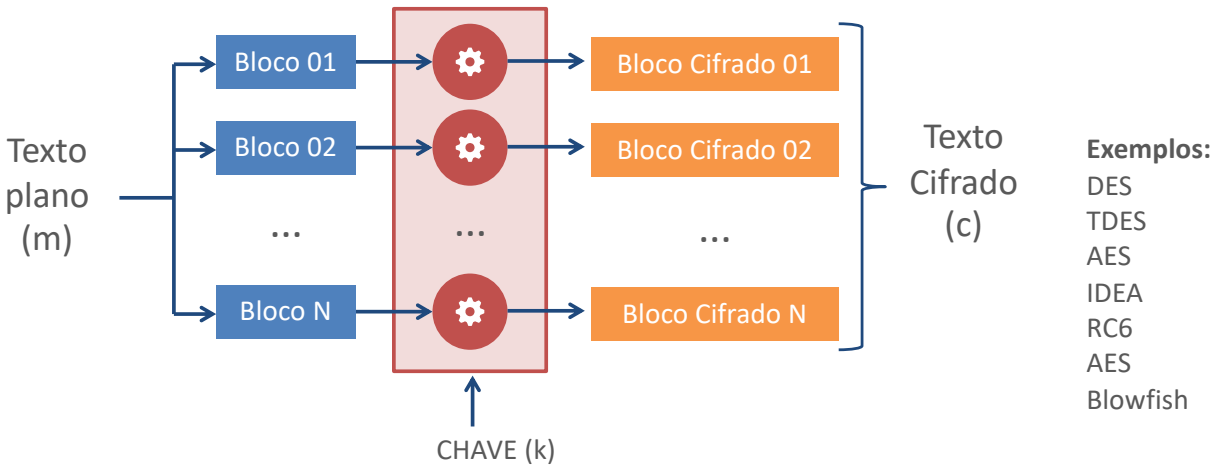
Cifras de bloco

- Cifra um conjunto de símbolos como um único bloco.
- O tamanho do bloco pode variar
  (64 bits no DES, 128 bits no AES, etc.).
- Cada bloco é cifrado de forma independente.

Cifras de bloco



Exemplos:
DES
TDES
AES
IDEA
RC6
AES
Blowfish

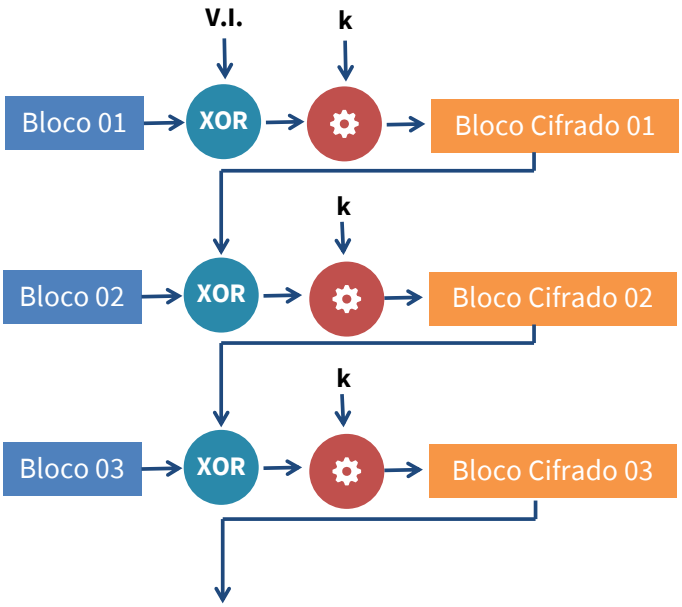
Cifras de bloco

- Se o mesmo bloco se repetir, os blocos cifrados serão iguais, facilitando a percepção de um padrão.
- Para evitar isso, existem algumas técnicas como a **realimentação**, em que o bloco anterior é usado na cifragem do bloco atual

Cifras de bloco por encadeamento

CBC (Cypher Block Chaining)

- Faz-se um XOR do bloco plano atual com o bloco cifrado anterior
- Para o primeiro bloco (sem bloco anterior), é feito um XOR com um vetor de inicialização (V.I.)



Cifras de bloco

VANTAGENS

- **Alta difusão**
  A informação de um símbolo é distribuída entre vários símbolos do texto cifrado.
- **Imunidade a alterações**
  É difícil inserir símbolos no texto cifrado sem detecção.

DESVANTAGENS

- **Baixa velocidade**
  Um bloco inteiro deve ser acumulado antes da cifragem ou decifragem começar.
- **Propagação de erros**
  O erro em um símbolo pode corromper todo o bloco.