УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №2

по предмету

Теория Информации

Вариант 6

Выполнил:

Логинов Д.C

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 ***36***). 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.

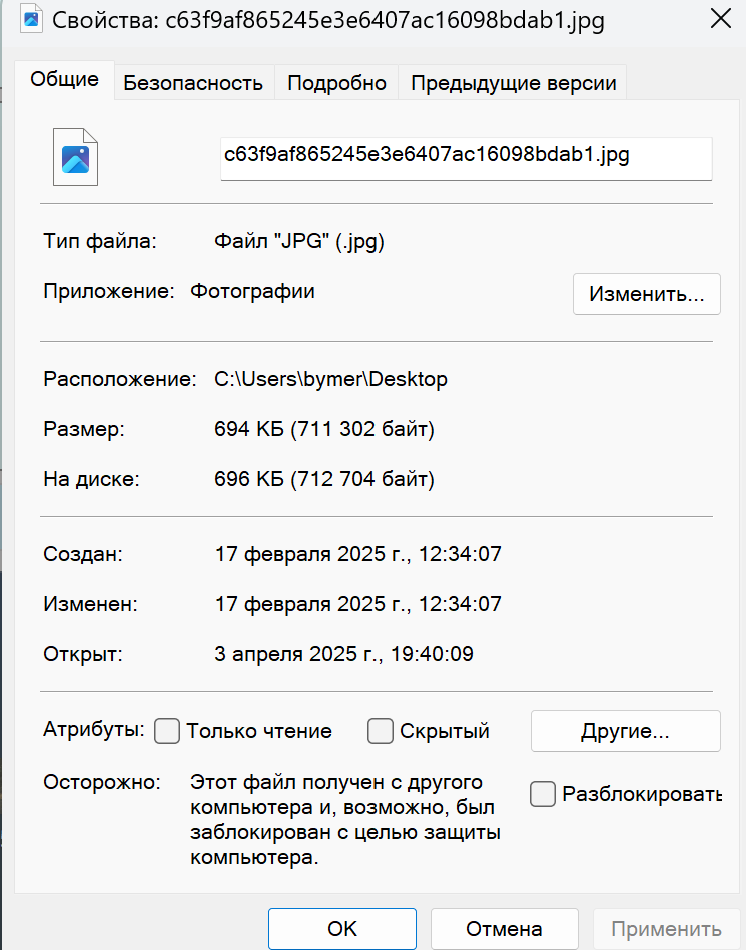
**Примитивный многочлен**

*x*28 +*x*3 + 1

**Тесты**

Excel с начальными состояниями регистров и таблицами для них прилагаются.

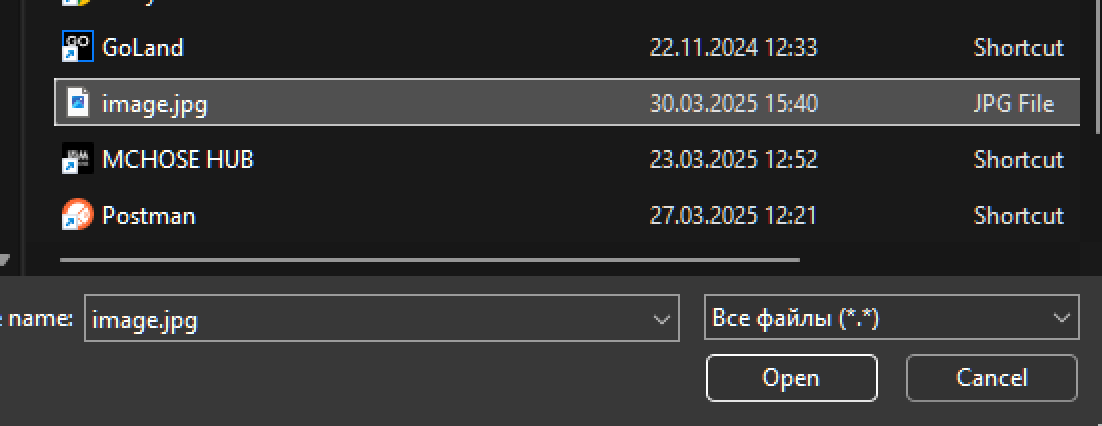
**Тест работа с картинкой:**

****

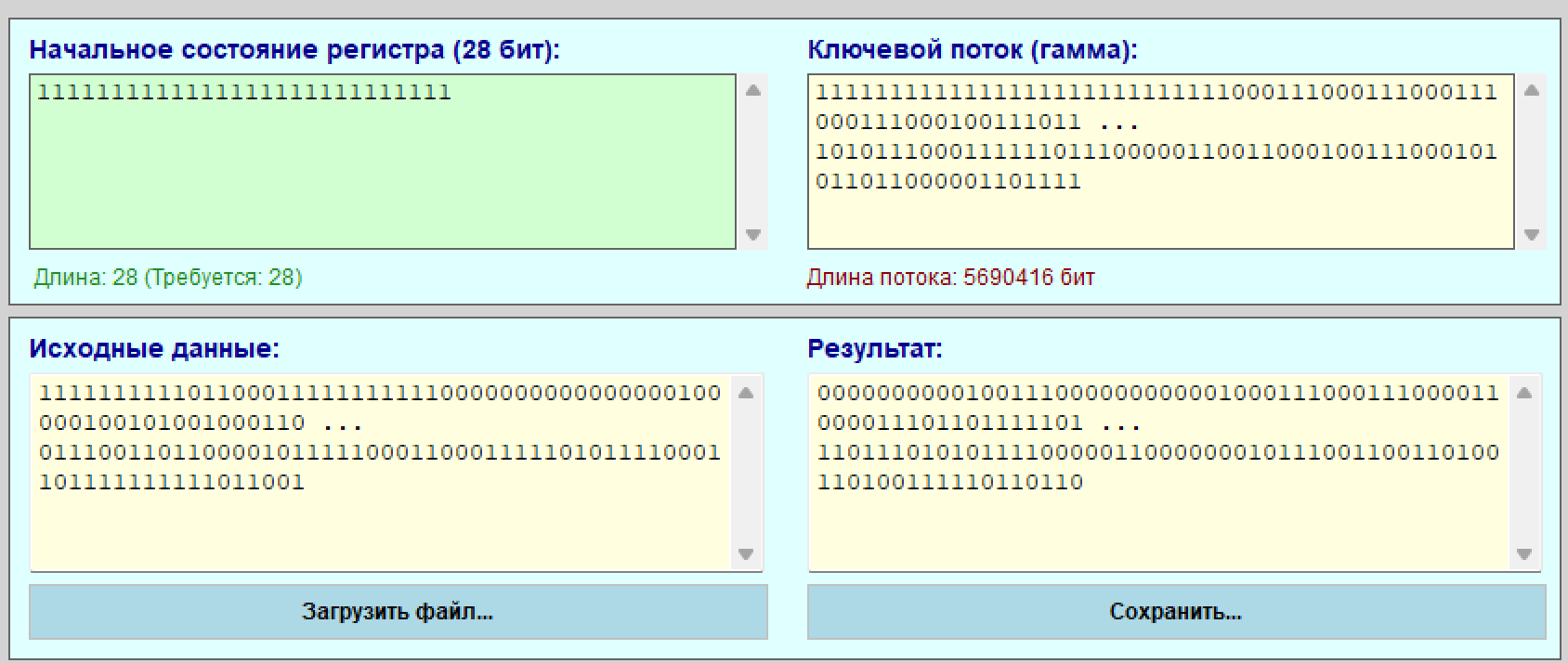
Исходное состояние файла

Начальное состояние регистра:

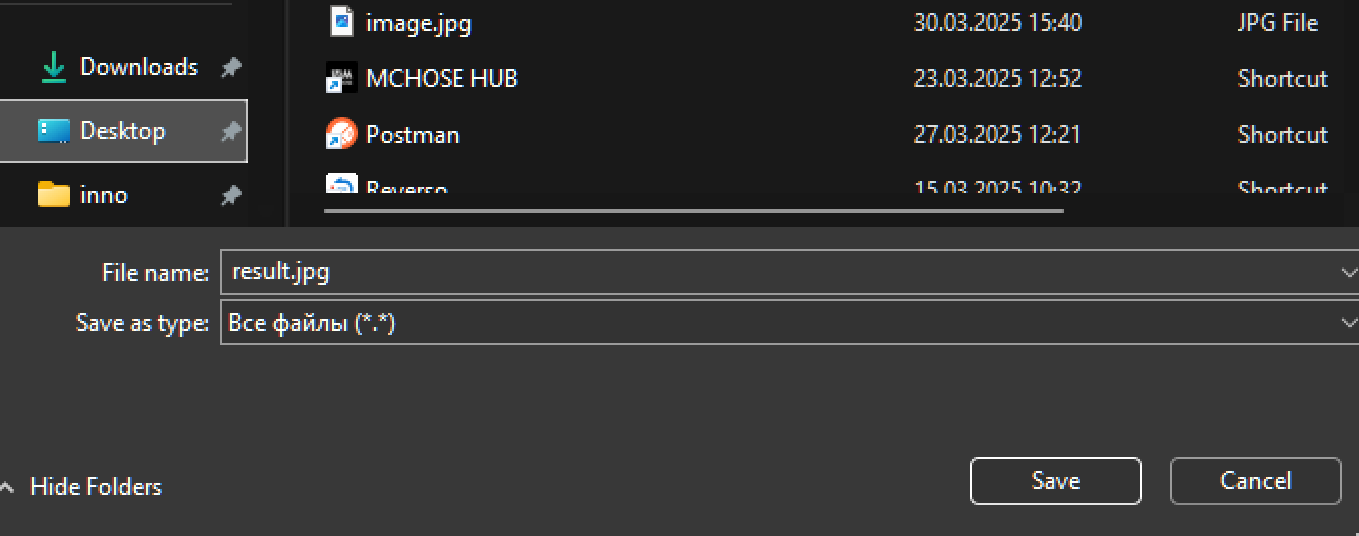
1111111111111111111111111111

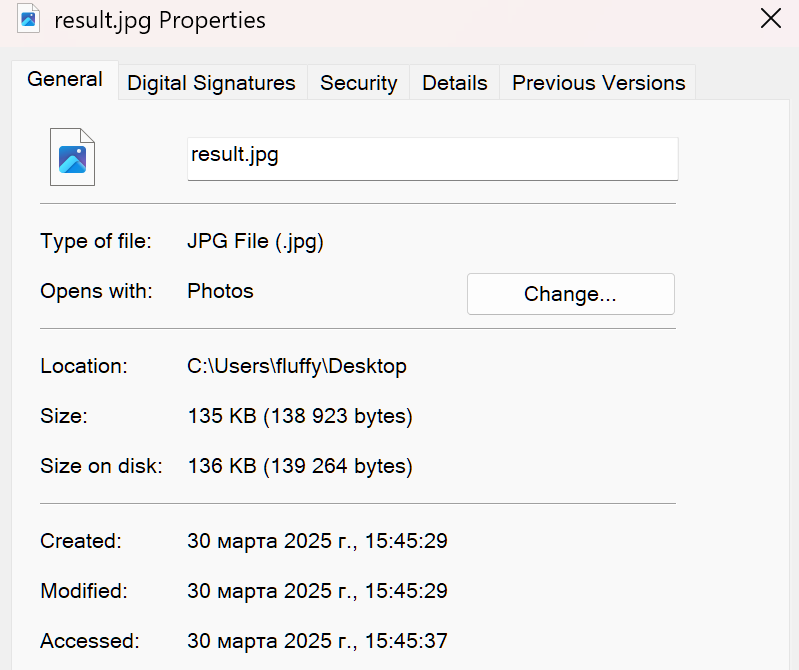
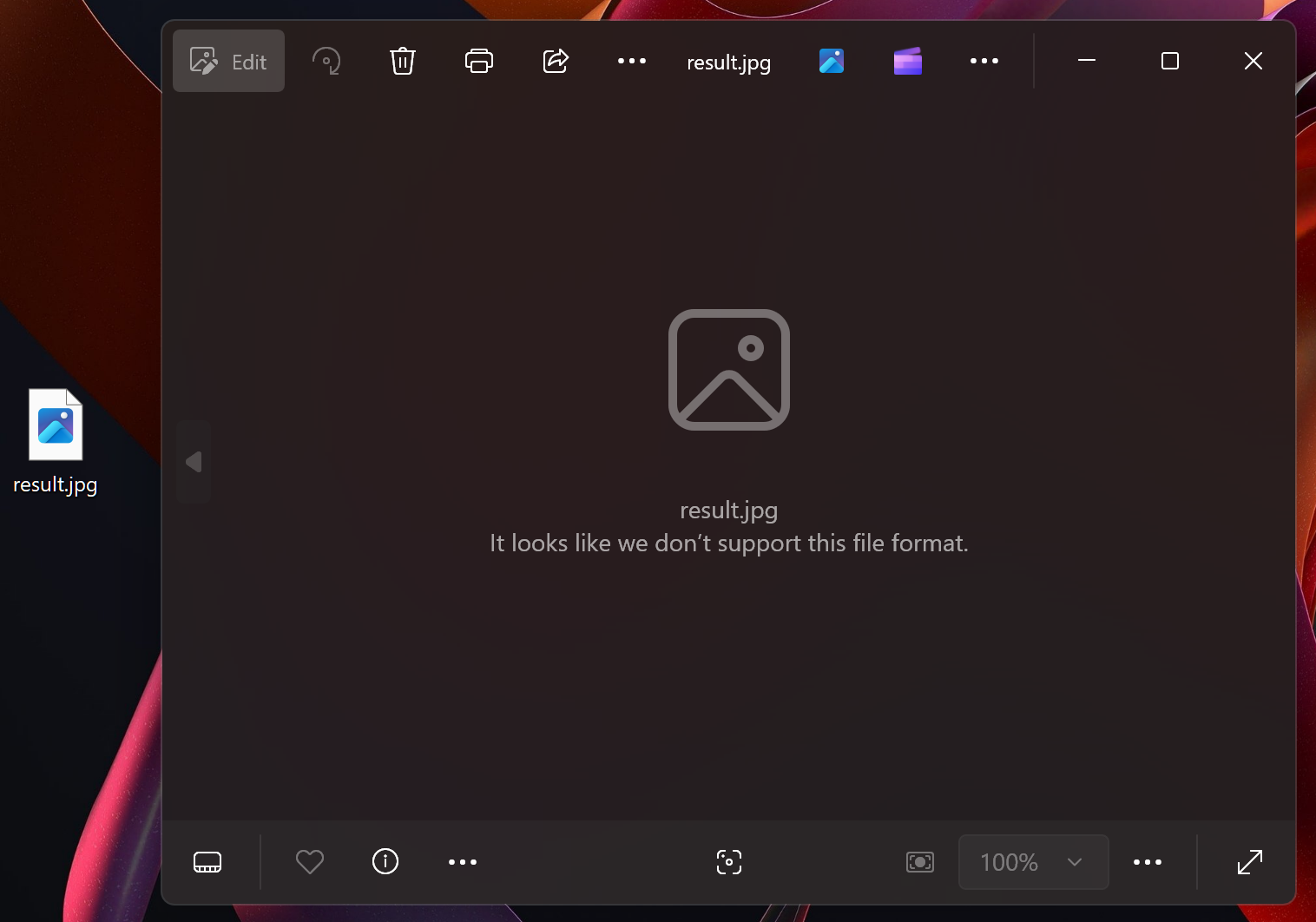
Выбираем image.jpg  


Шифруем:

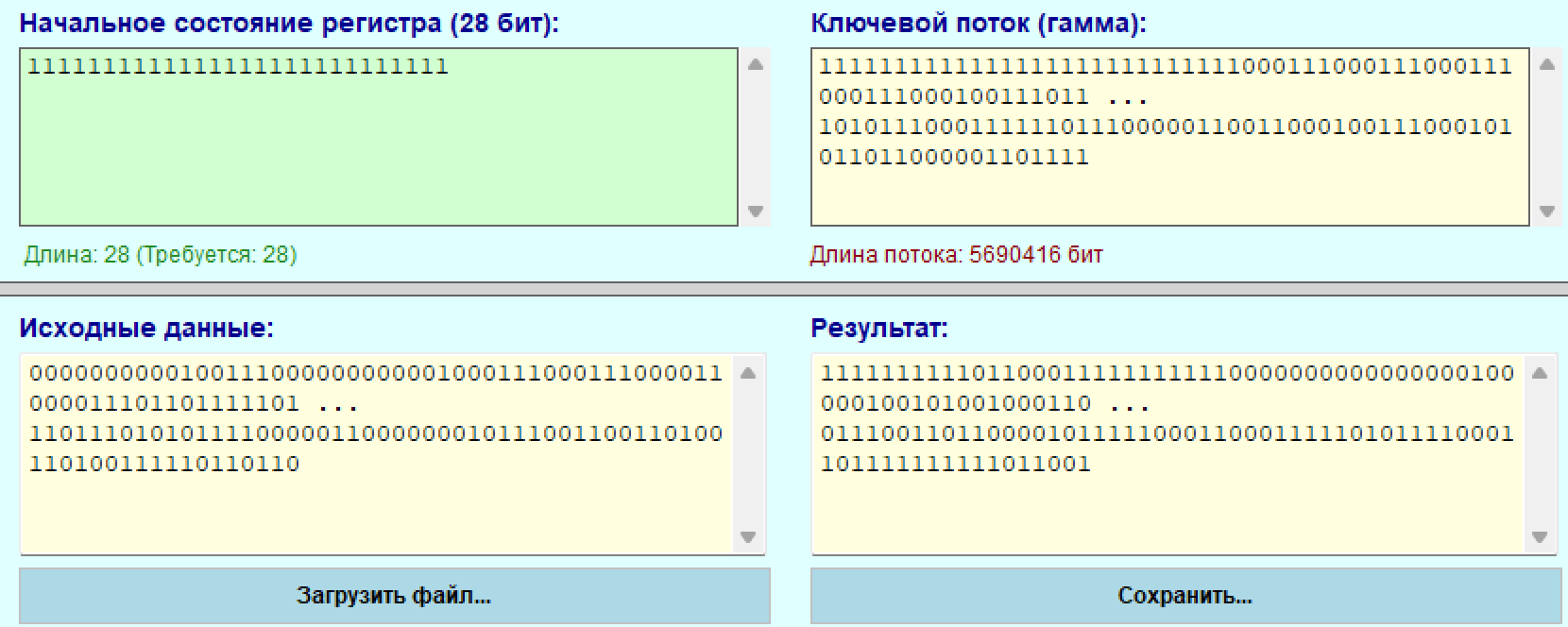


Сохраняем как result.jpg





Файл зашифрован, чтение картинки невозможно

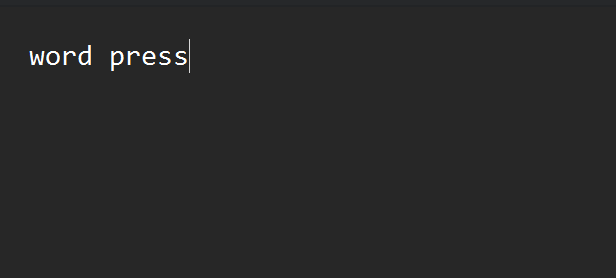
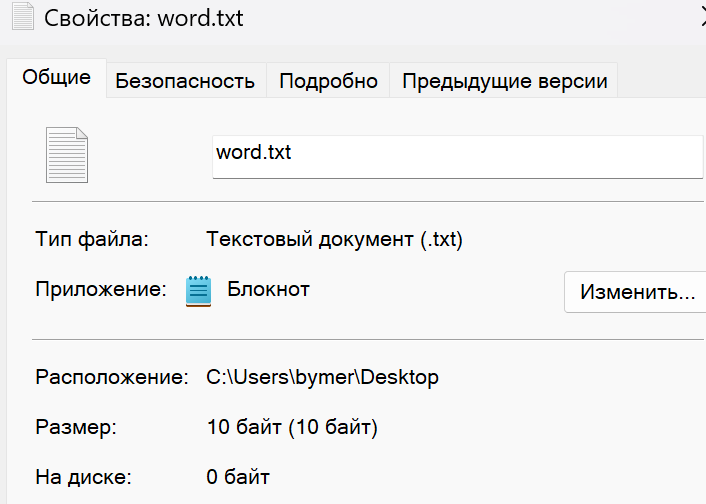
Дешифрируем:  
  
Сохраняем



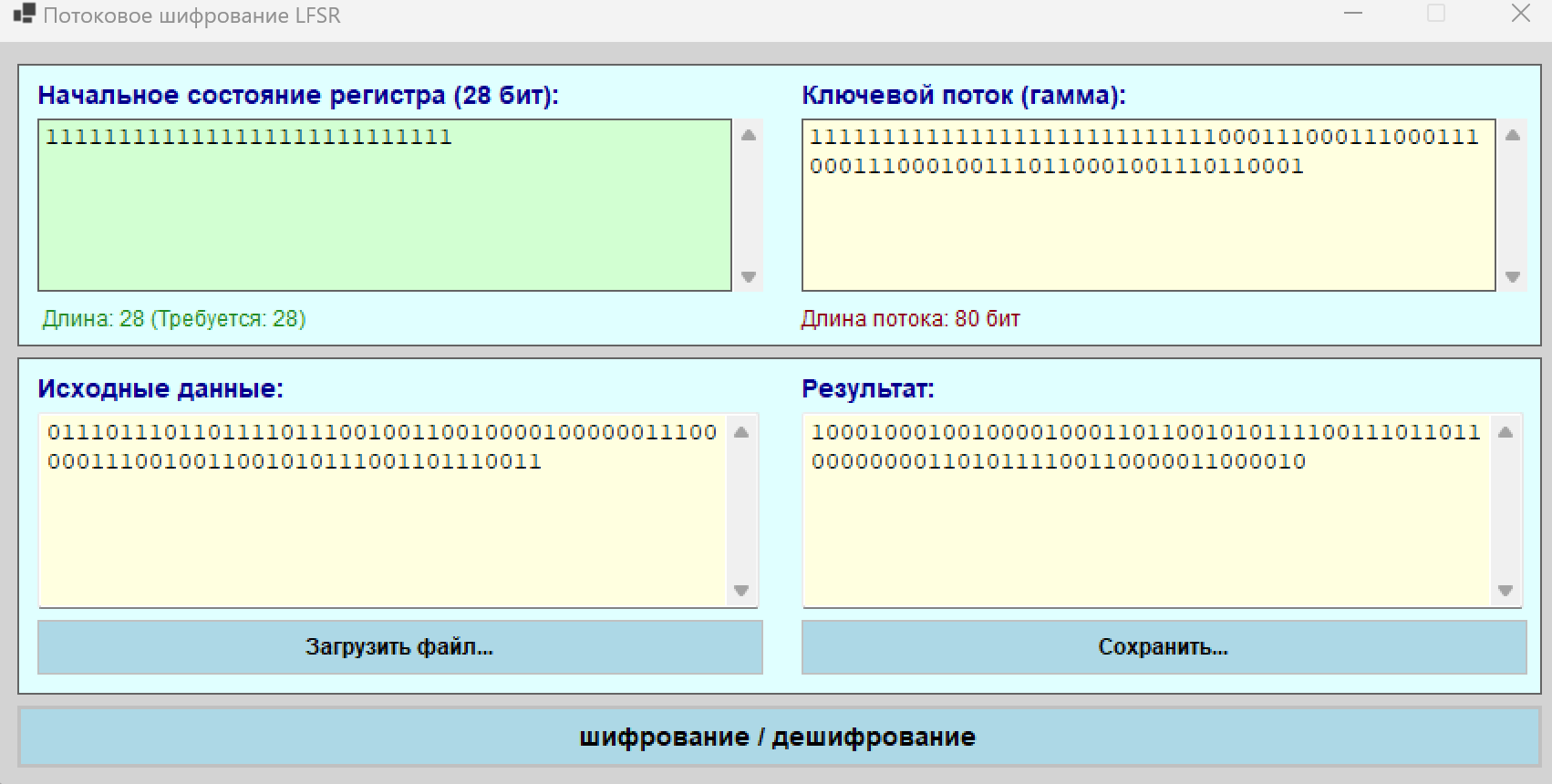
Расшифрованный файл читается так как раньше. Тест пройден

**Тест работы с текстом:**

Начальное состояние регистра: **11111111111111111111111111**

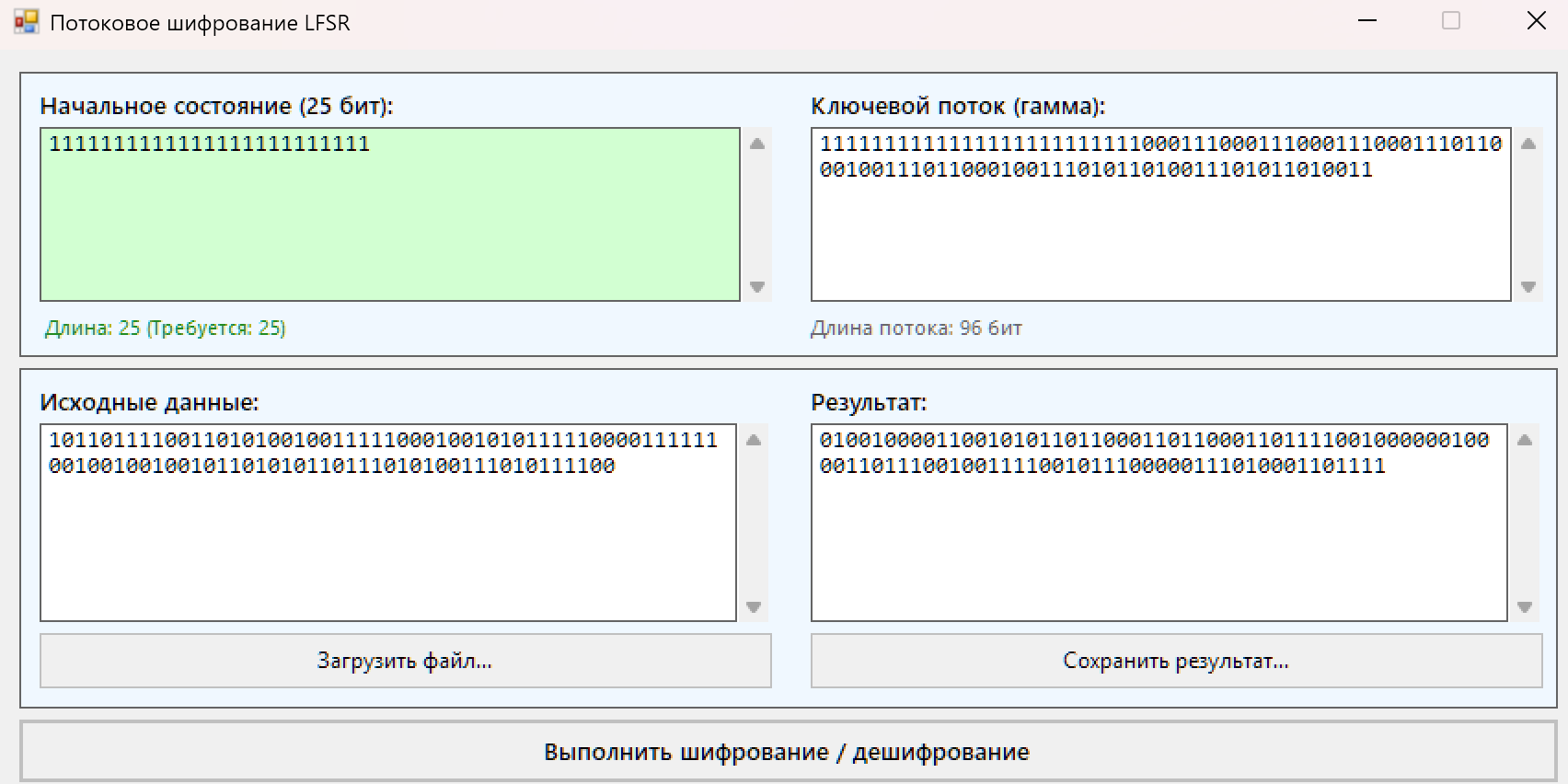


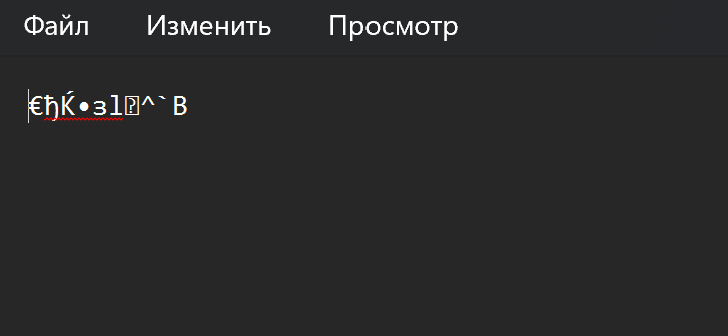
Исходный текстовый файл



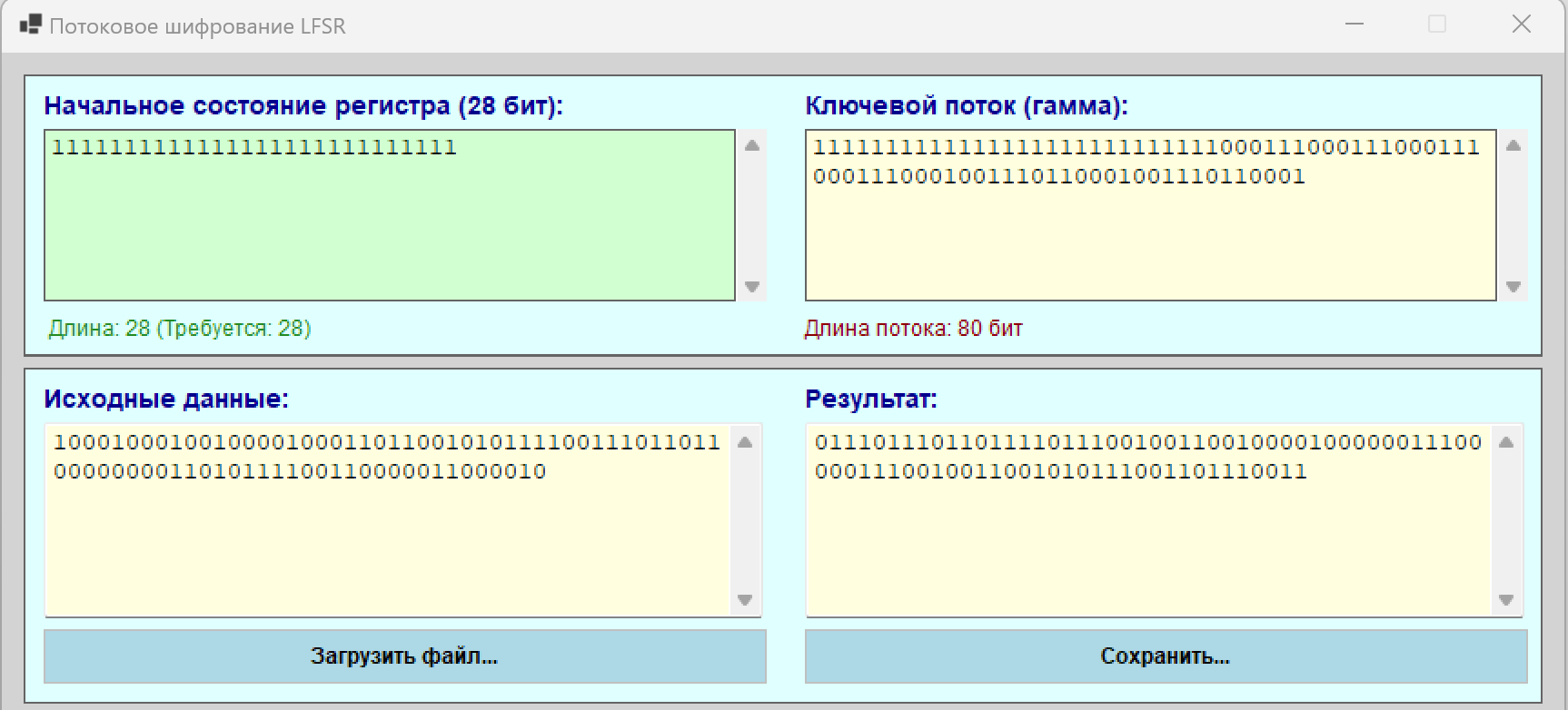
Шифрование файла

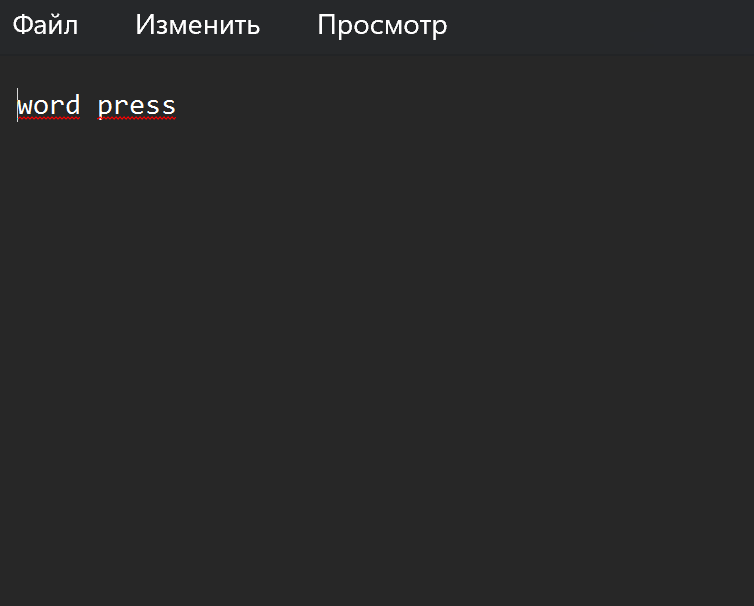
Зашифрованный файл





Расшифровывание файла





Расшифрованный текстовый файл с исходным текстом. Тест Пройден