Historia de Criptografía

Bit Shift:

Bitshift (desplazamiento de bits) es una operación que mueve los bits de un número binario hacia la izquierda o hacia la derecha. No es un algoritmo complejo por sí solo, sino una técnica fundamental usada en muchos algoritmos y sistemas computacionales.

Ejemplo de aplicación de Bit shift:

Supongamos que quieres "cifrar" la palabra **"Hola"** usando Bit Shift. El proceso sería:

Paso 1 — Convertir a binario (como ya lo hacemos en el script):

- H = 01001000
- o = 01101111
- l = 01101100
- a = 01100001

Paso 2 — Aplicar Shift Izquierda 2 posiciones a cada byte:

Cada grupo de 8 bits se mueve 2 posiciones hacia la izquierda, los 2 bits que salen por la izquierda se pierden y entran 2 ceros por la derecha:

H: 01001000 → 00100000 (los "01" salen, entran "00")

o: 01101111 → 10111100

l: 01101100 → 10110000

a: 01100001 → 10000100

Paso 3 — Para descifrar, haces Shift Derecha 2 posiciones y recuperas los bits originales.

Bit shift lo elegí porque:

- Es simple de implementar y entender
- Es extremadamente rápido

Ventajas:

- Alta velocidad
- Base de muchos algoritmos modernos

- Implementación sencilla
- Bajo consumo de memoria

Vulnerabilidades:

- No es seguro por sí solo
- Predecible (fácil de revertir)
- No provee confidencialidad real
- Vulnerable a análisis criptográfico