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?

Solución:

a)

- G1. Número de '1' = 7 ; Número de '0' = 7. Por tanto, se cumple.
- G2.

  Racha: 00 → longitud 2

  Racha: 1 → longitud 1

  Racha 0 → longitud 1

  Racha 1 → longitud 1

  Racha 00 → longitud 2

  Racha 111 → longitud 3

  Racha 0 → longitud 1

  Racha 11→ longitud 2

  Racha 0 → longitud 1

  Total: 9 rachas.

  ¿4 o 5 rachas tienen longitud 1? Sí

  ¿2 o 3 rachas tienen longitud 2? Sí

  ¿1 o 2 rachas tienen longitud 3? Sí

  Por tanto, se cumple el postulado 2

- G3. Calculamos la autocorrelación fuera de fase, AC(k)

K=1

00101001110110

01010011101100

AC(1) = (A-F) / T = 6-8 /14 = -2/14

K=2

00101001110110

10100111011000

AC(2) = (A-F) / T = 6-8 /14 = -2/14

K=3

00101001110110

01001110110001

AC(3) = (A-F) / T = 6-8 /14 = -2/14

K=4

00101001110110

10011101100010

AC(4) = (A-F) / T = 8-6 /14 = 2/14

Al no ser un valor constante, se puede afirmar que no se cumple el postulado G3.

Ejercicio 2:

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

Solución:

101001111 XOR 010010001 = 111011110

Ejercicio 3:

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

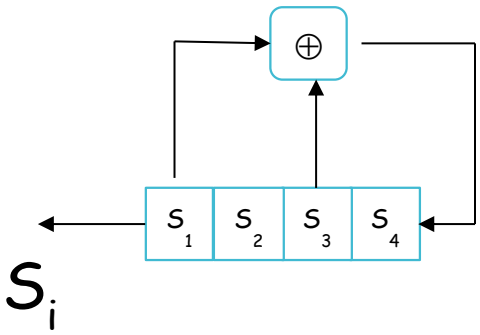
a) Sea la semilla del generador $S_1S_2S_3S_4$=0111 y sea el polinomio $f(x)=x^4+x^2+1$. Obtenga la secuencia de registros que resulta e indique su periodo y su complejidad lineal.

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.

Solución:

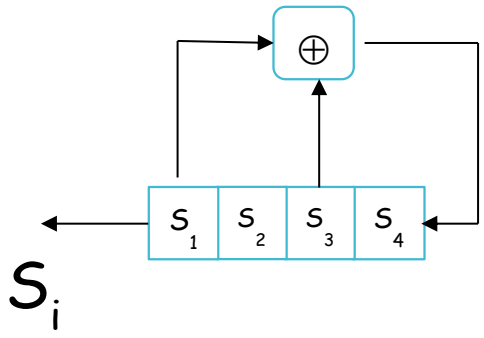
a)



ESTADO REGISTRO	BIT GENERADO
0111	0
1111	1
1110	1
1100	1
1001	1
0011	0
0111	0
1111	1

Periodo= 6; LC= 4

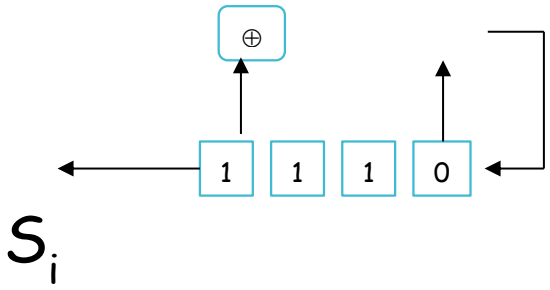
b)



ESTADO REGISTRO	BIT GENERADO
1101	1
1011	1
0110	0
1101	1
1011	1

Periodo= 3; LC= 4

c)



ESTADO REGISTRO	BIT GENERADO
1110	1
1101	1
1010	1
0101	0
1011	1
0110	0
1100	1
1001	1

0010	0
0100	0
1000	1
0001	0
0011	0
0111	0
1111	1
1110	1

Periodo =15; LC= 4

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

Solución:

Seleccionamos una clave de 256 bytes de longitud. Tenemos que lograr que el valor de j=i en cada paso para que al realizar el Swap (S[i],S[j]) S no varíe. Por tanto K[0]=K[1]=0, K[2]=255, K[3]=254… K[255]=2.