Cifrado simétrico en bloque

Introducción
Modos de cifrado

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
KISA

Introducción

- Cifrado simétrico: misma clave secreta para cifrar y descifrar.
- Se cifran bloques de bits: el mensaje se divide en bloques de longitud fija y se cifra bloque a bloque.
- El cifrado de cada bloque es independiente de su posición y de los bloques adyacentes. Si un bloque aparece repetido, siempre se cifra de la misma manera.

Confusión y difusión

Muchos algoritmos de cifrado simétrico dividen el mensaje en bloques de tamaño fijo y aplican sobre cada uno de ellos operaciones de confusión y difusión.

- *Confusión.* Trata de ocultar la relación entre el texto claro y el texto cifrado. Se consigue con la *sustitución*, que consiste en cambiar cada carácter del mensaje por otro diferente.
- *Difusión.* Diluye la redundancia del texto claro repartiéndola a lo largo de todo el texto cifrado. Se consigue con la *transposición*, que consiste en cambiar la posición de los caracteres del mensaje.

La mayoría de los algoritmos intercalan la confusión (para lo que se utilizan tablas de sustitución) y la difusión (realizada con permutaciones). Esta combinación se conoce como *cifrado producto*.

Ejemplo

Supongamos que el mensaje en claro M es

VERDE QUE TE QUIERO VERDE

El cifrado de César (es una sustitución; genera confusión) de M resulta

YHUGH TXH WH TXLHUR YHUGH

El mensaje cifrado es ininteligible. No obstante, mantiene las regularidades de M.

Consideremos ahora la permutación $P = (3651472)$. Partiendo el mensaje en bloques de 7 letras (sin espacios), obtenemos 3 bloques de mensaje

$$m_1 = VERDEQU,\ m_2 = ETEQUIE,\ m_3 = ROVERDE$$

Calculando $c_i = P(m_i),\ i = 1, 2, 3$ observamos que se difunden las regularidades de M

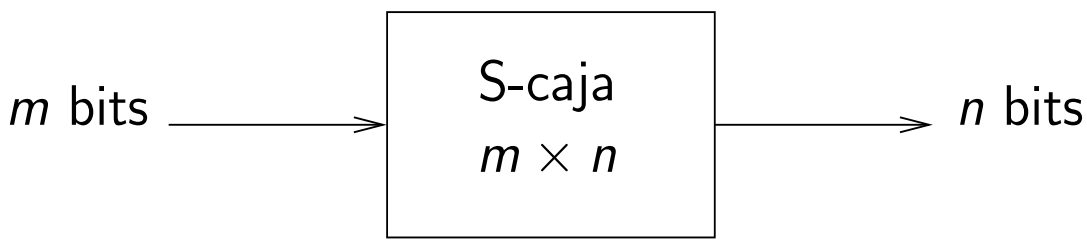
$$c_1 = RQEVDUE,\ c_2 = EIUEQET,\ c_3 = VDRREEO$$

S-Cajas

La confusión se consigue realizando sustituciones sencillas, para lo que se utilizan tablas pequeñas de sustitución llamadas *S-Cajas*.

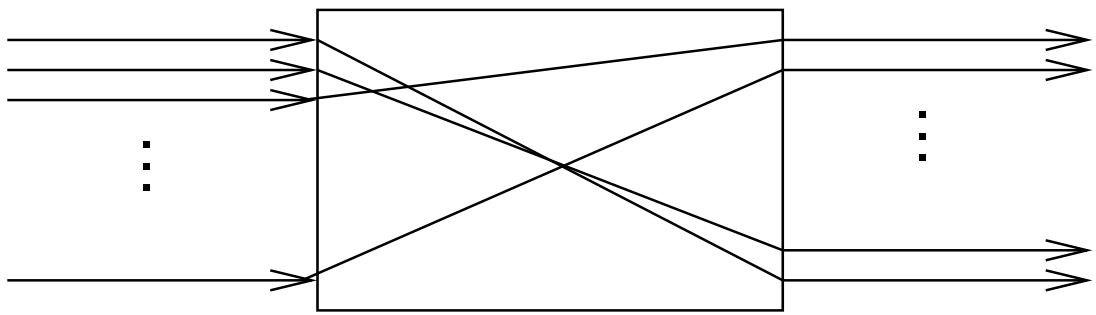
Una S-Caja $m \times n$ toma como entrada una cadena de m de bits y produce como salida una cadena de n bits.

El bloque original se divide en trozos de m bits y cada uno de ellos se sustituye por otro de n bits, haciendo uso de una S-Caja.



P-Cajas

La difusión se consigue realizando transposiciones, para lo que se utilizan tablas de permutación, llamadas *P-Cajas*.



Redes de Feistel

Algunos algoritmos, como el DES, utilizan lo que se denomina una *red de Feistel*. El primero en utilizarla fue el algoritmo *Lucifer*, diseñado por Horst Feistel y Don Coppersmith en 1973.

- Se divide el bloque en dos mitades L_0, R_0 (izquierda y derecha).
- A continuación se realiza un cifrado iterativo de n rondas. En cada ronda se utiliza una *clave de ronda*.
- La salida de cada ronda se utiliza como entrada de la siguiente.

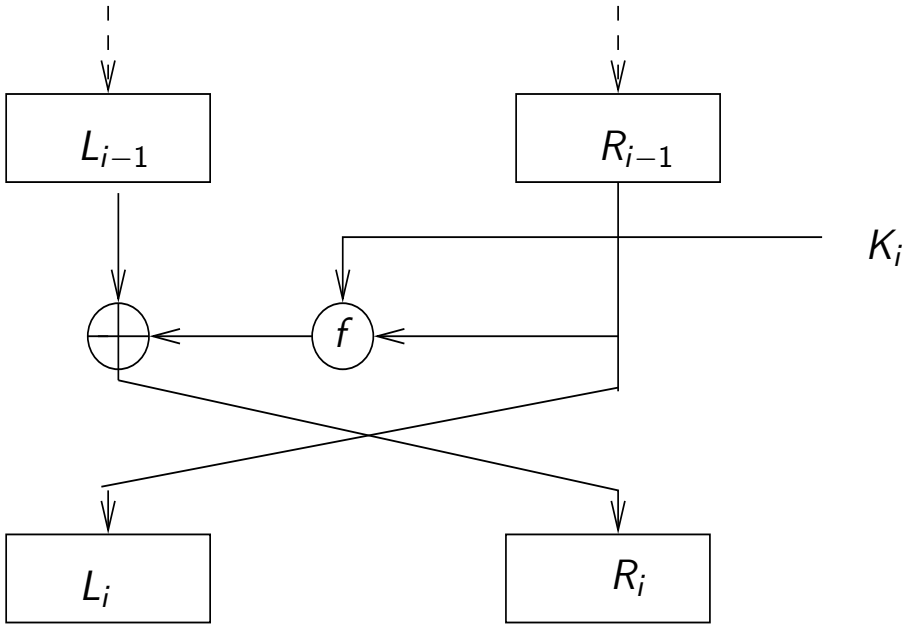
Las claves de ronda se generan a partir de una clave inicial compartida.

Para descifrar se aplica el mismo algoritmo, pero con las claves de ronda en orden inverso.

Las rondas

Para $i < n$,

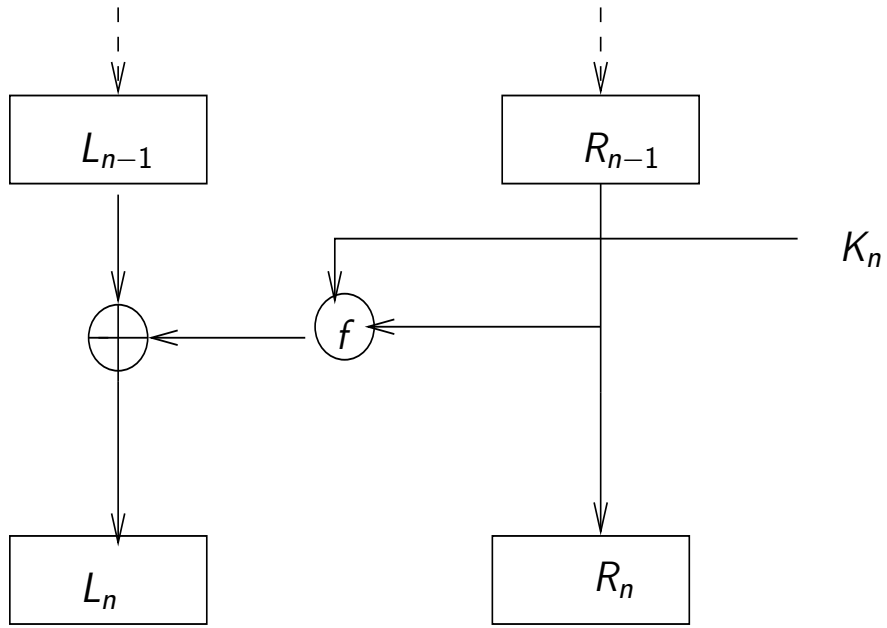
$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$



donde f es una función arbitraria, diferente para cada algoritmo, y K_i es la clave de la ronda i.

En la última ronda, se invierte el orden

$$L_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$
$$R_n = R_{n-1}$$



Para descifrar basta aplicar el mismo algoritmo, pero con las claves K_i en orden inverso.

Algunos criptosistemas simétricos

convocatoria (NBS)	1974
IBM (basado en Lucifer)	1974
DES	1977 (NBS, FIPS 46)
FEAL	Shizmizu, Miyaguchi 1987
IDEA	Lai 1992
SAFER	Massey 1994
RC5	Rivest 1995
AES-convocatoria	1997
MARS	finalistas
RC6	
Rijndael	
SERPENT	
Twofish	
AES	2001 (NIST, FIPS 197)

Modos de cifrado

Los algoritmos de cifrado en bloque trabajan sobre bloques de texto en claro y texto cifrado.

Estos algoritmos no se implementan solos, en forma directa.

Un *modo* combina el cifrado con cierto tipo de feedback, usando operaciones sencillas.

Objetivos de un modo de cifrado:

- Esconder regularidades del texto en claro.
- Aleatorizar la entrada.
- Incrementar la dificultad de manipulación del texto en claro y del cifrado.
- Permitir que diferentes mensajes en claro sean cifrados con la misma clave.

Los diferentes modos de funcionamiento dependen de la forma en que son cifrados los bloques sucesivos del mensaje.

Hay cuatro modos fundamentales:

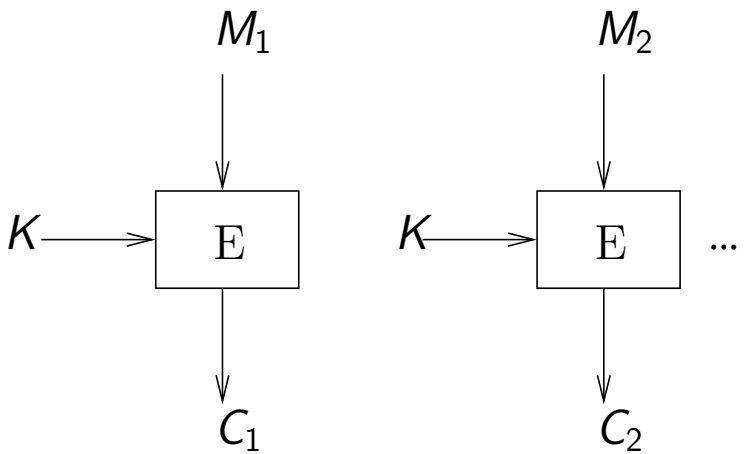
- ECB: Electronic Code Book mode.
- CBC: Cipher Block Chaining mode.
- CFB: Cipher Feed Back mode.
- OFB: Output Feed Back mode

Electronic Code Book (ECB)

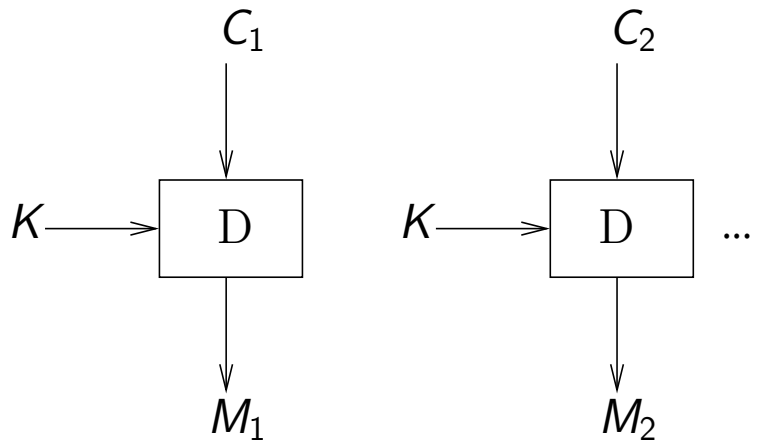
Es el método más sencillo y directo.

Se subdivide la cadena que se quiere cifrar en bloques de tamaño adecuado y se cifran todos ellos empleando la misma clave.

Si M_i es el bloque i y C_i su cifrado con la clave K:



Cifrado



Descifrado

$$C_i = \mathrm{E}(M_i, K)$$

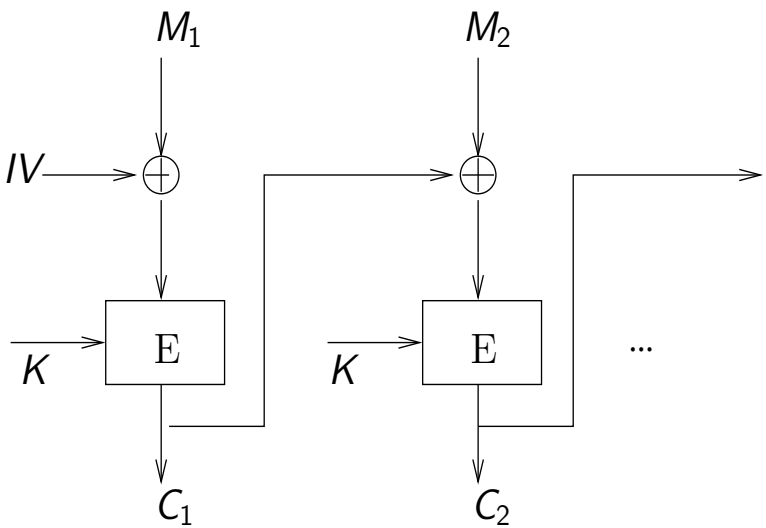
$$M_i = \mathrm{D}(C_i, K)$$

- Permite cifrar los bloques independientemente de su orden.
- Es resistente a errores. Si uno de los bloques sufre una alteración, el resto queda intacto.
- Si el mensaje presenta patrones repetitivos, el cifrado también los presentará. Un atacante puede efectuar un ataque estadístico.
- Un atacante puede realizar inserciones, sustituciones, permutaciones y eliminaciones.

Cipher Block Chaining (CBC)

Emisor y receptor intercambian un *vector de inicialización IV*.

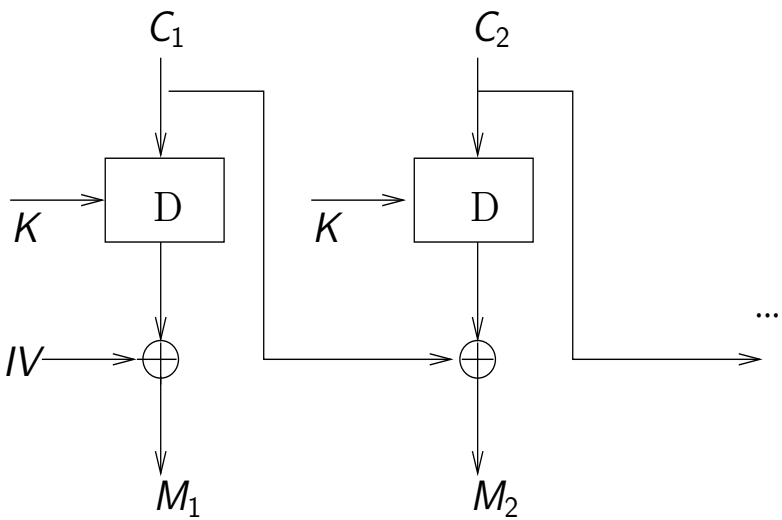
Antes de cifrar, cada bloque de mensaje en claro se suma mediante un XOR con el cifrado del bloque anterior. Para el primer bloque se utiliza el vector de inicialización IV.



Cifrado

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

$$C_0 = IV$$



Descifrado

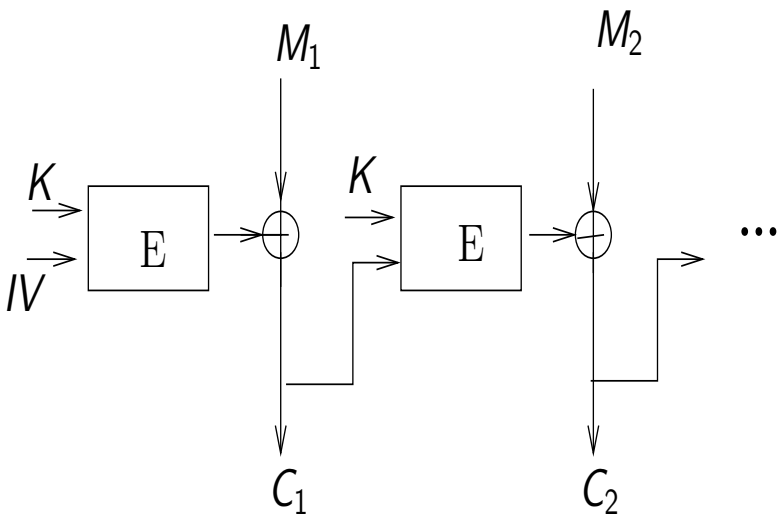
$$M_i = C_{i-1} \oplus \mathrm{D}(C_i, K)$$

$$C_0 = IV$$

- El emisor y receptor deben intercambiar, además de la clave, el vector de inicialización IV.
- Impide realizar inserciones, sustituciones, permutaciones y eliminaciones.
- Dos mensajes que difieran en un bit se cifran igual hasta el bloque en que está ese bit. Permite a un atacante identificar mensajes con inicios comunes. Para evitarlo: usar un vector de inicialización diferente para cada mensaje.

Cipher Feed Back (CFB)

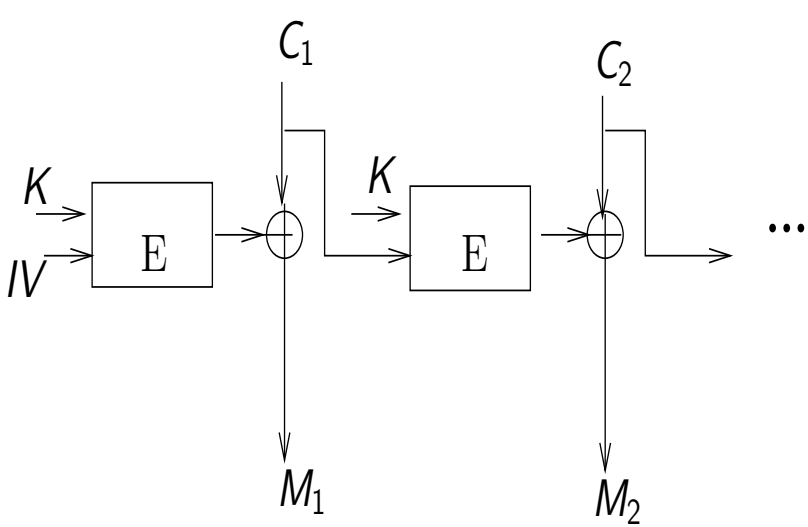
Cada bloque de mensaje en claro se suma mediante un XOR con el cifrado del criptograma anterior. Para el primer bloque se utiliza un vector de inicialización IV.



Cifrado

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

$$C_0 = IV$$



Descifrado

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

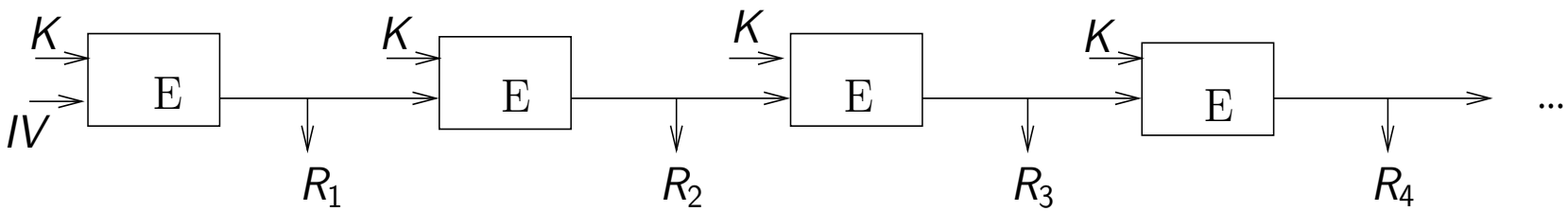
$$C_0 = IV$$

- El emisor y receptor deben intercambiar, además de la clave, el vector de inicialización IV.
- Tanto para cifrar como para descifrar, se usa únicamente la función de cifrado.
- Los cifrados de un mismo mensaje en claro son distintos si elegimos vectores de inicialización diferentes.

Output Feed Back (OFB)

Mediante cifrados consecutivos de un vector de inicialización IV, se calcula inicialmente una colección de vectores (tantos como bloques de mensaje a cifrar).

Cada uno de estos vectores se suma mediante un XOR con cada uno de los bloques del mensaje en claro.



Cifrado	Descifrado
$R_i = \mathrm{E}(R_{i-1}, K) \quad (R_0 = IV)$	$R_i = \mathrm{E}(R_{i-1}, K) \quad (R_0 = IV)$
$C_i = M_i \oplus R_i$	$M_i = C_i \oplus R_i$

El modo de cifrado OFB puede considerarse como un cifrado en flujo en el que el generador de claves está constituido por los cifrados (en bloque) sucesivos del vector de inicialización IV.

Fin de la sección