|  |
| --- |
|  |

Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение

высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

им. Н.П. ОГАРЁВА»

(ФГБОУ ВО «МГУ им. Н.П. Огарёва»)

Институт электроники и светотехники

Кафедра информационной безопасности и сервиса

ЛАБОРАТОРНАЯ РАБОТА №3

по теме:

«Шифры гаммирования»

Автор отчёта о лабораторной работе  А. Е. Конышев

подпись, дата

Обозначение лабораторной работы ЛР–02069964–02.03.02–08–23

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Проверил работу

канд. техн. наук, доц.  И. П. Карьгин

подпись, дата

Саранск 2023

**Генерация гаммы с помощью регистра сдвига с линейной обратной связью, используя полином x8 + x4 + x3 + x2 + 1.**

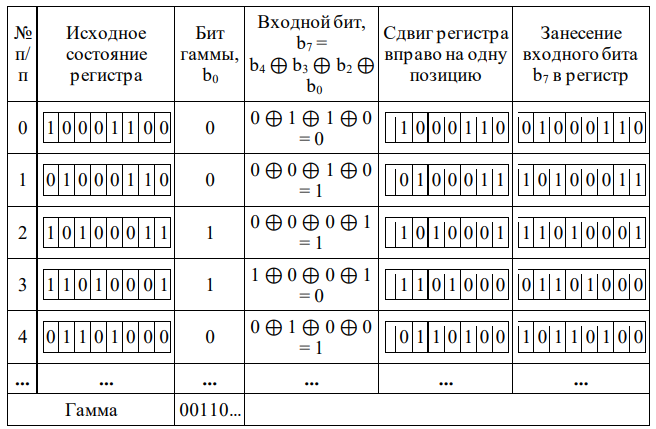
Регистр сдвига с линейной обратной связью (РСЛОС) – упорядоченный набор битов, у которого значение входного (вдвигаемого слева, старшего) бита равно линейной булевой функции от значений остальных битов регистра до сдвига.

Длиной регистра называется количества битов в нем. В качестве булевой

функции для РСЛОС чаще всего используют сложение по модулю 2. Такие РСЛОС обычно записывают в виде многочлена (полинома) или упорядоченной последовательности. Запись x8 + x4 + x3 + x2 + 1 или (8, 4, 3, 2, 0) означает, что длина регистра 8 битов, а входной бит рассчитывается по формуле b7 = b4 ⊕ b3 ⊕ b2 ⊕ b0 (для битов нумерация начинается справа и с нулевой позиции). Выходной (выдвигаемый справа, младший) бит будет являться частью генерируемой гаммы. Расчет требуемой гаммы осуществляется в цикле, на каждой итерации которого выполняются следующие операции:

1. Добавление выходного бита b0 к гамме.
2. Расчет входного бита bn-1 по формуле.
3. Сдвиг битов регистра вправо на одну позицию.
4. Занесение рассчитанного входного бита bn-1 в позицию n-1.

Пример генерации гаммы для регистра, инициализированного значением 100011002.



Примечание.

Для регистра длиной n максимальное количество состояний составляет 2n-1. Это число равно 2n–1, а не 2n, поскольку заполнение РСЛОС нулями влечет вывод регистром бесконечной последовательности нулей, что совершенно бесполезно. Таким образом, максимально возможная длина периода гаммы в битах составляет (2n–1), если из регистра для гаммы на каждой итерации брать один бит. Для получения такого максимального периода многочлен должен быть примитивным по модулю.

. Примитивный многочлен степени n – неприводимый многочлен, который является делителем x2^n-1, но не является делителем xd+1 для всех d, являющихся делителями 2n–1. Чем больше битов регистра используются для расчета входного бита, тем лучше (повышается стойкость). Многочлены с большим количеством членов называют плотными, с малым – разреженными.

**Работа программы.**

**Этап 1 (подготовительный).**

Для начала необходимо инициализировать 8 битовый регистр.Для этого переведем каждый символ строки “Конышев\_Артем\_Евгеньевич\_триста\_вторая\_группа\_первая\_подгруппа” в бинарный вид по кодировке windows 1251, где каждый символ займет 8 бит. Затем операцией xor необходимо сложить соответствующие биты символов строки, результат записать в соответствующий бит регистра (учитывая нумерацию битов регистра справа налево начиная с 0.

Регистр будет иметь вид 11010001.

**Этап 2.**

Требуется сгенерировать гамму, используя 10 итераций. В таком случае её длина составит 11 битов.

Вычисления и результат работы программы представлены ниже:

i | регистр | b0 | b7 | регистр->1бит | b7->регистр

---+----------+----+----+---------------+------------

0 | 11010001 | 1 | 0 | \_1101000 | 01101000

1 | 01101000 | 0 | 1 | \_0110100 | 10110100

2 | 10110100 | 0 | 0 | \_1011010 | 01011010

3 | 01011010 | 0 | 0 | \_0101101 | 00101101

4 | 00101101 | 1 | 1 | \_0010110 | 10010110

5 | 10010110 | 0 | 0 | \_1001011 | 01001011

6 | 01001011 | 1 | 0 | \_0100101 | 00100101

7 | 00100101 | 1 | 0 | \_0010010 | 00010010

8 | 00010010 | 0 | 1 | \_0001001 | 10001001

9 | 10001001 | 1 | 0 | \_1000100 | 01000100

10 | 01000100 | 0 | 1 | \_0100010 | 10100010

gamma: 10001011010