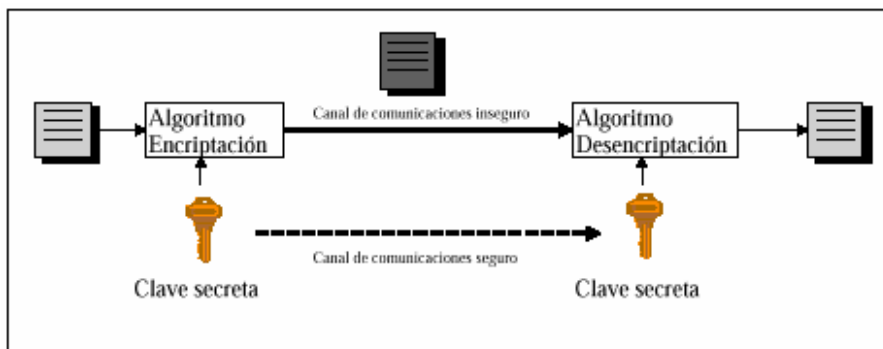


# ALGORITMOS SIMÉTRICOS

## INTRODUCCIÓN

Los algoritmos simétricos se caracterizan por utilizar la misma clave para cifrar y descifrar.



La seguridad en estos algoritmos está basada en la privacidad de la clave secreta, llamada simétrica porque es la misma para el emisor y el receptor. El emisor del mensaje genera una clave que después transmite a través de un canal de comunicaciones seguro a todos los usuarios autorizados a recibir sus mensajes. El principal problema de los sistemas simétricos es la distribución de las claves, que hoy en día se resuelve mediante sistemas asimétricos implementados para la transmisión de claves secretas.

Estos sistemas solo permiten confidencialidad, y no autenticación ni firma digital.

Para mantener la confidencialidad frente a posibles ataques, los algoritmos simétricos deben cumplir las siguientes condiciones:

Conocido el texto cifrado no se puede descifrar el texto ni adivinar la clave.

Conocido el texto en plano y el texto cifrado es más caro (en tiempo o dinero) descifrar la clave que el valor de la información.

La técnica de los algoritmos simétricos se basa en cifrar bloques de texto, el tamaño de los cuales puede ser constante o variable según el tipo de algoritmo. Existen 4 formas de funcionamiento:

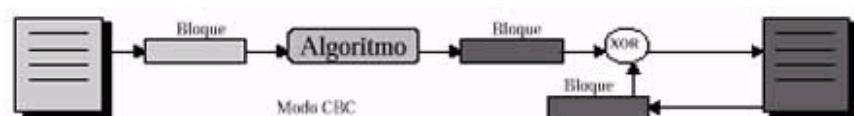
### Electronic CodeBook (ECB)

Los bloques de texto se cifran por separado.



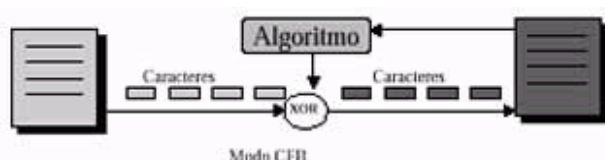
### Cipher Block Chaining (CBC)

Los bloques del texto cifrado se relacionan entre sí mediante funciones OR-EXCLUSIVA..



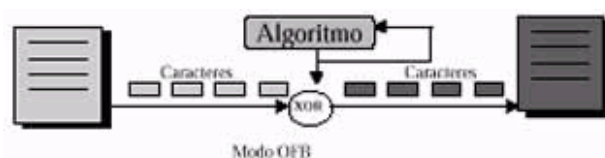
### Cipher FeedBack (CFB)

Se realiza una OR-EXCLUSIVA entre caracteres o bits aislados del texto y las salidas del algoritmo. El algoritmo utiliza como entradas los textos cifrados.



### Output FeedBack (OFB)

Funciona igual que el CFB, pero utiliza como entradas sus propias salidas, por lo tanto no depende del texto; es un generador de números aleatorios.



La principal ventaja de los algoritmos simétricos reside en que son más sencillos que los asimétricos, por lo que sus procesos son mucho más rápidos y simples.

Los algoritmos simétricos más utilizados son el DES y IDEA.

## DES (Data Encryption Standard)

En 1973 el National Bureau of Standard (NBS) adoptó el algoritmo DES (Data Encryption Standard) como estándar de cifrado para la seguridad de documentos oficiales.

El algoritmo cifra bloques de 64 bits con una clave de 56 bits más 8 de paridad. El algoritmo de descifrado es muy similar, con lo que se facilita su implementación en hardware y software.

Los inconvenientes de este algoritmo son los siguientes:

- Está considerado como secreto nacional en los EE.UU. Por esta razón no se puede comercializar en hardware ni en software fuera de los EE.UU. sin permiso del Departamento de Estado. A pesar de esto, es el algoritmo más extendido en el mundo.
- La clave es corta. Hasta ahora era suficiente con las máquinas existentes, pero se considera que próximamente se podrá romper con máquinas más potentes trabajando en paralelo a través de Internet. Por este motivo ya no es el estándar de seguridad en los EE.UU.

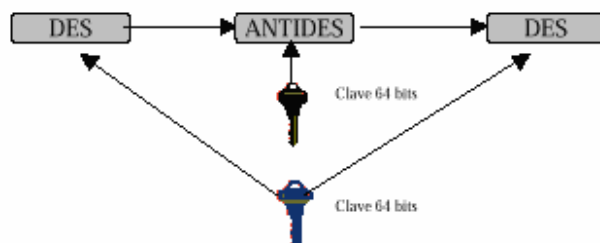
Las ventajas del algoritmo son las siguientes:

- Es el más utilizado en el mundo, lo que da lugar a que sea el más barato, más probado, utilizado por todo tipo de sistemas, etc.
- En 20 años nunca ha sido roto con un sistema práctico.
- Es muy rápido y fácil de implementar.

## TDES (Triple DES)

Se creó para evitar el problema de la clave corta. El triple DES está basado en tres iteraciones del algoritmo y utiliza una clave de 128 bits, siendo compatible con el DES simple.

Se utiliza una clave de 128 bits (16 de paridad y 112 de clave), se aplican 64 bits a los dos DES y otros 64 bits al DES inverso (ANTIDES) que se realiza entre los otros dos.



Con tres algoritmos se podría aplicar tres claves distintas, pero no se realiza de este modo para que sea compatible con el DES. Si la clave de 128 bits está formada por dos claves iguales de 64 bits el sistema se comporta como un DES.

simple.

## **IDEA (International Data Encryption Algorithm)**

En 1990, Lai y Massey del Swiss Federal Institute of Technology inventaron un nuevo algoritmo llamado IDEA. Este algoritmo está libre de restricciones y permisos nacionales y es de libre distribución por Internet. Esto ha hecho que sea un algoritmo muy popular, sobre todo fuera de los EE.UU., utilizándose en sistemas como UNIX en Europa, PGP para correo electrónico, etc.

Trabaja con bloques de texto de 64 bits y una clave de 128 bits. Puede trabajar con los 4 modos: ECB, CBC, CFB y OFB. Siempre opera con números de 16bits utilizando operaciones como OR-EXCLUSIVA, suma de enteros o multiplicación de enteros.

El algoritmo para descifrar es muy similar, por lo que es muy rápido y sencillo de programar.

Hasta ahora no ha sido nunca roto, y aunque no tiene la antigüedad del DES, su mayor longitud de clave le da mayor robustez.

## **Blowfish**

Blowfish es un algoritmo de cifrado por bloques, creado por Bruce Schneier y diseñado para ser rápido (cifra datos en modo de 32-bit a razón de 26 ciclos de reloj por byte), compacto (puede correr ocupando menos de 5Kb de memoria), simple (las únicas operaciones que se utilizan son sumar, XOR, y buscar la tabla de particiones en operaciones de 32-bits), seguro (la longitud de la clave de Blowfish es variable y puede tener una longitud de hasta 448 bits), y robusto (a diferencia de DES, la seguridad de Blowfish no disminuye por simples errores de programación).

El algoritmo de cifrado por bloques Blowfish, que cifra datos en bloques de 64-bits al mismo tiempo, es dividido en dos partes: claves de expansión y cifrado de datos.

Las claves de expansión convierten una clave de más de 448 bits en varias subclaves que totalizan 4168 bytes.

El cifrado de datos consiste en una función simple que permite 16 iteraciones. Cada iteración llamada Arounda consiste en la permutación

de una clave dependiente y una substitución de una clave y datos dependiente.

Blowfish utiliza un gran número de subclaves que deben ser preprocesadas antes de cualquier proceso de cifrado o descifrado.

La ordenación-P consiste en 18 subclaves de 32-bits, P1, P2, ...P18 y hay cuatro subcajas de 32-bit con 256 entradas cada una: S1,0 , S1,1 , ...S1,255 ; S2,0, S2,1,...S2,255 ; S3,0, S3,1,...S3,255; S4,0 S4,1,...S4,255.

## Stealth

El cifrado STEALTH TM es el nombre genérico para una familia de algoritmos simétricos de criptografía desarrollado por IQ international. Todas las variantes de la encriptación STEALTH incluyen las siguientes características:

1. *Alta velocidad de proceso.* Normalmente alrededor de 3MB por segundo en un procesador Intel 486/DX2 y 5MB en un Intel Pentium a 66Mhz.
2. *Muy seguro.* La técnica típica de la criptografía STEALTH utiliza 2 50.000 combinaciones teóricas, limitadas únicamente por la longitud de la clave. Todos los datos son cifrados de manera aleatoria y totalmente incomprensible. Pequeños cambios de clave suponen datos cifrados diferentes.
3. *Operación que llega al byte.* Hasta un simple byte puede ser cifrado o descifrado.
4. *Acceso aleatorio.* Cualquier volumen de datos puede ser descifrado/recifrado desde cualquier byte-offset accediendo de modo aleatorio completo.
5. *No existe expansión de datos.* Los datos cifrados tienen idénticos bytes de orden y longitud.
6. *Integridad de errores.* A diferencia de otros algoritmos, los errores no se propagan y las corrupciones en datos cifrados sólo afectarán a los bytes correspondientes de descifrado.
7. *No existen claves débiles.* A diferencia de otras fórmulas algorítmicas no existen claves de cifrado débiles inherentes.

El cifrado STEALTH TM está disponible en un número muy amplio de fórmulas y gran variedad de longitud de claves. Existen diversas variantes del cifrado STEALTH con variedad de plataformas como son los estándares 1040/1060.