Secuencias Psedualeatorias

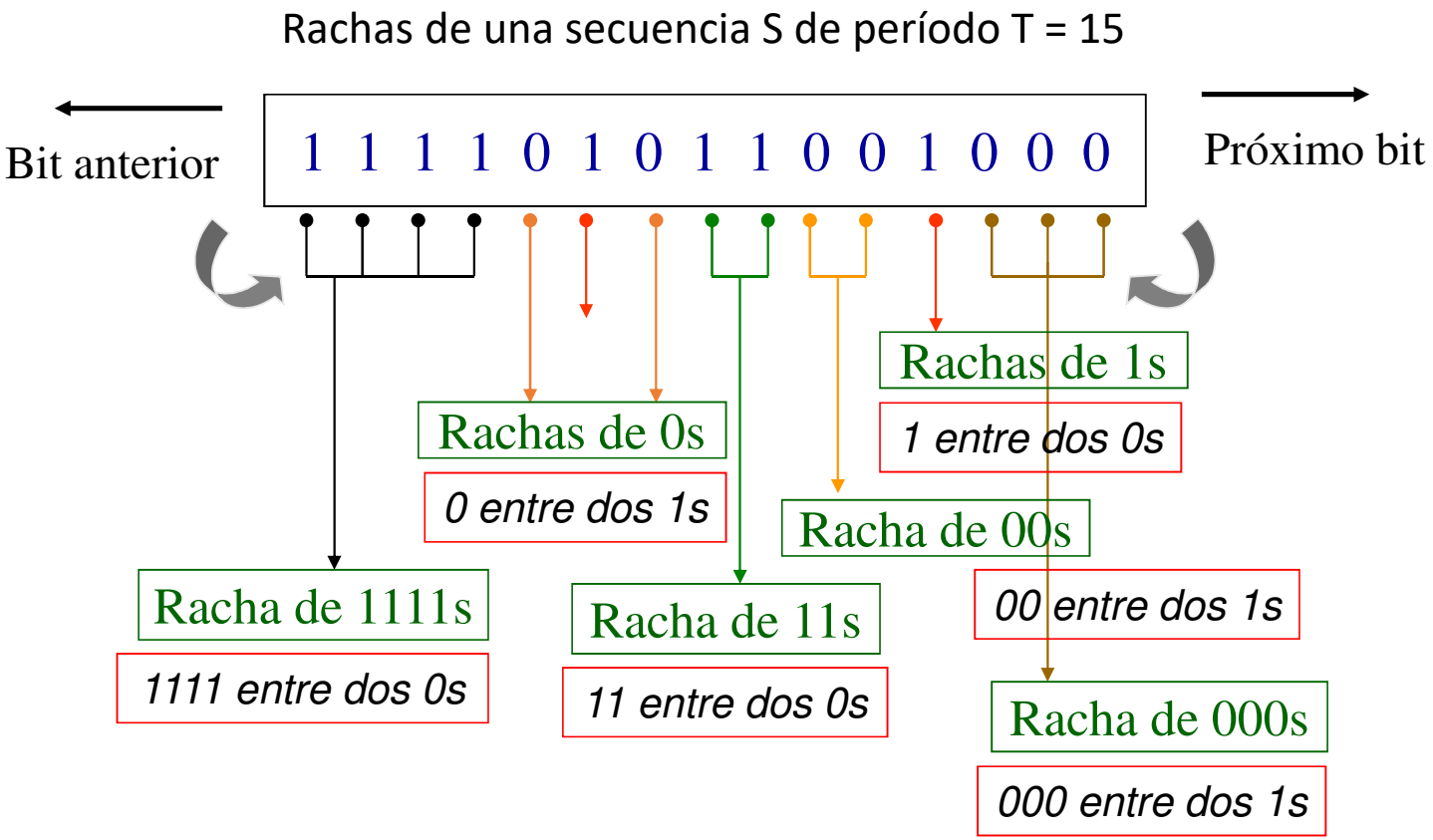
Roberto Gómez Cárdenas
rogomez@tec.mx
http://cryptomex.org
@cryptomex.org

Adecuado de: Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1

Características de la secuencia pseudoalatroia S

- Período:
  - La clave deberá ser tanto o más larga que el mensaje.
  - En la práctica se usará una semilla K de unos 120 a 250 bits en cada extremo del sistema para generar períodos superiores a 10^{35}.
- Distribución de bits:
  - La distribución de bits de unos (1s) y ceros (0s) deberá ser uniforme para que represente a una secuencia pseudoaleatoria. Para ello deberá cumplir los postulados de Golomb:
- Rachas de dígitos:
  - Uno o más bits entre dos bits distintos.
- Función de autocorrelación fuera de fase AC(k):
  - Desplazamiento de k bits sobre la misma secuencia Si.

Rachas de dígitos en una secuencia

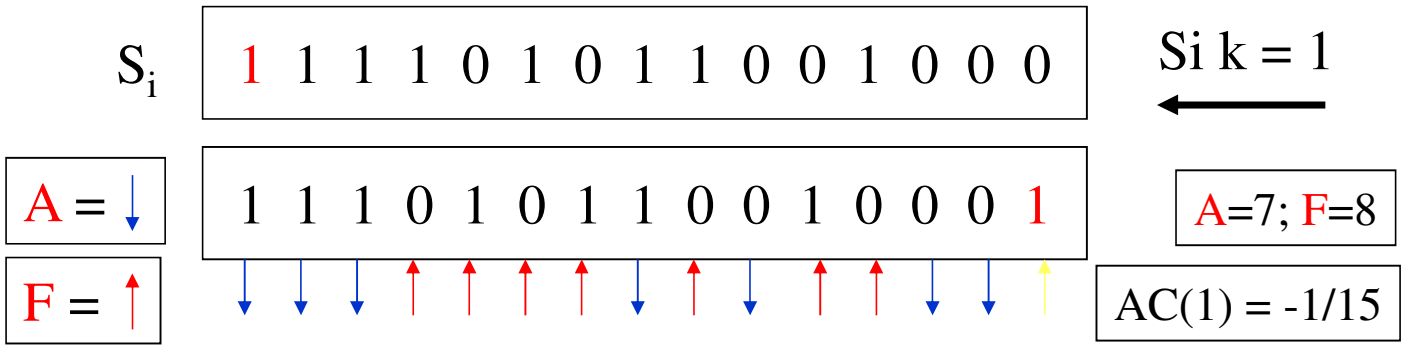


Autocorrelación fuera de fase AC(k)

- Función de autocorrelación:
  - Autocorrelación AC(k) fuera de fase de una secuencia Si de período T desplazada k bits a la izquierda:

$$C(k) = (A - F) / T$$

- Ejemplo Aciertos ⇒ bits iguales Fallos ⇒ bits diferentes



Primer postulado de Golomb G1

- Postulado G1:
- Deberá existir igual número de ceros que de unos. Se acepta como máximo una diferencia igual a la unidad.
- Ejemplo 1

1 1 1 1 0 1 0 1 1 0 0 1 0 0 0

  - La secuencia S_1 de 15 bits, hay 8 unos y 7 ceros. Sí cumple con el postulado G1.
- Ejemplo 2

0 1 0 1 1 1 0 0 1 0 0 1 0 0 0 1

  - La secuencia S_2 de 16 bits, hay 7 unos y 9 ceros. No cumple con el postulado G1.
- Significado
  - Si una secuencia S_i como la indicada cumple con G1, quiere decir que la probabilidad de recibir un bit 1 es igual a la de recibir un bit 0, es decir un 50%.

Segundo Postulado de Golomb G2

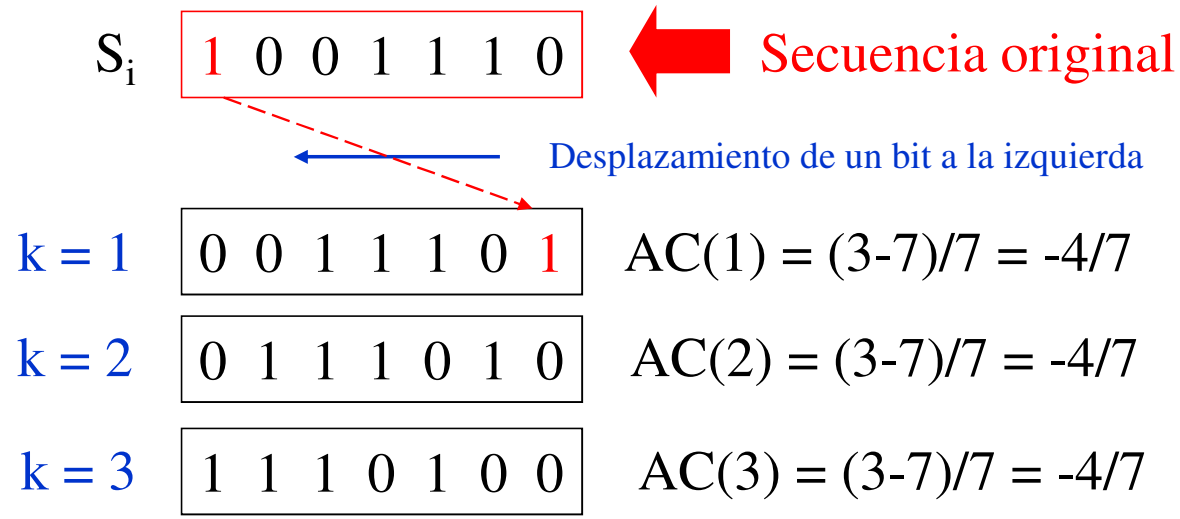
- En un período T, la mitad de las rachas de S_i serán de longitud 1, la cuarta parte de longitud 2, la octava parte de longitud 3, etc.
- Ejemplo

1 1 1 1 0 1 0 1 1 0 0 1 0 0 0

  - En la secuencia S_i de 15 bits, había 4 rachas de longitud uno, 2 rachas de longitud dos, 1 racha de longitud tres y 1 racha de longitud cuatro.
  - Este tipo de distribución en las rachas para períodos impares, es típica de las denominadas *m-secuencias.*
- Significado
  - Si una secuencia S_i como la indicada cumple con G2, quiere decir que la probabilidad de recibir un bit 1 o un bit 0, después de haber recibido un 1 o un 0 es la misma, es decir un 50%.

Tercer postulado de Golomb G3

- La autocorrelación AC(k) deberá ser constante para todo valor de desplazamiento de k bits.
- Ejemplo 1



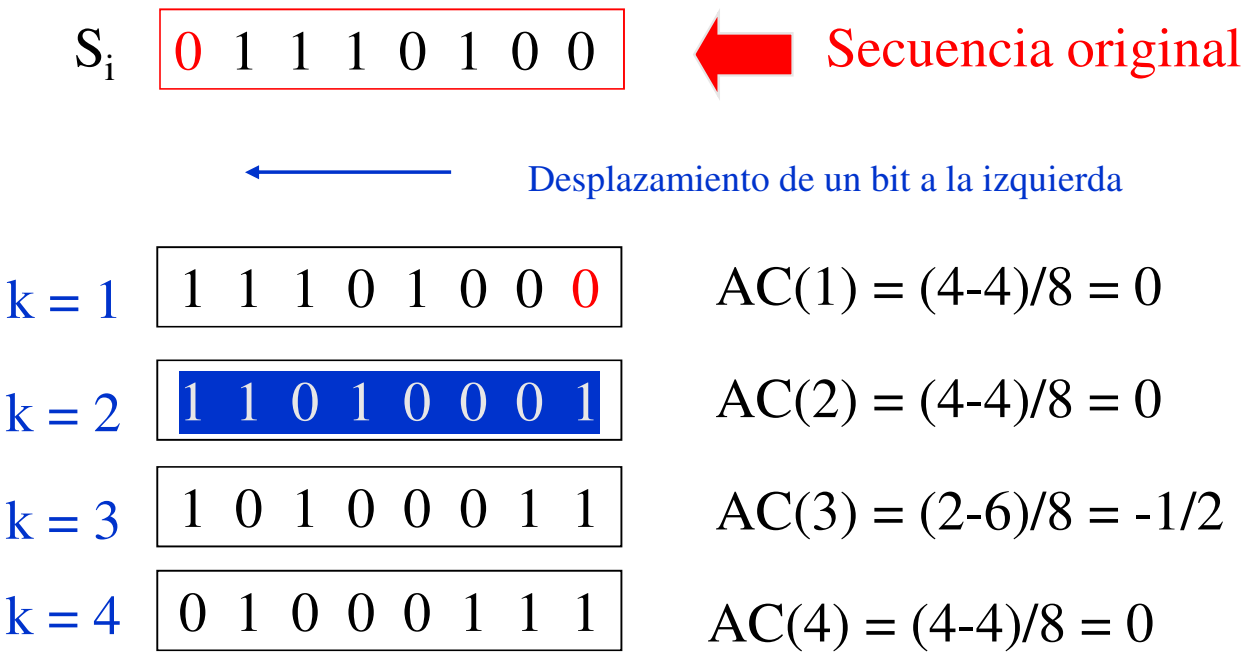
Tercer postulado de Golomb G3

- Continuación ejemplo

	1 0 0 1 1 1 0	Secuencia original
k = 4	1 1 0 1 0 0 1	AC(4) = (3-7)/7 = -4/7
k = 5	1 0 1 0 0 1 1	AC(5) = (3-7)/7 = -4/7
k = 6	0 1 0 0 1 1 1	AC(6) = (3-7)/7 = -4/7
k = 7	1 0 0 1 1 1 0	Secuencia original en fase

La secuencia S_i = 1001110 de 7 bits cumple con G3

Autocorrelación no constante



Autocorrelación no constante

S_i	0 1 1 1 0 1 0 0	Secuencia original
k = 5	1 0 0 0 1 1 1 0	AC(5) = (2-6)/8 = -1/2
k = 6	0 0 0 1 1 1 0 1	AC(6) = (4-4)/8 = 0
k = 7	0 0 1 1 1 0 1 0	AC(7) = (4-4)/8 = 0
k = 8	0 1 1 1 0 1 0 0	Secuencia original en fase

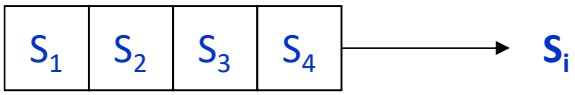
La secuencia S_i = 01110100 de 8 bits no cumple con G3

Significado: Si una secuencia cumple con el postulado G3 quiere decir que, independientemente del trozo de secuencia elegido por el atacante, no habrá una mayor cantidad de información que en la secuencia anterior.

Tipos de generadores lineales LFSR

- En función del polinomio asociado tendremos:
  - LFSR con polinomios factorizables
    - No serán criptográficamente interesantes.
  - LFSR con polinomios irreducibles
    - No serán criptográficamente interesantes.
  - LFSR con polinomios primitivos
    - Según los postulados de Golomb, este tipo de polinomio que genera todos los estados lineales posibles del cuerpo de trabajo n, será el que nos entregue una secuencia cifrante de interés criptográfico con período $T = 2^n - 1$.
- Nota
  - Como la única función de realimentación de un LFSR es un XOR, no estará permitida la cadena de todos ceros.

Ejemplo generador LFSR con f(x) factorizable



Sea $f(x) = x^4 + x^2 + 1$

S_i

f(x) es factorizable porque:

Sea $f(x_1) = f(x_2) = (x^2+x+1)$

$f(x) = f(x_1) \bullet f(x_2)$

$f(x) = (x^2+x+1) \bullet (x^2+x+1)$

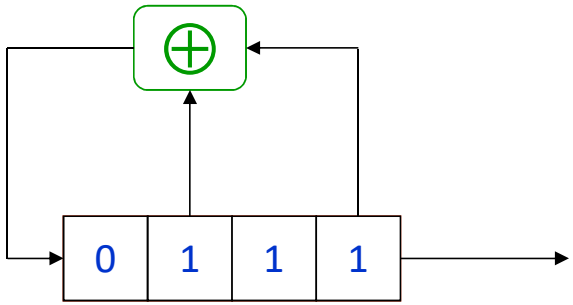
$f(x) = x^4+2x^3+3x^2+2x+1$

Tras la reducción módulo 2

Luego $f(x) = x^4 + x^2 + 1$

$f(x) = x^4 + x^2 + 1$

Sea la semilla:
$S_1S_2S_3S_4 = 0111$

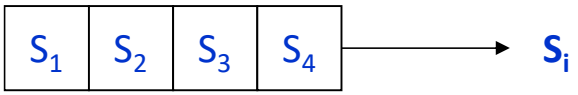


Registro	Bit S_i
0111	1
0011	1
1001	1
1100	0
1110	0
1111	1
0111	1

. . . semilla

$S_i = 111001$ T = 6

Generador LFSR con f(x) irreducible

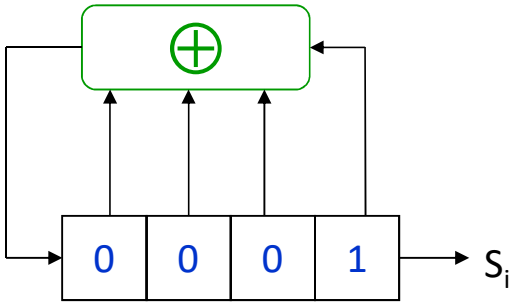


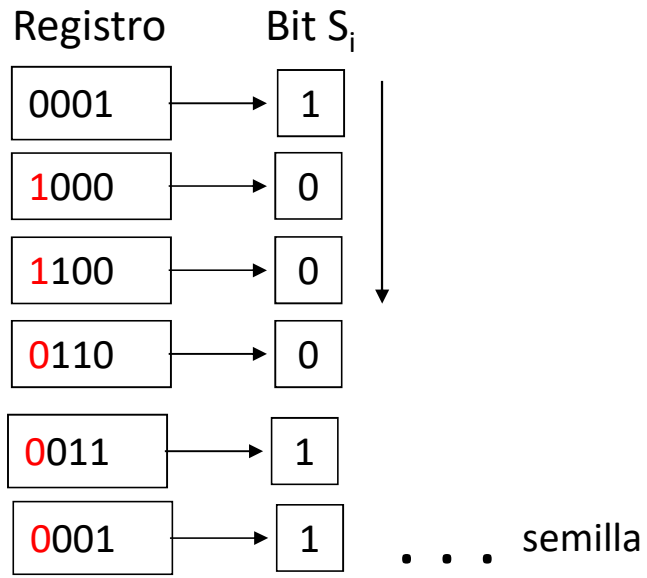
$f(x) = x^4 + x^3 + x^2 + x + 1$

Sea la semilla:
$S_1S_2S_3S_4 = 0001$

Sea $f(x) = x^4 + x^3 + x^2 + x + 1$

Es imposible factorizar en módulo 2 la función f(x) mediante dos polinomios $f(x_1)$ y $f(x_2)$ de grado menor





$S_i = 100011$ $T = 5$ siendo
$T_{máx} = 2^n - 1 = 2^4 - 1 = 15$

Generador LFSR con f(x) primitivo

Sea $f(x) = x^4 + x + 1$

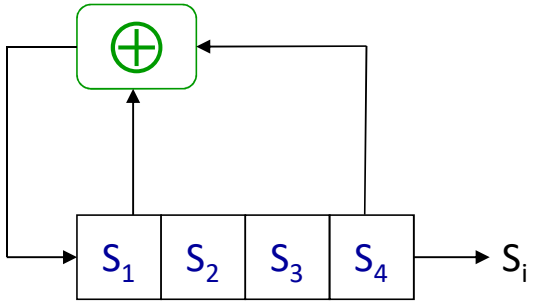
f(x) no es factorizable como $f(x_1) \bullet f(x_2)$ en módulo 2.

Será además un generador del grupo.

Existen $\phi(2^n - 1)/n$ polinomios primitivos

$f(x) = x^4 + x + 1$

$S_1S_2S_3S_4 = 1001$



Registro	Bit S_i
1001 →	1
0100 →	0
0010 →	0
0001 →	1
1000 →	0
1100 →	0
1010 →	0
1101 →	1
0110 →	0
0011 →	1

S_i = 100100011110101

T = 15 siendo

$T_{máx} = 2^n - 1 = 2^4 - 1 = 15$