Modos de operación de cifrado en bloques

Félix Delgado - Ana Núñez

Universidad de Valladolid

Curso 2020 - 2021

Modos de operación de cifrado en bloques

Punto de partida:

1. Un cifrador en bloques de tamaño n. $E_K : \Sigma^n \to \Sigma^n$.
2. Un mensaje $m \in \Sigma^p$

El cifrador se puede ver como un dispositivo que para el par de entradas $(M, K) \in \Sigma^n \times \mathcal{K}$ produce el cifrado $E_K(M) = E(M, K) \in \Sigma^n$.

$$E : \sigma^n \times \mathcal{K} \to \Sigma^n \; ; \qquad (M, K) \mapsto E(M, K)$$

La longitud del mensaje m puede ser arbitraria. Por lo tanto lo primero que hay que hacer es dividir el mensaje original en bloques del mismo tamaño: $m = m_1 m_2 \dots m_\ell$. El tamaño de cada uno de los bloques es $r \leq n$.

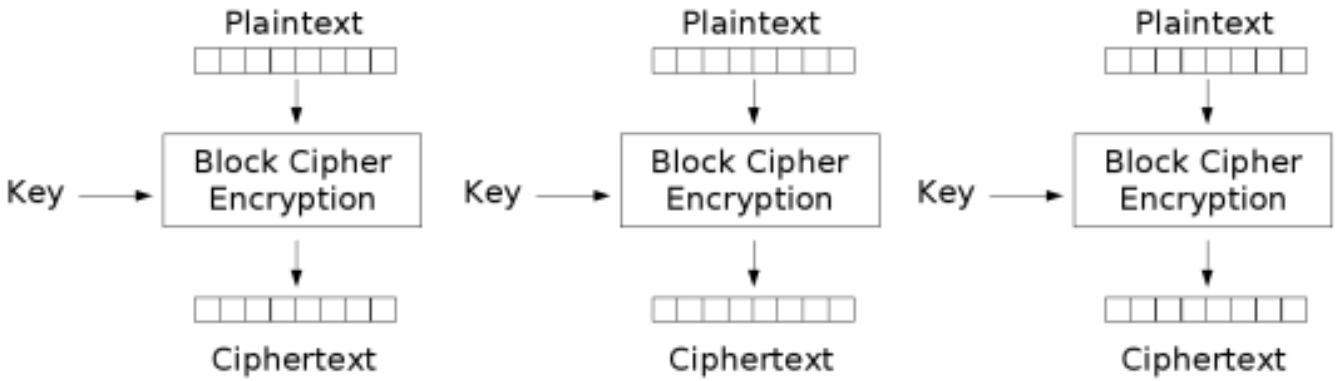
Si la longitud del mensaje no es múltiplo de la longitud de los bloques, es necesario añadir información de relleno al final, de forma que el mensaje original se pueda recuperar después ed descifrar.

Un posible mecanismo es rellenar con ceros el último bloque y añadir como último byte el número de bytes (o bits) añadidos.
Habitualmente los diferentes agentes suelen fijar un sistema de completar.

Modo ECB: Electronic Codebook

El modo ECB (*electronic codebook*) es el método más directo de aplicar cualquier técnica de cifrado en flujo. Consiste sencillamente en dividir el texto claro en bloques y cifrar cada uno de ellos independientemente, empleando la misma clave.
Siempre los datos de entrada son el mensaje $m = m_1, \ldots, m_t$ y la clave $k \in \mathcal{K}$. La salida es el mensaje cifrado $c = c_1, \ldots, c_t$.

- Para $i = 1, \ldots, t$: $c_i := E(m_i, K)$



Electronic Codebook (ECB) mode encryption

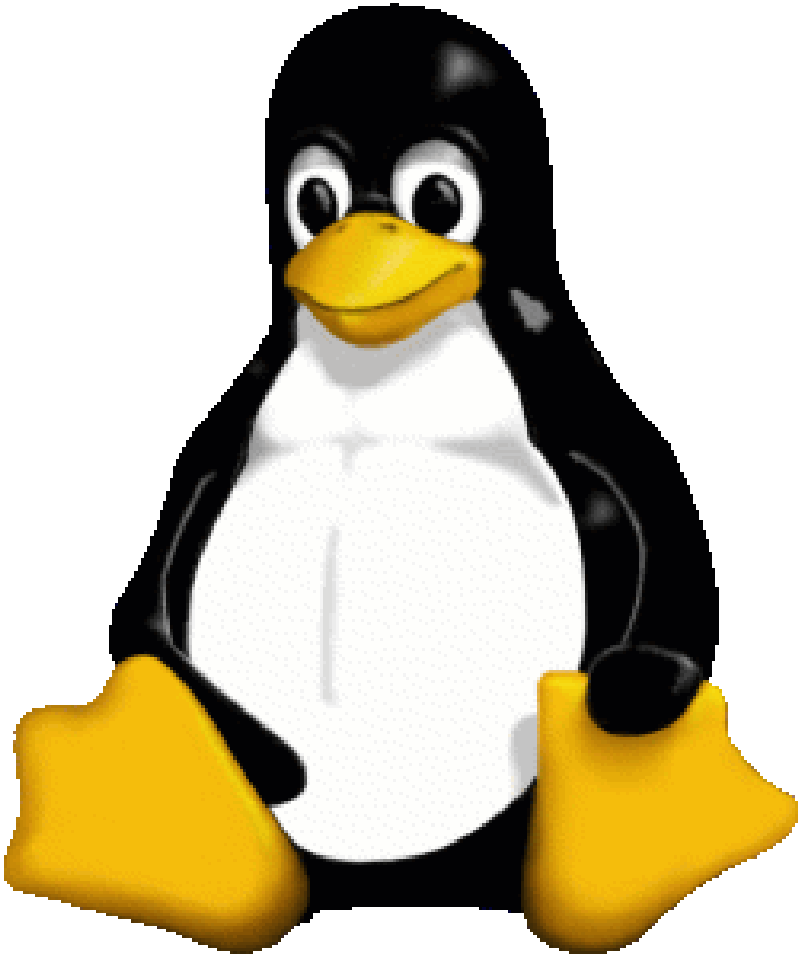
Modo ECB: Electronic Codebook

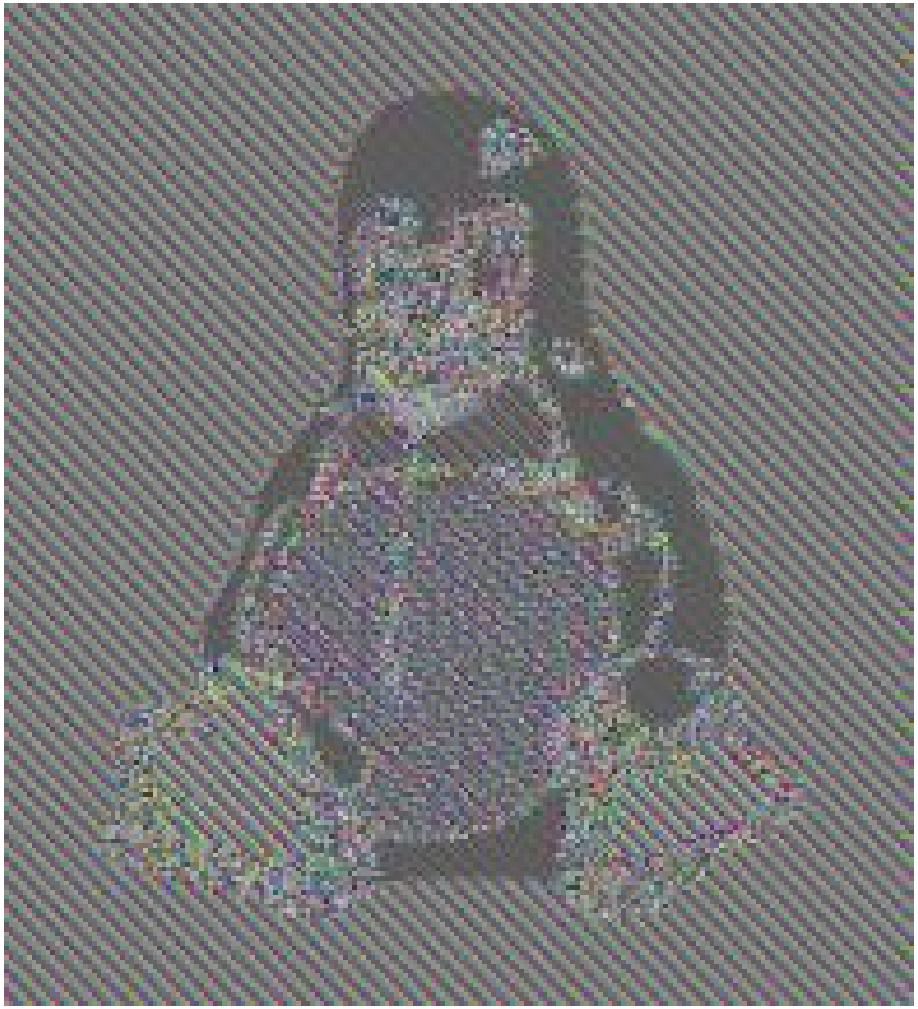
A su favor tiene el que pueden codificar los bloques de forma independiente de su orden, lo que es bueno en algunas ocasiones (cifrado de bases de datos, por ejemplo).

Riesgos:

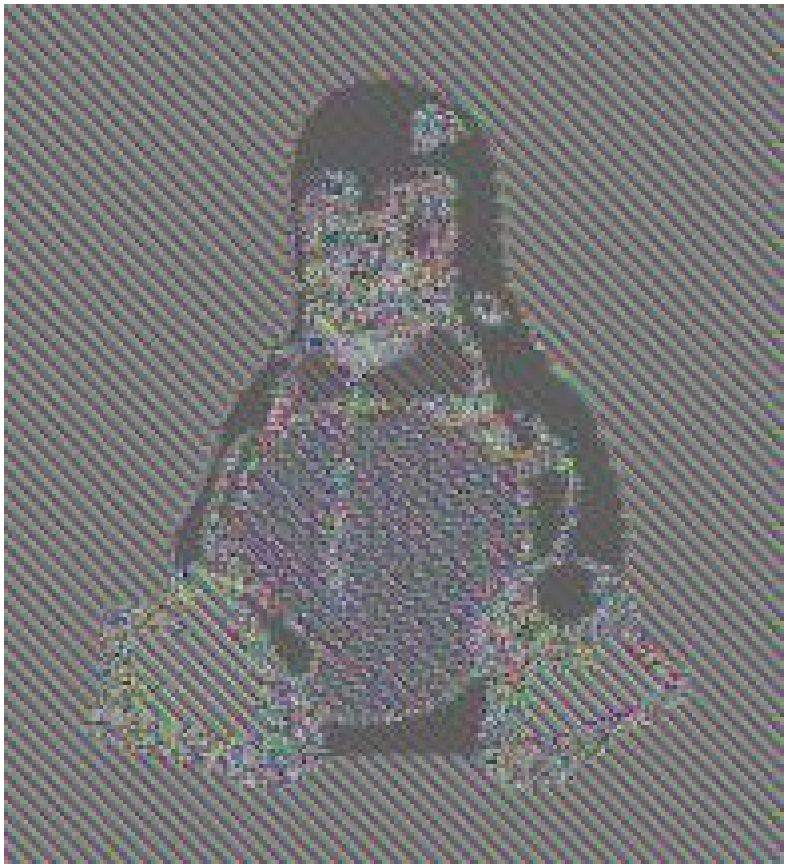
- Si el mensaje presenta patrones repetitivos, el cifrado también los tendrá, pues en este caso se puede extraer información a base de ataques estadísticos.
- El atacante puede cambiar un bloque incluso desconociendo la clave y el algoritmo de cifrado. Por ejemplo, en una comunicación bancaria se podrían sustituir los bloques correspondientes al número de cuenta por la versión codificada de nuestro número.

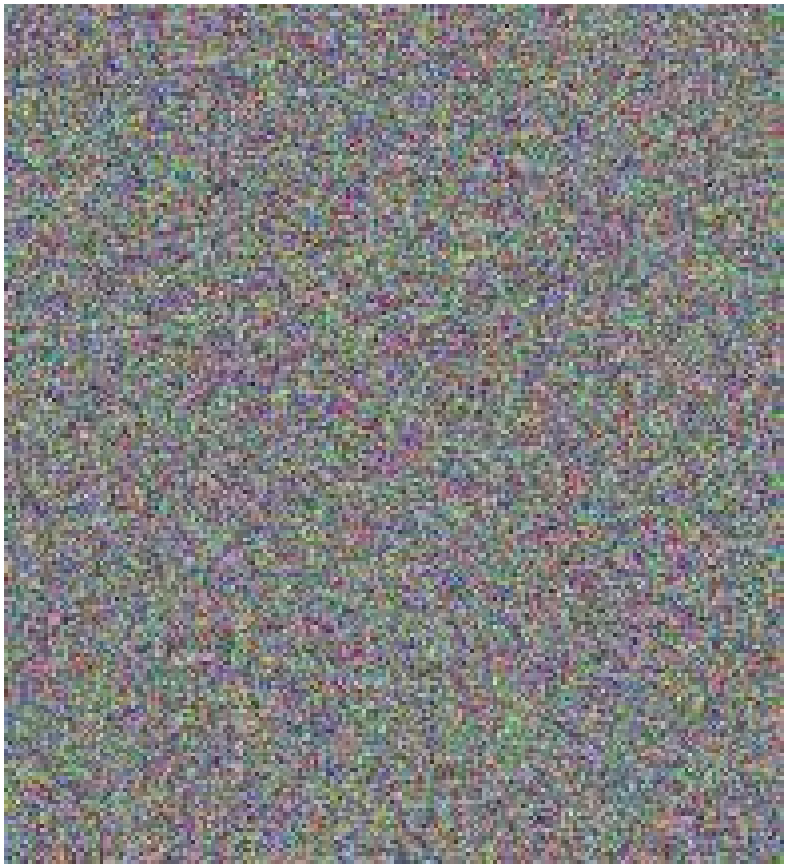
Modo ECB: Electronic Codebook





Modo ECB: Electronic Codebook





Modo CBC: Cipherblock chaining

El modo CBC (*cipherblock chaining*, *Encadenamiento de bloques cifrados*) utiliza en el cifrado de cada bloque el cifrado del anterior.
Por lo tanto, no se podrá sustituir simplemente un bloque cifrado por otro, ya que esta sustitución afecta a varios bloques en el mensaje descifrado (de hecho a dos).

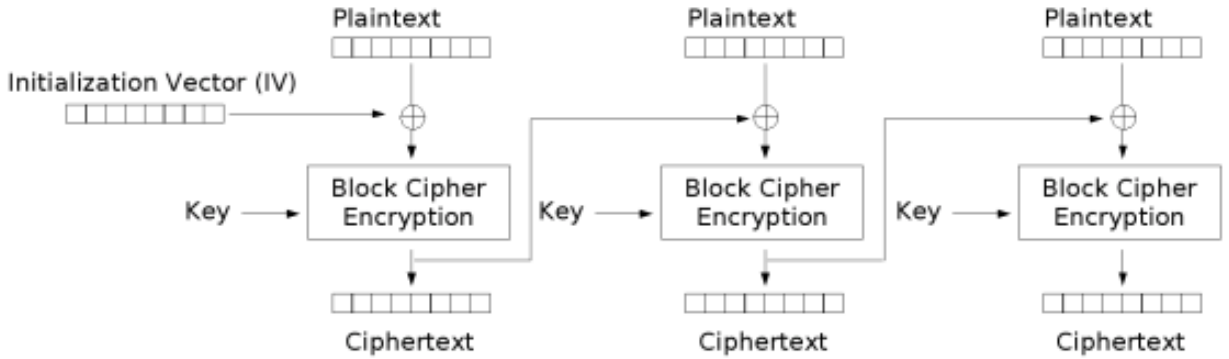
Se necesita en este modo un *vector de inicialización*, IV, de la misma longitud que los bloques, que se puede hacer público.

Modo CBC: Cipherblock chaining

Si la clave es k y E_k la operación de cifrado, entonces para encriptar un mensaje $m_1 \dots m_t$ siendo cada m_i un bloques de la longitud fijada, se calcula

$$c_0 = IV, \quad c_j = E_k(c_{j-1} \oplus m_j), \text{ para } 1 \leq j \leq t$$

y el mensaje se cifra por $c_1 \dots c_t$.



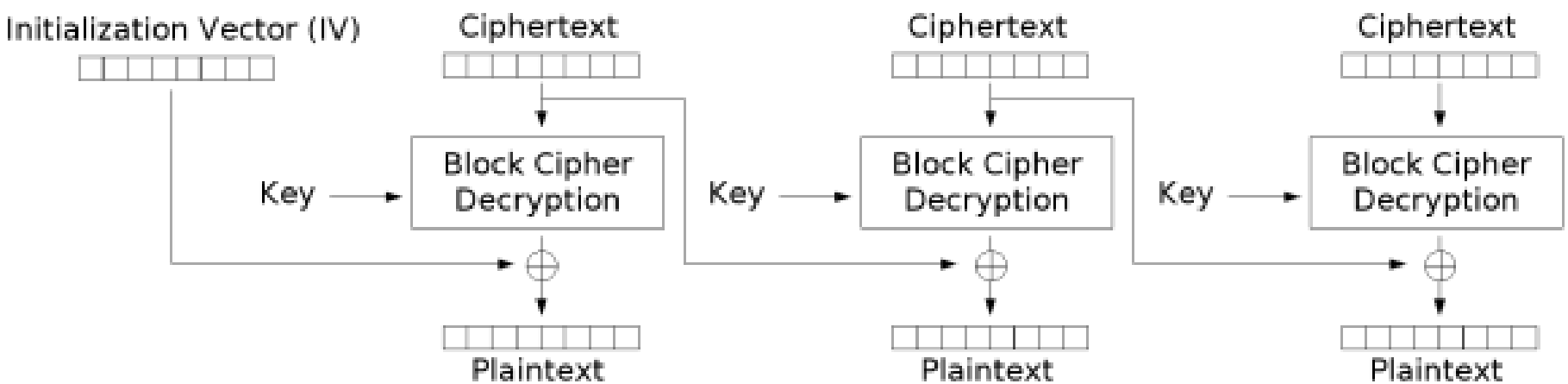
Cipher Block Chaining (CBC) mode encryption

Modo CBC: Cipherblock chaining

Es fácil deducir que la forma de descifrar es, si d es la clave de descifrado y D_d la operación de descifrado,

$$c_0 = IV, \quad m_j = c_{j-1} \oplus D_d(c_j), \text{ para } 1 \leq j \leq t.$$

En particular, en la recuperación de m_j solo intervienen los bloques cifrados c_{j-1} y c_j, por lo cual algún cambio en el cifrado que afecte a c_j se reflejará en m_j y m_{j+1} pero no en el resto de los bloques.



Cipher Block Chaining (CBC) mode decryption

Modo CFB: Cipher FeedBack

- El modo CFB (*cipher feedback*) se diferencia del anterior en que cada bloque se cifra y después se suma (con un XOR), con el siguiente bloque antes de cifrar este.
- Es decir, la función de cifrado no se usa directamente, sino que se utiliza para generar una sucesión de claves que luego se combinan con el mensaje.
- Una ventaja importante es que la longitud r de los bloques del mensaje se puede escoger menor que la longitud de bloque del algoritmo de cifrado, n. Esto hace que sea un modo adecuado para las situaciones en que se requiere enviar la información en *paquetes* de longitud menor que n (por ejemplo, en comunicaciones electrónicas).
- También es destacable que en este caso solo se necesita usar, tanto para codificar como para decodificar, la función de codificación del algoritmo original, y no la de decodificación.

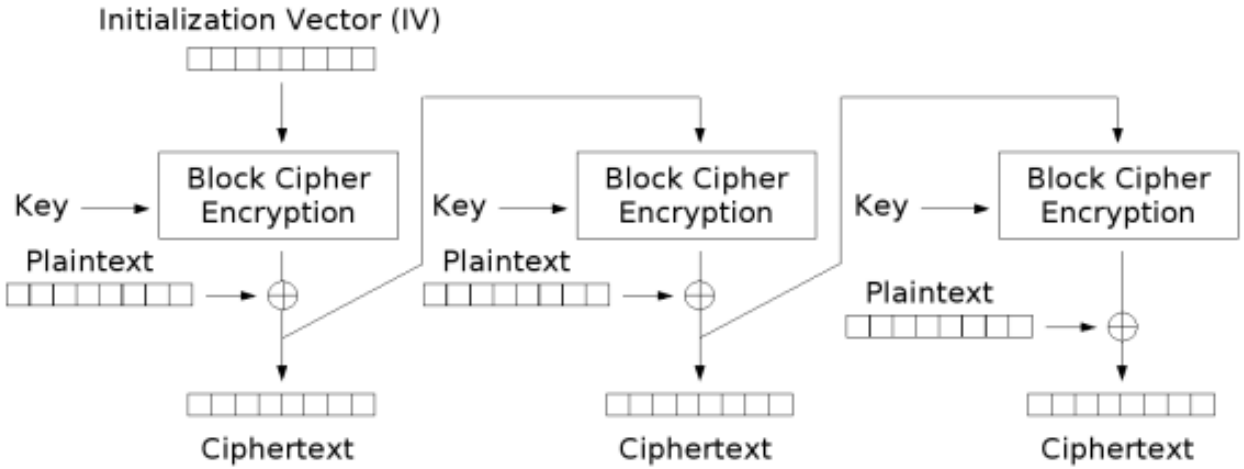
Modo CFB: Cipher Feedback

Se parte de un vector de inicialización, IV. Para encriptar un mensaje $m_1 \dots m_t$ siendo cada m_i un bloques de longitud r, se hace los siguiente:

1. $I_1 = IV$
2. Para $1 \leq j \leq t$:
   - $O_j = E_e(I_j)$
   - $c_j = m_j \oplus t_j$, donde t_j está formado por los r primeros bits de O_j
   - $I_{j+1} = 2^r I_j + c_j \mod 2^n$

Obsérvese que I_{j+1} está formado por n bits, de los cuales los primeros $n - r$ son los últimos $n - r$ bits de I_j, y los r últimos son los r bits de c_j.

Modo CFB: Cipher Feedback



Cipher Feedback (CFB) mode encryption

El desencriptado es parecido:

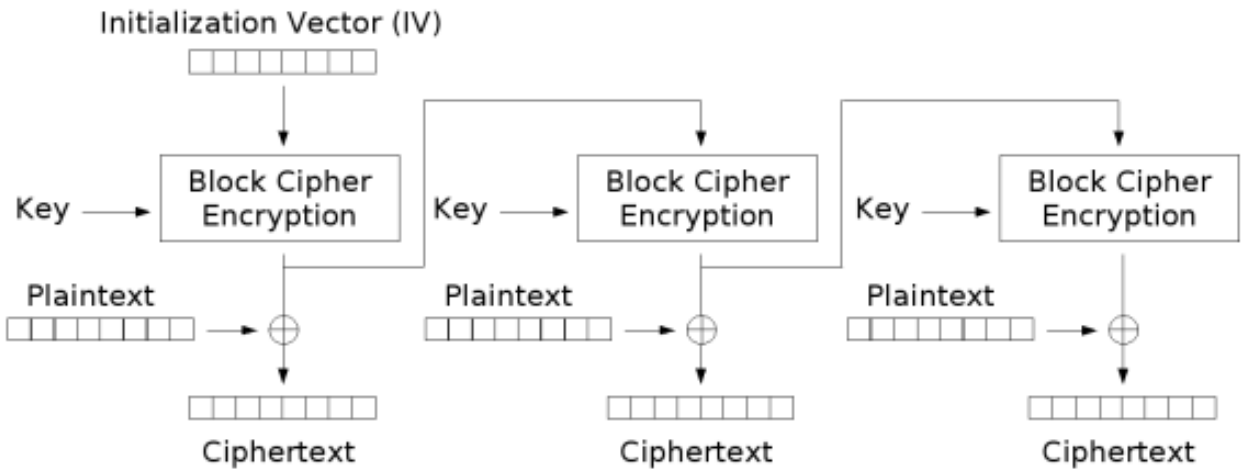
1. $I_1 = IV$
2. Para $1 \leq j \leq t$:
   - $O_j = E_e(I_j)$
   - $m_j = c_j \oplus t_j$, donde t_j está formado por los r primeros bits de O_j
   - $I_{j+1} = 2^r I_j + c_j \mod 2^n$

Modo OFB: Output FeedBack

Muy parecido al anterior. Si el algoritmo de cifrado es para bloques de longitud n, se elige cualquier $r \leq n$, y para codificar un mensaje $m_1 \dots m_t$ siendo cada m_i un bloques de longitud r, se hace los siguiente:

1. $I_1 = IV$
2. Para $1 \leq j \leq t$:
   - $O_j = E_e(I_j)$
   - $c_j = m_j \oplus t_j$, donde t_j está formado por los r primeros bits de O_j
   - $I_{j+1} = O_j$

Modo OFB: Output FeedBack



Output Feedback (OFB) mode encryption

Al igual que en el mod ECB, el encriptado de cada bloque se puede hacer independientemente del resto, la diferencia es que aquí se genera una sucesión de claves (que es independiente del mensaje) que se combinan con un XOR con el mensaje. Esto hace que la manipulación del texto cifrado sea más complicada.