# Modos de Operação de Cifras

Valério Rosset

Adaptado de: Cryptography and Network Security Fourth Edition by William Stallings and slides by Lawrie Brown

# Modos de Operação

- Cifradores de Bloco encriptam blocos de tamanho fixo
  - eg. DES com blocos de 64-bit blocks e chave de 56-bits
- Necessidade de (de)cifrar diferents tamanhos de dados
- Existem 5 modos de cifras definidos pelo NIST para o AES e DES: contendo modos de operação de bloco e de fluxo.

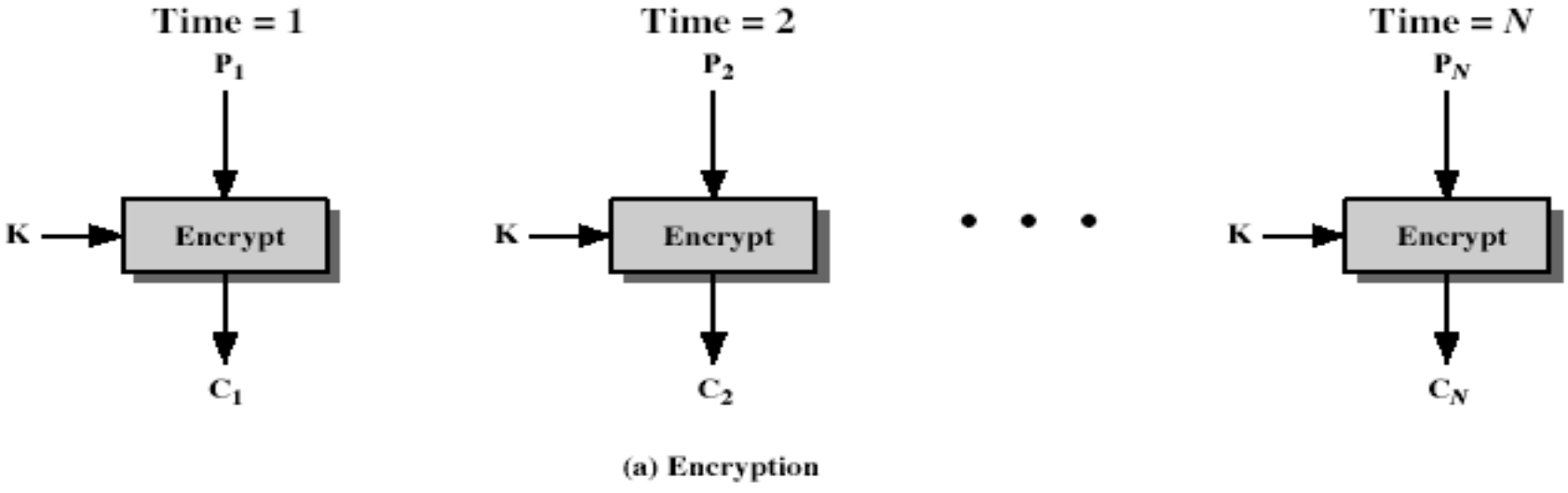
# Electronic Codebook Book (ECB)

- Mensagem é quebrada em blocos independentes para a cifragem.
- Cada bloco cifrado é único para cada bloco original, usando a mesma chave.
- Cada bloco então é cifrado de maneira independente

$$C_i = DES_{K1}(P_i)$$

- Uso: transmissão de valores únicos.

# Electronic Codebook Book (ECB)



# Vantagens e limitações do ECB

- Repetições podem aparecer no texto cifrado
  - Dois blocos consecutivos
  - Particularmente em imagens
  - Ou com mensagens estruturadas que mudam muito pouco
- Fraqueza está na cifragem independente dos blocos.

# Cipher Block Chaining (CBC)

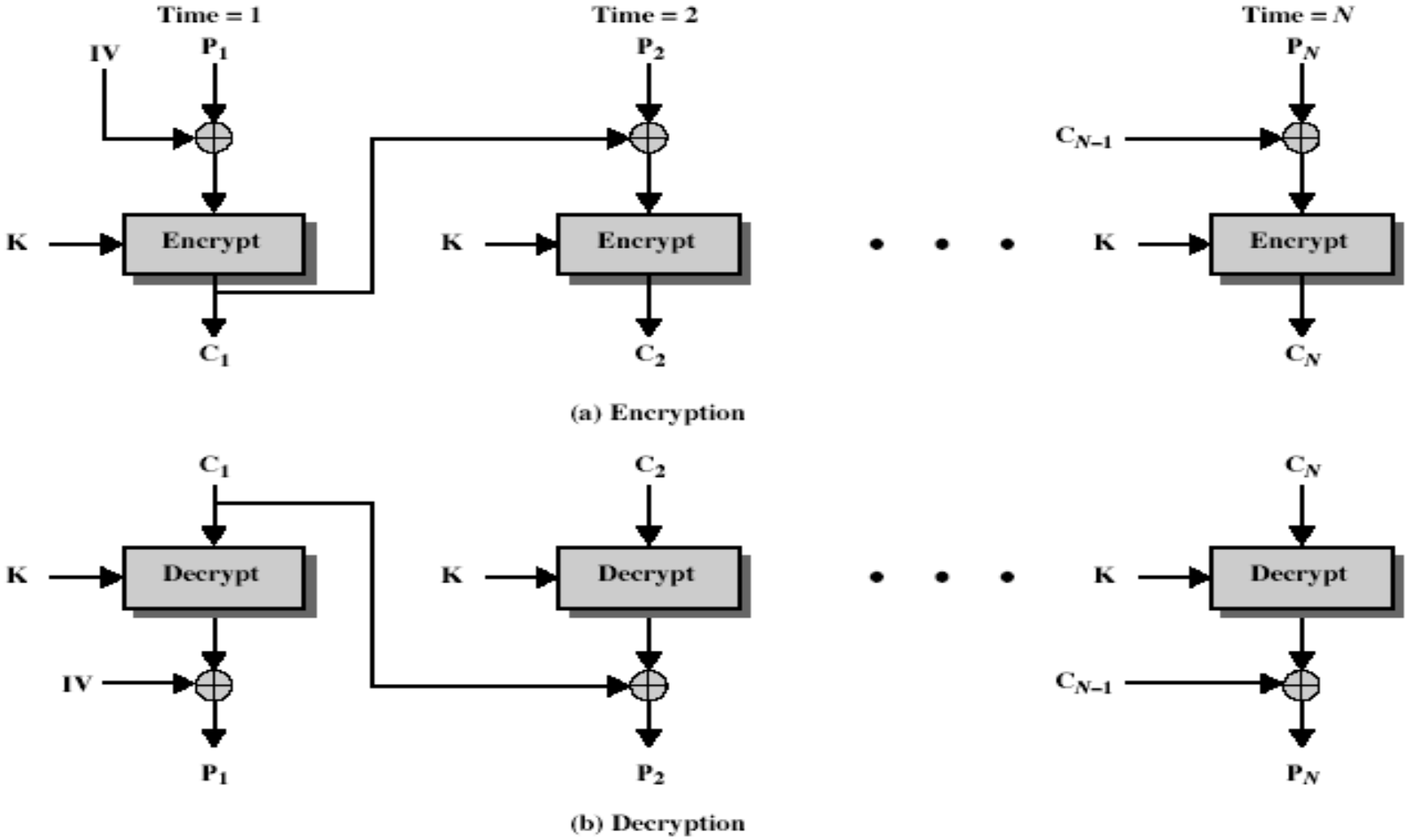
- Mensagem é quebrada também em blocos
- Blocos são ligados durante o processo de cifragem
- Cada bloco cifrado anterior é chaveado com o bloco de texto claro a ser cifrado.
- usa o Initial Vector (IV) para iniciar

$$C_i = DES_{K1}(P_i \text{ XOR } C_{i-1})$$

$$C_{-1} = IV$$

- Uso: Cifragem em massa, autenticação

# Cipher Block Chaining (CBC)



# Advantages and Limitations of CBC

- Um bloco cifrado depende de todod os blocos anteriores
- Qualquer mudança no bloco se propaga para os seguintes
- Necessita do **Initialization Vector** (IV)
  - Precisa ser conhecido pelo: sender & receiver
  - Não pode ser nulo, e pode ter valor fixo ou
  - Enviado com o uso de ECB antes da mensagem de dados.

# Message Padding

- Importante para completar possíveis blocos de dados menores que o esperado pelo cifrador de bloco.
  - Completar o último bloco com valores nullos (eg nulls)
  - Completar o último bloco com um contador de tamanho de pad
    - eg. [ b1 b2 b3 0 0 0 0 5]
    - means have 3 data bytes, then 5 bytes pad+count

# Cipher FeedBack (CFB)

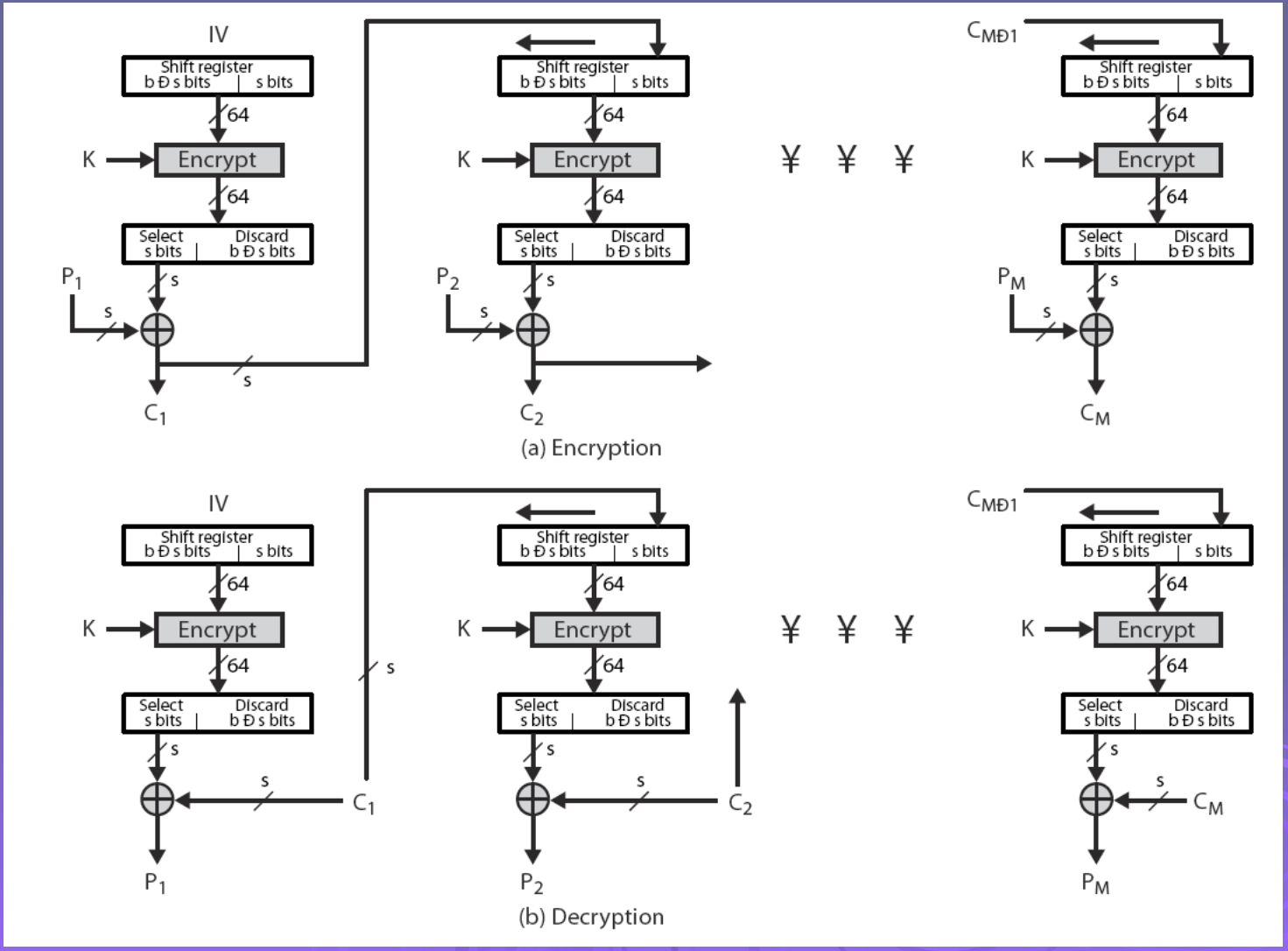
- Mensagem é tratada com o um fluxo de bits
- Adicionada a saída do cifrador de blocos
- O resultado final alimenta o próximo estágio (cipher feedback)
- Permite tamanho arbitrário de bits (1,8, 64 or 128 etc)
  - Definido como: CFB-1, CFB-8, CFB-64, CFB-128 etc
- Mais eficiente usando todos os bits do bloco (64 or 128)

$$C_i = P_i \text{ XOR } DES_{K1}(C_{i-1})$$

$$C_{-1} = IV$$

- USo: cifragem de fluxos, autenticação

# Cipher FeedBack (CFB)



# Advantages and Limitations of CFB

- Apropriado quando dados chegam em bits/bytes
- Limitação é ter que esperar pelo cifrador de blocos em cada estágio.
- Usa apenas o modo cifragem do cifrador de blocos.
- Erros se propagam por vários blocos

# Output FeedBack (OFB)

- Messagem é tratada com um fluxo de bits/bytes
- output do cifrador é adicionado a mensagem (output feedback)
- feedback é independente da mensagem
- Pode ser pré-computado

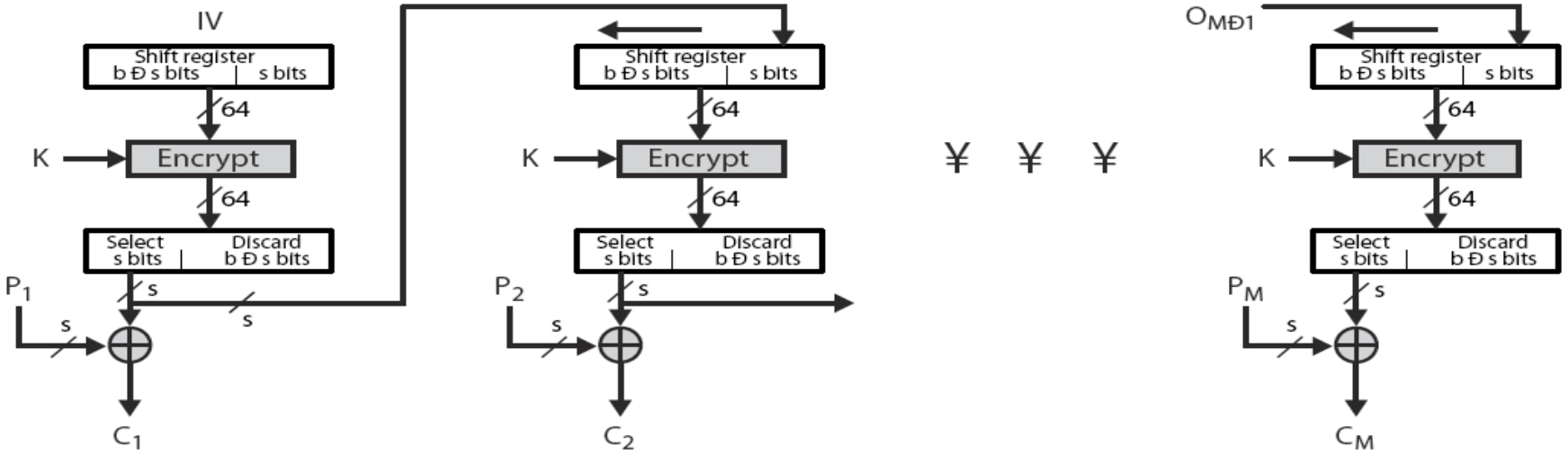
$$C_i = P_i \text{ XOR } O_i$$

$$O_i = DES_{K1}(O_{i-1})$$

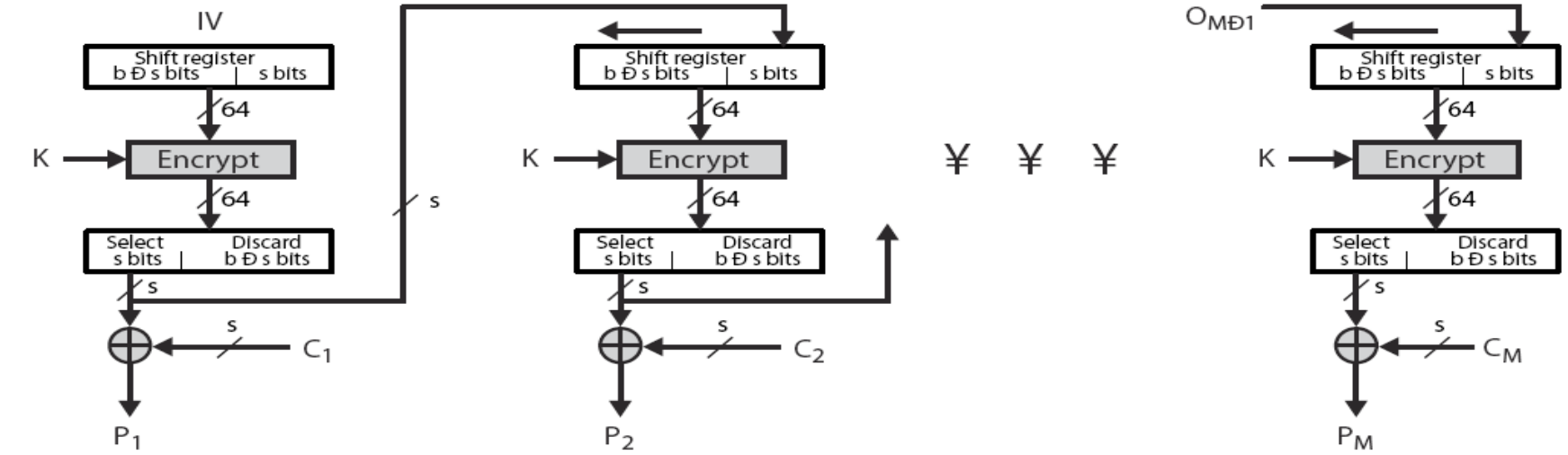
$$O_{-1} = IV$$

- uses: cifragem de fluxo em canais com ruído

# Output FeedBack (OFB)




(a) Encryption




(b) Decryption

# Advantages and Limitations of OFB

- Erros de bit não se propagam
- 
- Mais vulnerável a modficação
- 
- sender & receiver precisam de sincronismo

# Counter (CTR)

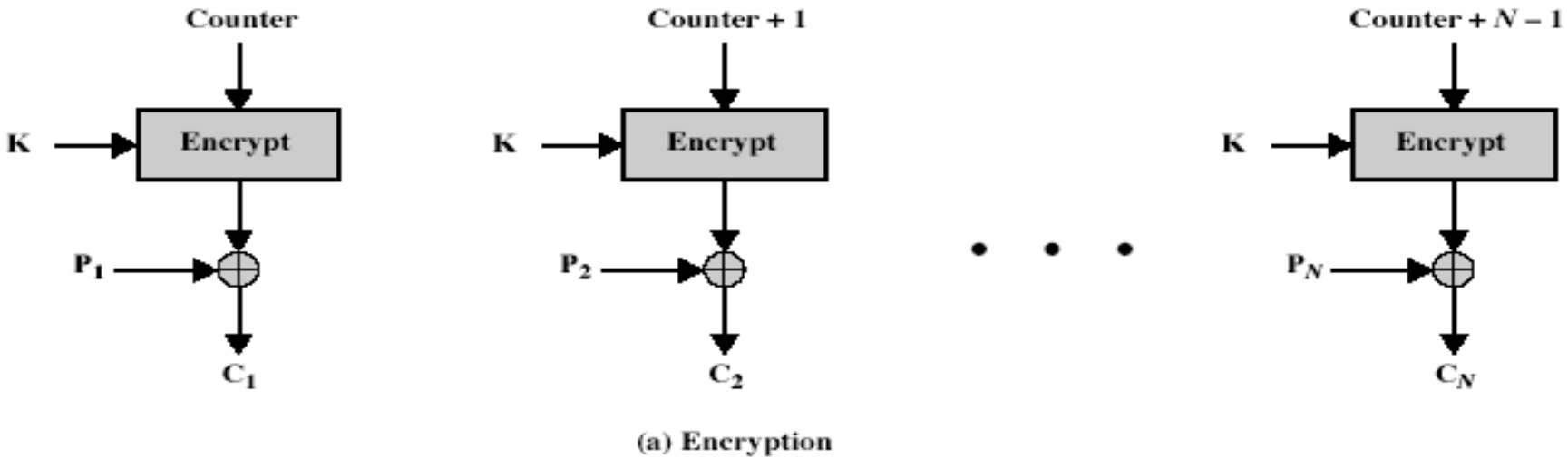
- Similar ao OFB usando um valor de contador em cada estágio ao invés de um feedback.
- Precisa de uma chave e contador diferentes para cada bloco

$$C_i = P_i \text{ XOR } O_i$$

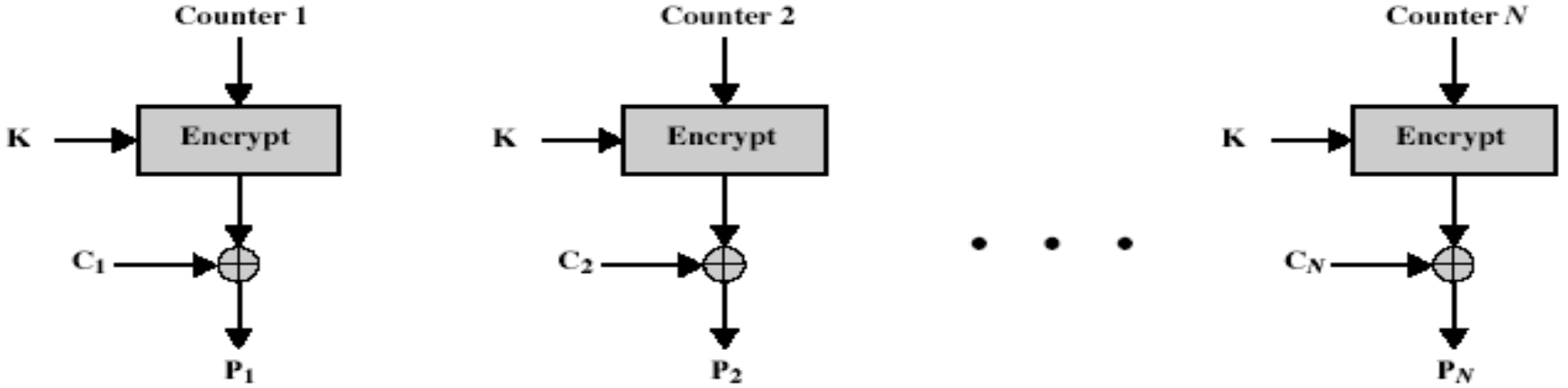
$$O_i = DES_{K1}(i)$$

- uso: high-speed network encryptions

# Counter (CTR)




(a) Encryption



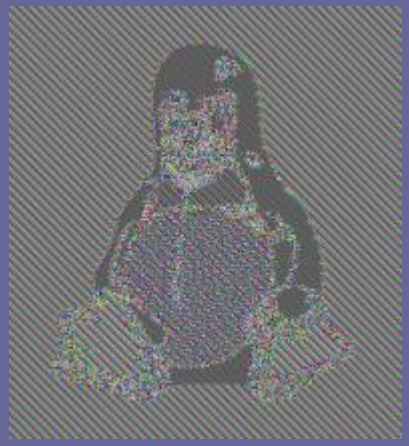

(b) Decryption

# Vantagens e Limitações do CTR

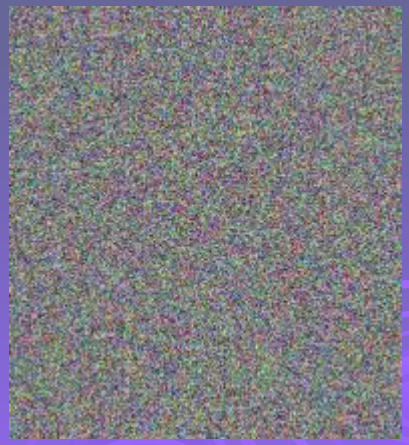
- Eficiência
  - Pode cifrar paralelamente em h/w ou s/w
  - Pode ser pré-processado
  - Bom para links de alta velocidade
- Acesso aleatório a blocos de dados
- Segurança compatível com outros modos desde que assegurado o não reuso do contador por razões de quebra da cifra.

# Exemplo de Resultado com Diferentes Modos de Cifra

ECB



CBC ou outro



# Atividade

- Implemente o modo ECB, CBC e CRT e use-os com o S-DES  para cifrar uma imagem de sua escolha. Depois compare os resultados com o descrito no slide anterior.