УО «Белорусский государственный университет   
информатики и радиоэлектроники»

Кафедра ПОИТ

Тесты по лабораторной работе № 2  
по предмету «Теория информации»  
Вариант 5

Выполнила:

Сучёк Е.А.

гр. 351003

Проверила:

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 LFSR1 (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.

Таблица 1

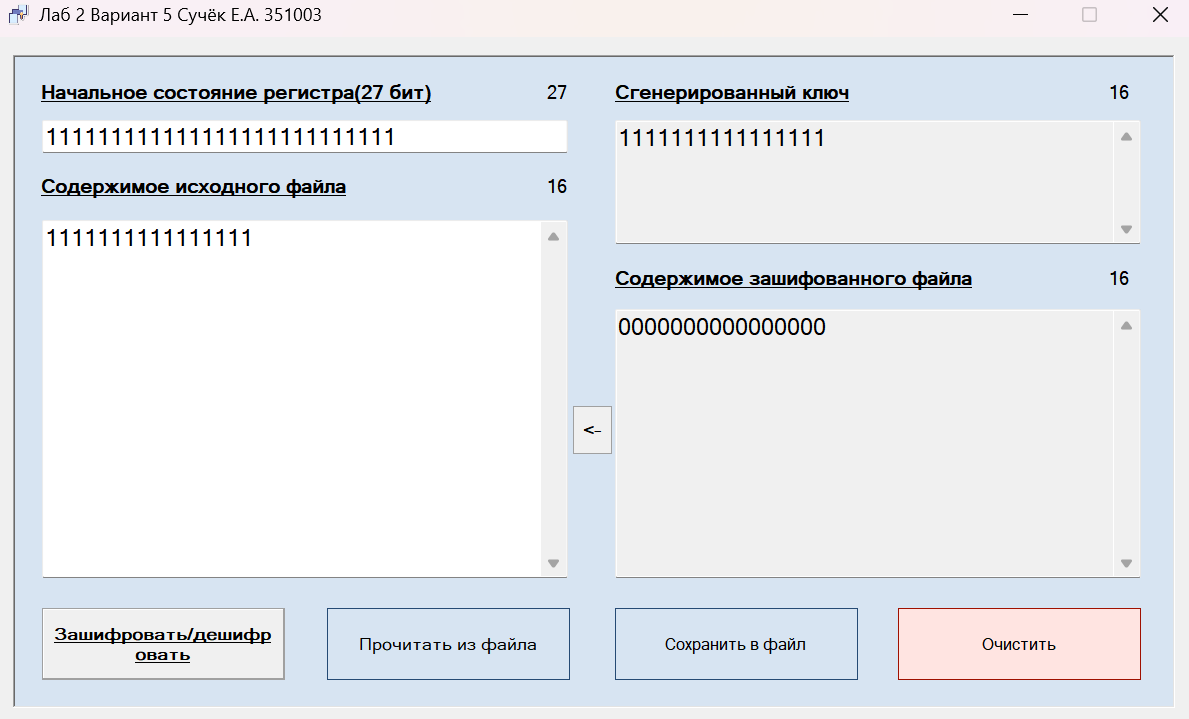
|  |  |
| --- | --- |
| **Степень многочлена** | **Номер варианта** |
| **5** |
| LFSR | **27** |

Примитивный многочлен: x27 + x8 + x7 + x + 1

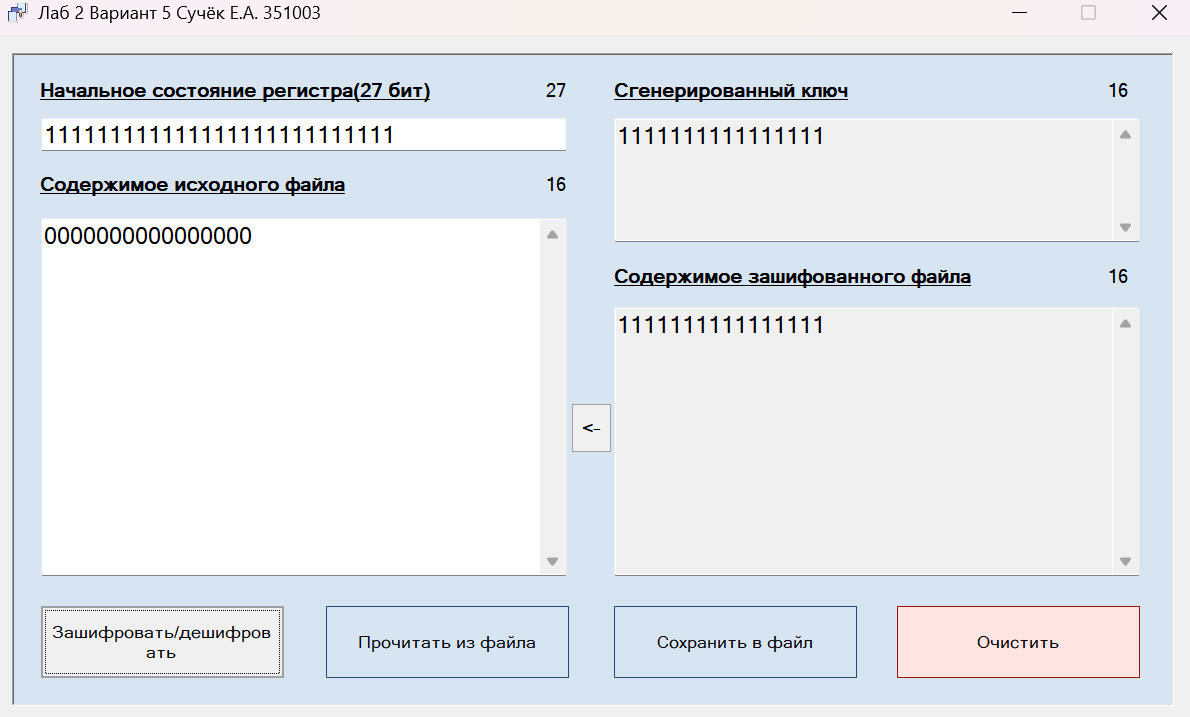
**Тесты**

* 1. **Корректные исходные данные(все единицы, ключ длиннее исходных данных)**

**Процесс шифрования:**

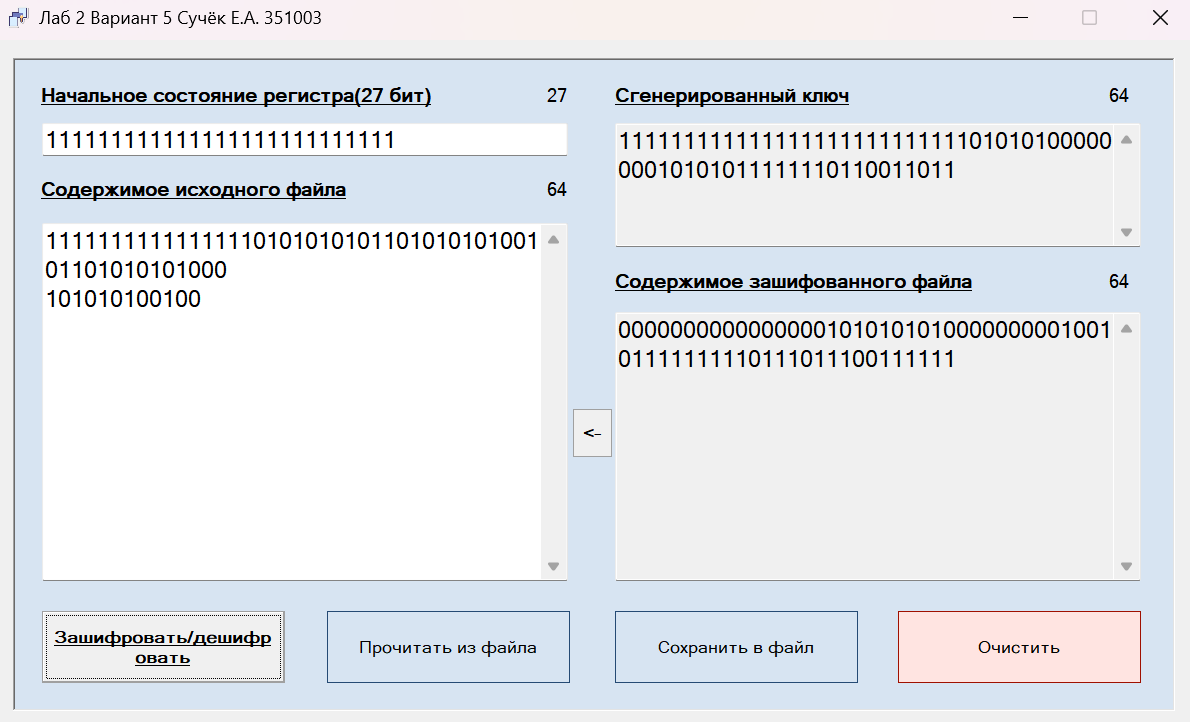


**Процесс дешифрования:**

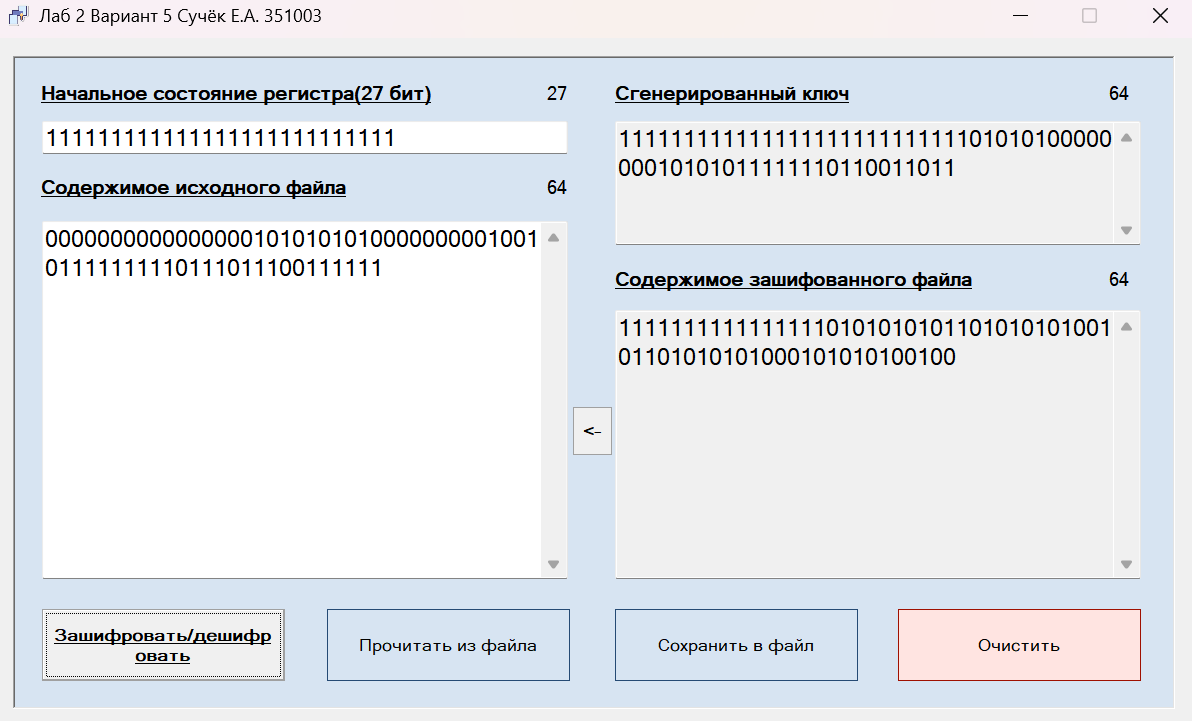


* 1. **Корректные исходные данные(исходные данные длиннее ключа)**

**Процесс шифрования:**



**Процесс дешифрования:**

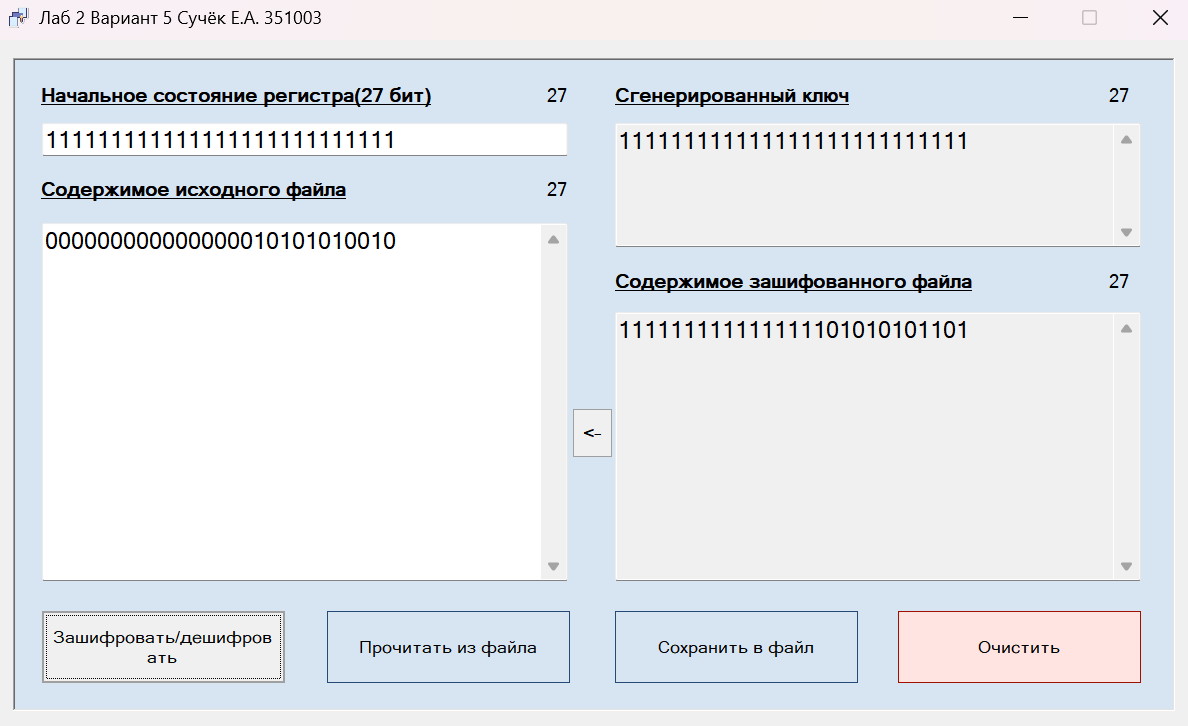


0000000000000000101010101000000000100101111111110111011100111111

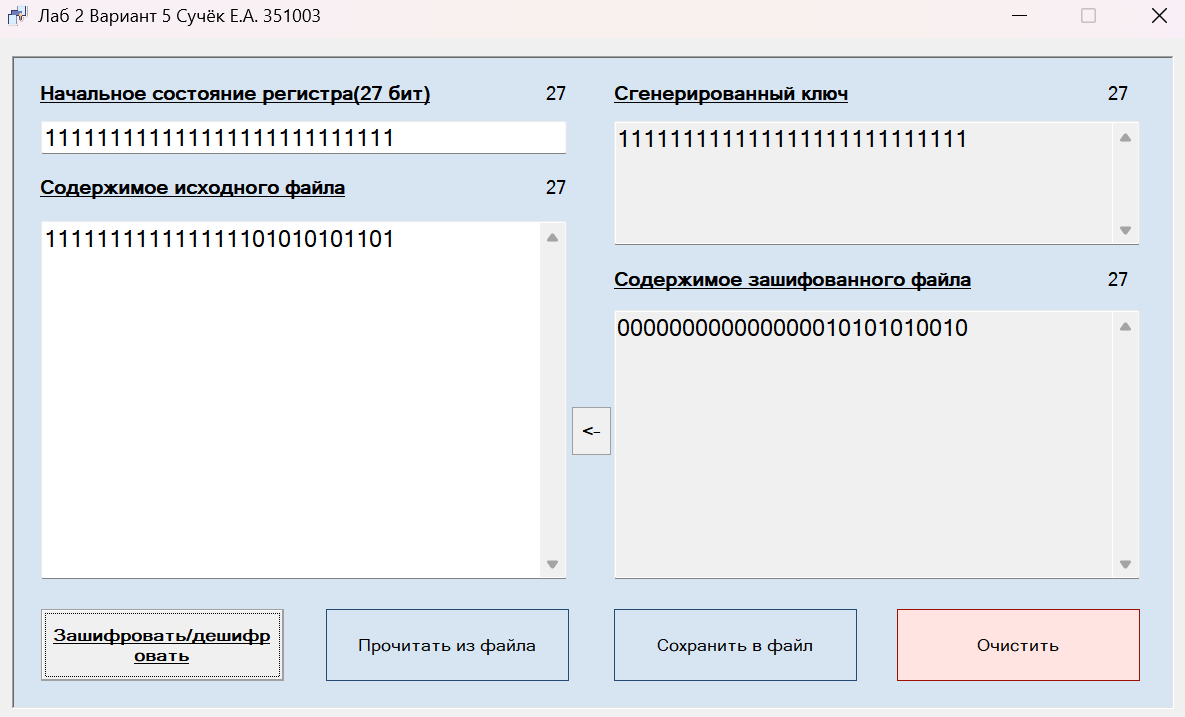
1111111111111111010101010110101010100101101010101000101010100100

* 1. **Корректные исходные данные(длины исходных данных и ключа равны)**

**Процесс шифрования:**

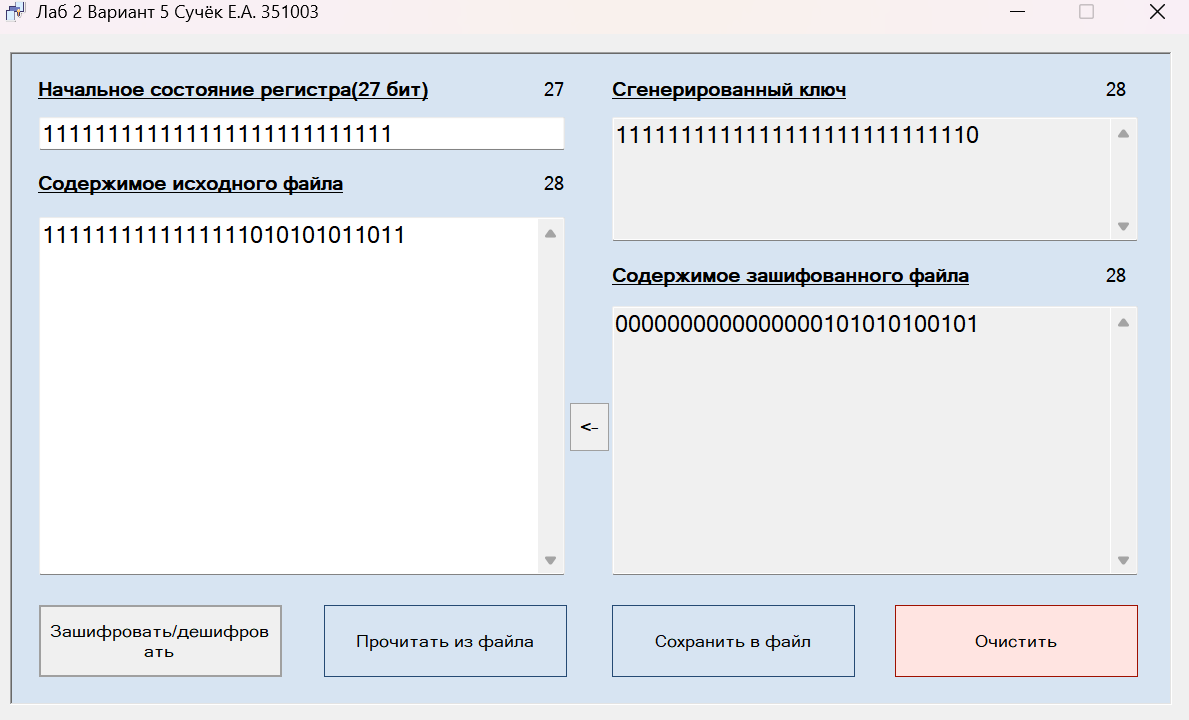


**Процесс дешифрования:**

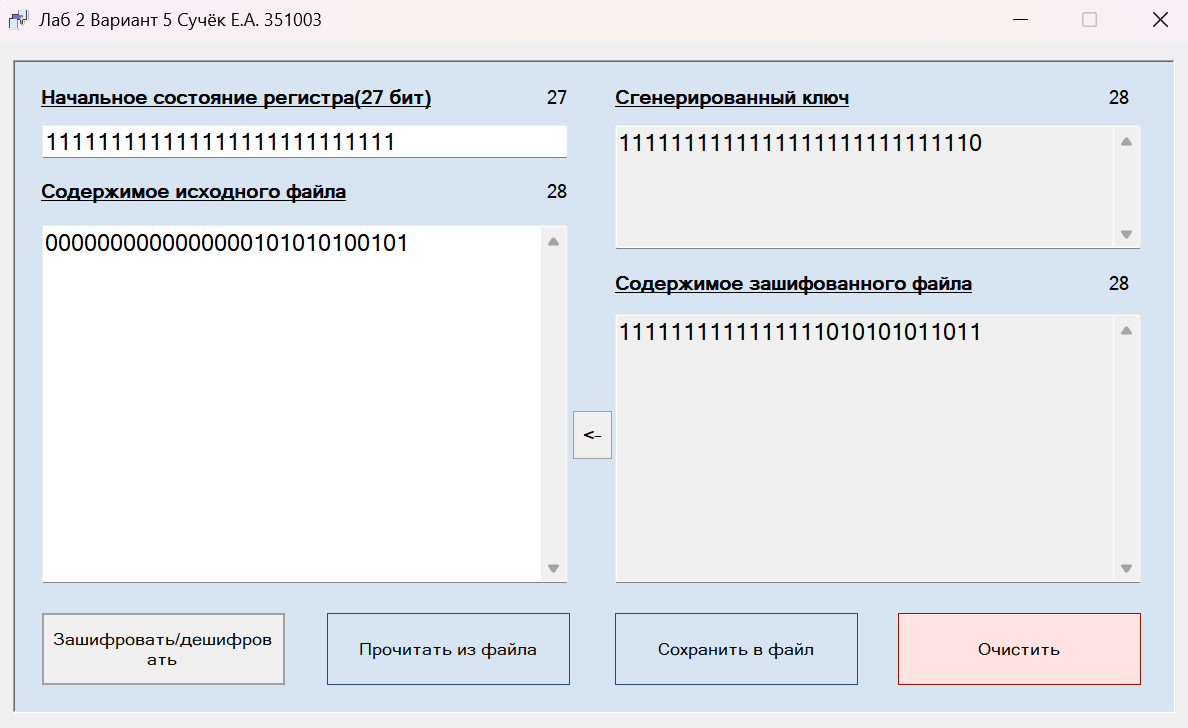


* 1. **Корректные исходные данные(разница на 1 символ)**

**Процесс шифрования:**

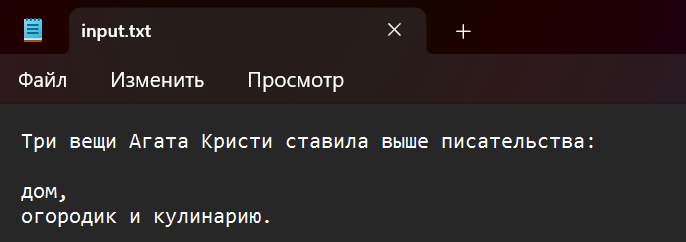


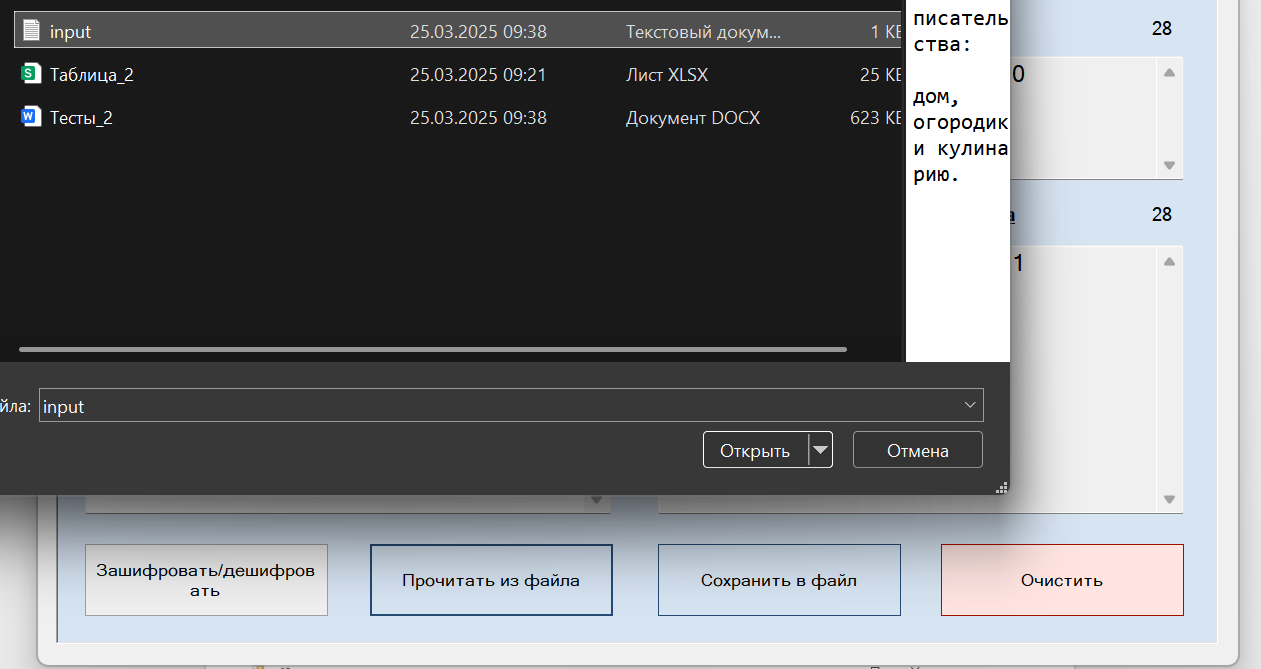
**Процесс дешифрования:**



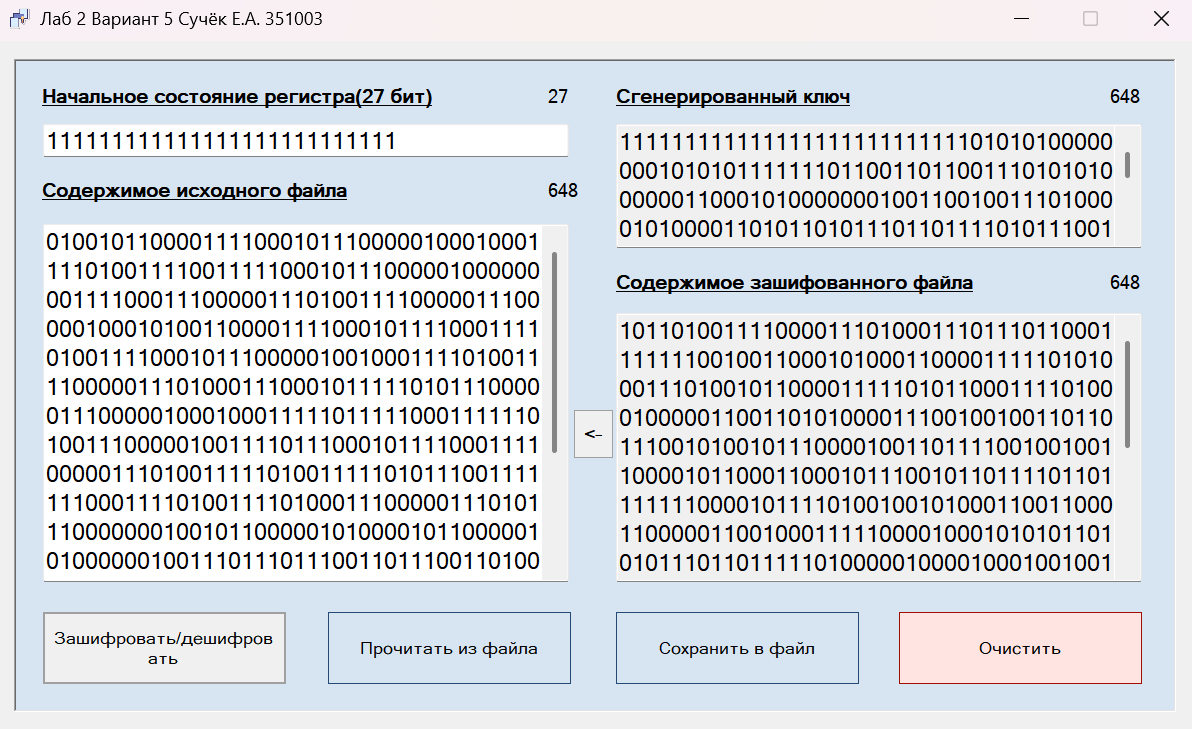
* 1. **Корректные исходные данные(файл .txt)**

**Исходное содержимое файла input.txt:**

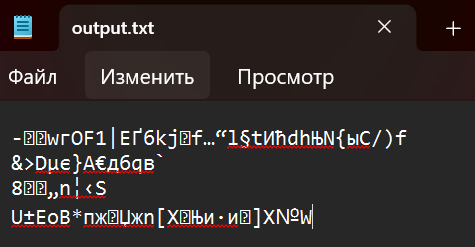




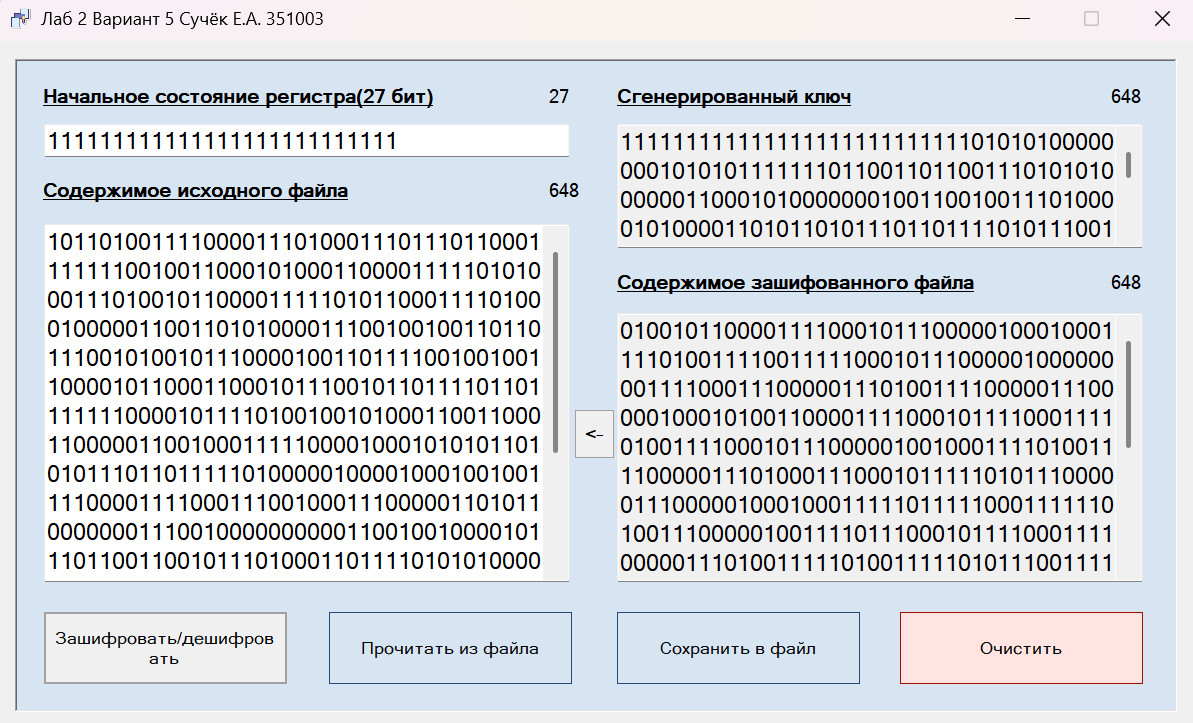
**Процесс шифрования:**



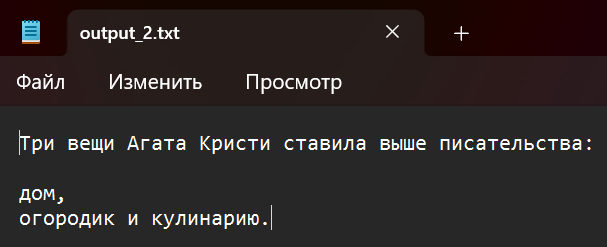
**Содержимое файла output.txt с результатом шифрования:**



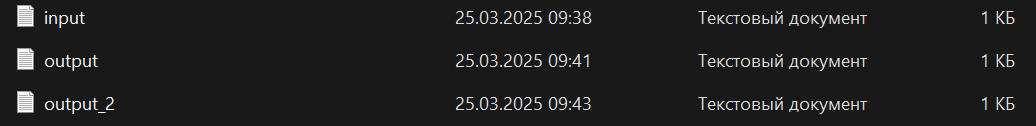
**Процесс дешифрования:**



**Содержимое файла output\_2.txt с результатом дешифрования:**

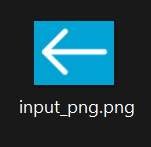


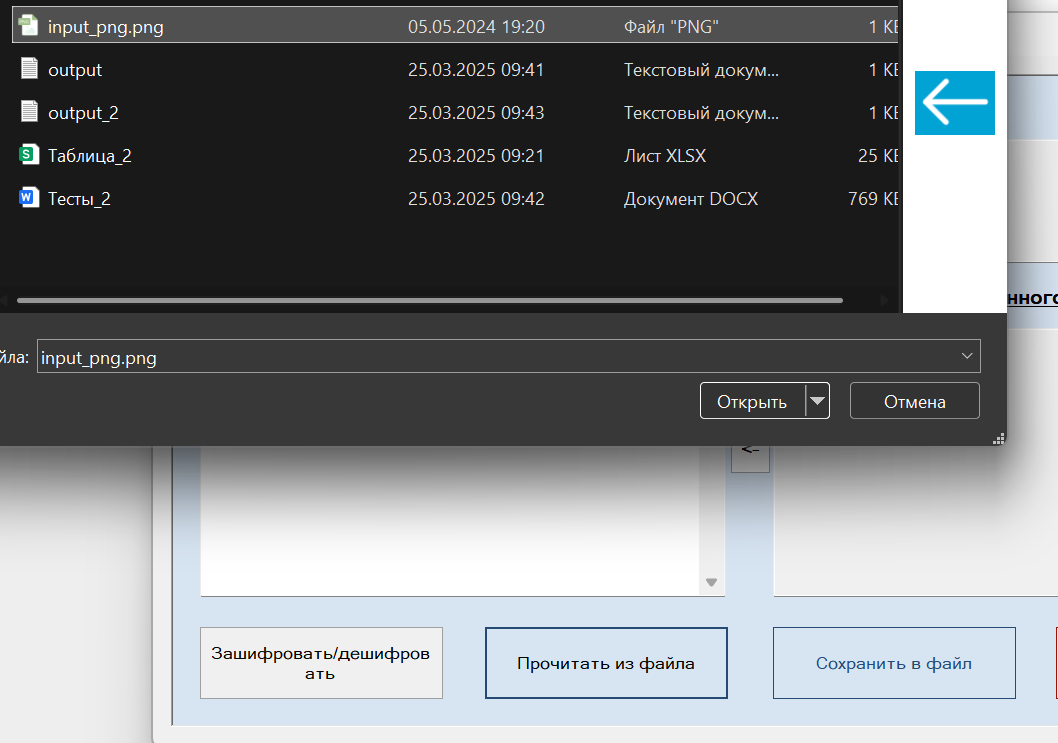
**Скриншот с датами создания файлов:**



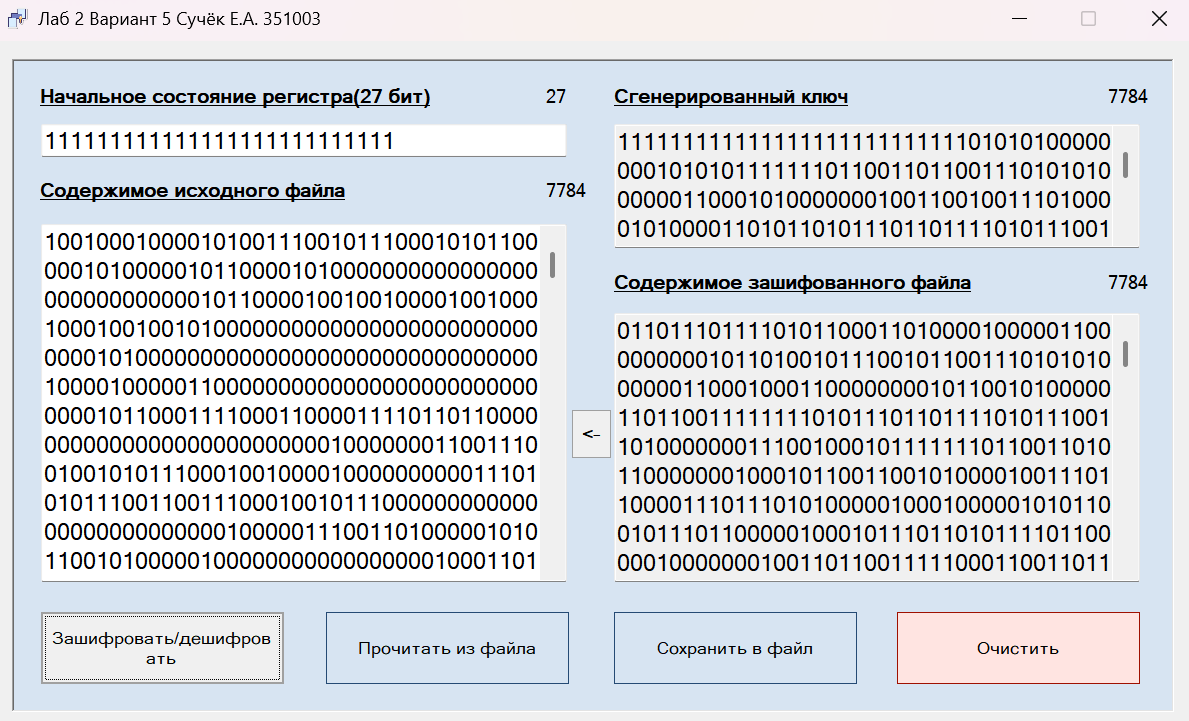
* 1. **Корректные исходные данные(файл .png)**

**Исходное содержимое файла input\_png.png:**





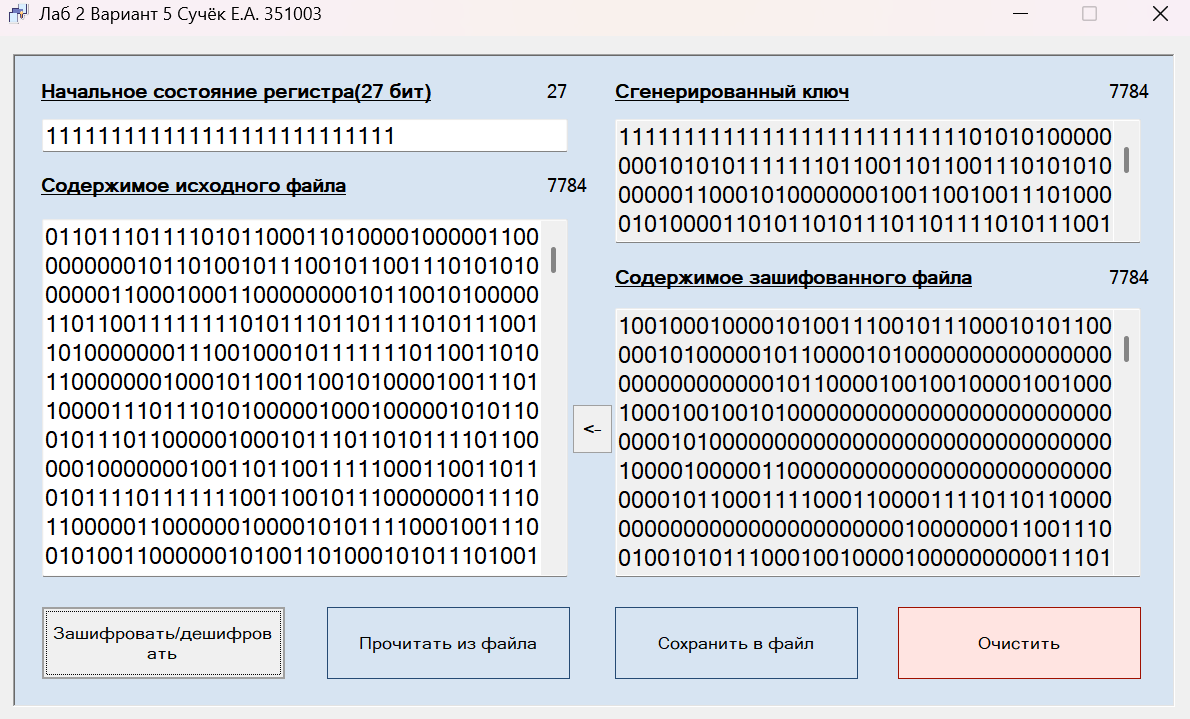
**Процесс шифрования:**



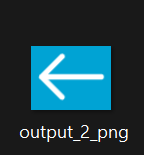
**Файл output\_png.png с результатом шифрования:**



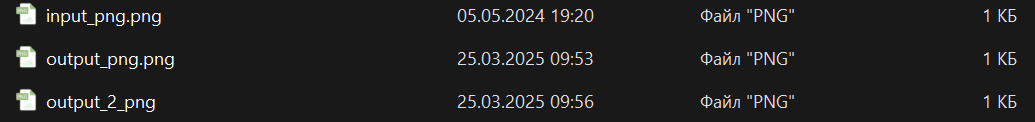
**Процесс дешифрования:**



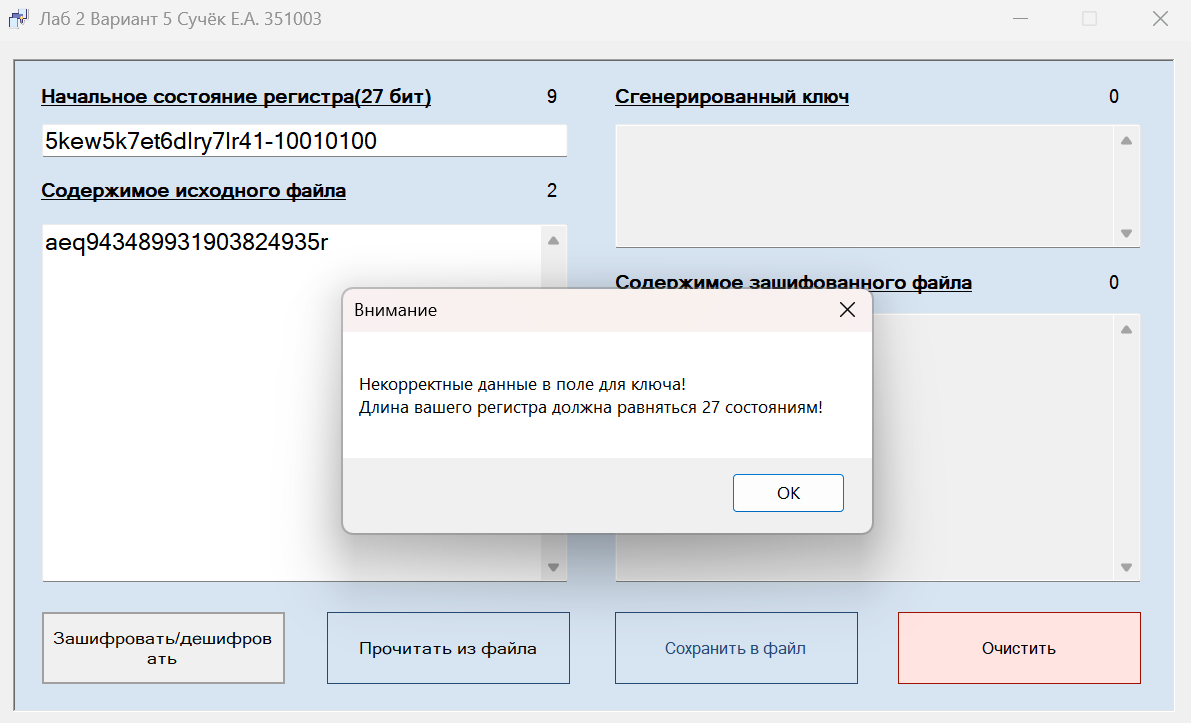
**Содержимое файла output\_2\_png.png с результатом дешифрования:**



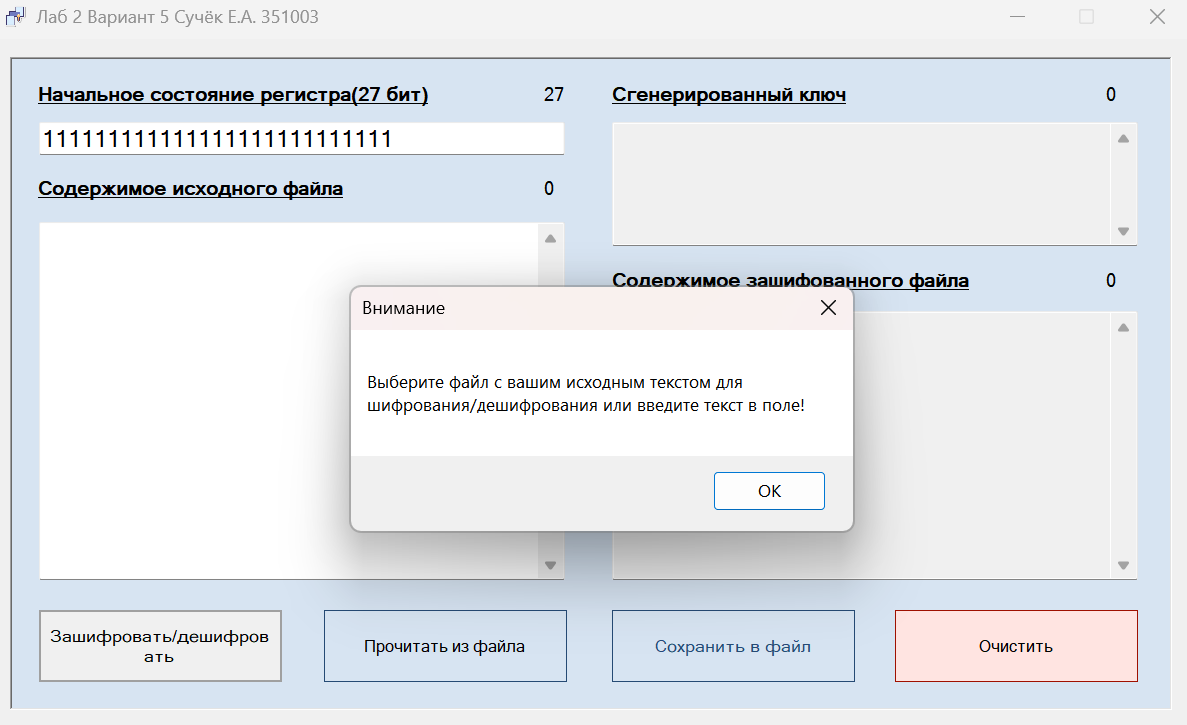
**Скриншот с датами создания файлов:**



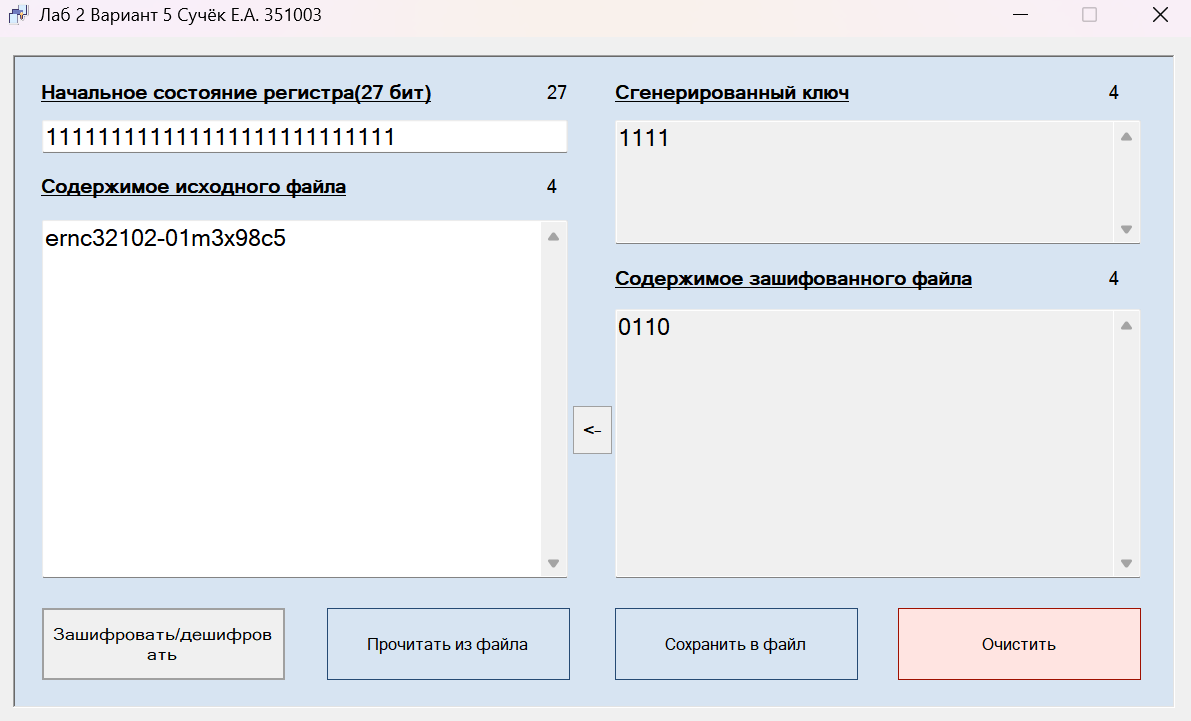
**1.7 Некорректные данные в поле ключа**



* 1. **Некорректные данные в поле исходных данных(пустое поле)**



* 1. **Некорректные данные в поле исходных данных(возможен ввод с клавиатуры)**



Некорректные данные в поле исходных данных просто игнорируются.