El cifrado en bloques es una técnica básica de cifrado utilizada hoy en dia en el mundo de las comunicaciones digitales, ya que esta se adapta de manera excepcional a la codificación de datos, su versatilidad hace que se utilice en muchas otras técnicas y aplicaciones como la base para la implementación de estas.

Las técnicas que pertenecen a este tipo de cifrado transforman una cadena de bits de longitud fija en una unidad de igual longitud pero inteligible para un posible atacante o tercero no autorizado.

La manera en la que se separan los bloques de bits esta denominado como “modo de operación”, dos de los más utilizados y de los que se hablará a continuación son el “ECB” (Electronic Code-Book) y “CBC” (Cipher-block chaining).

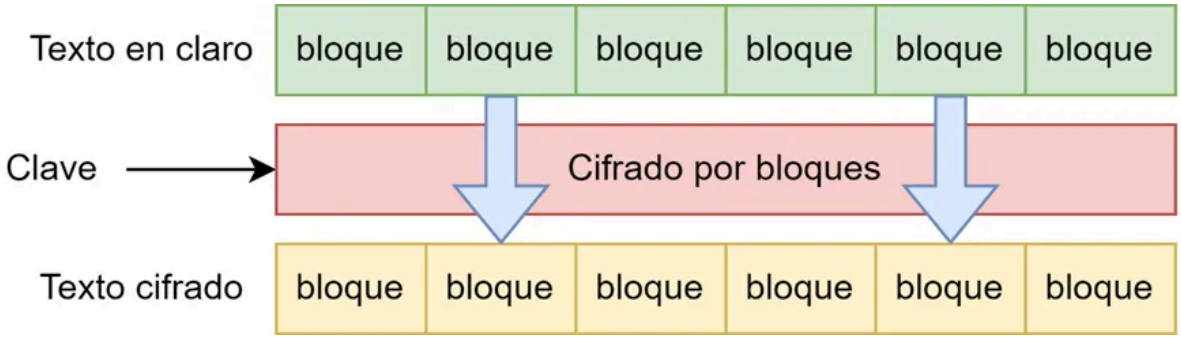

Figura 1. Cifrado en bloques basico

ECB

Este modo de operación es el más simple, ya que se limita a partir el mensaje en bloques y cerrarlos por separado. Se destaca por la posibilidad de romper el mensaje en bloques y cifrarse en paralelo, sin embargo, el hecho de cifrar los bloques por separado implica que cuando se cifre un bloque con cierto valor, siempre se obtendrá el mismo resultado, lo cual hace posible ciertos ataques. Además al ser bloques separados es vulnerable ante la modificación no deseada de partes del mensaje por parte de terceros no autorizados.

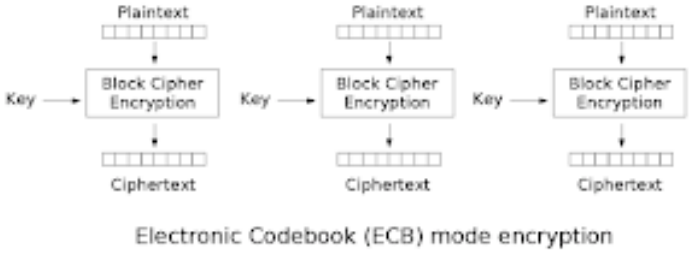

Figura 2. Cifrado con modo ECB

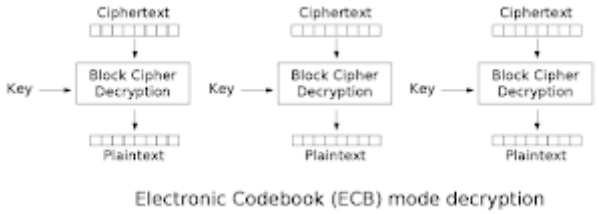

Figura 3. Descifrado con modo ECB

CBC

Este modo de operación es una extensión del ECB, que agrega ciertas medidas para ser más seguro. Se utiliza la división por bloques y se utiliza una operación XOR para combinar el cifrado del bloque anterior con el texto plano del bloque actual. Para realizar esto se utiliza un vector de inicialización, el uso de este vector aumenta la seguridad de este modo de cifrado, por lo que es necesario que este sea aleatorio y no predecible para evitar posibles vulnerabilidades. Una posible desventaja de este modo de operación es su naturaleza secuencial, ya que no es posible paralelizarlo.

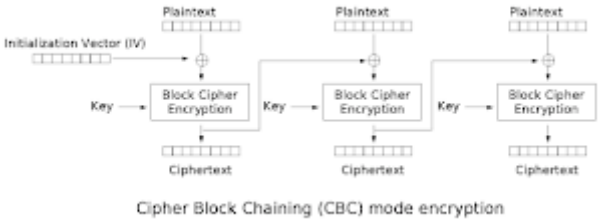

Figura 4. Cifrado con modo CBC

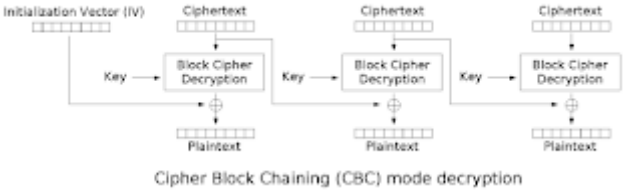

Figura 5. Descifrado con modo CBC

Diferencias entre utilizar el modo ECB y CBC al cifrar información

El modo ECB como se mencionó anteriormente es un modo que es la base para muchas técnicas y modo de operación de cifrados de bloque, este siendo el más básico de todos, por lo que lo hace una herramienta bastante versátil al aplicarse junto a otras técnicas, sin embargo, si el aplicarla como única medida puede resultar en muchas vulnerabilidades de seguridad. Al contrario, el modo CBC es una técnica más segura de cifrado por sí sola, es mucho más aplicable de manera singular, sin embargo no tiene tanta flexibilidad de ser

aplicada a las otras técnicas y modos, ya que se utiliza para su caso de uso específico que probablemente no se adapte a otros modos que no utilicen operaciones XOR para su cifrado.

Referencias Bibliográficas

Osorio, J. (2023). Un Análisis Profundo de los Modos de Cifrado: ECB, CBC. Extraído de: Medium

Ibero, J. (s.f.) El cifrado en bloque, ECB y CBC. Extraido de iberasync.es

Lerch, D. (2007) Modos de cifrado: ECB, CBC, CTR, OFB y CFB. Extraído de blogspot.com