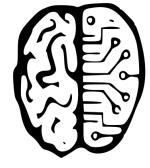
Cifrado en flujo

Características del cifrado en flujo
Generación de secuencias pseudoaleatorias

Universidad del País Vasco
Euskal Herriko Unibertsitatea

KISA



Características del cifrado en flujo

- Es un cifrado simétrico.
- El mensaje se cifra bit a bit.
- Se usa la misma clave para cifrar y para descifrar.
- La comunicación es segura si el procedimiento de cifrado se mantiene secreto.
- Son rápidos. Tasa de cifrado: la del canal de transmisión.
- Tienen fácil implementación hardware.

Ejemplo [Cifrado de Vernam (1917)]

EMISOR

M :	1001010011101010
K :	1010000110101010
$C = M \oplus K$:	0011010101000000

RECEPTOR

C :	0011010101000000
K :	1010000110101010
$M = C \oplus K = M \oplus K \oplus K$:	1001010011101010

Teorema (Shannon, 1949)

El cifrado de Vernam es incondicionalmente seguro si:

- *K secuencia aleatoria,*
- *de período tan largo como el mensaje,*
- *se utiliza una sola vez.*

Observaciones:

- Hay que generar la clave aleatoria K.
- Hay que transmitir la clave.
  - Problema: Si M es grande, K es grande (tan grande como M).
  - En lugar de transmitir K, se generan claves pseudoaleatorias iguales en ambos extremos de la comunicación, a partir de una clave inicial K_0.
  - Se transmite la clave inicial K_0 (mediante Criptografía de clave pública).

Así, el cifrado en flujo presenta dos componentes básicos:

- El generador de claves: RKG (*"Random Key Generator"*).
- La función de cifrado: E.

El generador de claves RKG

Genera una secuencia binaria pseudoaleatoria (z_i) a partir de una clave de inicialización K_0:

$$\mathrm{RKG}(K_0) = (z_i),\ i = 0, 1, 2, \ldots$$

La función de cifrado E

Realiza operaciones booleanas:

$$c_i = \mathrm{E}(z_i, m_i),\ i = 0, 1, 2, \ldots$$

E debe ser computacionalmente sencilla, invertible. Ejemplo: XOR

Procedimiento de cifrado-descifrado en flujo

Sea $M = m_0 m_1 m_2 \dots m_n$ mensaje

- Emisor
  - Generador de claves: $\mathrm{RKG}(K_0) = (z_i)$
  - La función de cifrado E: $c_i = \mathrm{E}(z_i, m_i)$
- Receptor
  - Generador de claves: $\mathrm{RKG}(K_0) = (z_i)$
  - La función de cifrado E: $m_i = \mathrm{E}^{-1}(z_i, c_i)$

Generación de secuencias pseudoaleatorias

Hemos de estudiar:

1. Concepto de aleatoriedad.
2. Caracterización y medida de aleatoriedad.
3. Generadores pseudoaleatorios:
   - 3.1 Generadores congruenciales (generadores de números enteros).
   - 3.2 Registros de desplazamiento (g. de bits).
   - 3.3 Generadores basados en funciones hash, cifrados simétricos, firmas digitales* (g. de bits).
   - 3.4 Generadores basados en RSA* (g. de números enteros).

* Para su estudio se necesitan conocimientos que veremos más adelante.

Definición (Secuencia aleatoria)

Una secuencia de bits $(s_i) = (s_0, s_1, s_2, \ldots)$ *se considera* aleatoria *si la probabilidad de conocer un bit conocidos los anteriores, es de* $\frac{1}{2}$.

Una secuencia de números enteros $(s_i) = (s_0, s_1, s_2, \ldots)$, $s_i \in \mathbb{Z}_n$, $n \in \mathbb{N}$, *se considera* aleatoria *si la probabilidad de conocer un término conocidos los anteriores, es de* $\frac{1}{n}$.

Caracterización y medida de aleatoriedad

Hemos de introducir parámetros que permitan evaluar si una secuencia puede considerarse aleatoria, o en qué grado. Ello se efectúa mediante:

- Función de autocorrelación.
- Tests de Golomb.
- Tests estadísticos sencillos: test de frecuencias, test de 2-ráfagas, test de póker, test de m-ráfagas.
- Otros tests estadísticos.

Definición (Secuencia periódica)

$(s_i) = (s_0, s_1, \ldots)$ *es* periódica *si existe* T *tal que*

$$s_{i+T} = s_i, \quad i = 0, 1, \ldots \tag{1}$$

Entonces, se denomina:

- *período* al valor mínimo de T que cumple (1),
- *ciclo* a los elementos de un período: $(s_0, s_1, \ldots, s_{T-1})$.

Ejemplo

La siguiente secuencia es periódica de período 5:

s_i	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	$\ldots$
s_i	0	1	0	1	1	0	1	0	1	1	0	1	$\ldots$

$$s_{i+5} = s_i, \quad i = 0, 1, 2, \ldots$$

Definición (Función de autocorrelación)

$(s_i) = (s_0, s_1, \ldots)$ *secuencia de bits periódica de período* T.
Función de autocorrelación*:*

$$C(t) = \frac{1}{T}\sum_{i=0}^{T-1}(2s_i - 1)(2s_{i+t} - 1), \quad 0 \leq t \leq T-1.$$

Nota: La función de autocorrelación puede calcularse para todo $t \in \mathbb{N}$ definiendo $C(t) = C(t-T)$ para todo $t \geq T$.

Observación:

$$\begin{array}{lll} si\ \ s_i = s_{i+t} & \rightarrow & (2s_i - 1)(2s_{i+t} - 1) = \ \ 1, \\ si\ \ s_i \neq s_{i+t} & \rightarrow & (2s_i - 1)(2s_{i+t} - 1) = -1. \end{array}$$

Ejemplo

Consideremos la secuencia periódica de período 10:

$$(s_i) = (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, \ldots)$$

Calculemos la autocorrelación entre un ciclo, y un ciclo desplazado $t = 3$:

s_i	1	0	1	1	1	0	0	1	0	0
s_{i+3}	1	1	0	0	1	0	0	1	0	1
$(2s_i - 1)(2s_{i+3} - 1)$	1	−1	−1	−1	1	1	1	1	1	−1

por tanto,

$$C(3) = \frac{1}{10} \sum_{i=0}^{9} (2s_i - 1)(2s_{i+3} - 1) = 0.2$$

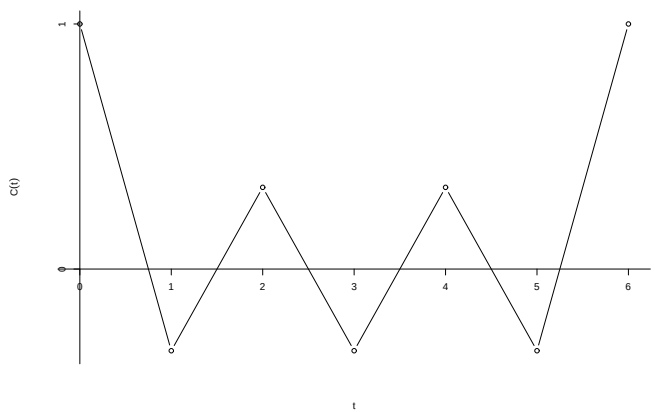
Ejemplo

La siguiente secuencia es periódica de período 6:

$$(s_i) = (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, \ldots)$$

Calculemos su función de autocorrelación para $0 \leq t \leq 6$:

$t = 0$	s_i	1	0	1	0	0	0	$C(0) = 1$
$t = 1$	s_{i+1}	0	1	0	0	0	1	$C(1) = -1/3$
$t = 2$	s_{i+2}	1	0	0	0	1	0	$C(2) = 1/3$
$t = 3$	s_{i+3}	0	0	0	1	0	1	$C(3) = -1/3$
$t = 4$	s_{i+4}	0	0	1	0	1	0	$C(4) = 1/3$
$t = 5$	s_{i+5}	0	1	0	1	0	0	$C(5) = -1/3$
$t = 6$	s_{i+6}	1	0	1	0	0	0	$C(6) = 1$



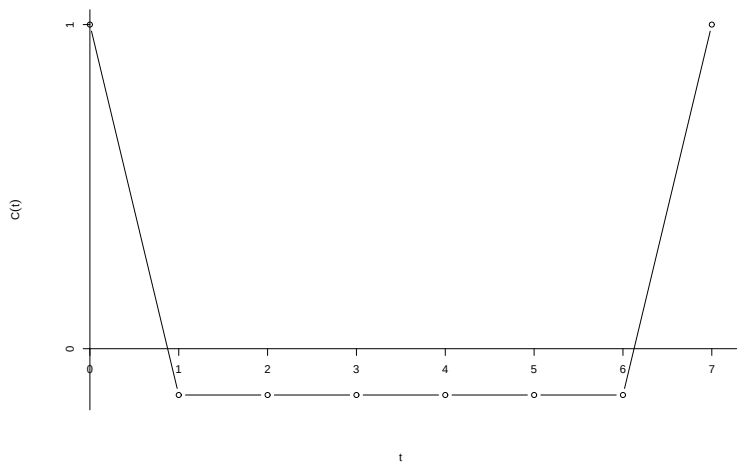
Ejemplo

La siguiente secuencia es periódica de período 7:

$$(s_i) = (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, \ldots)$$

Comprobar que

$$C(t) = \begin{cases} 1, & t = 0 \\ -\frac{1}{7}, & t = 1, 2, \ldots, 6 \end{cases}$$



Nota

- En una secuencia de bits $(s_i) = (s_0, s_1, s_2, \ldots)$, los bits pueden aparecer repetidos.
- Denominaremos *grupo* de bits a una ráfaga de bits repetidos. Es decir, un grupo de bits está formado por todos los bits consecutivos iguales entre dos distintos.
- Un grupo puede tener longitud: $1, 2, 3, \ldots$

Ejemplo

Sea la secuencia

$$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, \ldots)$$

Los grupos en esta secuencia y sus longitudes son:

$$\underbrace{1}_{(1)}\ \underbrace{0}_{(1)}\ \underbrace{11}_{(2)}\ \underbrace{0}_{(1)}\ \underbrace{1}_{(1)}\ \underbrace{0000}_{(4)}\ \underbrace{11}_{(2)}\ \underbrace{00}_{(2)}\ \underbrace{1}_{(1)}\ \underbrace{000}_{(3)}\ \underbrace{1}_{(1)}\ \ldots$$

Postulados de aleatoriedad de Golomb (1967)

Son condiciones necesarias que una secuencia aleatoria de bits debe cumplir, pero no son condiciones suficientes para que una secuencia pueda considerarse aleatoria.

Son los siguientes:

1. En todo ciclo la diferencia entre 1's y 0's es, a lo sumo, 1.
2. En todo ciclo la mitad de los grupos tienen un elemento, la cuarta parte tienen dos, la octava parte tres, ...
3. En todo ciclo la mitad de los grupos de k elementos es de 1's y la otra mitad de 0's.
4. La autocorrelación $C(t),\ 0 < t < T$, es constante.

Ejemplo

Consideremos la anterior secuencia periódica de período 7:

$$(s_i) = (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, \ldots)$$

Análisis de los postulados de Golomb sobre (s_i):

grupos	n^0 de grupos	n^0 teórico de grupos
0	1	1
1	1	1
00	1	0.5
11	0	0.5
000	0	0.25
111	1	0.25
	4	

$$C(t) = -\frac{1}{7}, \ t = 1, 2, \ldots, 6$$

Fin de la sección