Потоковое шифрование

Яковлев Вадим, гр. 051003

Вариант 5

Проверка генератора LFSR:

Полином: x^27+x^8+x^7+x+1=0

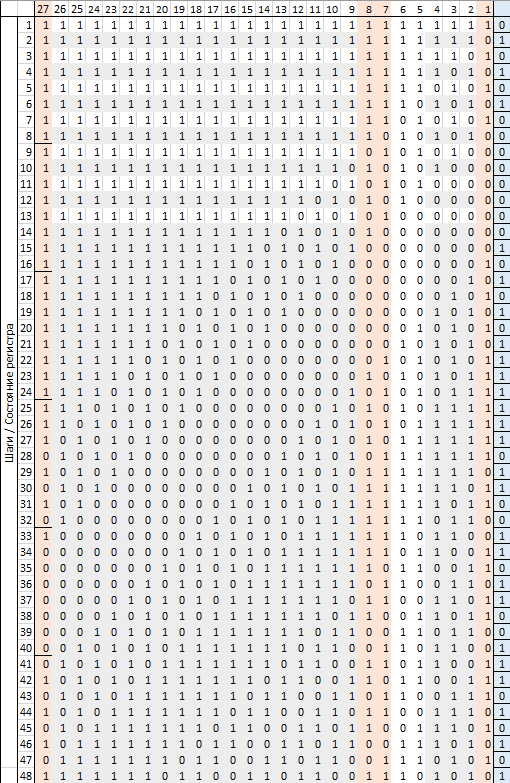
Начальное состояние регистра: 27 единиц.

Исходные данные для шифрования (байтовое представление):

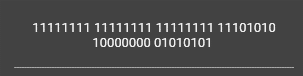
11010000 10110000 11010000 10110001 11010000 10110011

Ожидаемый ключ (столбец регистра с номером 27):

11111111 11111111 11111111 11101010 10000000 01010101



Полученный ключ:



Проверка шифрования:

Исходные данные (в байтах):

11010000 10110000 11010000 10110001 11010000 10110011

Ключ (в байтах):

11111111 11111111 11111111 11101010 10000000 01010101

11010000 10110000 11010000 10110001 11010000 10110011

xor

11111111 11111111 11111111 11101010 10000000 01010101

=

00101111 01001111 00101111 01011011 01010000 11100110

Ожидаемый результат (в байтах):

00101111 01001111 00101111 01011011 01010000 11100110

Полученный результат:

