Universidad
Carlos III de Madrid

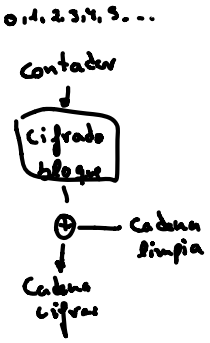
COSEC LAB · *Dpto. Informática*

Universidad Carlos III de Madrid

Cifradores de flujo Enunciados

Seguridad en las Tecnologías de la Información
Curso 2016/2017

1. Cifradores de flujo



i. RC4

→ El del vector que hay que intercambiar posiciones.

- 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. 0's

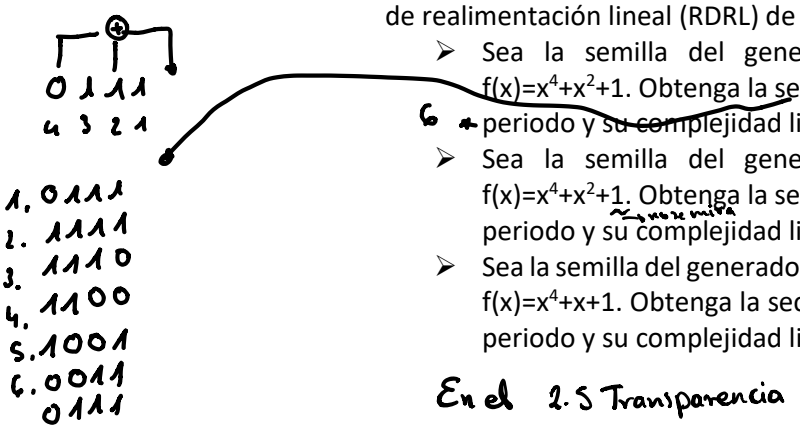
En 2.3.3 diapo 27

ii. Vernam

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

⊕ 101001111
010010001
111011110

iii. LFSR



- Considere un generador de bits constituido por un registro de desplazamiento de realimentación lineal (RDRL) de 4 posiciones.
  - 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. → ¿?
  - 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.
  - 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.

6 → no es mía

En el 2.5 Transparencia 18.

(ii) ➢ Sea la semilla del generador $S_1S_2S_3S_4$=0111 y sea el polinomio $f(x)=x^4+x^3+1$. Obtenga la secuencia de registros que resulta e indique su

0 1 1 1 → 1

0 − 1 1 1 1 → 0 Secuencia resultado: 011110

1 − 1 1 1 0 → 0

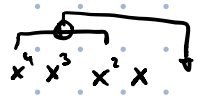
1 − 1 1 0 0 → 1

1 − 1 0 0 1 → 1

1 − 0 0 1 1 → 1

0 − 0 1 1 1 → Se ha repetido.

➢ Sea la semilla del generador $S_1S_2S_3S_4$=1101 y sea el polinomio $f(x)=x^4+x^3+1$. Obtenga la secuencia de registros que resulta e indique su periodo y su complejidad lineal.



1 1 0 1 1

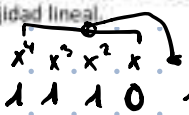
Secuencia: 110

1 − 1 0 1 1 → 0

1 − 0 1 1 0 → 1

0 − 1 1 0 1 → 1

➢ 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.



1 1 1 0 1 Secuencia: 1110101100010001

1 − 1 1 0 1 0	1 1 0 0 1 0	0 0 1 1 1 1
1 − 1 0 1 0 1	1 0 0 1 0 0	0 1 1 1 1 0
1 − 0 1 0 1 1	0 0 1 0 0 0	1 1 1 1 0 0
0 − 1 0 1 1 0	0 1 0 0 0 1	
1 − 0 1 1 0 0	1 0 0 0 1 1	
0 1 1 0 0 1	0 0 0 1 1 1	

Viernes 13 => 12:00 h

Jueves 12 => 12:30 h

20:30 h

Martes 17 => 16:45 h

Viernes 20 => 9:30 h

10:30 h

9 L
10 M
11 X
12 J
13 V
14 S
15 D
16 L
17 M
18 X
19 J
20 V