Universidad
Carlos III de Madrid
Grupo SeTI · *Dpto. Informática*

TEMA 2. CRIPTOGRAFÍA
T 2.3 CRIPTOSISTEMAS SIMÉTRICOS. CIFRADORES DE BLOQUE Y FLUJO (parte 1)

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC

Curso 2016-2017

CONTENIDOS

- **Métodos de cifra moderna**
- Criptosistemas simétricos
  - Cifradores de bloque
    - Introducción
    - Esquema de Feistel
    - Modos de operación
    - Cifradores de bloque: Ventajas y desventajas

Parte 1 de las transparencias

    - DES
    - AES

Parte 2

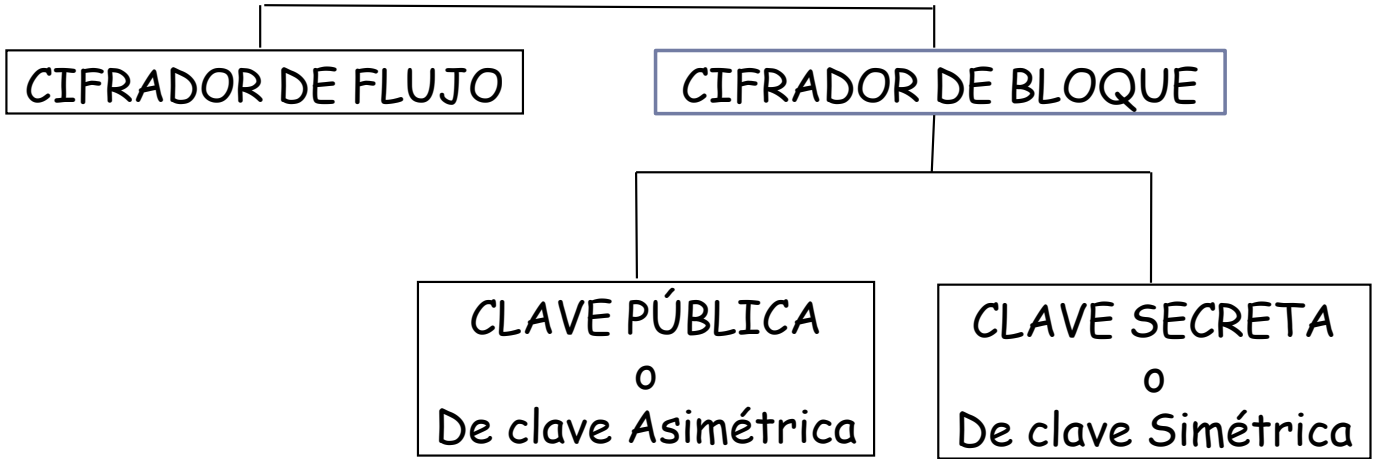
  - Cifradores de flujo

Parte 3

MÉTODOS DE CIFRA MODERNA

- Clasificación
  - Tipo de operaciones realizadas
    - En general, substituciones y transposiciones. No puede perderse información. Los más comunes usan el producto de varias ops.
  - Número de claves usadas
    - Simétricos o con una clave (también conocido como algoritmos de clave secreta)
    - Asimétricos o con dos claves (también conocido como algoritmos de clave pública)
  - Tipo de procesamiento del texto en claro
    - Por bloques (algoritmos de cifrado en bloque)
    - Como un flujo continuo de bytes o de bits (algoritmos de cifrado en flujo)

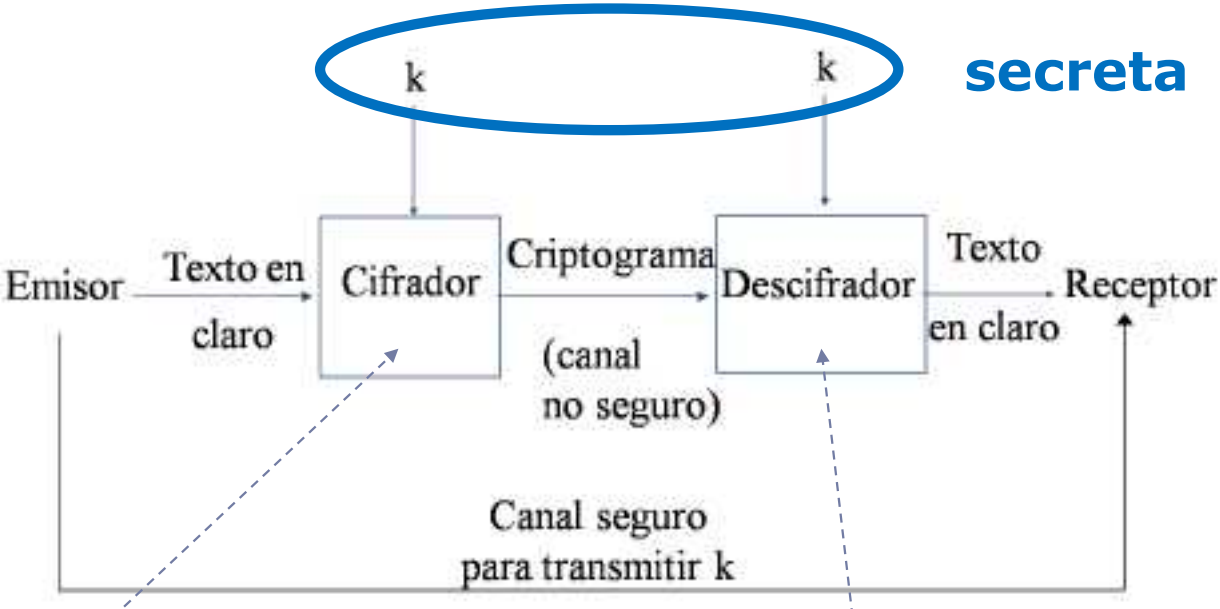
MÉTODOS DE CIFRA MODERNA



Cifrado hibrido, para pasar la clave privada se pasa cifrada simetricamente y una vez con la clave privada descifro la pública.
El mensaje es conocido pero no como descifrarle, y la clave que lo descifra se pasa cifrada con un cifrado simetrico que es conocido, y cuando lo descifra puede descifrar la pública

MÉTODOS DE CIFRA MODERNA

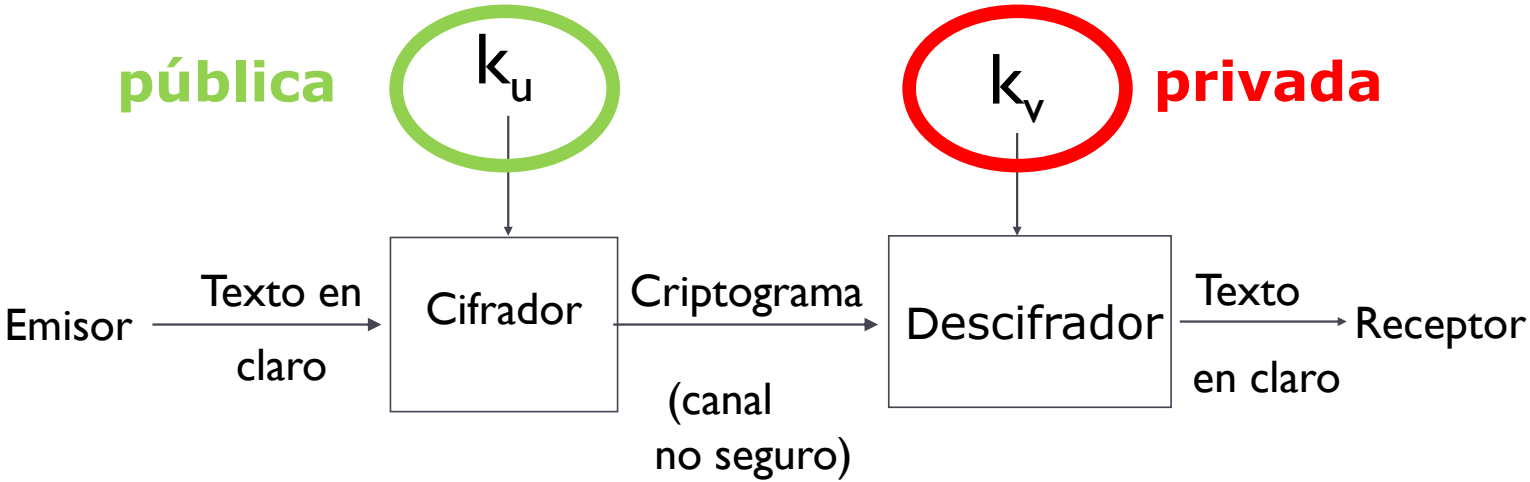
Modelo de criptosistema de clave **simétrica**



$C = E(k, M) = E_k(M)$ $\qquad$ $M = D(k, C) = D_k(C)$

MÉTODOS DE CIFRA MODERNA

Modelo de criptosistema de clave **asimétrica**



$C = E(k_u, M) = E_{k_u}(M)$ $\quad M = D(k_v, C) = D_{k_v}(C)$

CONTENIDOS

- Métodos de cifra moderna
- Criptosistemas simétricos
  - Cifradores de bloque
    - **Introducción**
    - Esquema de Feistel
    - Modos de operación
    - Cifradores de bloque: Ventajas y desventajas
    - DES
    - AES
  - Cifradores de flujo

Introducción

Descomponemos el mensaje en bloques de símbolos de igual longitud

- Descomponen M en bloques de símbolos de igual longitud:

HOY HAY CLA SE

$$M_1, M_2, \ldots M_n$$

- Cifran cada bloque con la misma clave

$$C = E_k(M) = E_k(M_1)\, E_k(M_2) \ldots E_k(M_n)$$

- Tamaño de bloques típicos 64, 128 o 256 bits

- Mapeo reversible entre bloques de M y C

Introducción

- Sustituciones de "caracteres" extremadamente largos
  - 64 bits o más

- Cifrador de bloque ideal
  - n: tamaño de bloque. Ej: 64
  - Se puede definir como una tabla de sustitución (mapeo) de 2^n bits de texto-claro a 2^n bits de texto-cifrado

Pasar

  - Existen $2^n!$ asignaciones arbitrarias de texto-claro—texto-cifrado == $2^n!$ (transformaciones) == $2^n!$ claves posibles
  - No es práctico
    - La propia tabla de sustitución es la clave, con longitud = $n \cdot 2^n$ bits
    - Para n = 64 → longitud de la clave es aproximadamente 10^{21} bits

Introducción

Cifradores de Bloque más conocidos

Algoritmo	Bloque (bits)	Clave (bits)	Rondas
Lucifer	128	128	16
DES	64	56	16
Twofish	128	variable	variable
RC2	64	variable	18
RC5	variable	variable	variable
SAFER	64	64	8
IDEA	64	128	8
Skipjack	64	80	32
RIJNDAEL	128	128 o más	flexible

CONTENIDOS

- Métodos de cifra moderna
- Criptosistemas simétricos
  - Cifradores de bloque
    - Introducción
    - **Esquema de Feistel**
    - Modos de operación
    - Cifradores de bloque: Ventajas y desventajas
    - DES
    - AES
  - Cifradores de flujo

Esquema de Feistel

- Cifrador de bloque (Feistel 1975)
  - Usar un subconjunto de las $2^n!$ posibles claves
    - Tamaño del bloque de texto = n bits
    - Tamaño de la clave = k bits $\quad k \leq n$
    - Número de posibles claves = 2^k
  - Aplicación práctica de los conceptos (Shannon 1949)
    - Cifrado producto Dentro de las claves se hace mediante operaciones de
      - Sustitución (S-box)
      - Permutación (P-box)
    - Se obtiene una alta *difusión* y una alta *confusión*

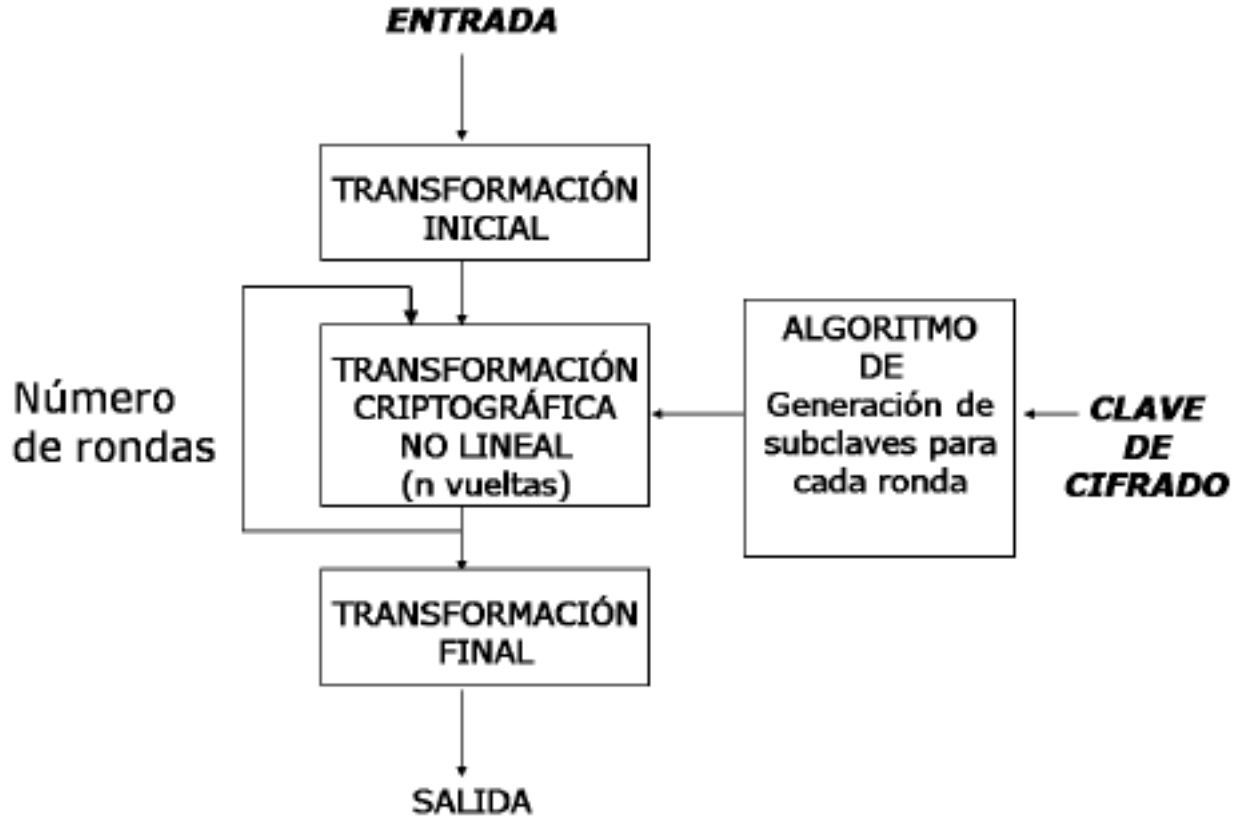
Esquema de Feistel

- Métodos para frustrar criptoanálisis
  - Difusión
    - disipar la estructura estadística de M en C
    - que cada bit de C dependa de muchos de M
    - se logra aplicando una permutación sobre M y una función sobre el resultado de dicha permutación

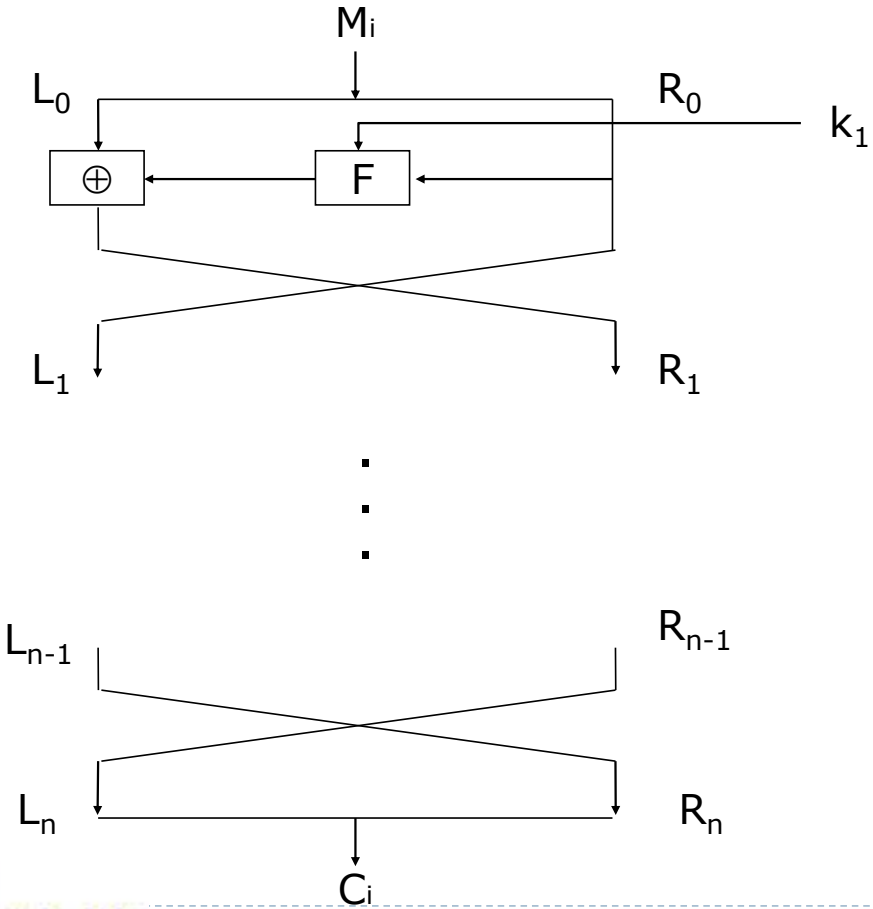
Antes de cifrar Permutación → cifrar → Permutar

  - Confusión
    - busca complicar la relación estadística entre C y k
    - se logra mediante sustituciones complejas

Esquema de Feistel



Esquema de Feistel



Esquema de Feistel

- Dividir bloque en dos mitades iguales

La parte Right no hace nada
La parte Left se hace xor con la subclave y Right

- Sustitución en la mitad izquierda
  - XOR de dicha mitad con el resultado de aplicar una función de ronda F no lineal a la parte derecha
    - F depende de la subclave de ronda

- Permutación de las dos mitades resultantes

LR → RL
LR → RL → LR
Para no hacer en cada paso el proceso de xor con el derecho y mezclar.

- Proceso repetido n rondas → Para mayor seguridad se realizan + rondas.

Esquema de Feistel

- Misma circuitería para cifrar y descifrar
  - Sólo cambiar el orden de las subclaves
  - Se precisa de una última permutación de las dos mitades en la última ronda (en la figura de la trasparencia 14:)
    - $L_{n+1} = R_n$
    - $R_{n+1} = L_n$
  - Demostración

- Reduce el problema de diseño, prácticamente, a:
  - Hallar un buen algoritmo de expansión de clave
  - Hallar una buena función de ronda F

- La mayoría siguen este esquema pero no todos

Esquema de Feistel

- Tamaño de bloque
  - Mayor tamaño, mayor seguridad, menor velocidad
  - 64 o más
- Tamaño de clave
  - Mayor tamaño, mayor seguridad, menor velocidad
  - 128 o más
- Número de rondas
  - Mayor número, mayor seguridad, menor velocidad
  - Valor típico 16
- Función de ronda y algoritmo de expansión de clave
  - Mayor complejidad, mayor resistencia a criptoanálisis

+ grande
↓
+ seguro
↓
- rapido

"más seguro"

CONTENIDOS

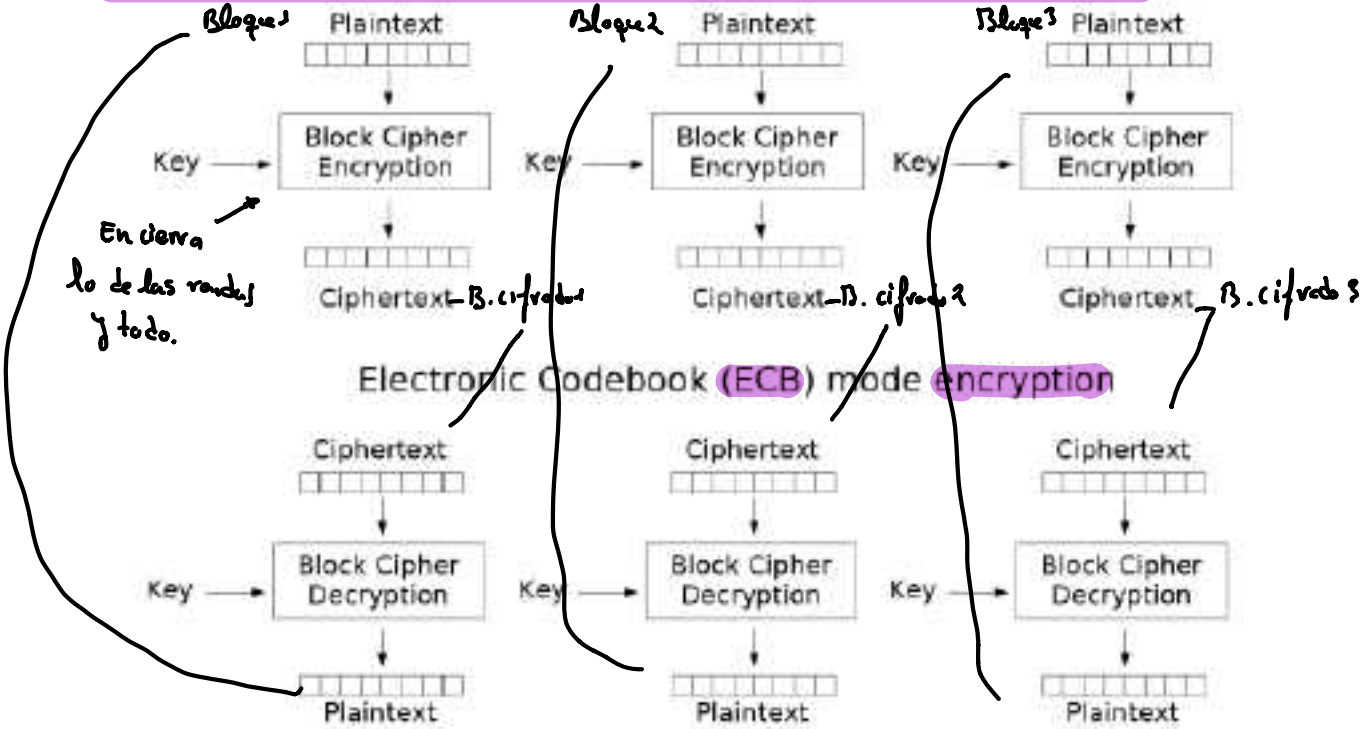
- Métodos de cifra moderna
- Criptosistemas simétricos
  - Cifradores de bloque
    - Introducción
    - Esquema de Feistel
    - **Modos de operación**
    - Cifradores de bloque: Ventajas y desventajas
    - DES
    - AES
  - Cifradores de flujo

Modos de Operación

- Técnica para mejorar el efecto de un algoritmo criptográfico o para su adaptación a una aplicación
- Se pueden aplicar a cualquier cifrador de bloque
- Cinco modos estandarizados por el NIST

Modo Electronic CodeBook (ECB)

- Mismo bloque de entrada genera mismo bloque a la salida



Modo Electronic CodeBook (ECB)

- Mismo bloque de entrada genera mismo bloque a la salida

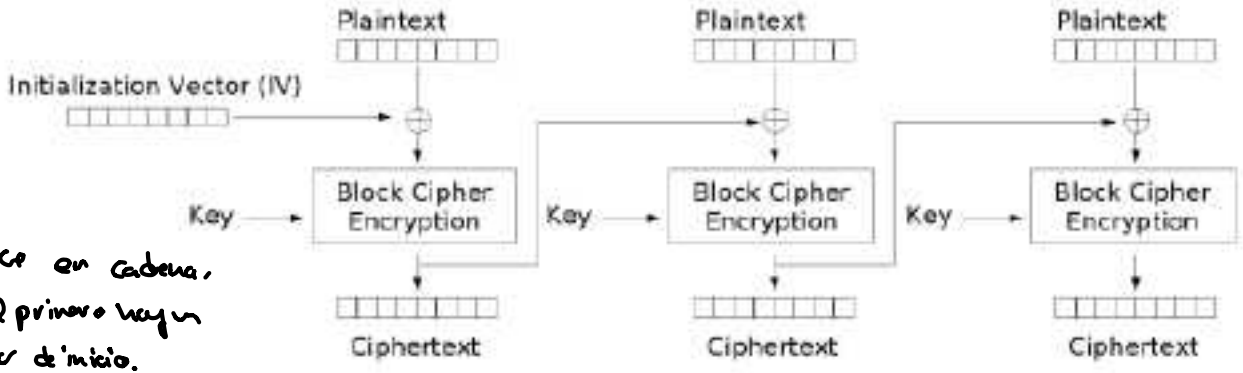
Imagen original	Imagen cifrada a usando modo ECB	Imagen cifrada usando cualquier otro modo de operación



Modo Electronic CodeBook (ECB)

- Ventajas:
  - Cifrado y descifrado se puede paralelizar
  - Transmisión segura de un bloque (e.g. clave simétrica)
  - Los errores de transmisión no se propagan entre bloques
- Desventajas:
  - Bloques repetidos dan como resultado criptogramas repetidos
  - Es posible alterar el orden de los bloques, modificar su contenido, repetirlos o eliminarlos
    → Y eso da información al atacante.
  - Necesita relleno (**padding**) del último bloque a 64 bits (8 bytes)
    - Ej: PKCS5 padding especifica completar con bytes cuyo valor sea el número de bytes a completar;
    - Ej; rellenar con ceros todos los bytes a completar excepto el último, cuyo valor será el número de bytes a completar;
    - si el tamaño del mensaje sí es múltiplo del tamaño de bloque, se añade un bloque entero de padding por convención

Modo Cipher Block Chaining (CBC)



Se hace en cadena, pero el primero hay un vector de inicio. Se hace XOR del texto limpio con el cifrado del bloque anterior

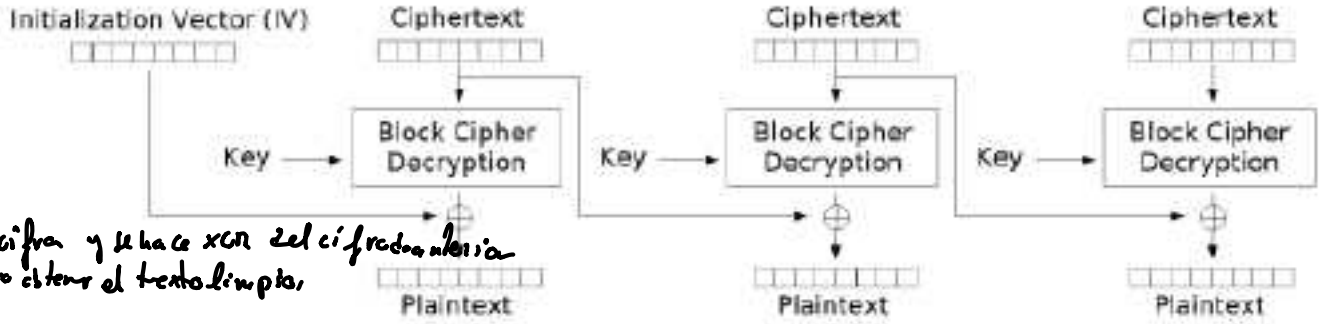
Cipher Block Chaining (CBC) mode encryption

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

Cifra(texto limpio$_n$ XOR texto cifrado$_{n-1}$) ... el inicial

- IV confidencial entre interlocutores por integridad
  - Usar ECB para su transmisión

Modo Cipher Block Chaining (CBC)



Se descifra y se hace XOR con el cifrado anterior para obtener el texto limpio.

Cipher Block Chaining (CBC) mode decryption

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$$

descifrado del cifrado) XOR texto cifrado anterior

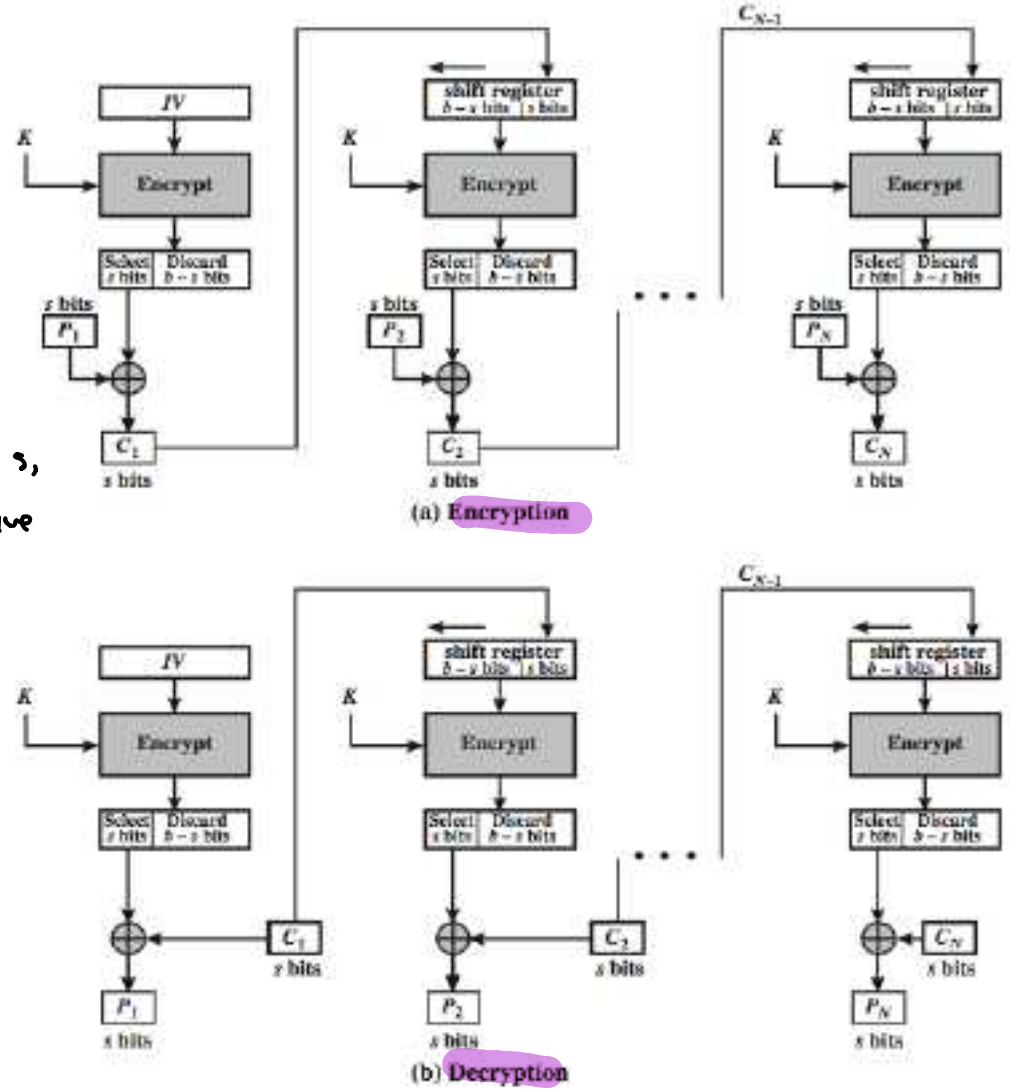
- Un error en Ci afecta a dos Mi
- Requiere **padding**
- Existen algunos ataques sobre TLS por cómo se utiliza CBC

Modo Cipher FeedBack Mode (CFB)

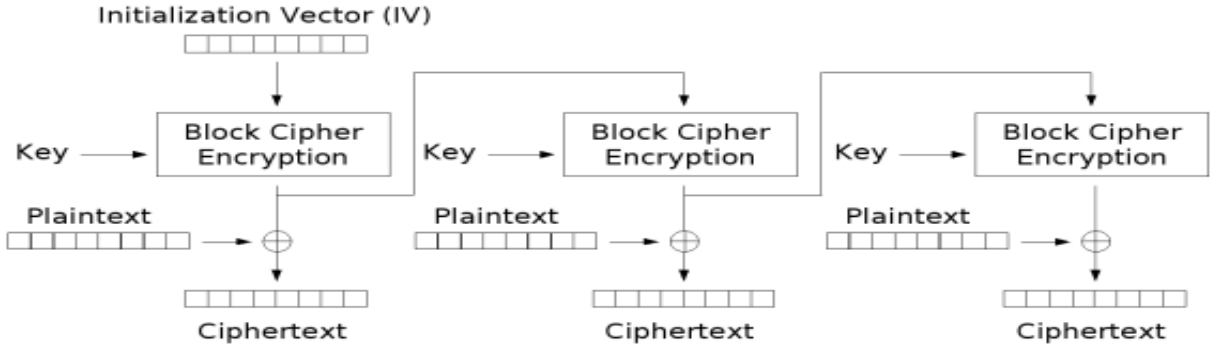
- Usa un registro de desplazamiento
- Opera sobre *segmentos* menores que el bloque
- Un error en Ci afecta a dos Mi
- Permite conversión de un c. de bloque en uno de flujo
  - La serie cifrante depende del texto en claro

Modo Cipher FeedBack Mode (CFB)

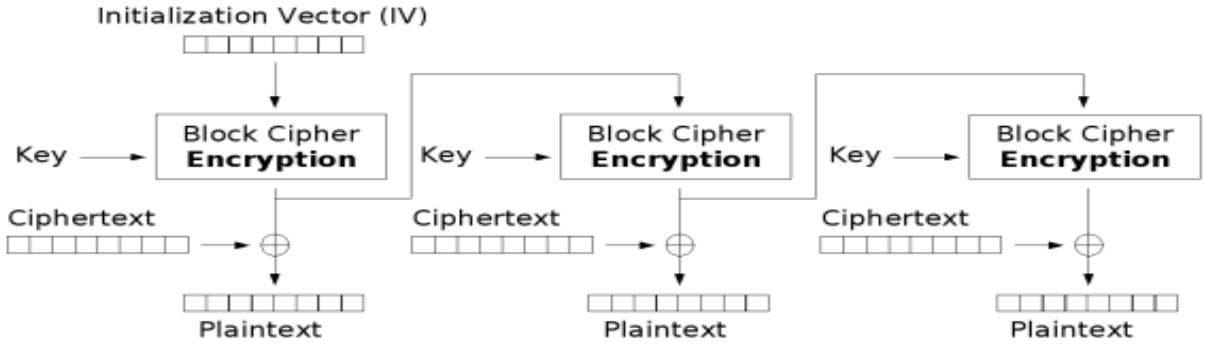
Cifro el mensaje y cojo s bits del que voy a hacer XOR con una clave P de tamaño s, y ese es el texto cifrado, que lleva



Modo Output FeedBack Mode (OFB)



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

Modo Output FeedBack Mode (OFB)

- IV ha de ser un nonce
- Ventaja: un error en Ci afecta a un solo Mi (en un bit)
- Se descartan los bits sobrantes para el último bloque
- Permite conversión de un c. de bloque en uno de flujo
  - La serie cifrante no depende del texto en claro
  - Opera sobre bloques no sobre segmentos

Modo Counter (CTR)

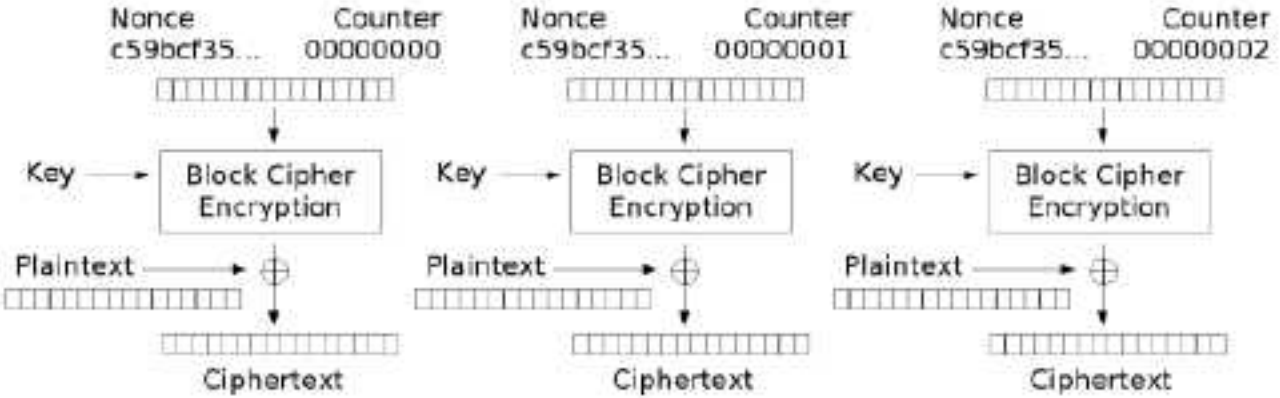
- Utiliza un contador del tamaño de bloque (n)
- Se inicializa con un nonce y se le suma 1 mod 2^n en bloques consecutivos
- Se descartan los bits sobrantes para el último bloque
- Permite conversión de un c. de bloque en uno de flujo
  - La serie cifrante no depende del texto en claro
  - Opera sobre bloques no sobre segmentos

Modo Counter (CTR)

Lo que lo hace muy importante y usado.

- El modo counter se ha impuesto por su simplicidad y por permitir el acceso aleatorio (paralelización)

El contador se inicializa con un nonce valor aleatorio no utilizado antes, y se van cifrando el contador con el bloque cifrador.

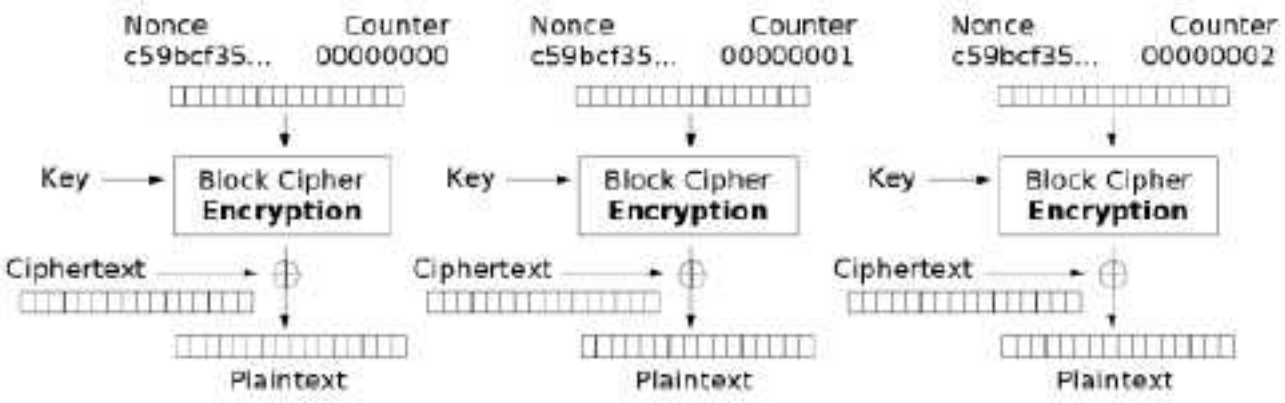


Counter (CTR) mode encryption

Y el contador cifrado se hace un XOR con el bloque de texto limpio, y genera el texto cifrado.

contador ca nonce → ⬡
↓
bloque cifro
↓
contador cifrado
↓
⊕ texto cifrado.
↑
texto limp

Modo Counter (CTR)



Counter (CTR) mode decryption

- Un error en Ci afecta a un solo Mi (en un bit)

CONTENIDOS

- Métodos de cifra moderna
- Criptosistemas simétricos
  - Cifradores de bloque
    - Introducción
    - Esquema de Feistel
    - Modos de operación
    - **Cifradores de bloque: Ventajas y desventajas**
    - DES
    - AES
  - Cifradores de flujo

Cifradores de bloque. Ventajas y desventajas

- Uso general: Confidencialidad
- Ventajas:
  - Alta difusión y confusión en el criptograma
  - Fácil implementación
  - Simetría
    - Cifrado y descifrado prácticamente idénticos
    - La misma circuitería permite cifrar y descifrar (no siempre, e.g. AES)
  - Eficiencia
    - Velocidad de cifra muy alta, (aunque menor que la obtenida por cifradores de flujo)

Cifradores de bloque. Ventajas y desventajas

- Desventajas:
  - Exigen un canal seguro (distribución de claves)
  - Gestión de un gran número de claves
  - Eficiencia
    - Menor tasa de cifrado que los de flujo al tener que leer antes el bloque completo
    - Longitud total de M debe ser un múltiplo del tamaño del bloque: la longitud del texto resultante mayor
  - Seguridad y robustez
    - Un error en un bit en C se propaga a todo el bloque
    - Vulnerable a ataques si se repiten bloques
  - Texto se alarga por relleno de bloques + símbolos de relleno proporcionan pistas a los criptoanalistas