Practico 4 de Criptografia-2007

1): Calcular el output del LFSR $(x^4 + x^3 + x^2 + x + 1, 4)$ con estado inicial 1111.

2): Hallar todos los ciclos del LFSR $(x^4 + x^2 + x + 1, 4)$.

3): Usando LFSRs:

$$L_1 = (x^3 + x^2 + 1, 3)$$
$$L_2 = (x^4 + x + 1, 4)$$
$$L_3 = (x^5 + x^4 + x^3 + x^2 + x + 1, 5)$$

use L_1 para controlar L_2, L_3 con el alternating step generator, y calcule una veintena de bits.

4): Repetir el ejercicio anterior, pero ahora use L_1 para controlar L_3 con el shrinking generator.

5): En cada caso, use el algoritmo de Berlekamp-Massey para encontrar la complejidad lineal y polinomios conectivos para las siguientes secuencias:

a) 0000 1001 0110 0111 1100

b) 1111 0001 0011 0101

c) 010 111 001 100 011

d) 1011 1010 1111 1011 1

6): Encuentre el ciclo del FCSR dado por $q = 29$ con estado inicial 0000 1. (recordar que hay que escribir $q = 2q_1 + 2^2q_2 + ... + 2^nq_n - 1$ da los taps).

7): Supongamos que se tienen 100 generales, que deben coordinar una acción. Votaran sobre que acción a tomar, y la acción con la mayoria de votos sera llevada a cabo. Ante el peligro de que el enemigo intercepte las comunicaciones, cada par de generales encripta sus comunicaciones con una clave distinta. Ademas, la clave que A usa para mandarle mensajes a B es distinta de la que B usa para mandarle mensajes a B (para que el enemigo no sepa si A le esta diciendo a B lo mismo que B le esta diciendo a A).

Una posibilidad seria que los generales usaran RC4. Supongamos que las claves son seleccionadas al azar, que las elecciones son “Ataquemos” o “Defenderr”, (la “r” extra es para que los mensajes tengan la misma longitud, de lo contrario es facil saber cual se mandó) y supongamos que la propuesta que gana, lo hace con el 70% de los votos. Probar entonces que un enemigo que intercepte todos los mensajes puede saber cual acción tomaran los generales, aun sin poder quebrar ninguna clave.