УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №2

по предмету

Теория Информации

Вариант 12

Выполнил:

Студент В.С.

Проверил:

Болтак С.В.

Группа 351004

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 ***34***). 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/расшифрован- ный файл.

**Примитивный многочлен**

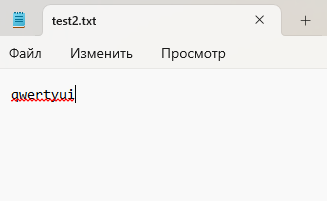
*X*34 + *x*15 + *x*14 + *x* + 1

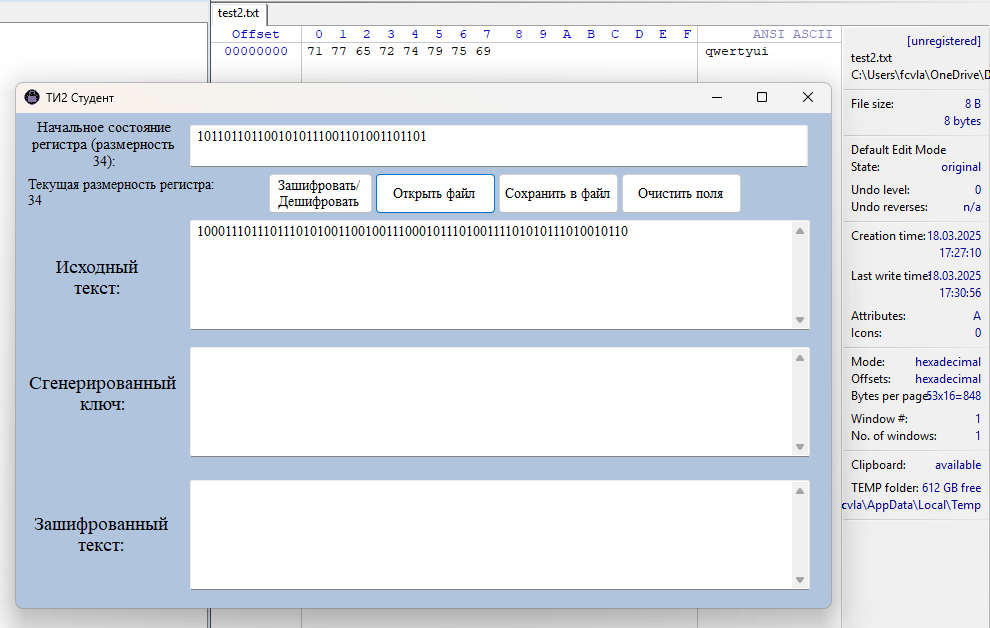
**Тесты**

1. **Текстовый файл**

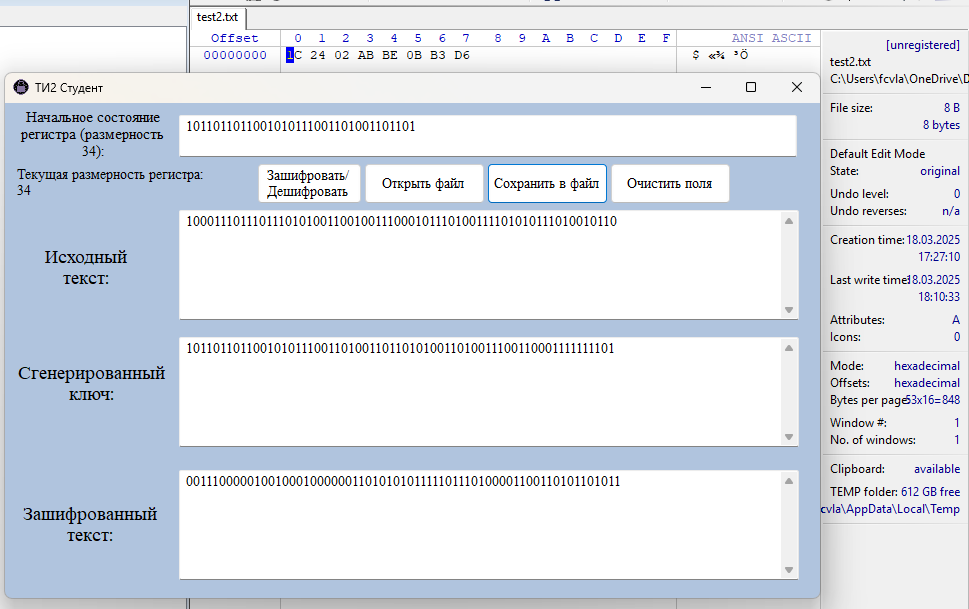
Начальное состояние регистра: 1011011011001010111001101001101101

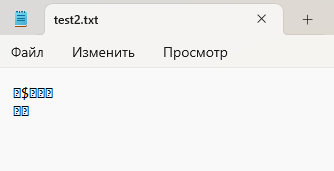
**Открыл тестовый файл**



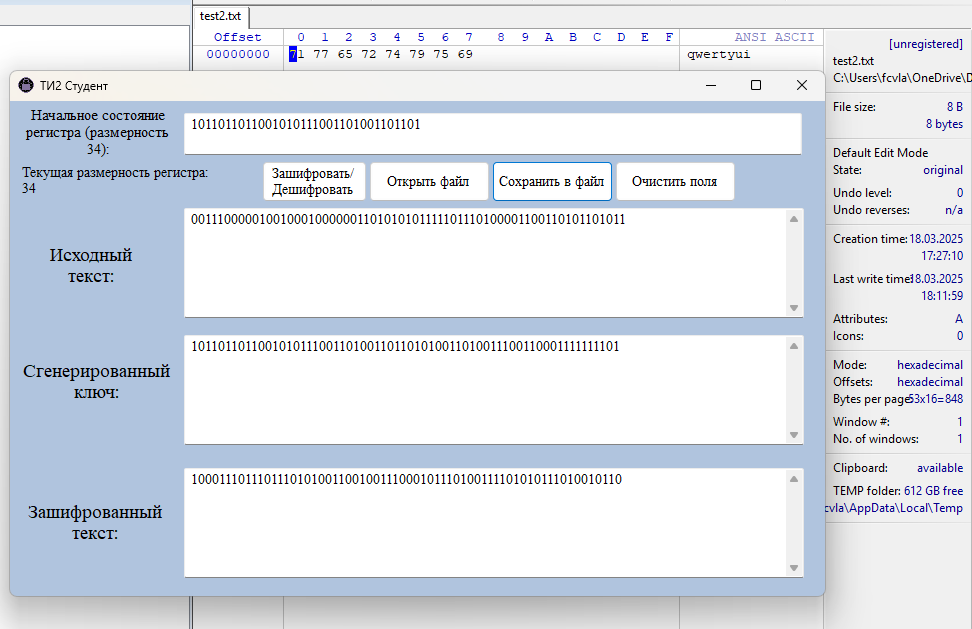


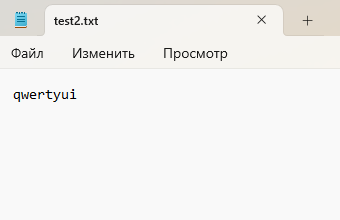
**Зашифровал тестовый файл, вид после сохранения**





**Дешифровал зашифрованный файл и сохранил, вид после сохранения**

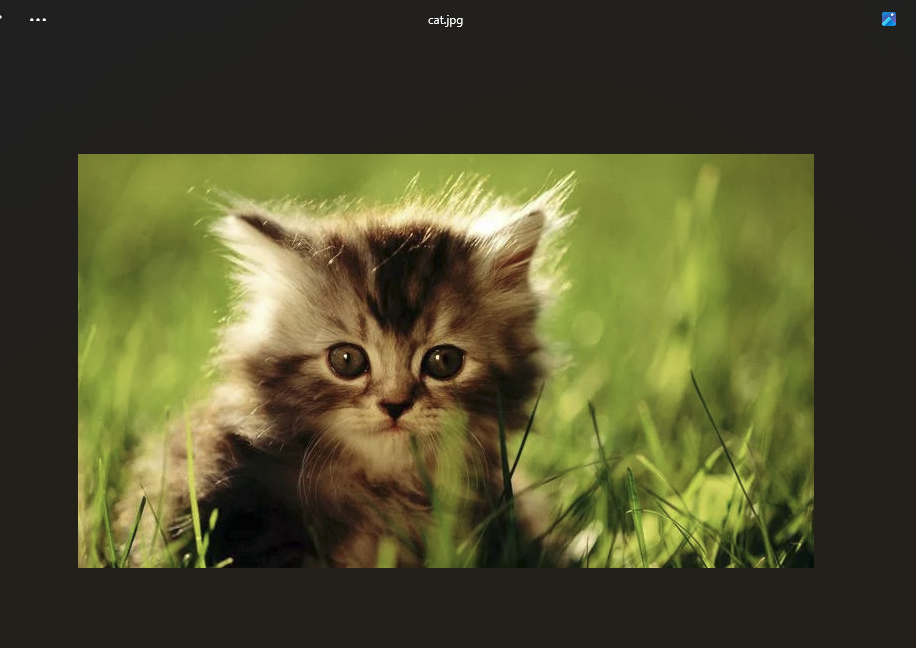


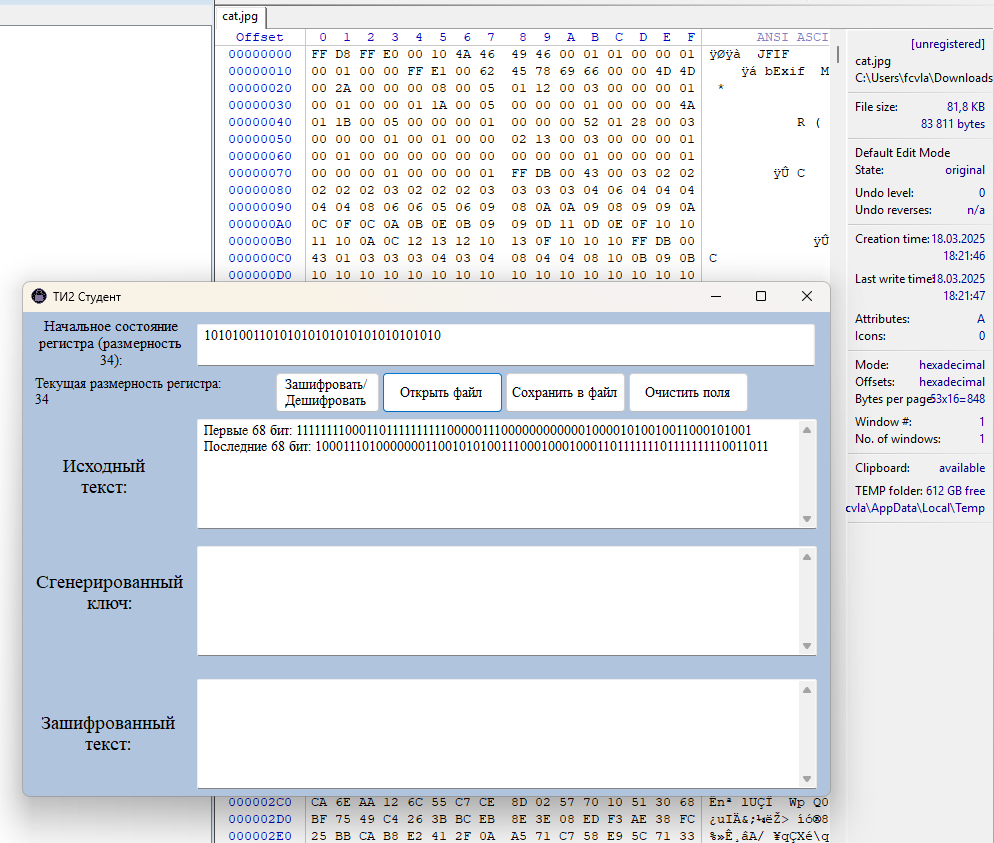


1. **Файл с изображением:**

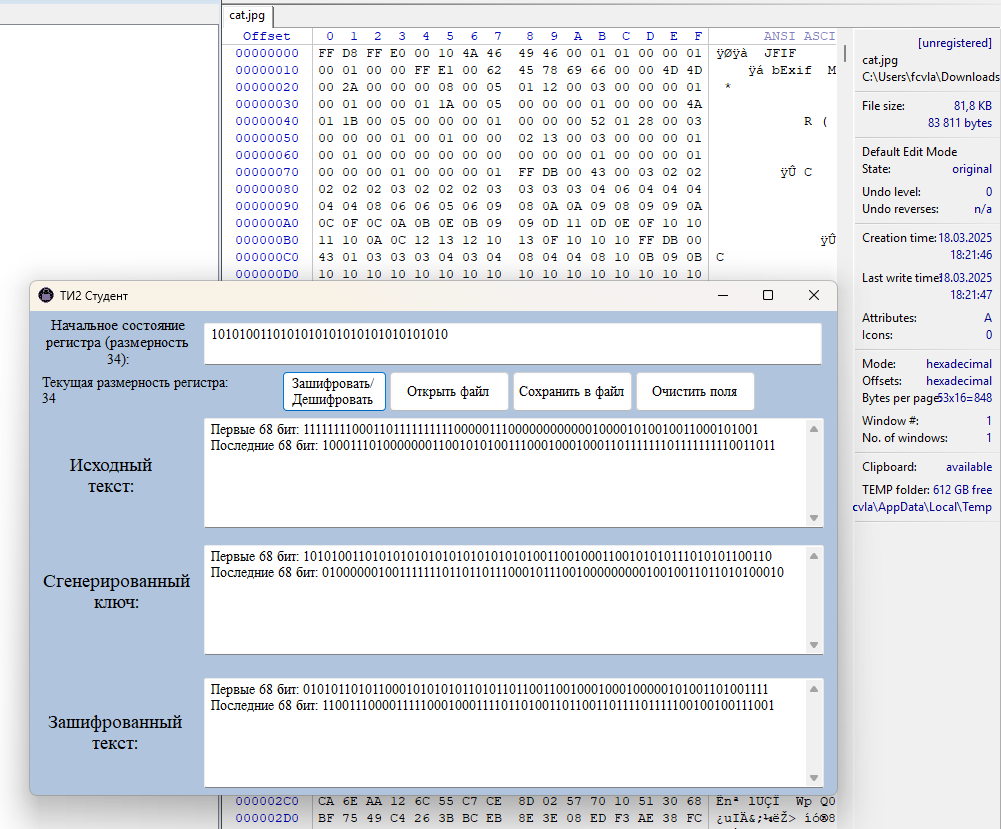
Начальное состояние регистра: 1010100110101010101010101010101010

**Открыл тестовый файл**

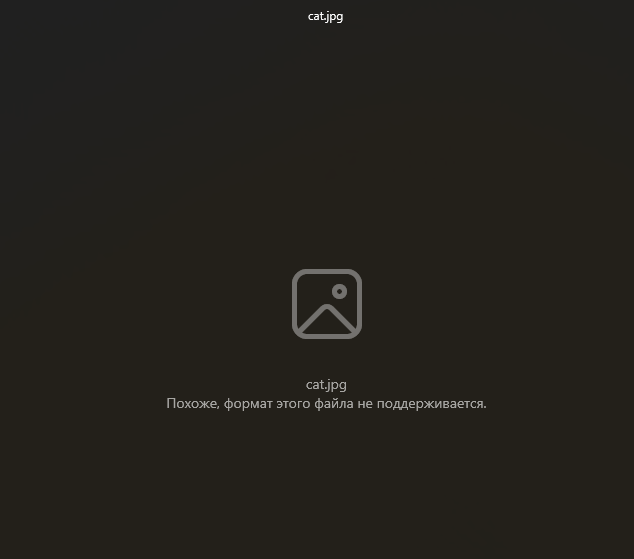




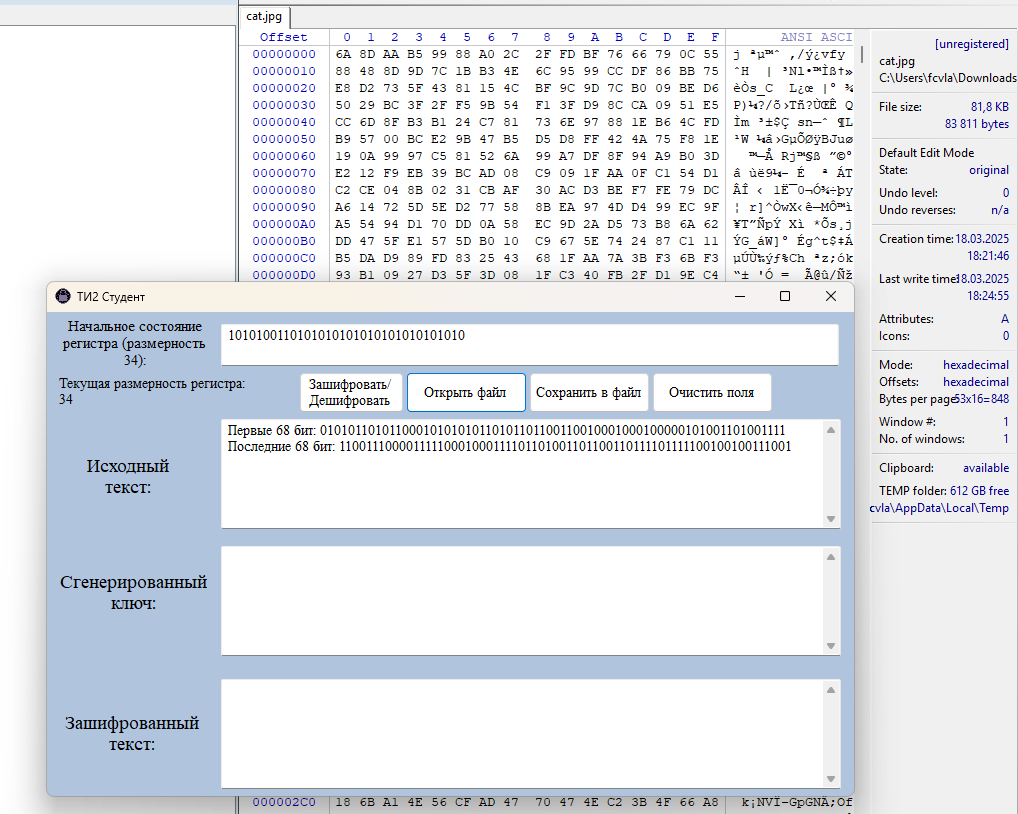
**Зашифровал тестовый файл**



**Вид файла после того, как зашифровал**



**Открыл зашифрованный файл**



**Дешифровал зашифрованный файл и сохранил, вид после сохранения**

