PRÁCTICA: Modos de cifrado en bloque

Objetivo: Modo CBC de operación en cifrado en bloque (usando AES).

Desarrollo:

En el modo CBC, cada bloque de texto en claro se combina antes de cifrarse mediante un XOR con el bloque previo de texto cifrado. De esta forma, cada bloque de texto cifrado depende de todos los bloques de texto en claro anteriores.

Implementación:

En esta práctica debes implementar el modo de cifrado CBC usando para ello el cifrado en bloque AES.

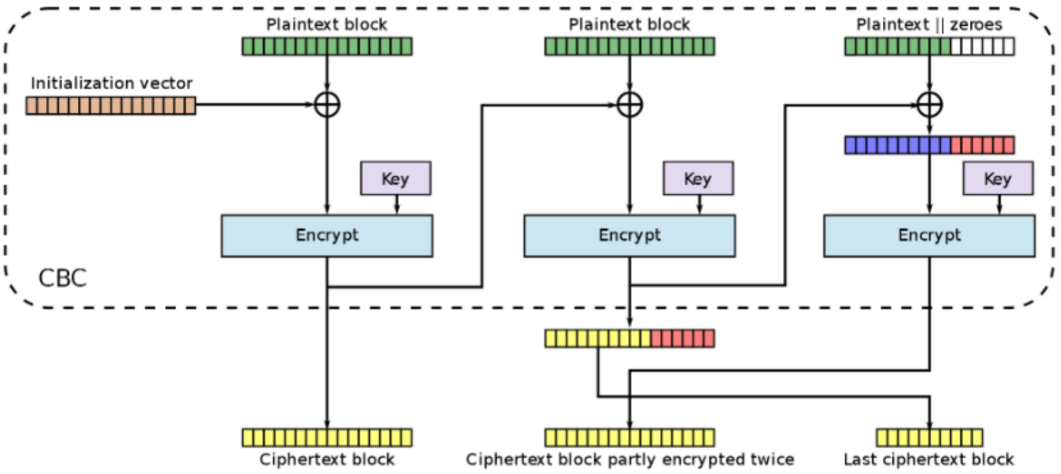
Ejemplo 1:
Entrada:

Clave: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Bloque 1 de Texto Original: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
Bloque 2 de Texto Original: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Salida:

Bloque 1 de Texto Cifrado: 69 C4 E0 D8 6A 7B 04 30 D8 CD B7 80 70 B4 C5 5A
Bloque 2 de Texto Cifrado: 4F 63 8C 73 5F 61 43 01 56 78 24 B1 A2 1A 4F 6A

Opcional: Cipher stealing es una técnica que se suele usar cuando la longitud del mensaje no es múltiplo de la longitud del bloque. Consiste en modificar el procesamiento de los dos últimos bloques de forma que un trozo del penúltimo bloque cifrado se usa para completar el último bloque de texto antes de cifrarlo. El texto cifrado final, para los últimos dos bloques, consiste en el bloque final cifrado, más el penúltimo bloque parcial (con la porción "robada" omitida).



Ejemplo Opcional:
Entrada:

Clave: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Bloque 1 de Texto Original: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
Bloque 2 de Texto Original: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 --

Salida:

Bloque 1 de Texto Cifrado: 4F 63 8C 73 5F 61 43 01 56 78 24 B1 A2 1A 4F 6A
Bloque 2 de Texto Cifrado: 69 C4 E0 D8 6A 7B 04 30 D8 CD B7 80 70 B4 C5 --