Electronic Codebook (ECB)

Ing. Max Alejandro Antonio Cerna Flores

Agenda

- ¿Que es un cifrado en bloque?
- ¿Que es el modo de operación de cifrado en bloque?
- Historia
- Vector de Inicialización
- Padding (Rellenado)
- ¿Qué es el modo de cifrado ECB?

¿Que es un cifrado en bloque?

Es un algoritmo determinista que opera en grupos de bits de longitud fija, llamados bloques, siendo componentes elementales definidos en el diseño de muchos protocolos criptográficos y se utilizan ampliamente para cifrar grandes cantidades de datos.

Aunque son aptos para cifrar un bloque con una llave fija a la vez cuentan con una variedad de modos de operación que permiten su uso repetido de forma segura para lograr los objetivos de seguridad de confidencialidad y autenticidad.

Operan con bloques completos, por lo que es necesario que la última parte del bloque sea rellenada.

¿Que es un cifrado en bloque?

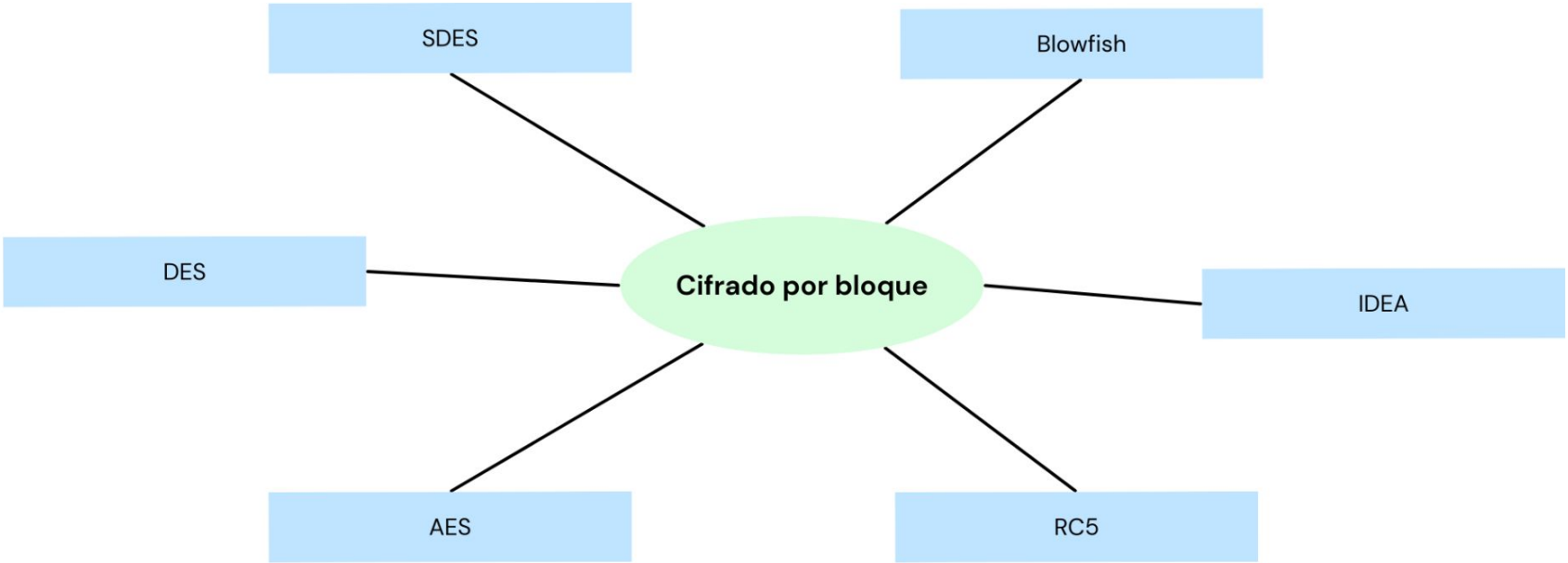
El diseño moderno de este se basa en el concepto de un cifrado de producto por iteración.

Claude Shannon analizó estos y los sugirió como un medio para mejorar la seguridad mediante la combinación de operaciones simples como sustituciones y permutaciones.

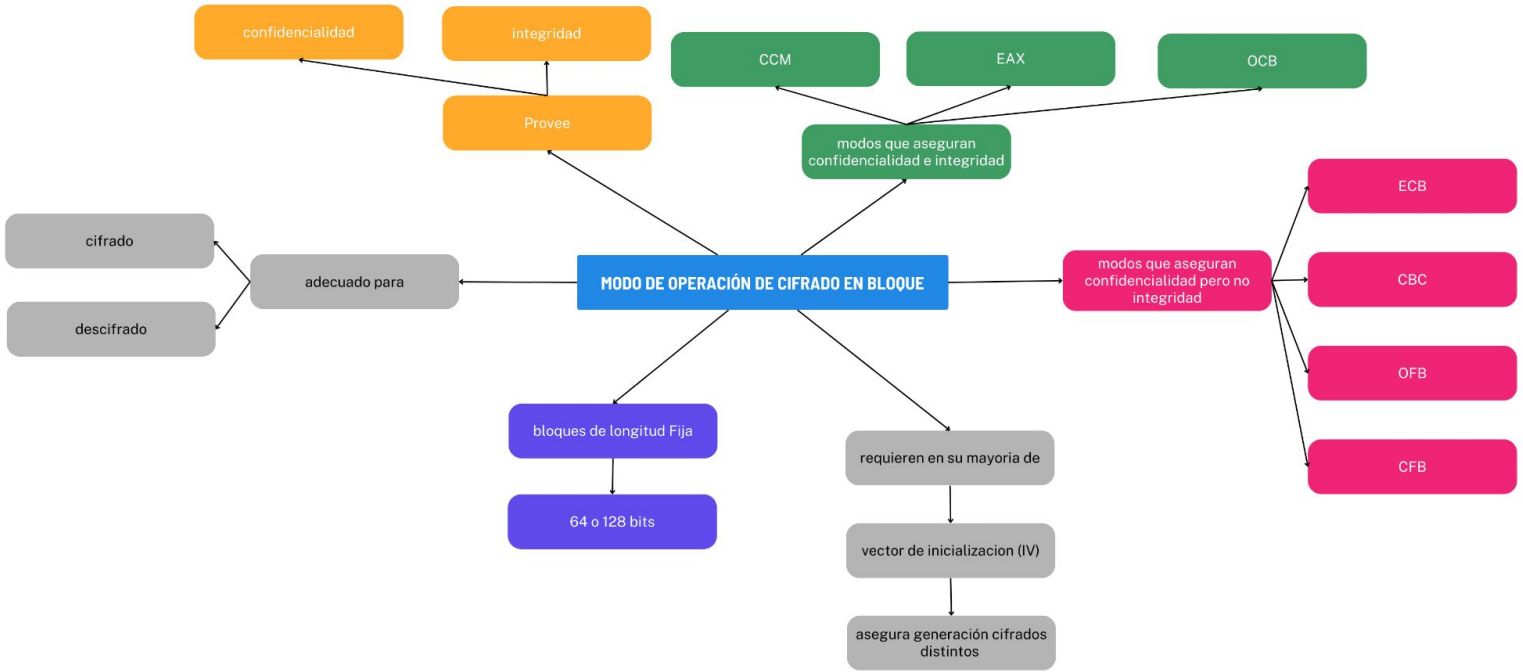
Los cifrados de productos por iteración llevan a cabo el cifrado en varias rondas.

Una implementación generalizada de tales cifrados denominada red Feistel en honor a Horst Feistel.

¿Que es un cifrado en bloque?



¿Que es el modo de operación de cifrado en bloque?



Historia

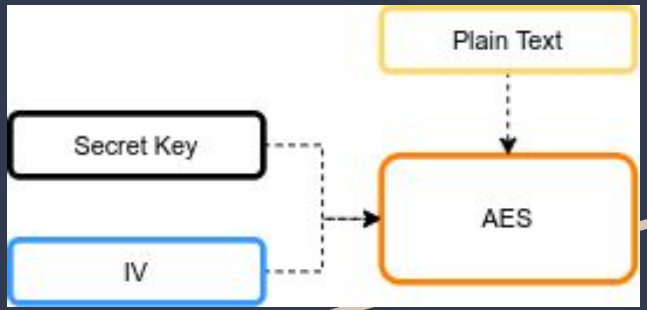
Los primeros modos de operación, ECB, CBC, OFB y CFB, datan de 1981 y se especificaron en FIPS 81(Federal Information Processing Standards Publications).

La manipulación se puede detectar con un código de autenticación de mensaje separado como la firma digital.

La comunidad criptográfica observó que combinar un modo de confidencialidad con un modo de autenticidad podría ser difícil y propenso a errores.

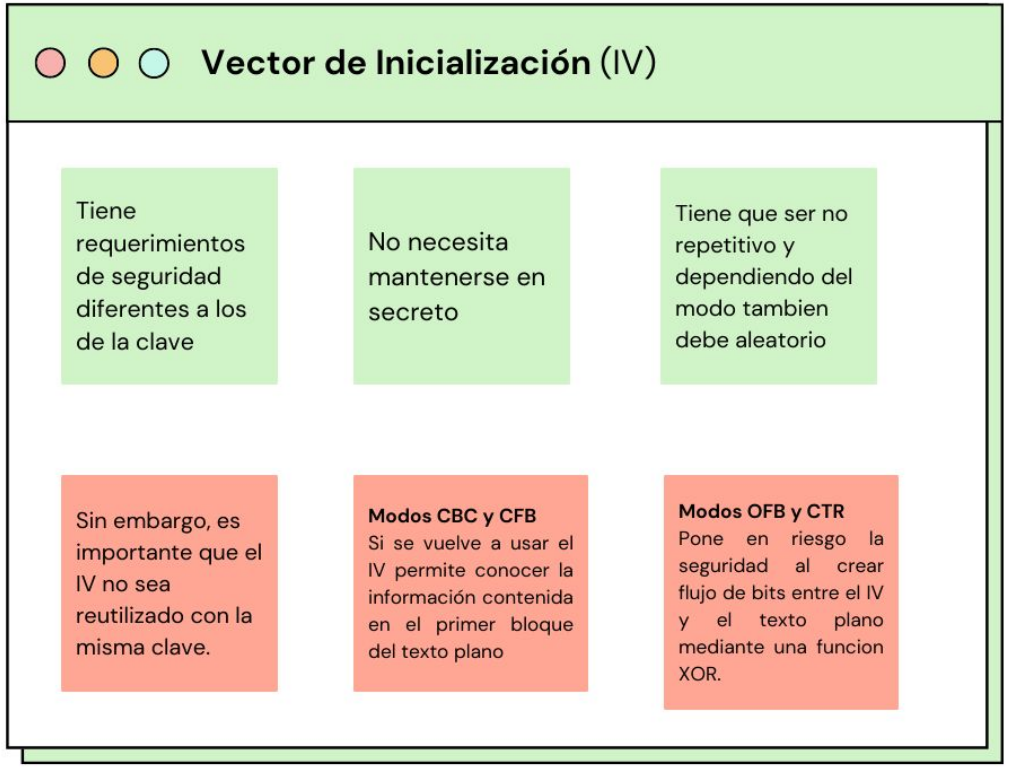
Los modos de operación están definidos por una serie de organismos de normalización reconocidos a nivel nacional e internacional.

Vector de Inicialización



Es un bloque de bits que es utilizado por varios modos de operación para hacer aleatorio el proceso de cifrado y por lo tanto generar distintos textos cifrados incluso cuando el mismo texto plano es cifrado varias veces, sin la necesidad de regenerar la clave, siendo la regeneración un proceso lento.

Vector de Inicialización



Padding

Dado que los algoritmos de cifrado por bloque utilizan bloques de tamaño fijo (ej. DES con 64 bits), pero los mensajes son de longitud variable, es necesario rellenar el espacio del bloque.

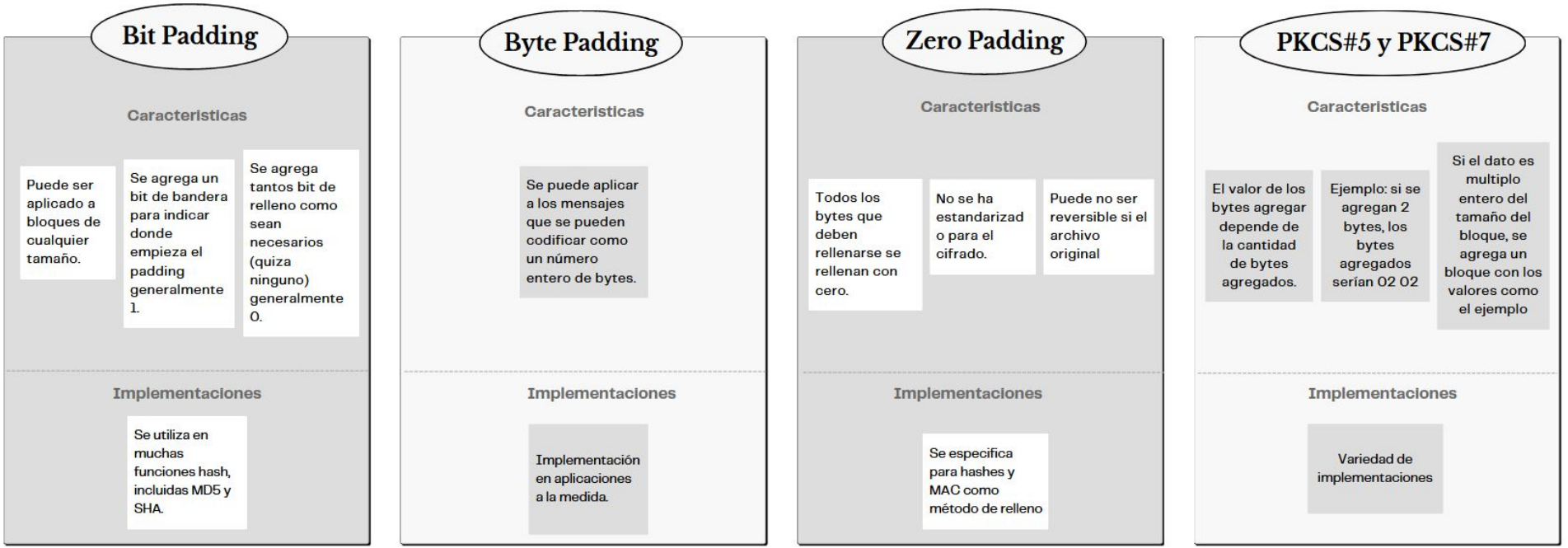
En algunos modos de operación como ECB y CBC el último bloque de texto debe ser rellenado antes del proceso de cifrado.

El relleno más simple consiste en agregar null bytes al texto plano.

Debe ser posible recuperar la longitud del texto original.

Los esquemas CBC como *ciphertext stealing* o *residual block termination* agregando complejidad adicional en el proceso.

Tipos de Padding



Otros tipos de Padding

ANSI X9.23

ISO 10126

ISO/IEC 7816-4

¿Qué es el modo de cifrado ECB?

Es el modo más simple de todos.

Se considera inseguro.

No usa el vector de inicialización.

ECB marcó el hito de ser uno de los primeros modos de cifrado por bloques, que permiten la encriptación de cantidades mayores de información.

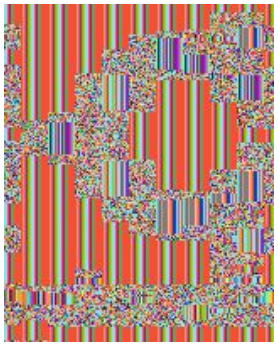
El principal fallo de seguridad de este método es que los mismos bloques de texto plano siempre producen los mismos textos cifrados.

El mensaje es dividido en bloques, cada uno de los cuales es cifrado de manera separada.

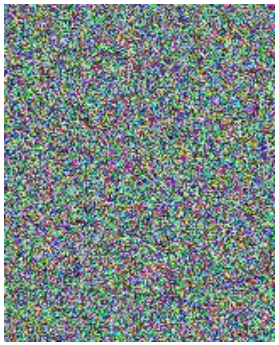
No proporciona una auténtica confidencialidad y no es recomendado para protocolos criptográficos.

¿Qué es el modo de cifrado ECB?

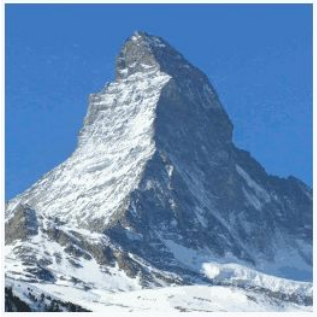
original

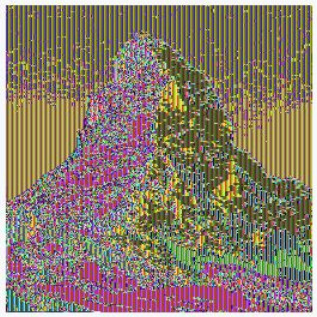


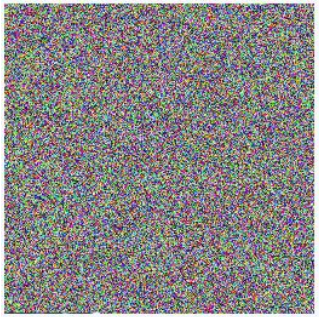
ECB



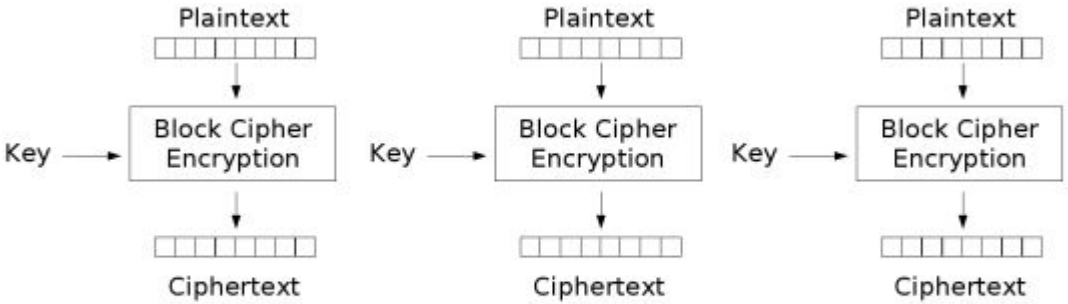
otro modo



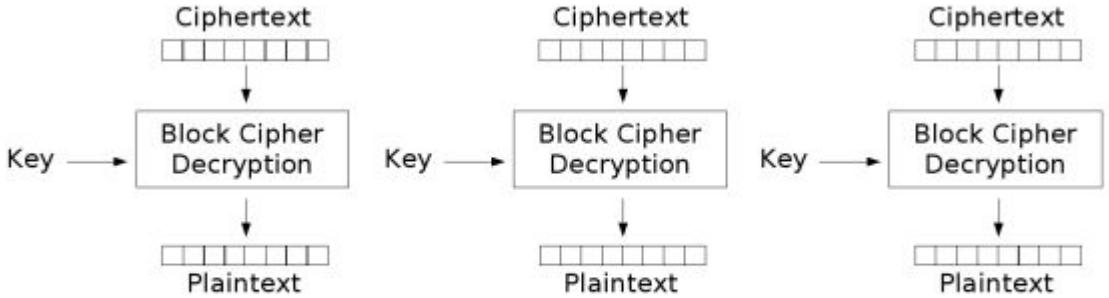




¿Qué es el modo de cifrado ECB?



¿Qué es el modo de cifrado ECB?



Electronic Codebook (ECB) mode decryption