УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №2

по предмету

Теория Информации

Вариант 8

Выполнил:

Романовский М.И.

Проверил:

Болтак С.В.

Группа 351004

Минск 2025

**Задание:**

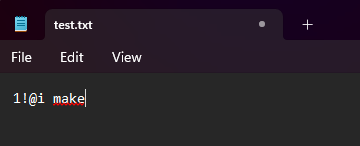
Реализовать систему потокового шифрования и дешифрования для файла с любым содержимым с помощью генератора ключевой последовательности на основе линейного сдвигового регистра с обратной связью LFSR1 (размерность регистра ***30***). Начальное состояние регистра ввести с клавиатуры. Поле для ввода состояния 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.

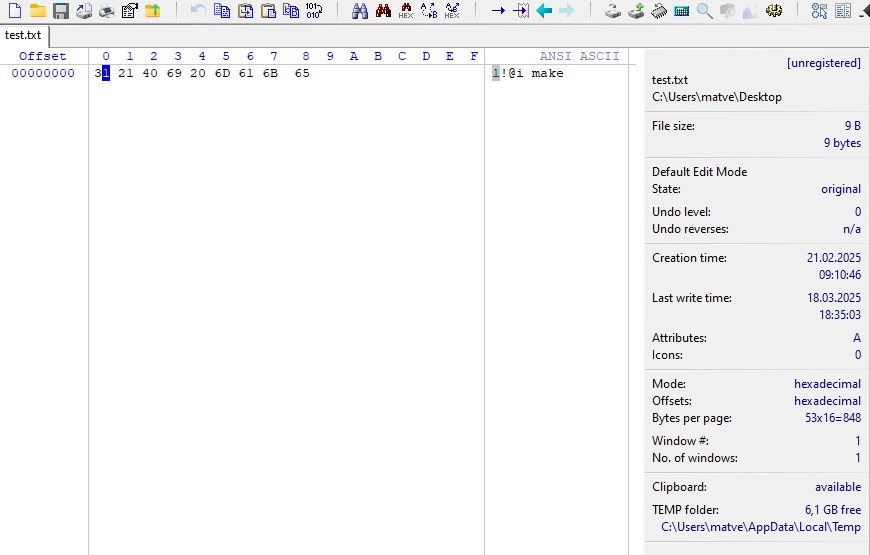
**Примитивный многочлен**

*x*30 + *x*16 + *x*15 + *x*+ 1

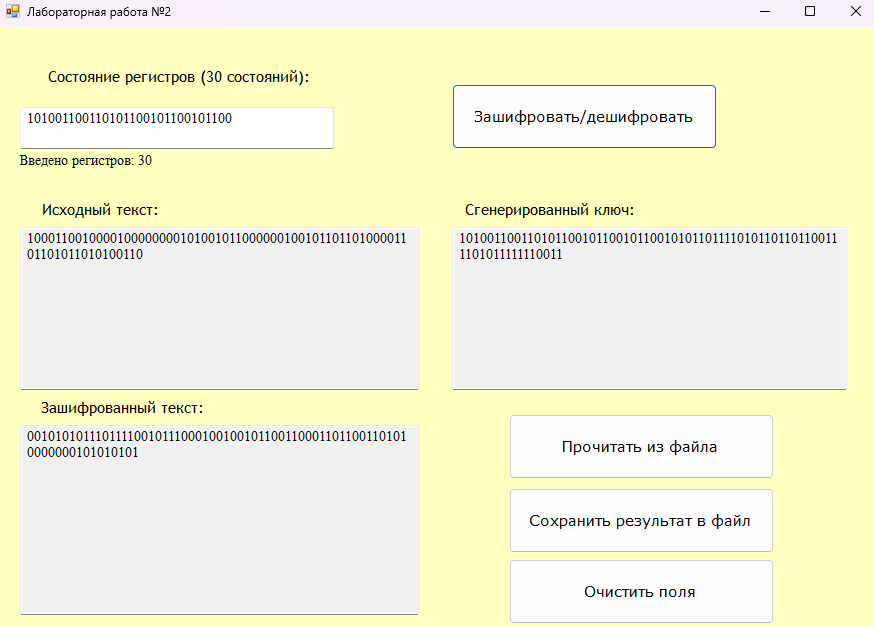
**Текстовый документ**

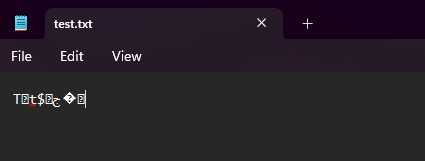
Начальное состояние регистров: 101001100110101100101100101100.

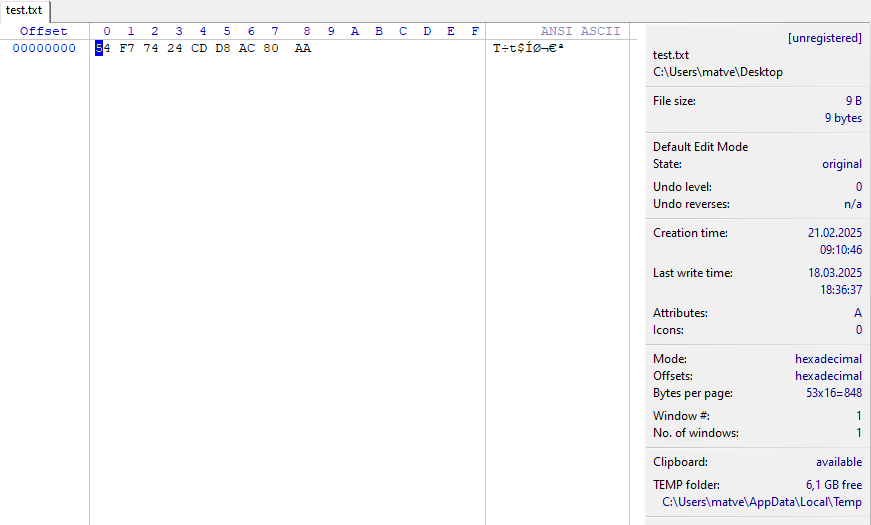
****

****

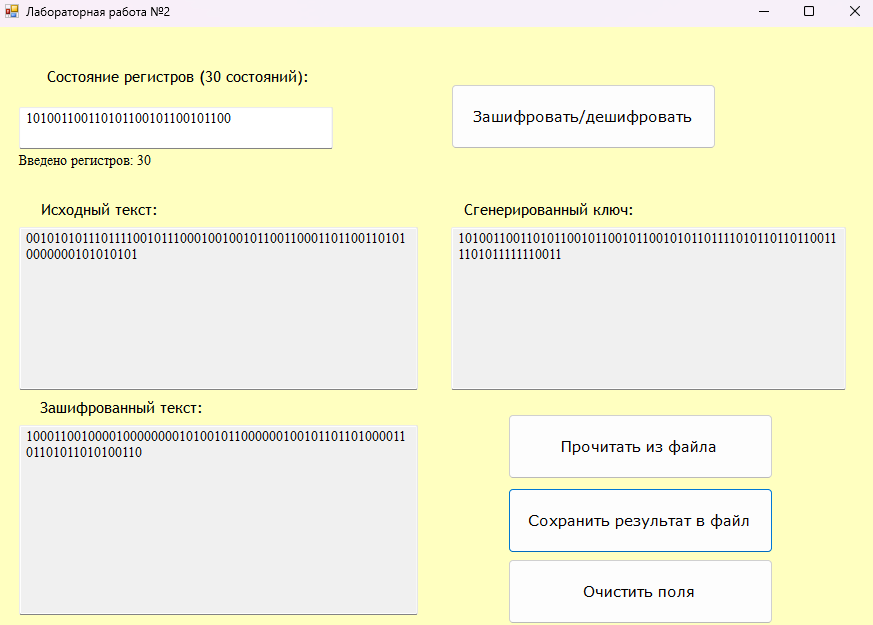
Шифровка:

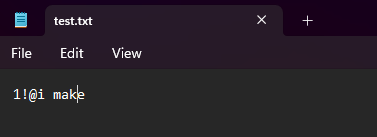
****

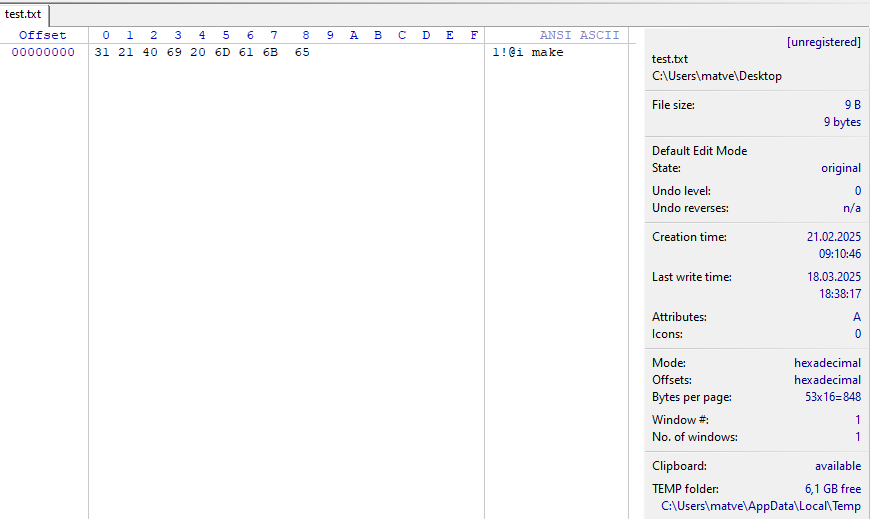
****

****

Дешифровка:

****

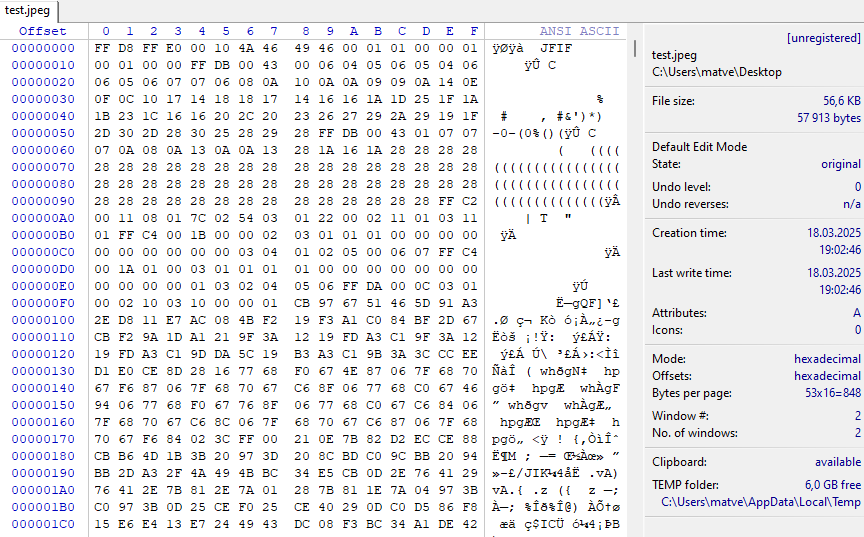
****

****

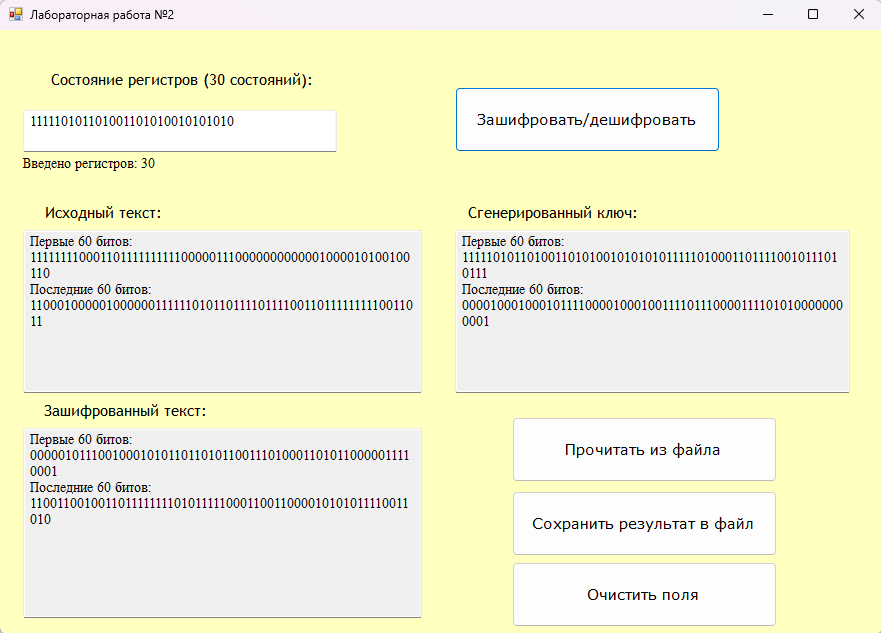
**Изображение (jpeg-формат):**

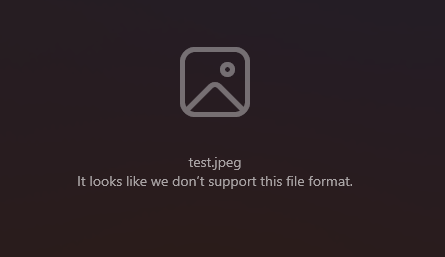
Начальное состояние регистров: 111110101101001101010010101010.

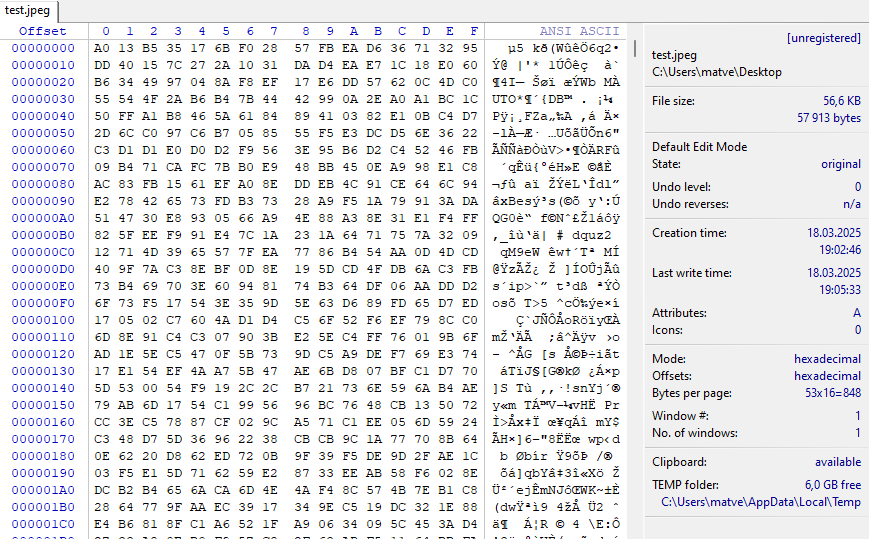




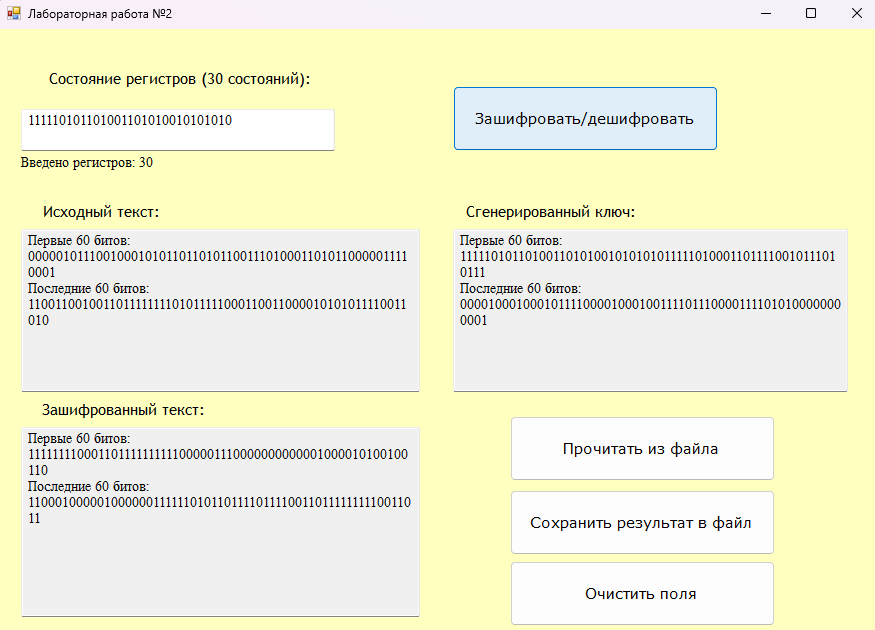
Шифровка:

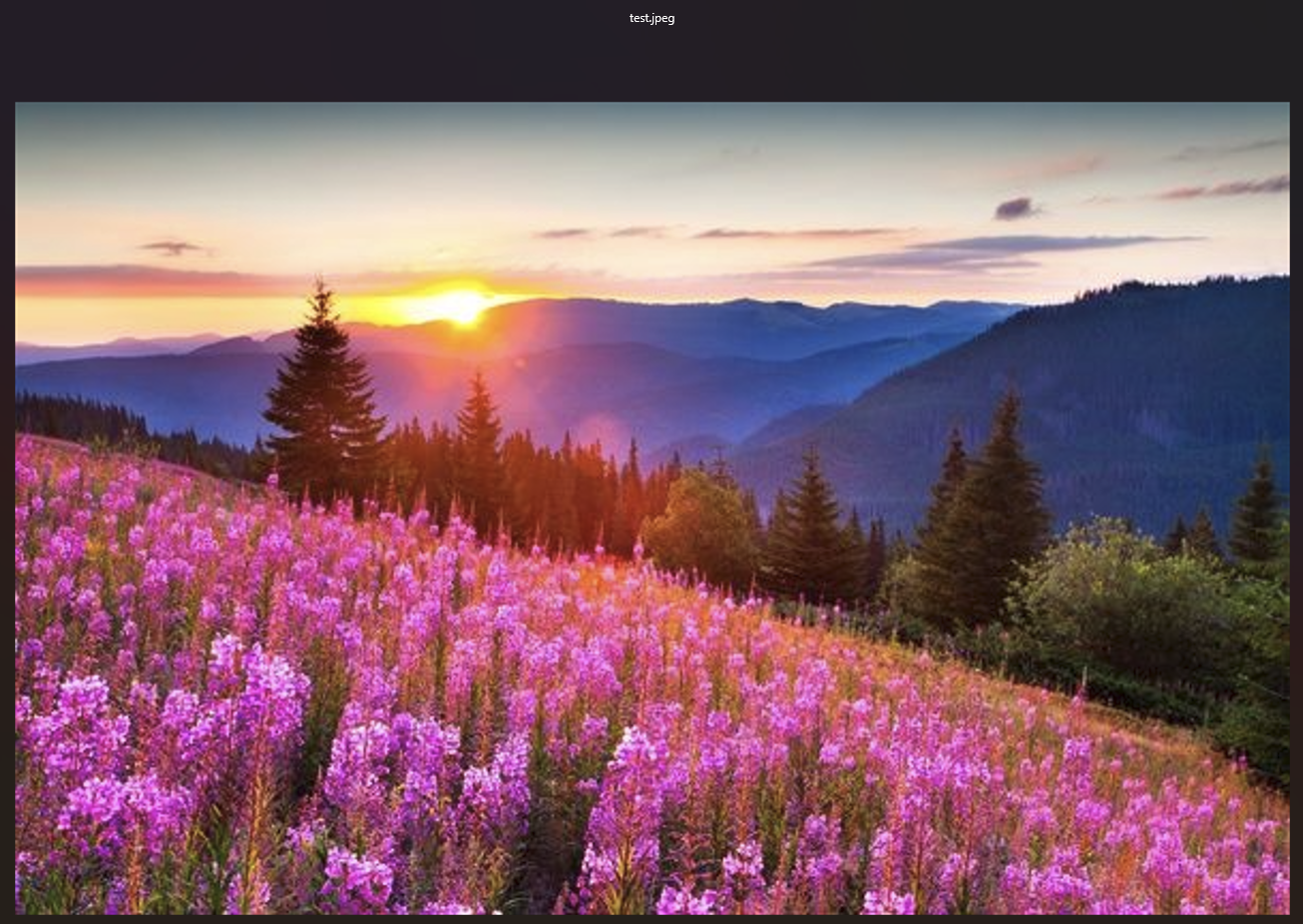


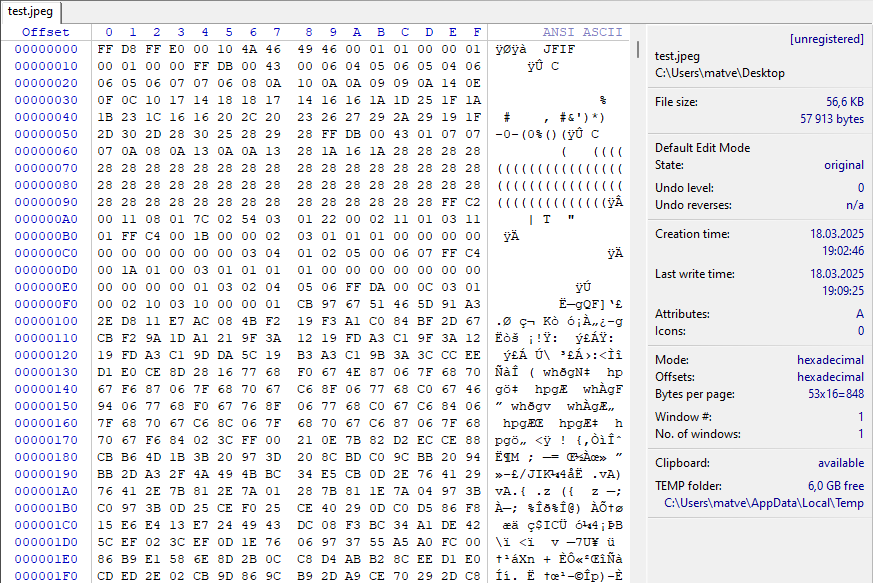




Дешифровка:

****

****

****