UNIVERSIDAD CARLOS III DE MADRID

Cifradores de bloque de clave secreta

Benjamín Ramos Álvarez
Pablo Martín González
Departamento de Informática

Cifradores digitales

- Introducción
- Clasificación de los cifradores por la naturaleza de su método de alimentación
  - de Bloque
  - de Flujo

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque

- Introducción
- Clasificación según el tipo de clave
  - Simétricos, de clave única, clave compartida o clave secreta
  - Asimétricos, de pareja de claves o de clave pública

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Introducción
- Características / 1
  - El texto en claro M se divide en bloques M_1, M_2 M_3 ... de igual tamaño (en bits)
  - El tamaño del bloque depende del algoritmo empleado
    - Prefijado
    - Elegible entre valores predeterminados

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Características / 2
  - Cada bloque se cifra separadamente de los demás
    - Sin dependencia de otros bloques
    - Con dependencia (bloques encadenados)
      - con bloques del texto en claro
      - con bloques del criptograma
      - mixto

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Ventajas
  - Rapidez en el cifrado / descifrado
  - Elección de bloques a cifrar / descifrar
  - Elección en el orden del cifrado / descifrado

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Inconvenientes / 1
  - Si en el cifrado de un bloque no influye ningún otro bloque:
    - Dos bloques de igual texto en claro pueden producir el mismo criptograma
    - La repetición del mismo texto cifrado puede ser una pista para el criptoanalista

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Inconvenientes / 2
  - La longitud del texto en claro debe ser múltiplo del tamaño del bloque
    - Uso de caracteres de relleno en bloques incompletos (último bloque)
    - La longitud del cifrado puede ser mayor que la del texto en claro (por lo anterior)
    - El último bloque del criptograma podría proporcionar información al criptoanalista.

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modos de cifrado (relación entre los bloques)
  - ECB, *Electronic Code Book*
  - CBC, *Cipher Block Chainin*
  - CFB, *Cipher FeedBack*
  - OFB, *Output FeedBack*

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo ECB, *Electronic Code Book* / 1
  - Cada bloque M_i da lugar a su correspondiente C_i con la misma clave K para todos los bloques $C_i = E(M_i, K)$
  - Independencia de cada bloque a la hora de cifrar y descifrar
  - Permite el cifrado de bloques seleccionados, sin necesidad de cifrar todo el mensaje

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo ECB, *Electronic Code Book* / 2
  - Se podría tener un libro con todos los textos en claro (p.e. con 64 bits, 2^{64} textos) y sus correspondientes cifrados (para una misma clave)
  - Al no encadenar bloques en su cifrado, facilita el ataque ante criptogramas con bloques normalizados de texto en claro

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

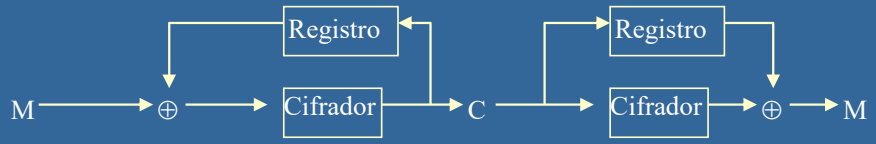
Cifradores de bloque con clave secreta

- Modo ECB, *Electronic Code Book* / 3
  - Es, en definitiva, el más débil de los modos de cifradores de bloque; sin embargo, se utiliza en algunos pasos de otros criptosistemas

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo CBC, *Cipher Block Chainin* / 1



  - Cifrado $C_i = E(C_{i-1} \oplus M_i, K)$ con valor de inicio $C_0 = VI$, del tamaño del bloque
  - VI se envía al receptor cifrado en ECB (aunque con el propio algoritmo) y debe ser distinto en cada mensaje a cifrar

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo CBC, *Cipher Block Chainin / 2*
  - Para descifrar, $M_i = D(C_i, K) \oplus C_{i-1}$
  - Se comprueba fácilmente que

    $D(E(C_{i-1} \oplus M_i, K), K) \oplus C_{i-1} = C_{i-1} \oplus M_i \oplus C_{i-1} = M_i$

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

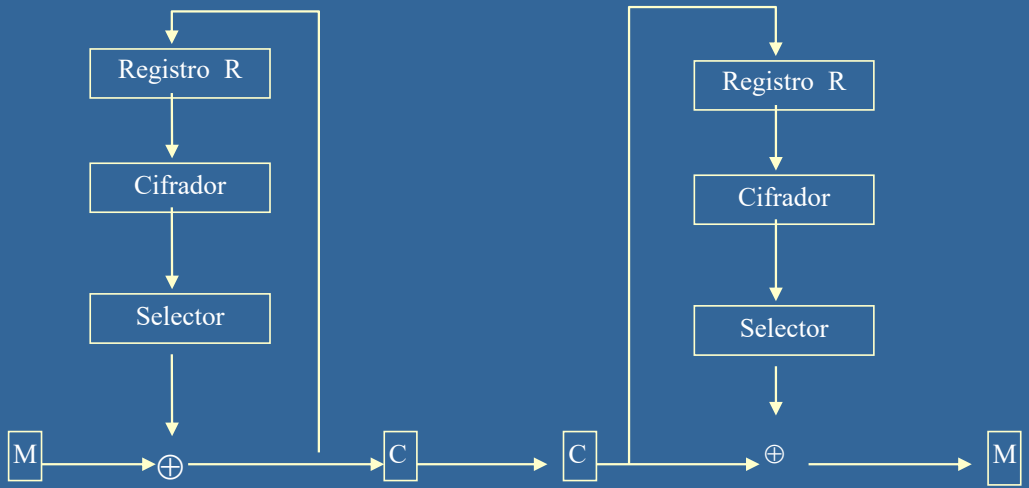
Cifradores de bloque con clave secreta

- Modo CBC, *Cipher Block Chainin* / 3
  - La recepción de un símbolo erróneo en un bloque C_n afectará a dos bloques contiguos de texto en claro recuperado, M_n y M_{n+1}
  - Idóneo para cifrar ficheros secuenciales; no así para pequeños campos o BD, donde es más problemático

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo CFB, *Cipher FeedBack* / 1



  - Llamado cifrado en modo realimentado de m bits, con m arbitrario (m=1, m=8)

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo CFB, *Cipher FeedBack* / 2
  - Los m bits mas significativos de la salida del cifrador se extraen por el Selector y se operan mediante o-exclusivo con m bits del texto en claro
  - El resultado son m bits del criptograma que, por un lado, se envían a la línea de transmisión y, por el otro, realimentan al registro de desplazamiento R, por la derecha

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo CFB, *Cipher FeedBack* / 3
  - R es cargado por un VI, que debe cambiarse de vez en cuando y enviarse al destinatario, para enmascarar las repeticiones del primer carácter de longitud m en cada sesión de cifrado. Este VI se puede transmitir en claro, pues no afecta a la seguridad del criptosistema puesto que se cifra

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

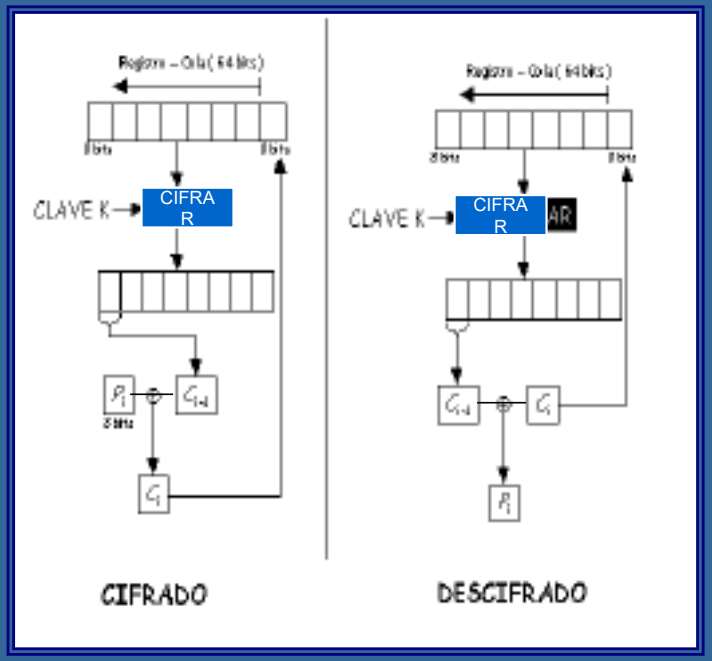
Cifradores de bloque con clave secreta

- Modo CFB, *Cipher FeedBack* / 4
  - Un error en un bit del criptograma origina un error en el texto en claro recuperado; además, cuando el error entra en R, afecta a los bloques posteriores, hasta su eliminación de R tras el desplazamiento de m bits

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

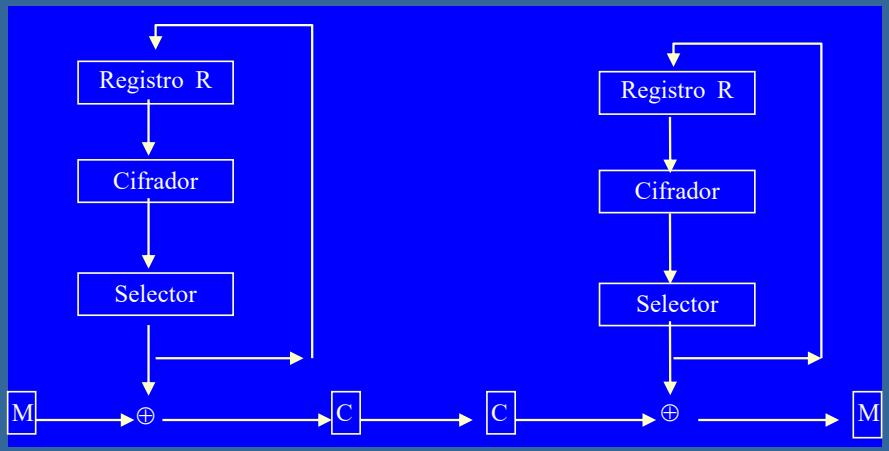
- Modo CFB, *Cipher FeedBack* / 5



Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo OFB, *Output FeedBack* / 1

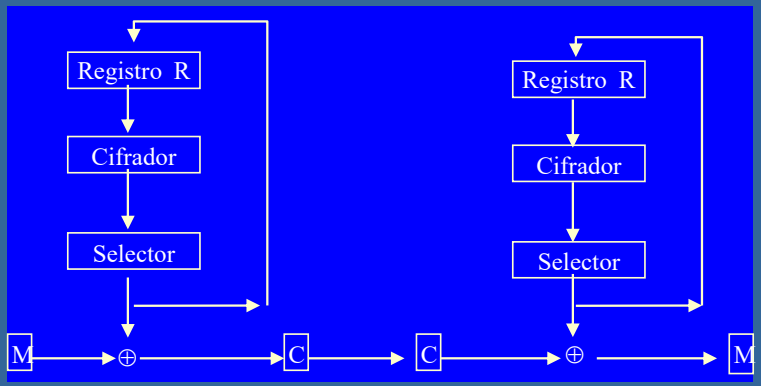


- Permite construir un cifrador de flujo tipo Vernam, a partir de un cifrador de bloque

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo OFB, *Output FeedBack* / 2

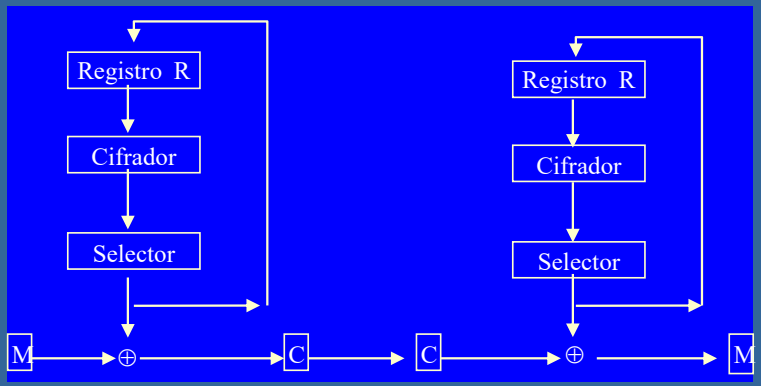


- El cifrador va obteniendo la serie cifrante que interviene o-exclusivo con el texto en claro (serie seudoalatoria e idealmente tan larga como el texto)

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo OFB, *Output FeedBack* / 3

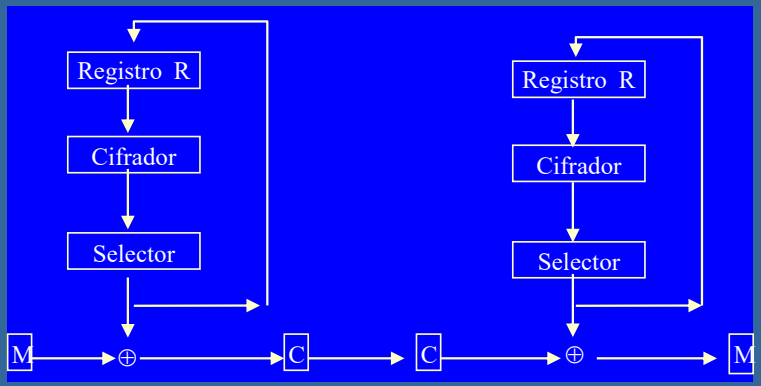


- La realimentación se obtiene de la salida del propio cifrador
- R parte con un valor inicial, que debe ir variando

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid

Cifradores de bloque con clave secreta

- Modo OFB, *Output FeedBack* / 4



- No propaga errores: un error en el símbolo cifrado sólo se acusa en el correspondiente símbolo del texto en claro

Benjamín Ramos Álvarez ©
Pablo Martín González
Universidad Carlos III de Madrid