Cipher Feedback (CFB) Full-Block

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:

   Mensaje: cuaderno continuo **clave:** practico - 70 72 61 63 74 69 63 6F

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

   bloque 1: cuaderno - 63 75 61 64 65 72 6E 6F

   bloque 2: continuo - 63 6F 6E 74 69 6E 75 6F

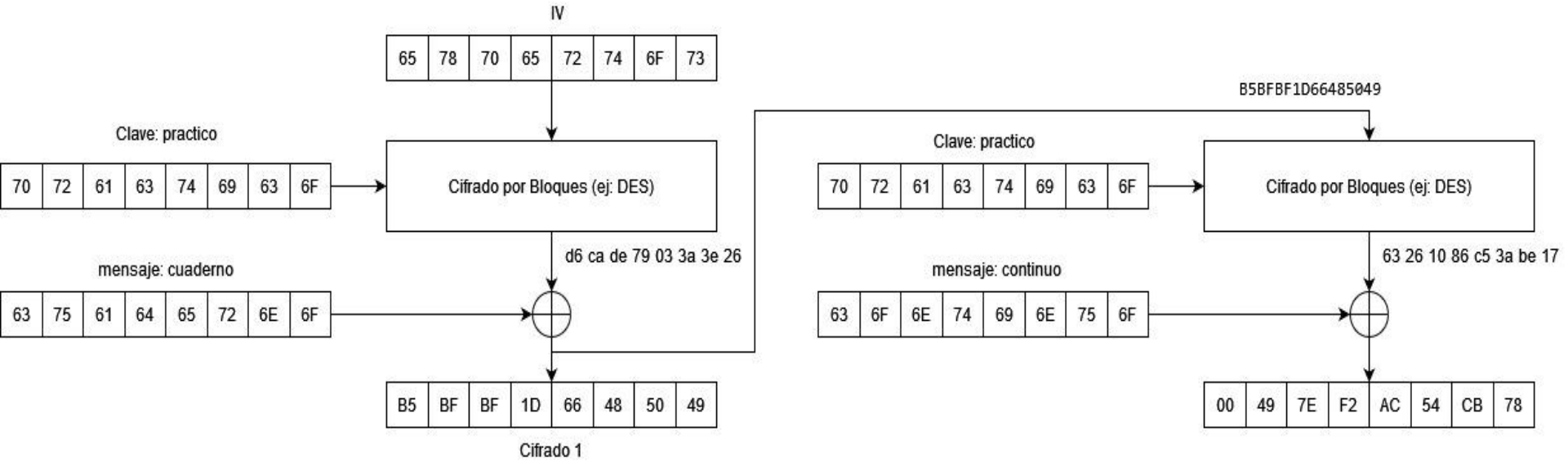
4. Se define IV aleatorio de longitud del bloque (ej: 64 bits).

   65 78 70 65 72 74 6F 73

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

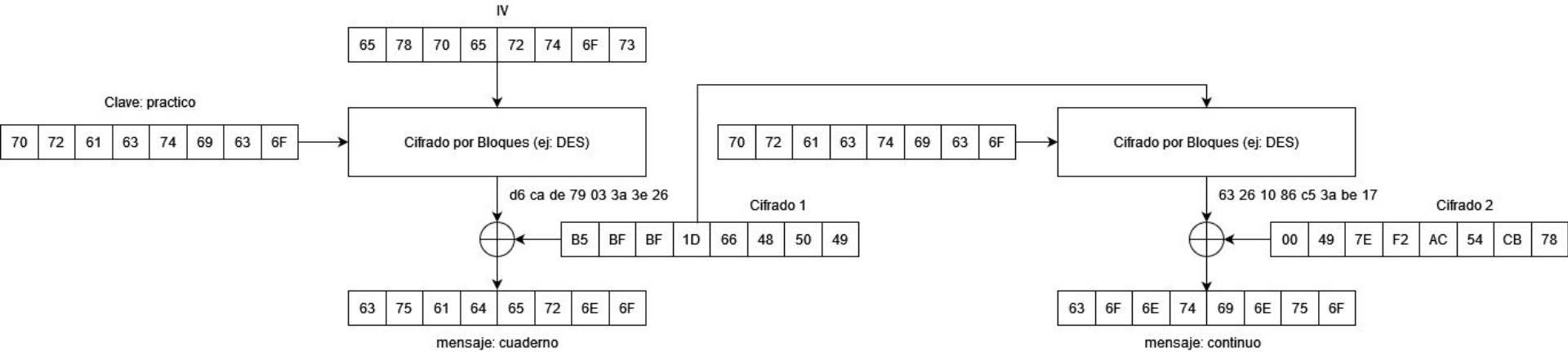
¿Cómo funciona?

Cifrado



¿Cómo funciona?

Descifrado



Desventajas

- 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.