

УО «Белорусский государственный университет информатики и радиоэлектроники»
Кафедра ПОИТ

Отчет по лабораторной работе №2
по предмету
Теория Информации
Вариант 16

Выполнил:
Ушаков А.Д.

Проверил:
Болтак С.В.
Группа 351001

Минск 2025

Задание:

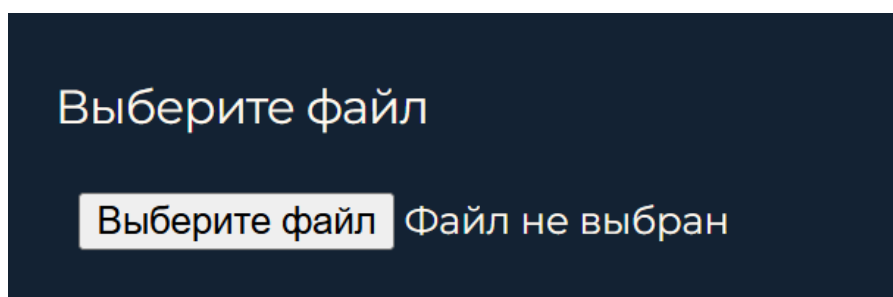
Реализовать систему потокового шифрования и дешифрования для файла с любым содержимым с помощью генератора ключевой последовательности на основе линейного сдвигового регистра с обратной связью LFSR1 (размерность регистра 38). Начальное состояние регистра ввести с клавиатуры. Поле для ввода состояния 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

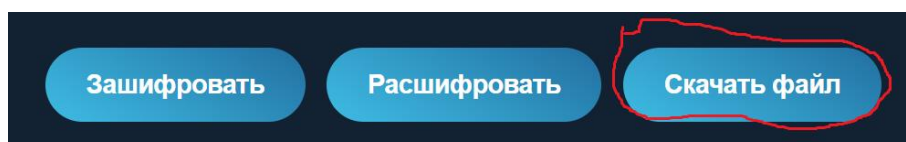
$$x^{38} + x^6 + x^5 + x + 1$$

Работа с файлами

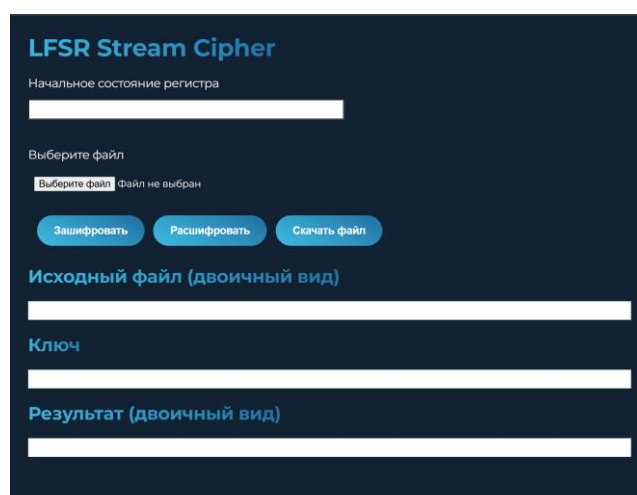
Взятие исходного файла:



Загрузка результата файла:



Общий внешний вид страницы:



Тесты

Текстовый файл, шифрование

The screenshot shows the LFSR Stream Cipher web application on the left and WinHex on the right. In the web application, the 'Исходный файл (двоичный вид)' field contains the binary string '01001000 01000101', which is circled in purple. A purple arrow points from this field to the WinHex window. In WinHex, the file 'test1.txt' is open, showing the same binary data at offset 0. The file's properties on the right show a creation date of 13.03.2025 19:17:12. Below the main window, a smaller WinHex window shows the file 'test1.txt' with the character 'He' circled in green.

Текстовый файл, зашифрованный

The screenshot shows the LFSR Stream Cipher web application on the left and WinHex on the right. In the web application, the 'Исходный файл (двоичный вид)' field contains the binary string '01001000 01000101'. A red arrow points from this field to the WinHex window. In WinHex, the file 'test1.txt' is open, showing the binary data at offset 0. The file's properties on the right show a creation date of 19.03.2025 17:43:19. Below the main window, a smaller WinHex window shows the file 'test1.txt' with the character 'He' circled in green. A red arrow points from the 'Исходный файл (двоичный вид)' field to the 'test1.txt' file in the smaller window.

Текстовый файл, дешифрование

The screenshot shows the LFSR Stream Cipher web application and the WinHex hex editor. In the LFSR interface, a file named 'test1 (1).txt' is selected for decryption. The initial state of the register is shown as a sequence of 1s. The key is also shown as a sequence of 1s. The result of the decryption is shown as a sequence of 0s and 1s. In the WinHex editor, the file 'test1 (1).txt' is open, showing the decrypted content 'He' in the ASCII view. The file properties show it was created on 19.03.2025 at 17:50:09.

Картинка, шифрование

The screenshot shows the LFSR Stream Cipher web application and the WinHex hex editor. In the LFSR interface, a file named 'image.png' is selected for encryption. The initial state of the register is shown as a sequence of 1s. The key is also shown as a sequence of 1s. The result of the encryption is shown as a sequence of 0s and 1s. In the WinHex editor, the file 'image.png' is open, showing the encrypted content in the hex view. The file properties show it was created on 13.03.2025 at 19:20:55.

Картинка, зашифрованный

The screenshot shows the LFSR Stream Cipher application interface. The 'Выберите файл' (Select file) button is highlighted with a red box. The 'Исходный файл (двоичный вид)' (Original file (binary view)) section displays a large block of binary data. The 'Результат (двоичный вид)' (Result (binary view)) section also displays a large block of binary data. A green arrow points from the 'Результат' section to the 'WinHex' application window, which shows the binary data of the encrypted image file. The 'WinHex' window displays a hex dump of the file 'image.png' (21.2 KB) located at 'C:\Users\PC\Downloads'. The file's creation date is 19.03.2025 17:59:48, and its last modification date is 19.03.2025 17:59:49. The file's attributes are listed as 8 Bit (±): 83, 16 Bit (±): -6 317, 32 Bit (±): -399 382 701, and Двоичн.: 01010011.

Картинка, дешифрование

The screenshot shows the LFSR Stream Cipher application interface. The 'Выберите файл' (Select file) button is highlighted with a red box. The 'Исходный файл (двоичный вид)' (Original file (binary view)) section displays a large block of binary data. The 'Результат (двоичный вид)' (Result (binary view)) section also displays a large block of binary data. A green arrow points from the 'Результат' section to the 'WinHex' application window, which shows the binary data of the decrypted image file. The 'WinHex' window displays a hex dump of the file 'image (1).png' (21.2 KB) located at 'C:\Users\PC\Downloads'. The file's creation date is 19.03.2025 18:02:43, and its last modification date is 19.03.2025 18:02:43. The file's attributes are listed as 8 Bit (±): -119, 16 Bit (±): 20 617, 32 Bit (±): 1 196 314 761, and Двоичн.: 10001001. A circuit diagram is also visible in the background of the WinHex window.