Cipher-block chaining (CBC)

Ing. Max Alejandro Antonio Cerna Flores

Agenda

- Elementos requeridos
- ¿Cómo funciona?
- Desventajas y Vulnerabilidades

Elementos Requeridos

Operación XOR

Vector de Inicialización

Clave

Texto plano o mensaje

Método de cifrado de bloque.

¿Cómo funciona?

1. Se define el tamaño del bloque. (ej: 64 bits - 8 caracteres en ASCII)
2. Se define mensaje y clave:

   Mensaje: batallas anonimas **clave:** integras - 69 6E 74 65 67 72 61 73

3. Se separa el mensaje en bloques de longitud definida.

   bloque 1: batallas - 62 61 74 61 6C 6C 61 73

   bloque 2: anonimas - 61 6E 6F 6E 69 6D 61 73

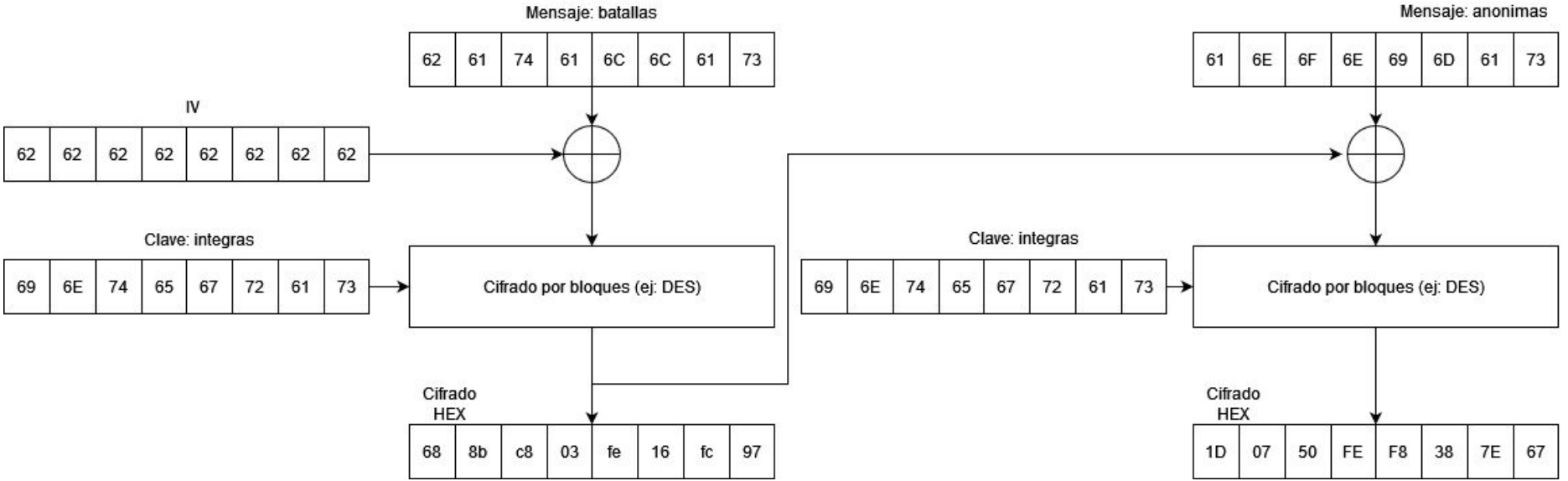
4. Se define IV aleatorio de longitud del bloque (ej: 64 bits).

   62 62 62 62 62 62 62 62

5. Escoger método de cifrado por bloques: **DES**

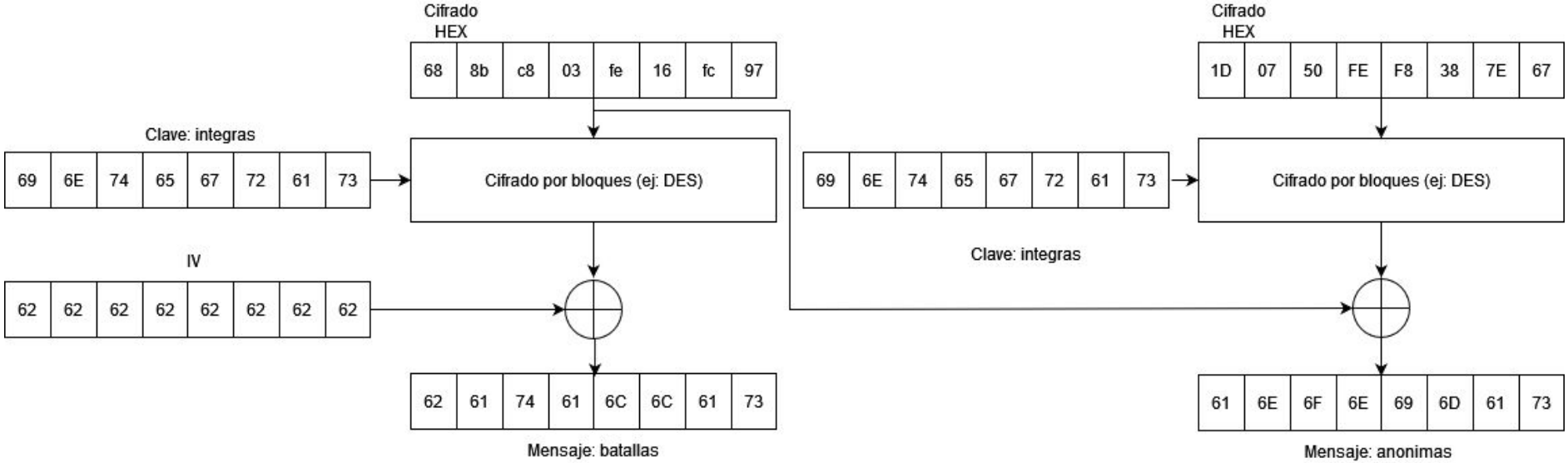
¿Cómo funciona?

Cifrado



¿Cómo funciona?

Descifrado



Desventajas y Vulnerabilidades

- Al ser un método secuencial, no es funcional para ser resuelto en paralelo.
- No permite hacer cambios rápidos en la información cifrada.
- Propagación de errores: Un solo bit erróneo durante la transmisión de un bloque provocará el descifrado incorrecto del bloque siguiente.
- Vulnerable a ataques de oráculo de relleno.

Desventajas y Vulnerabilidades

“Un atacante puede usar un oráculo de relleno, en combinación con la manera de estructurar los datos de CBC, para enviar mensajes ligeramente modificados al código que expone el oráculo y seguir enviando datos hasta que el oráculo indique que son correctos. Desde esta respuesta, el atacante puede descifrar el mensaje byte a byte.” - ***Vulnerabilidades de temporalización con descifrado simétrico en modo CBC al usar el relleno***

https://learn.microsoft.com/es-es/dotnet/standard/security/vulnerabilities-cbc-mode