Cipher Feedback (CFB)

Ing. Max Alejandro Antonio Cerna Flores

Agenda

- Elementos requeridos
- ¿Cómo funciona?
- Desventajas

Elementos Requeridos

Operación XOR

Vector de Inicialización

Clave

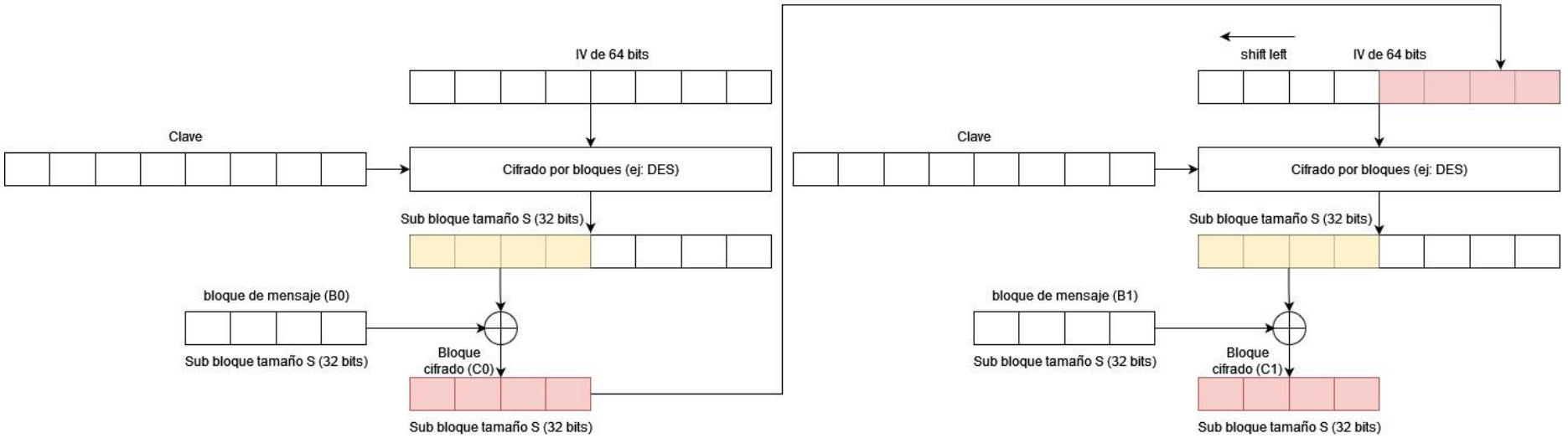
Texto plano o mensaje

Método de cifrado de bloque.

¿Cómo funciona?

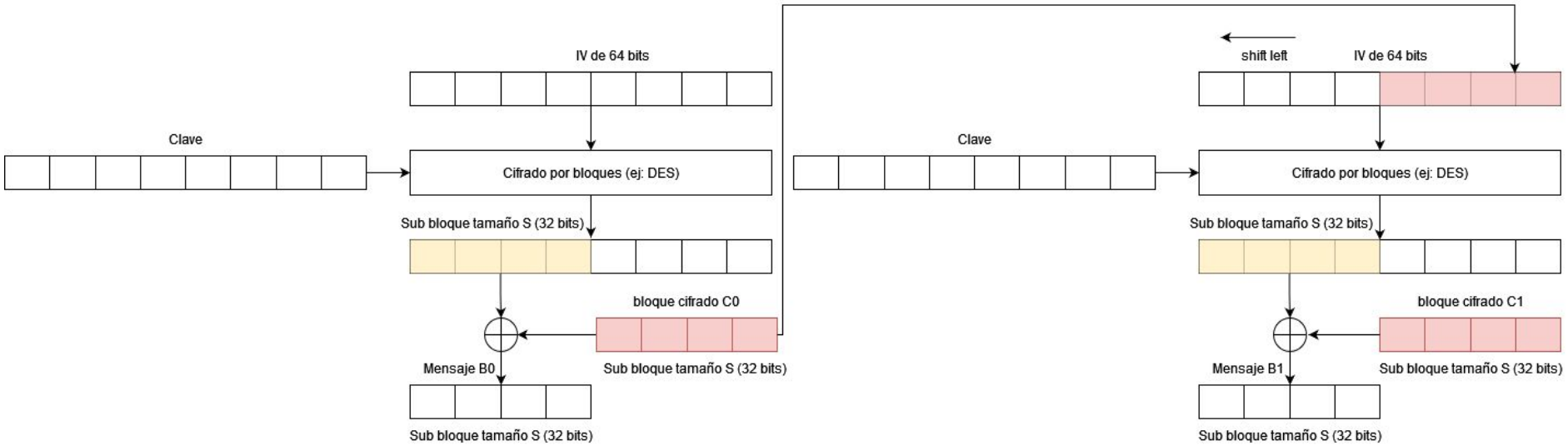
1. Se define el tamaño del bloque. (ej: 64 bits - 8 caracteres en ASCII).
2. Se define un tamaño del sub-bloque **“s”** (1 < s < bloque) ej: 32 bits.
3. Se define mensaje y clave a utilizar.
4. Se separa el mensaje en bloques de longitud “s” (ej: 32 bits).
5. Se define IV aleatorio de longitud del bloque (ej: 64 bits).
6. Escoger método de cifrado por bloques: **DES**

¿Cómo funciona?



¿Cómo funciona?

Descifrado



Ventajas y Desventajas

- Dado que existe cierta pérdida de datos debido al uso del registro de desplazamiento, es difícil aplicar el criptoanálisis.
- El error de transmisión se propaga debido al cambio de bloques.