УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Тесты к лабораторной работе №2

по предмету

Теория Информации

Вариант 4

Выполнила:

Писарчик. Е.А.

Проверила:

Болтак С.В.

Группа 351004

Минск 2025

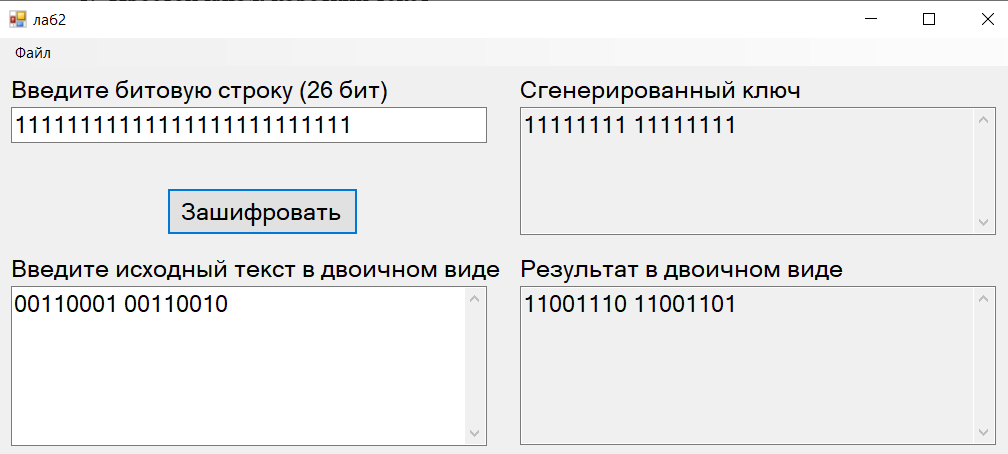
**Задание:**

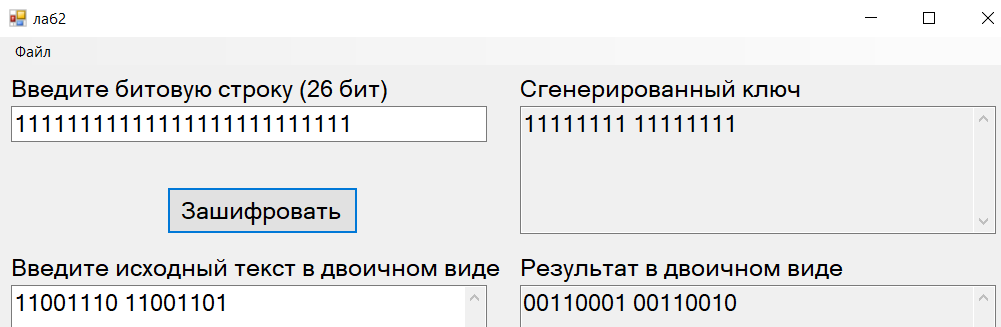
Реализовать систему потокового шифрования и дешифрования для файла с любым содержимым с помощью генератора ключевой последовательности на основе линейного сдвигового регистра с обратной связью LFSR1 (размерность регистра ***37***). Начальное состояние регистра ввести с клавиатуры. Поле для ввода состояния 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:x26 + x8 + x7 + x1 + 1

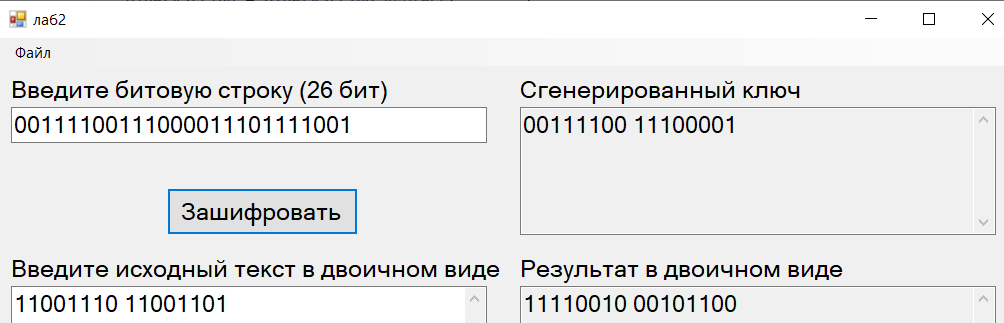
**Тесты**

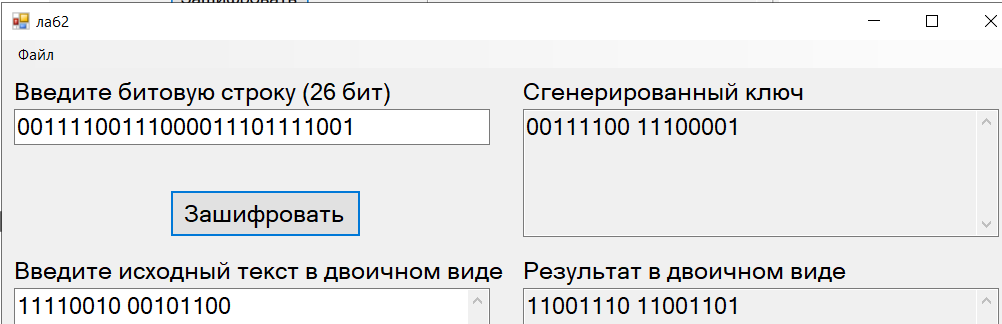
1. Простой ключ, короткий текст



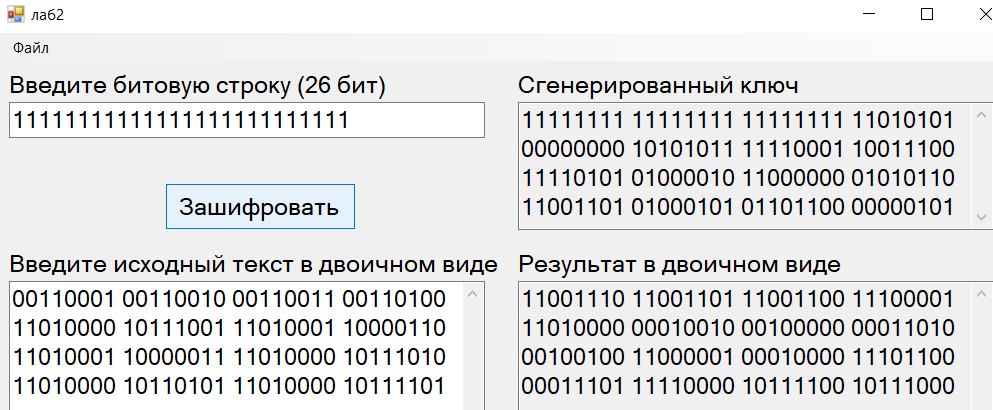


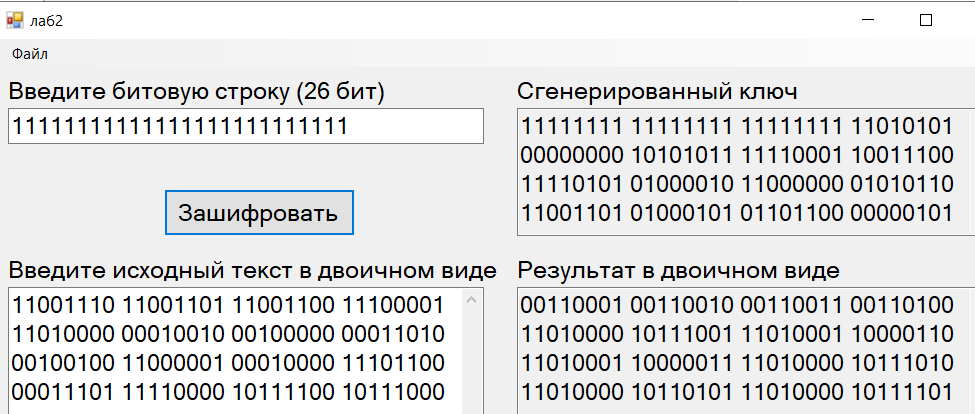
1. Сложный ключ, короткий текст



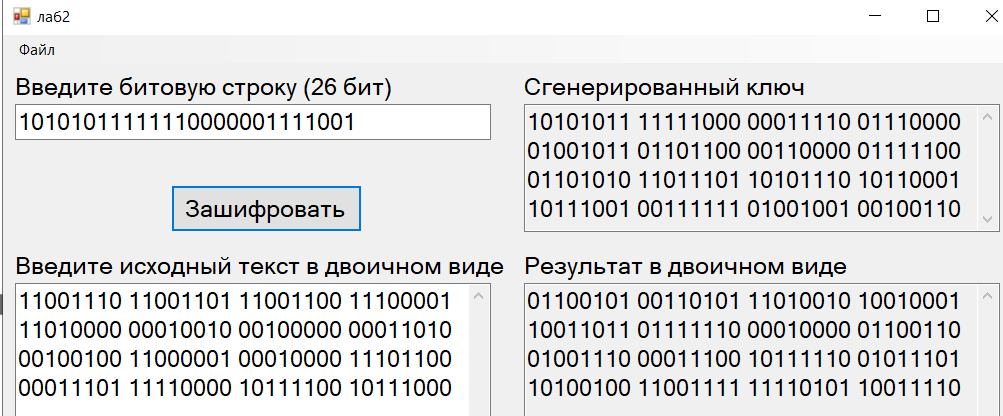


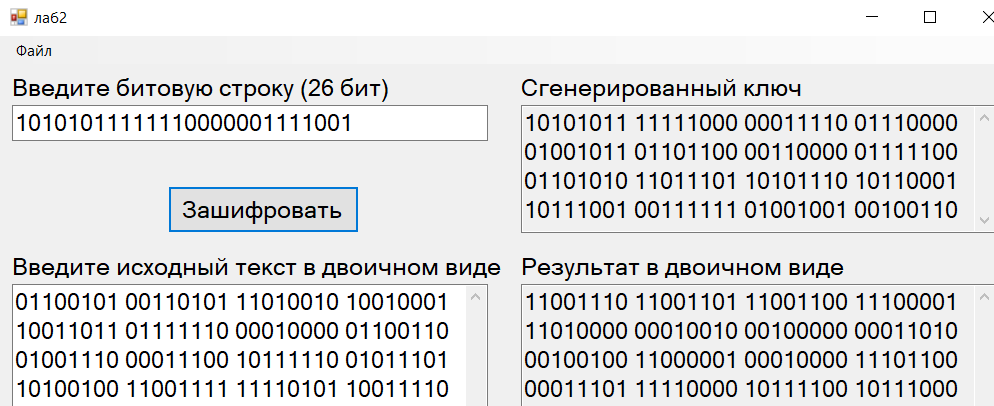
1. Простой ключ, длинный текст





1. Сложный ключ, длинный текст



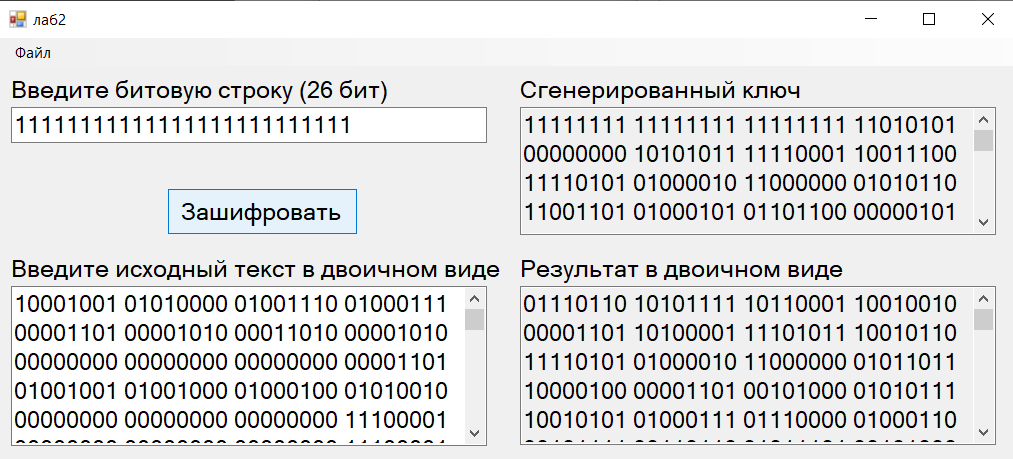


1. Файл с картинкой (.png)

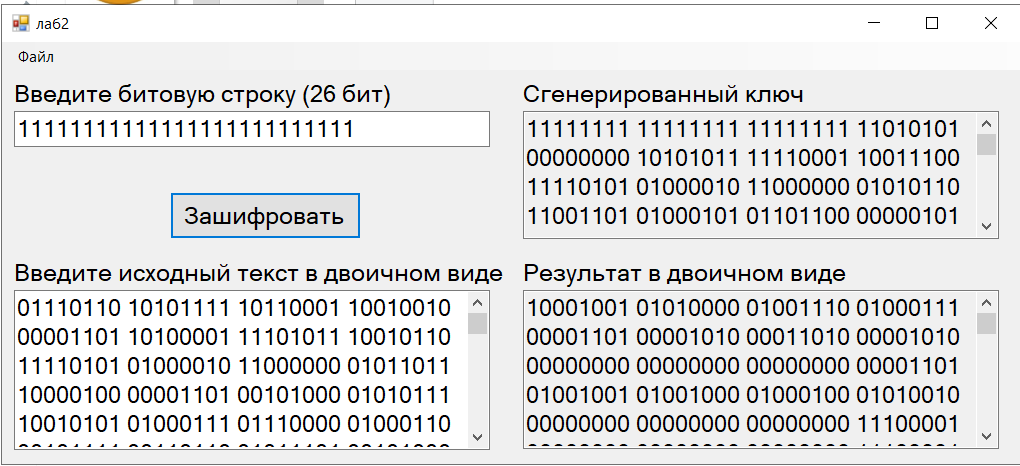
Исходная картинка:



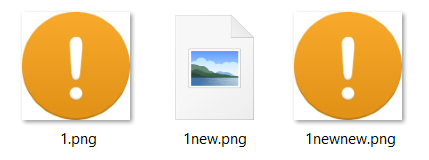
Шифрование:



Расшифровка:

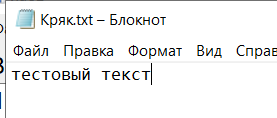


Сохраним в файл, и получим прежнюю картинку:

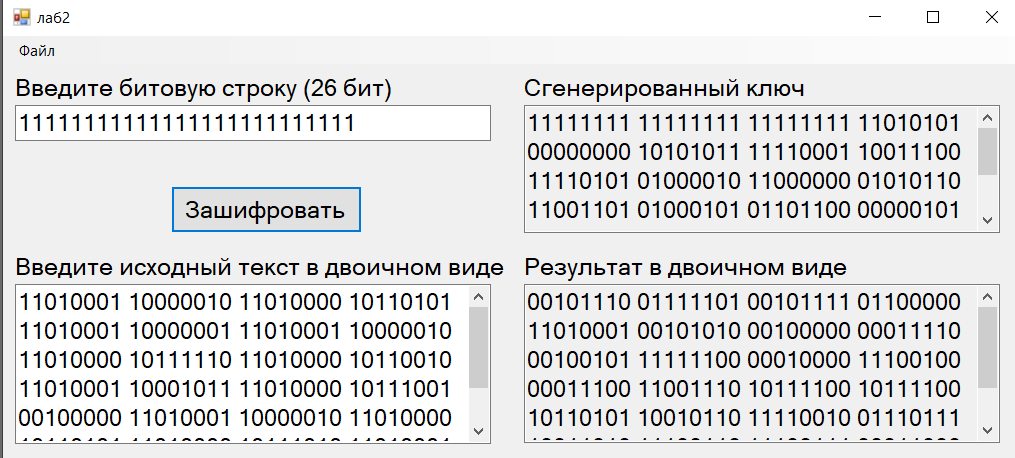


1. Файл с текстом (.txt)

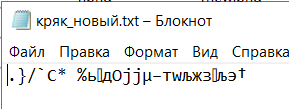
Исходный файл:



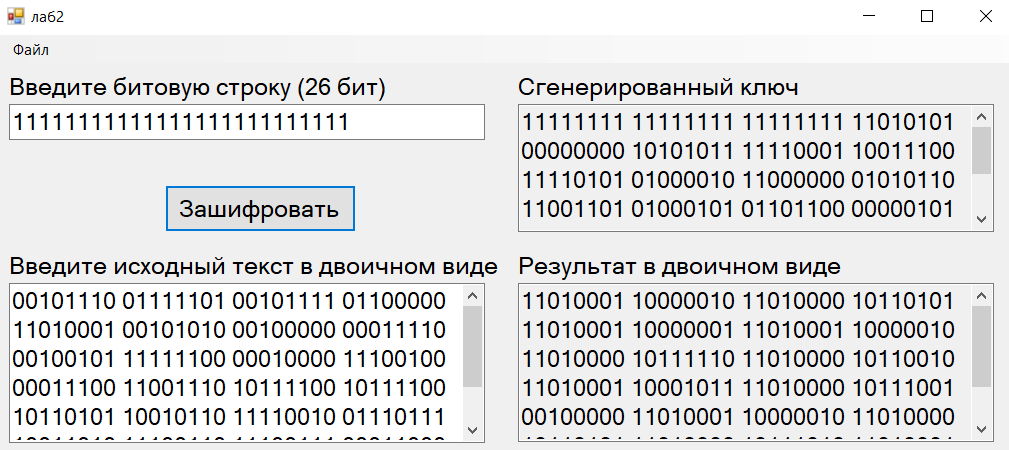
Шифрование:



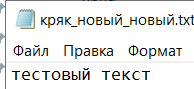
Сохранила в файл, вот результат:



Расшифровка:



Снова сохранила в файл:

 Получилось то, что и было.

Ввод некорректных символов запрещён, можно вводить только “0”, “1” и пробел.