Output Feedback (OFB)

Ing. Max Alejandro Antonio Cerna Flores

Agenda

- Elementos requeridos
- ¿Cómo funciona?
- Desventajas

Elementos Requeridos

Operación XOR

Vector de Inicialización

Clave

Texto plano o mensaje

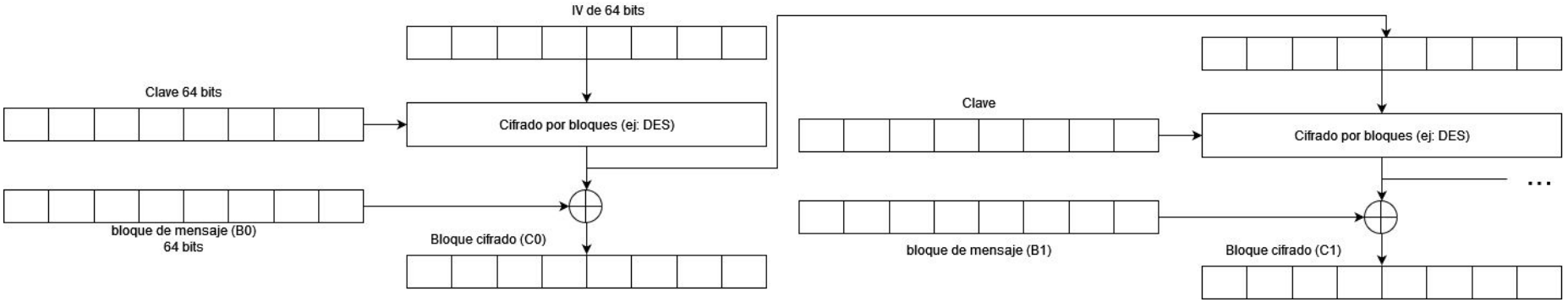
Método de cifrado de bloque.

¿Cómo funciona?

1. Se define el tamaño del bloque. (ej: 64 bits - 8 caracteres en ASCII).
2. Se define mensaje y clave a utilizar.
3. Se separa el mensaje en bloques (ej: 64 bits).
4. Se define IV aleatorio de longitud del bloque (ej: 64 bits).
5. Escoger método de cifrado por bloques: **DES**

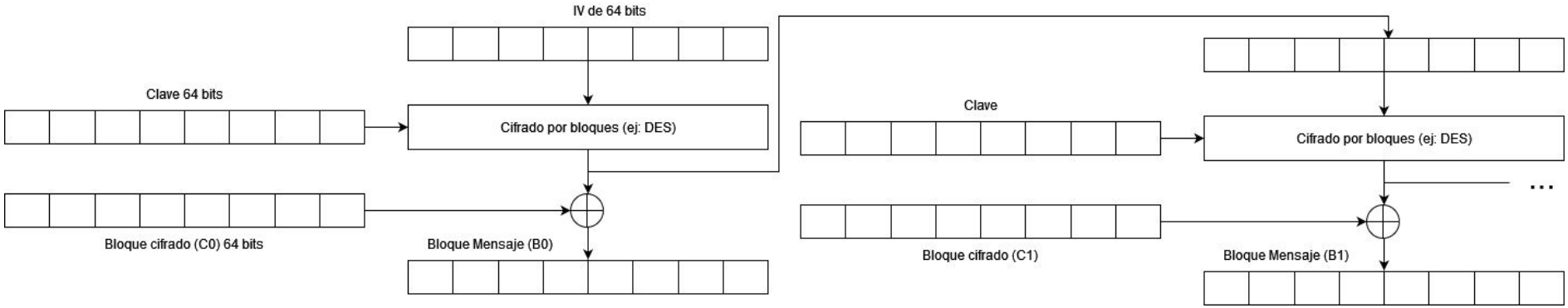
¿Cómo funciona?

Cifrado



¿Cómo funciona?

Descifrado



Ventajas y Desventajas

- El error de propagación de bit corrupto se resuelve en este modo, ya que está libre de errores de bit en el bloque de texto plano.
- No se puede realizar en paralelo.
- Las operaciones de cifrado de bloques se pueden realizar con anticipación, lo que permite que el paso final se realice en paralelo una vez que el texto o el texto cifrado esté disponible.