**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) 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** | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| LFSR1 | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** |
| LFSR2 | **31** | **32** | **33** | **34** | **35** | **36** | **37** | **38** |
| LFSR3 | **39** | **40** | **23** | **24** | **25** | **26** | **27** | **28** |