Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Criptosistemas simétricos: Flujo"

Ejercicios propuestos

Ejercicio 1:

Postulados de Golomb

a) Dada la secuencia: 00101001110110 ¿Se cumplen?

Ejercicio 2:

Cifrar el texto en claro: 101001111, con la clave 010010001, generada aleatoriamente, suponiendo un cifrado de Vernam.

Ejercicio 3:

Considere un generador de bits constituido por un registro de desplazamiento de realimentación lineal (RDRL) de 4 posiciones:

a) Sea la semilla del generador $S_1S_2S_3S_4$=0111 y sea el polinomio $f(x)=x^4+x^2+1$. Obtenga la secuencia de registros que resulta e indique su periodo y su complejidad lineal.
b) Sea la semilla del generador $S_1S_2S_3S_4$=1101 y sea el polinomio $f(x)=x^4+x^2+1$. Obtenga la secuencia de registros que resulta e indique su periodo y su complejidad lineal.
c) Sea la semilla del generador $S_1S_2S_3S_4$=1110 y sea el polinomio (primitivo) $f(x)=x^4+x+1$. Obtenga la secuencia de registros que resulta e indique su periodo y su complejidad lineal.

Ejercicio 3:

Considere el cifrador de flujo RC4. ¿Qué valor de la clave deja el estado S sin cambios en la fase de inicialización? Es decir, a la salida de esta fase el vector S debe contener los valores de 0 a 255 en orden ascendente.