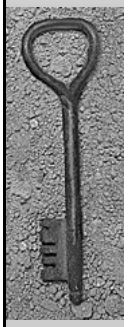
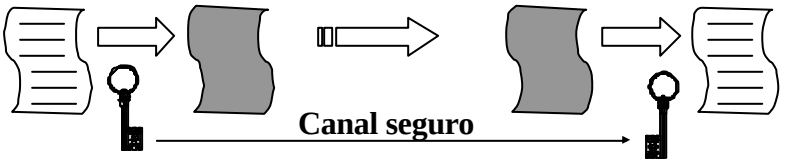
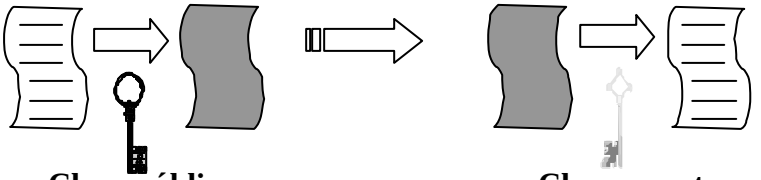


Criptografía Moderna

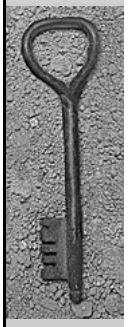
– **Criptosistemas Simétricos o de Clave Secreta:**



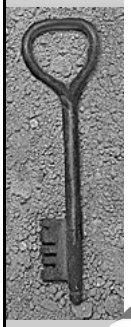
– **Criptosistemas Asimétricos o de Clave Pública:**



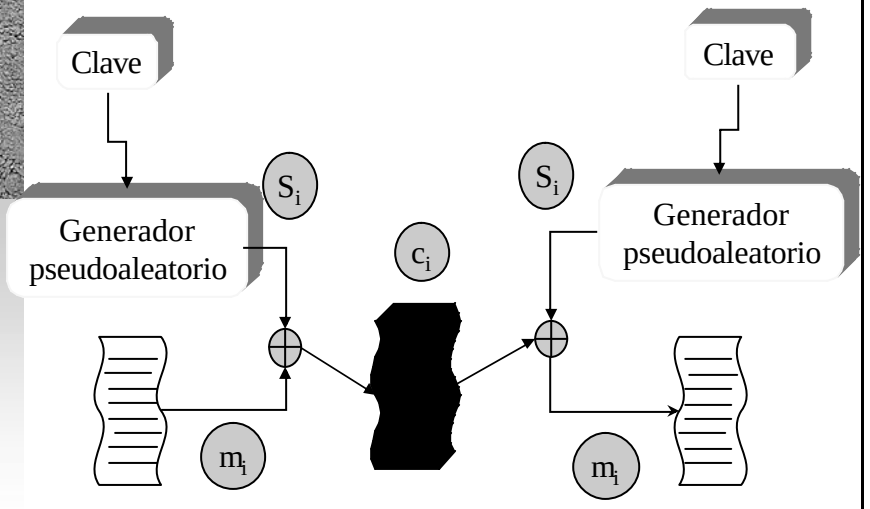
Clave pública **Clave secreta**

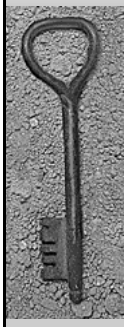


Criptografía Moderna



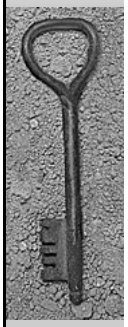
Cifrado en Flujo





Cifrado en Flujo

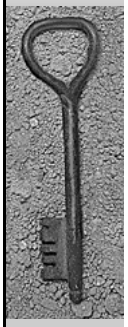
- El emisor usa una semilla secreta y un algoritmo determinista (generador pseudoaleatorio) para generar una secuencia binaria.
- Con la secuencia generada y el texto en claro expresado en binario se realiza una xor bit a bit.
- Realizando la misma operación con el texto cifrado y la misma secuencia pseudoaleatoria se recupera el texto en claro.
- **La seguridad del sistema se basa únicamente en las características de la secuencia de clave**



Cifrado en Flujo

Propiedades de las secuencias cifrantes:

- Periodo T muy alto.
- Postulados de pseudoaleatoriedad de Golomb:
  1. Unos y ceros deben aparecer con idéntica frecuencia.
  2. En cada periodo, la mitad de las rachas es de longitud 1, la cuarta parte de longitud 2, la octava de 3, etc. Las rachas de ceros y de unos deben aparecer con idéntica frecuencia para cada longitud.
  3. Autocorrelación AC(k)=(NºCoinc-NºDif)/T. El número de coincidencias entre una secuencia y su desplazada k posiciones no debe aportar ninguna información sobre el periodo, para cualquier k no múltiplo de T.



Cifrado en Flujo: Generadores de Secuencia

$$X_{i+1} = a X_i + b \pmod{m}$$

- Congruencial
- Generador Blum Blum Shub

  p, q (= 3 mod 4), n = pq

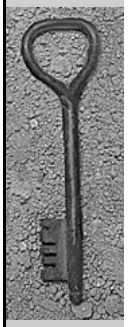
  X número aleatorio en [1, n - 1] primo con n.

  $s_0 = X^2 \pmod{n}$

  $s_{i+1} = s^2_i \pmod{n}$

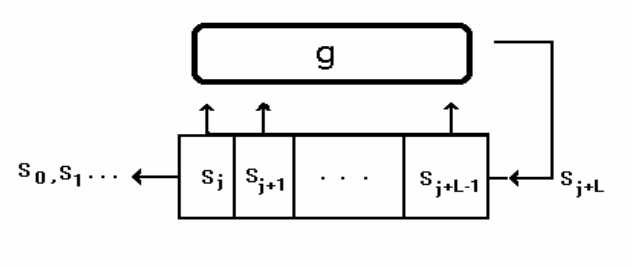
  z_i = el bit menos significativo de s_i.

  La secuencia de salida es $z_1, z_2, \ldots, z_i$

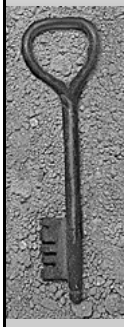


Cifrado en Flujo: Generadores de Secuencia

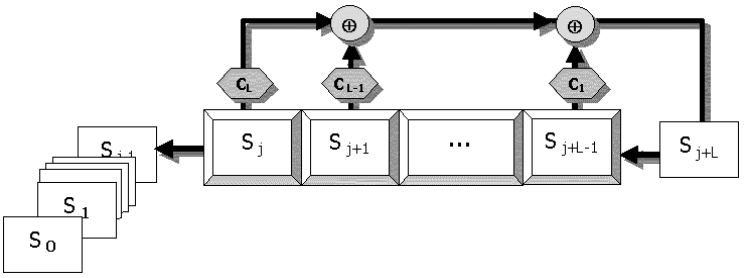
- Registro de Desplazamiento Realimentado:
  - Linealmente.
  - No Linealmente.



➢ **Función de realimentación g no-singular: Secuencia periódica**

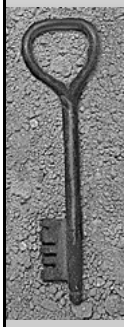


Cifrado en Flujo: RDRL



Polinomio de realimentación: $C(x)=1+c_1x+c_2x^2+\ldots+c_Lx^L$

- Factorizable: Periodo depende de semilla
- Irreducible: Periodo no depende de semilla, y divisor de 2^L-1
- Primitivo: periodo máximo 2^L-1 e independiente de la semilla
- Nº de polinomios primitivos de grado L $=Fi(2^L-1)/L$



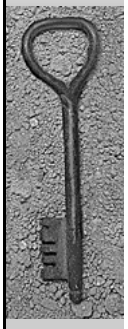
1000
0001
0011
0111
1111
1110
1101
1010
0101
1011
0110
1100
1001
0010
0100

PN-Secuencias

- Ejemplo: $C(x)=1+x+x^4$

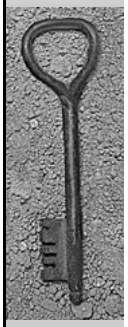
Postulados de Golomb:

1. 7 ceros, 8 unos
2. 0, 1 :2 veces,
   00,11: 1 vez
   000: 1 vez
   1111: 1 vez
3. AC(k)=-1/15

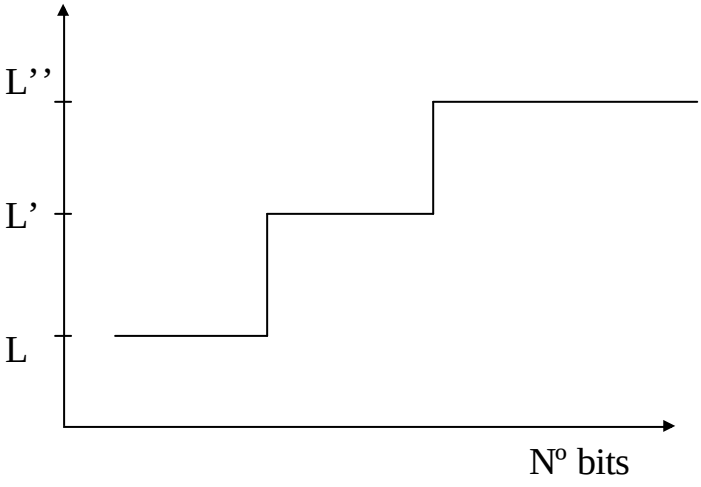


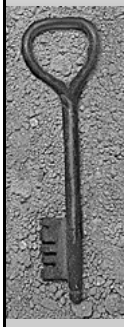
Complejidad Lineal

- Dada una secuencia producida con un RDRL de longitud L bastan 2L bits para resolver el sistema de L ecuaciones con L incógnitas y descubrir los coeficientes de realimentación.
- Cualquier secuencia periódica se puede generar con un RDRL no singular
- Complejidad lineal: Longitud del menor RDRL que genera la secuencia

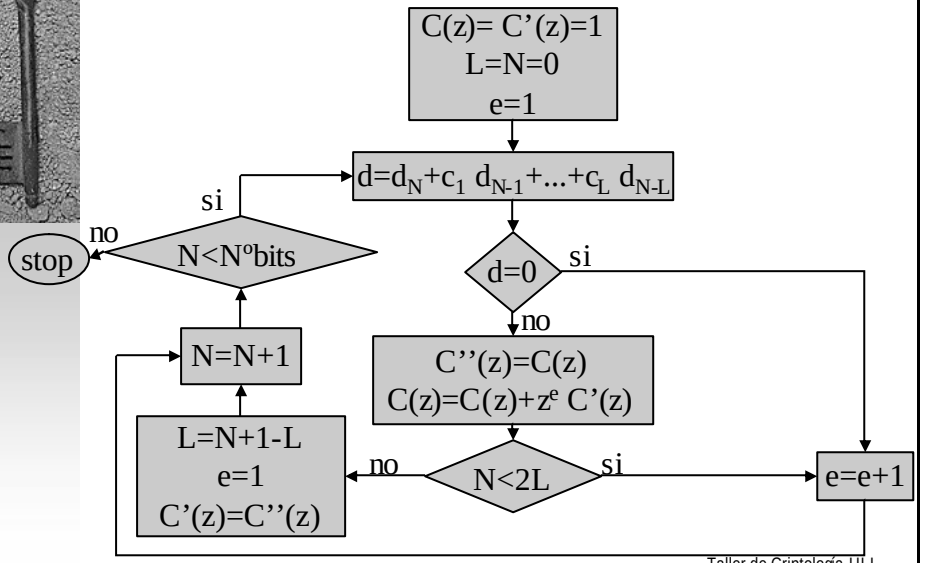


Complejidad Lineal



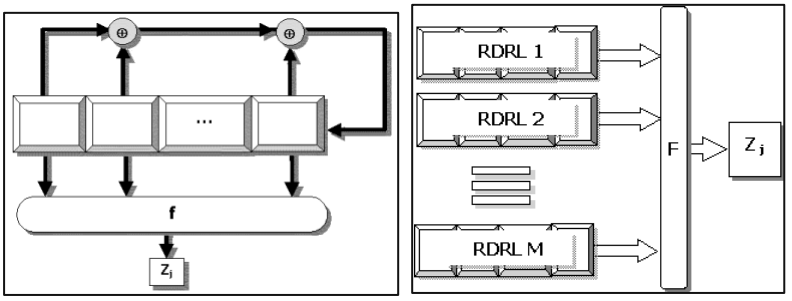


Algoritmo de Berlekamp-Massey



Cifrado en Flujo: Generadores de Secuencia

- Filtrado no lineal
- Combinador no lineal



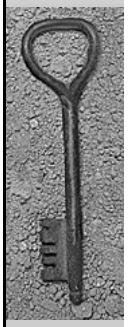
Filtrado no Lineal

- Complejidad lineal acotada por $\sum_{i=1}^{m} \binom{L}{i}$

(siendo m el orden de la función de filtrado f)

- Principios de diseño:

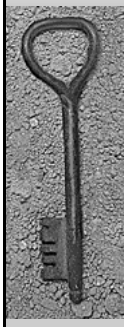
1. Usar registro con polinomio primitivo para lograr periodo máximo
2. Orden de la función del orden L/2
3. Incluir en f término lineal y términos de orden pequeño para lograr buena distribución de 0 y 1
4. Incluir en f términos de cada orden
5. Que la semilla determine algún término de f



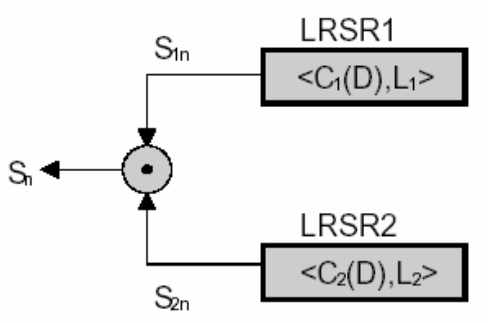
Combinadores no Lineales

- If gcd (L_i, L_j) = 1 and $C_1(D)$ ... $C_M(D)$ irreducibles entonces: $CL(S_1,...S_M) = F(L_1,...,L_M)$

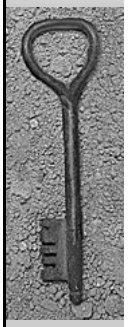
1. Simple combinación de varios registros (con relojes sincronizados)
2. De control paso a paso (un registro controla el reloj de los demás) (Beth-Piper, Gollman, Bilateral)
3. Multi-reloj (los relojes de los registros con independientes) (Massey-Rueppel)



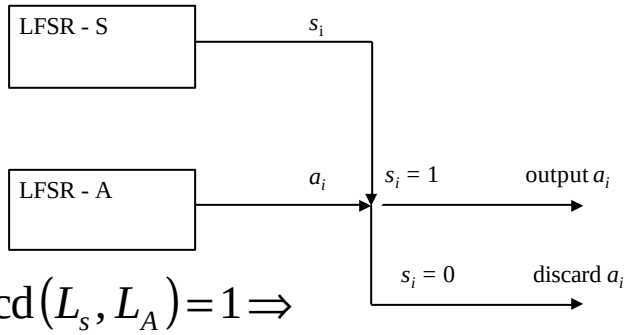
Combinadores no Lineales: Generador de Hadamard



$$if\ \gcd(L_1, L_2) = 1 \Rightarrow \begin{cases} T = mcm(T_1, T_2) \\ CL = L_1 \cdot L_2 \end{cases}$$



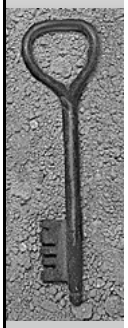
Combinadores no Lineales: Generador Shrinking



$$if\ \gcd(L_s, L_A) = 1 \Rightarrow$$

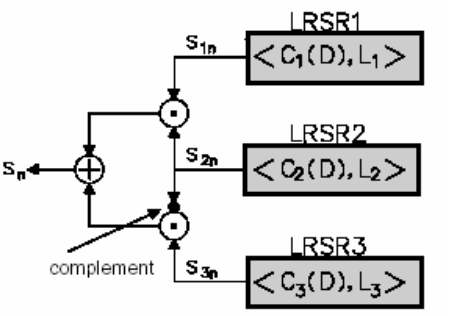
$$T = (2^{L_A} - 1) \cdot 2^{L_S - 1}$$

$$L_A \cdot 2^{L_S - 2} < CL < L_A \cdot 2^{L_S - 1}$$



Combinadores no Lineales: Generador de Geffe

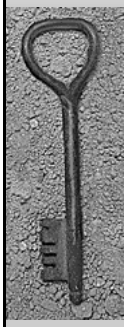
$$F(x_1, x_2, x_3) = x_1 x_2 \oplus x_2 x_3 \oplus x_3$$



- Si L_i son primos entre sí y los polinomios son primitivos:

$$CL = L_1 L_2 + L_2 L_3 + L_3$$

$$T = (2^{L_1} - 1) \cdot (2^{L_2} - 1) \cdot (2^{L_3} - 1)$$

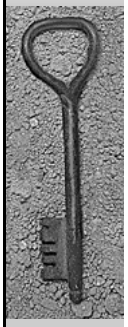


Combinadores no Lineales: Generador de Geffe

x_1	x_2	x_3	$z = F(x_1,x_2,x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

• Balanceado (1º y 2º postulados de Golomb), pero no 3º porque

$$P(z = x_1) = 3/4.$$



Combinadores no Lineales: Generador de Beth-Piper

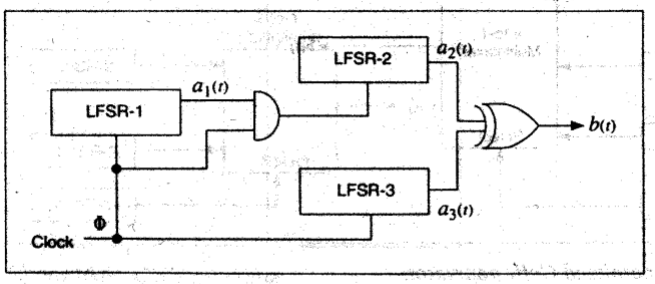


Figure 16.9 Beth-Piper stop-and-go generator.

$$CL = (2^{L_1} - 1) \cdot L_2 + L_3$$

$$T = (2^{L_1} - 1)(2^{L_2} - 1)(2^{L_3} - 1)$$

$$P(b(t) + b(t+1) = a_3(t) + a_3(t+1)) = 3/4$$

Combinadores no Lineales: Generador Bilateral

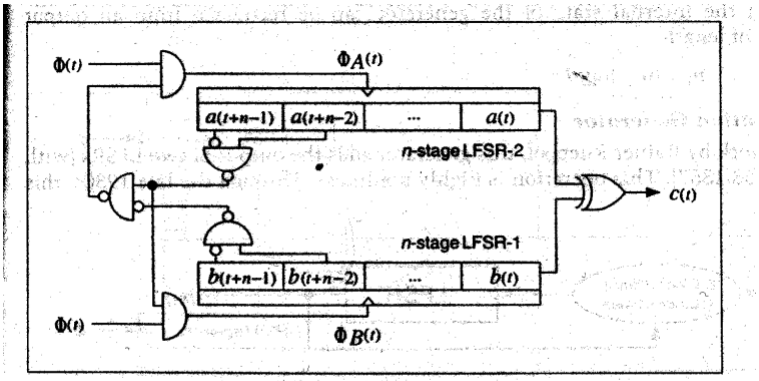
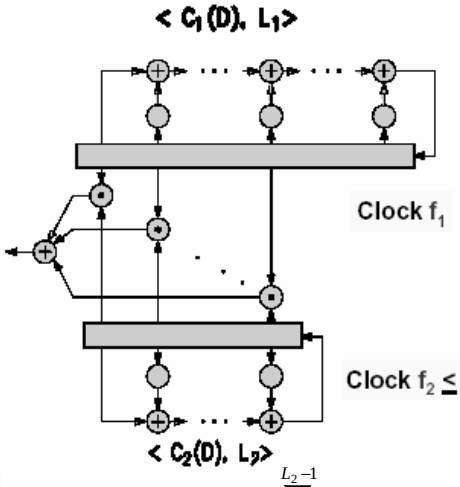


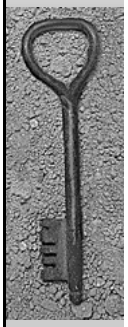
Figure 16.11 Bilateral stop-and-go generator.

$$CL \approx T \approx (5 \bullet 2^{L-2}) - 1$$

Combinadores no Lineales: Generador de Massey-Rueppel

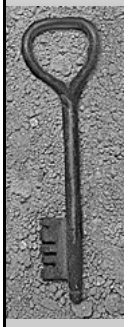


- Combinación que suma los productos internos de cada bit con los dos estados
- Los RDRL pueden tener diferentes tasas de reloj (d = Clock f_1 / Clock f_2)
- Si gcd(L_1,L_2)=1, C_1, C_2 primitivos y $L_2 = L_1$:
  - CL= $L_1.L_2$
  - T = mcm(T_1, T_2)



Combinadores no Lineales: Generador en Cascada

- Su ventaja está en su diseño modular y repetitivo, permitiendo la concatenación de un número indefinido de generadores, obteniendo de esta manera enormes periodos y altas complejidades lineales.
- Se recomienda utilizar no menos de quince generadores en cascada.



Combinadores no Lineales: Generador de Gollmann

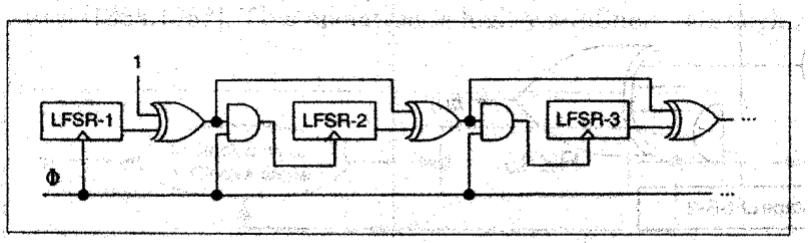


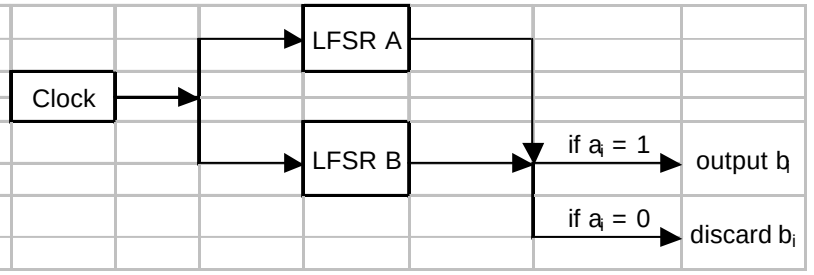
Figure 16.16 Gollmann cascade.

$$CL \geq L(2^L - 1)^{m-1}$$

$$T = (2^L - 1)^m$$

Combinadores no Lineales: Generador Stop-and-Go

- el reloj del subgenerador es controlado por otro subgenerador



Combinadores no Lineales: Generador Umbral

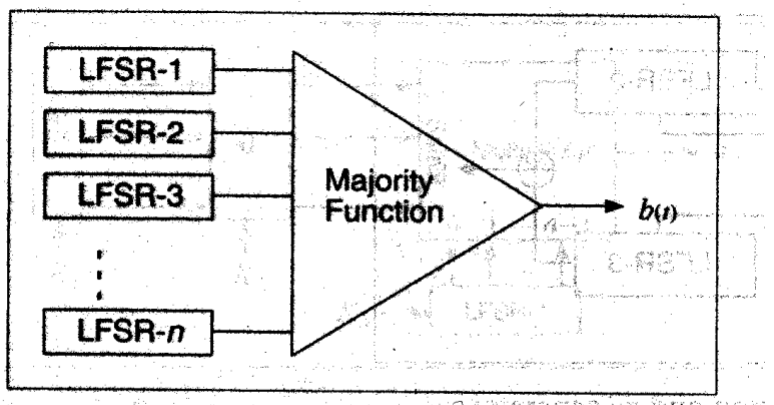
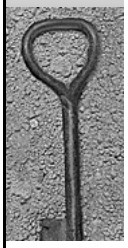


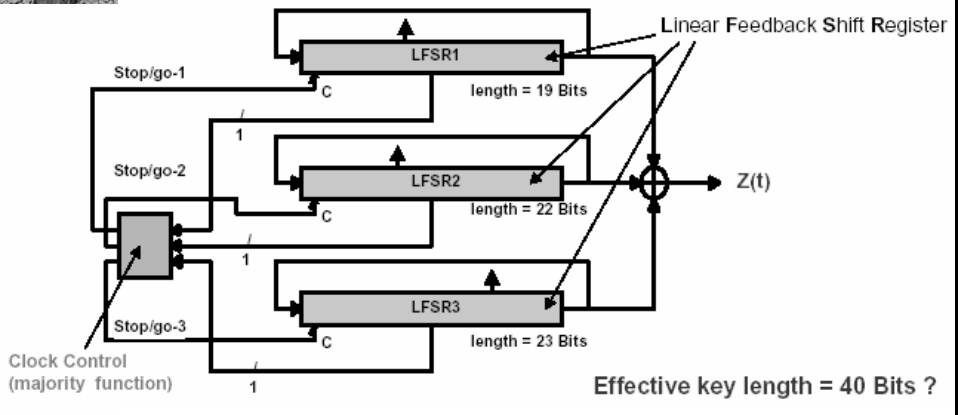
Figure 16.12 Threshold generator.

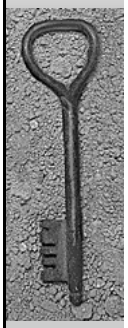


Combinadores no Lineales: Generador A5 para GSM

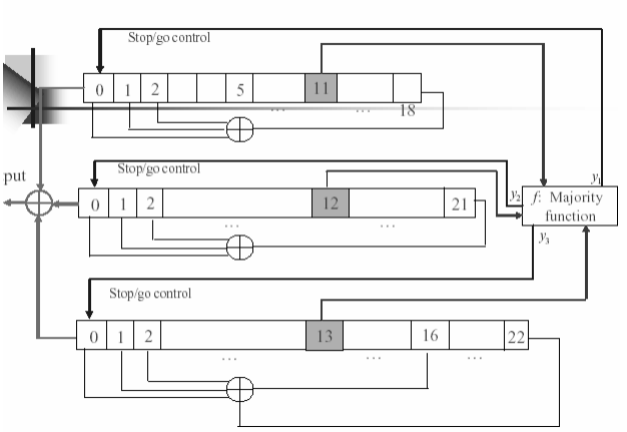
Clave de 64 bits: Semillas de los LFSR

LSFRs conocidos de periodos $2^{19} - 1$, $2^{22} - 1$, $2^{23} - 1$

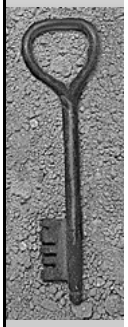




Combinadores no Lineales: Generador A5 para GSM



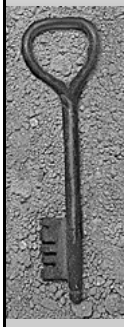
@G. Gong, 2003



Combinadores no Lineales: Generador A5 para GSM

Función Mayoría f:

$f(a(t+11),b(t+12),c(t+13)) = (y_1, y_2, y_3)$	$a(t+11)$	$b(t+12)$	$c(t+13)$
(1,1,1)	0 1	0 1	0 1
(1,1,0)	0 1	0 1	1 0
(0,1,1)	0 1	1 0	1 0
(1,0,1)	1 0	0 1	1 0



Combinadores no Lineales: Generador A5 para GSM

- Para cifrar transmisiones aéreas entre el MS y el BTS
- Una conversación GSM se envía como una secuencia de 228 bits cada 4,6 miliseg.
- El periodo es de aprox. $(4/3)(2^{23}-1)$.
- Existe el problema llamado de la colisión, debido a que diferentes semillas de los registros pueden producir la misma clave (el 70% de semillas distintas producen distintas claves)
- Una debilidad del protocolo de seguridad de GSM es que la identidad de los móviles no siempre se cifra en la transmisión aérea
- Puede romperse con un PC en pocas horas (Con un Pentium III comprobar 2^{54} claves requiere 250 horas)
- Se pueden hacer ataques por denegación de servicio