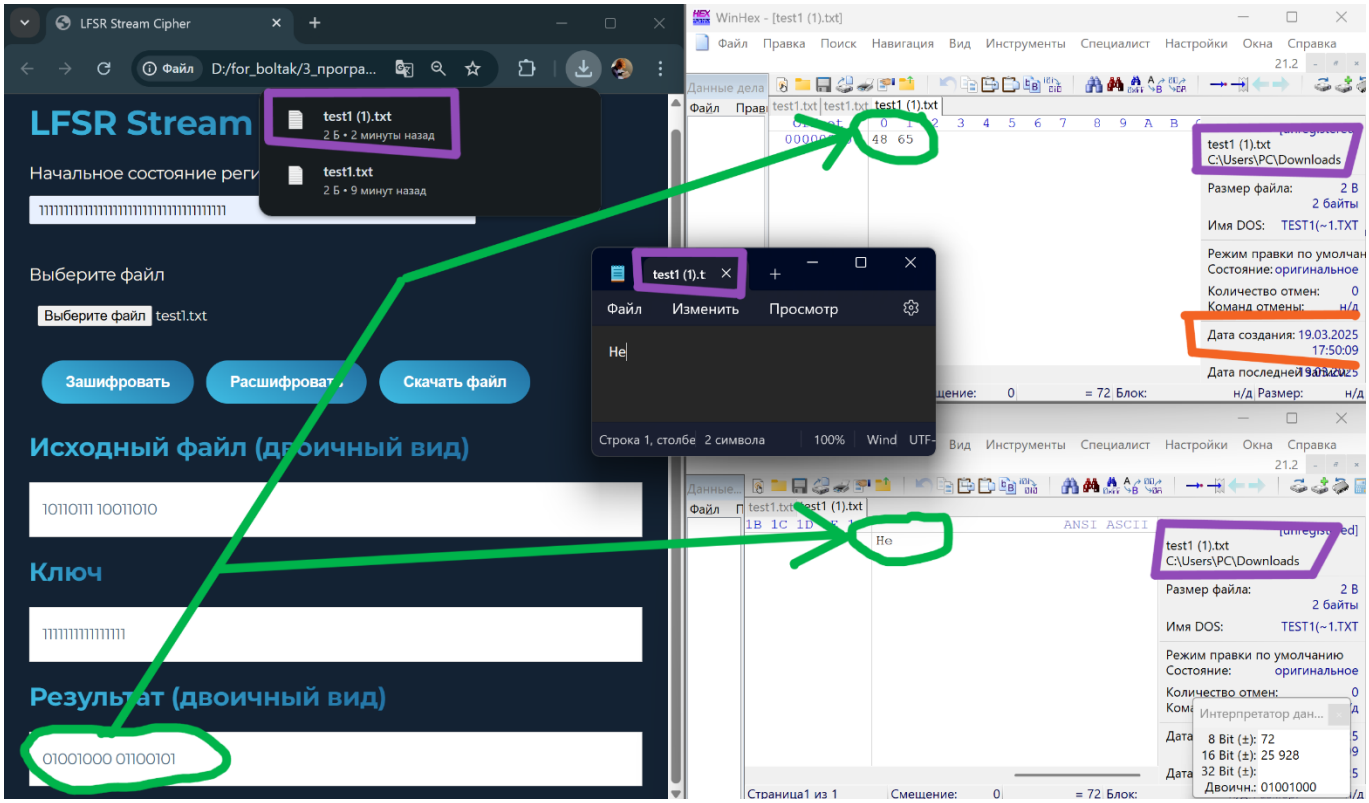
Текстовый файл, шифрование



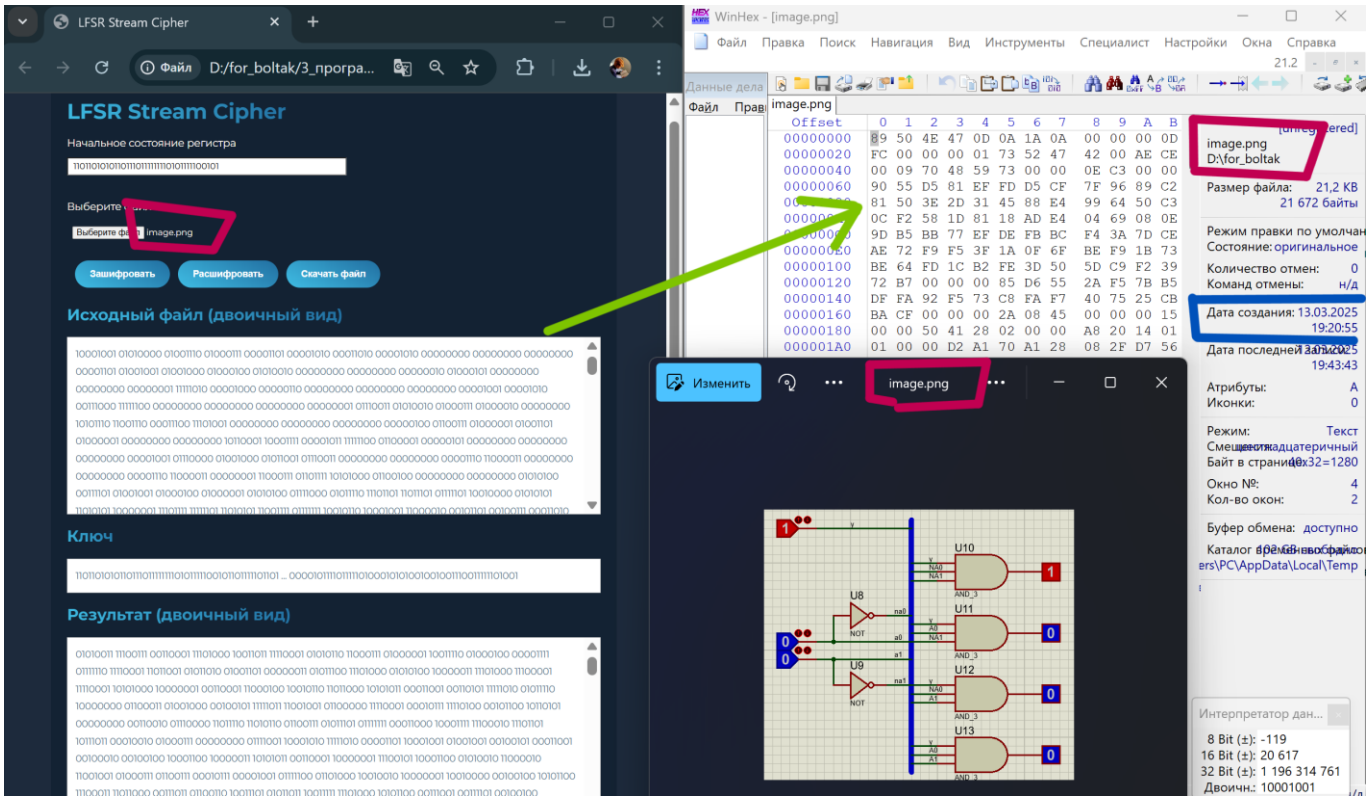
Текстовый файл, зашифрованный



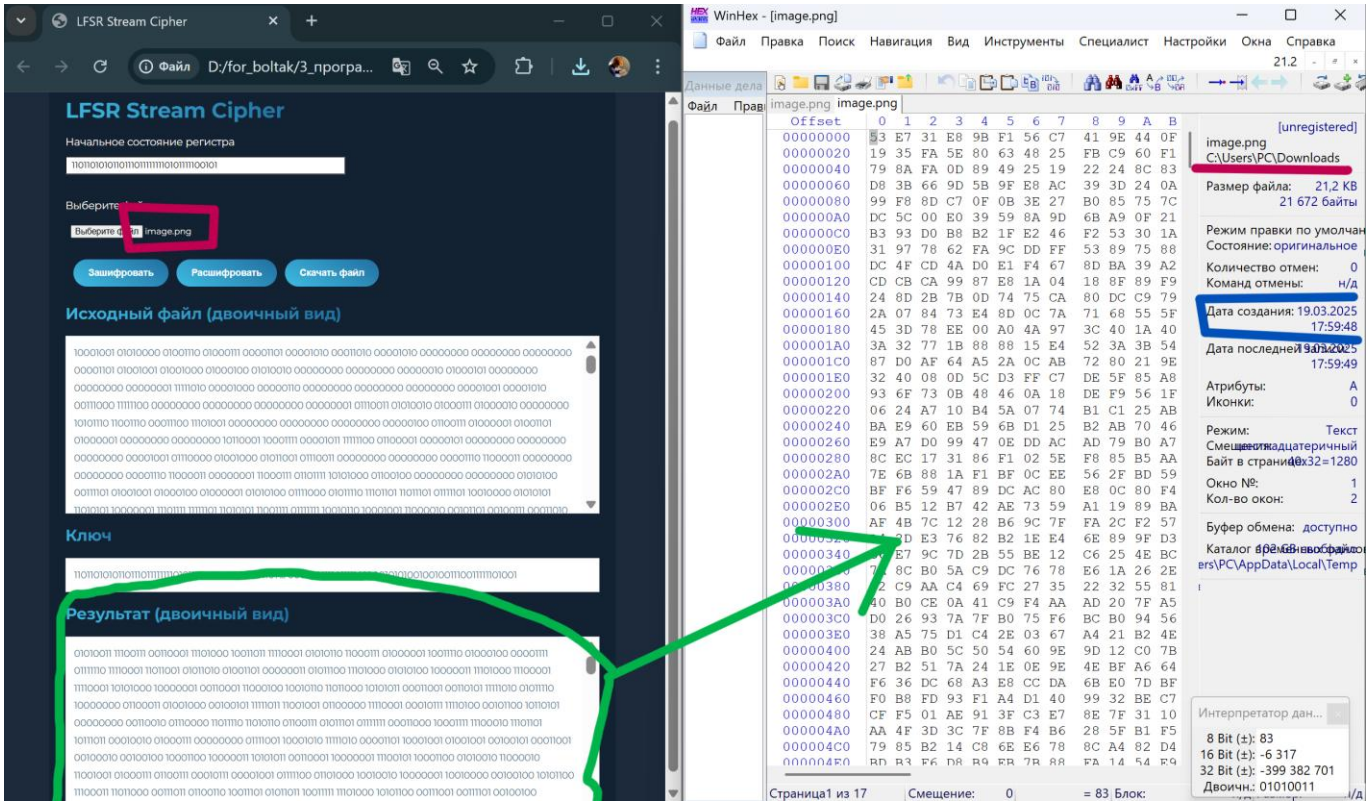
Текстовый файл, дешифрование



Картинка, шифрование



Картинка, зашифрованный



Картинка, дешифрование