Cifras de bloco
Modos de operação

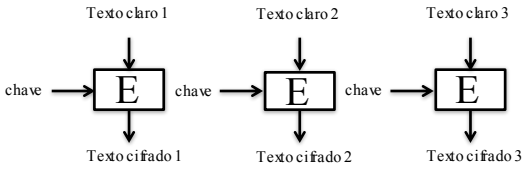
Prof. Dr. Avelino Francisco Zorzo
Faculdade de Informática – PUCRS

Modos de operação

- Um modo de operação define como uma cifra de bloco é aplicada para cifrar uma mensagem.
- Alguns exemplos de modos de operação
  - *Electronic code book mode* (ECB)
  - *Cipher Block Chaining mode* (CBC)
  - *Cipher feedback mode* (CFB)
  - *Output feedback mode* (OFB)
  - *Counter mode* (CTR)

Modo 1: *Electronic Codebook*

- O modo de operação mais simples

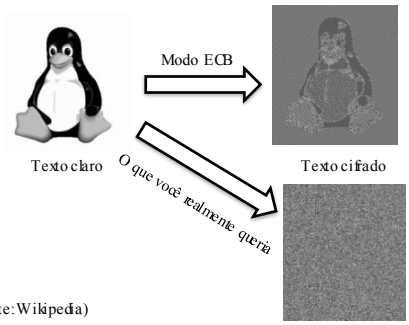


$Texto\ cifrado\ 1 = E(k, Texto\ claro\ 1)$ $Texto\ claro\ 1 = D(k, Texto\ cifrado\ 1)$

Propriedades do ECB

- ECB: operação determinísitica
  - mesmo bloco de texto claro na entrada → mesma saída
- Problemático na prática

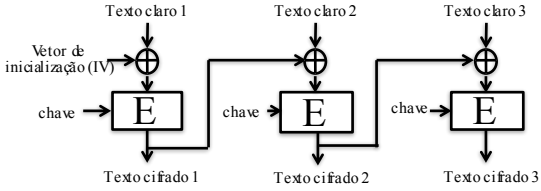
Vazamento de informação



(Fonte: Wikipedia)

Modo 2: *Cipher Block Chaining*

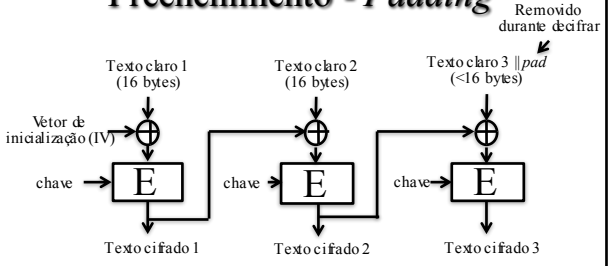
- Um dos modos mais usados



$Texto\ cifrado\ 1 = E(k, IV \oplus Texto\ claro\ 1) \Rightarrow Texto\ claro\ 1 = \boxed{D(k,\ Texto\ cifrado\ 1) \oplus IV}$

E o i-ésimo bloco?

Preenchimento - *Padding*



PKCS7: para n>0, n byte *pad* é: n n n n .. n

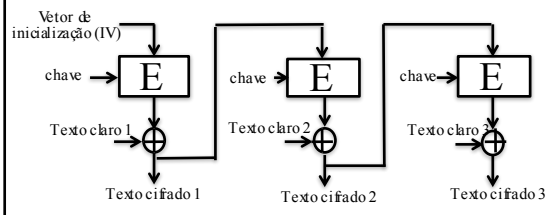
Pergunta: o que acontece se a mensagem é múltipla do tamanho do bloco?

Propriedades do CBC

- Devido ao IV aleatório, a mesma mensagem de entrada pode gerar diferentes saídas (ótimo!!)
- Se um bloco do texto claro mudar, então todos os blocos to texto cifrado subsequentes serão afetados
  - Será uma propriedade útil para gerar um código de autenticação de mensagem (*MAC*)
- Se todo um bloco de texto cifrado for perdido, CBC consegue se recuperar (mas não se somente um byte for perdido)
- Cifrar não pode ser paralelizada (ruim!!)

Modo 3: *Cipher feedback*

- Transforma uma cifra de bloco em uma cifra de fluxo

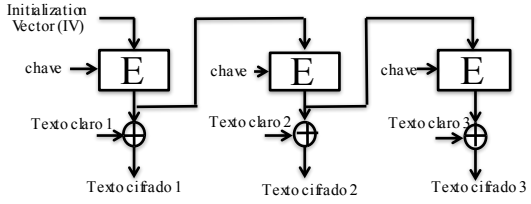


Propriedades do CFB

- Se um bloco inteiro do texto cifrado for perdido, CFB consegue se recuperar.
- Mas se um byte ou um bit é perdido, CFB não se recupera – dados não podem ser decifrados.
- Somente a operação de cifrar é usada.
- Não é possível cifrar paralelamente.
- Mas é possível decifrar paralelamente
  - Por que e como?

Modo 4: OFB mode

- Essencialmente, uma cifra de fluxo

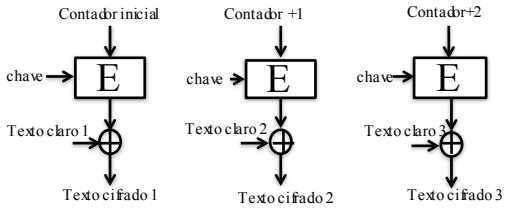


Propriedades do OFB

- As operações de cifrar e decifrar são exatamente as mesmas (assim como na cifra de uso único)

Modo 5: *Counter* (CTR)

- Se tornando muito popular (trocar CBC)



Propriedades do CTR

- Assim como o OFB, CTR é essencialmente uma cifra de fluxo
- As operações de cifrar e decifrar são as mesmas.
- É possível paralelizar as duas operações (uma grande vantagem sobre o CBC)

Fim.