UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança da Informação
Aula 5 – Criptografia. Objetivos e Tipos. Cifras de Bloco e Fluxo

Prof. Dr. Eng. Fred Sauer

fsauer@gmail.com

http://www.fredsauer.com.br

Criptografia
Introdução: Criptologia

- Criptologia = Criptografia + Criptoanálise.
- Criptografia = Métodos e protocolos para segurança de informação.
- Criptoanálise = Testar e validar métodos criptográficos.

- Do grego, *kryptós, que significa "escondido"*
- *gráphein, que significa "escrita"*

- A história registra o uso de criptografia desde os tempos do Império Romano.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Introdução

- Criptografar (encriptar)
- Decriptografar (decriptar)
- Algoritmo
- Chaves
- Tamanho da Chave

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Objetivos

- Confidencialidade das mensagens
- Integridade de dados
- Identificação de entidades
- Autenticação de mensagens
- Autorização e Controle de acesso
- Certificação
- Anonimato
- Não-repúdio

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Fatores de Sucesso

- A confidencialidade das chaves.
- A dificuldade de adivinhar as chaves.
- A dificuldade de inverter o algoritmo de criptografia sem saber a chave.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Por dentro das operações: XOR

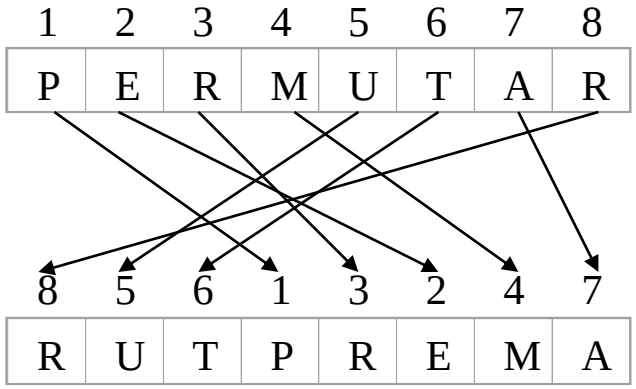
- Ou exclusivo (eXclusive OR): operandos diferentes resultam em “1” ; operandos iguais resultam em “0”
- Tabela-verdade:

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

- Reversibilidade: $a \oplus b \oplus a = b, \forall a, b$

Criptografia
Por dentro das operações: Permutação

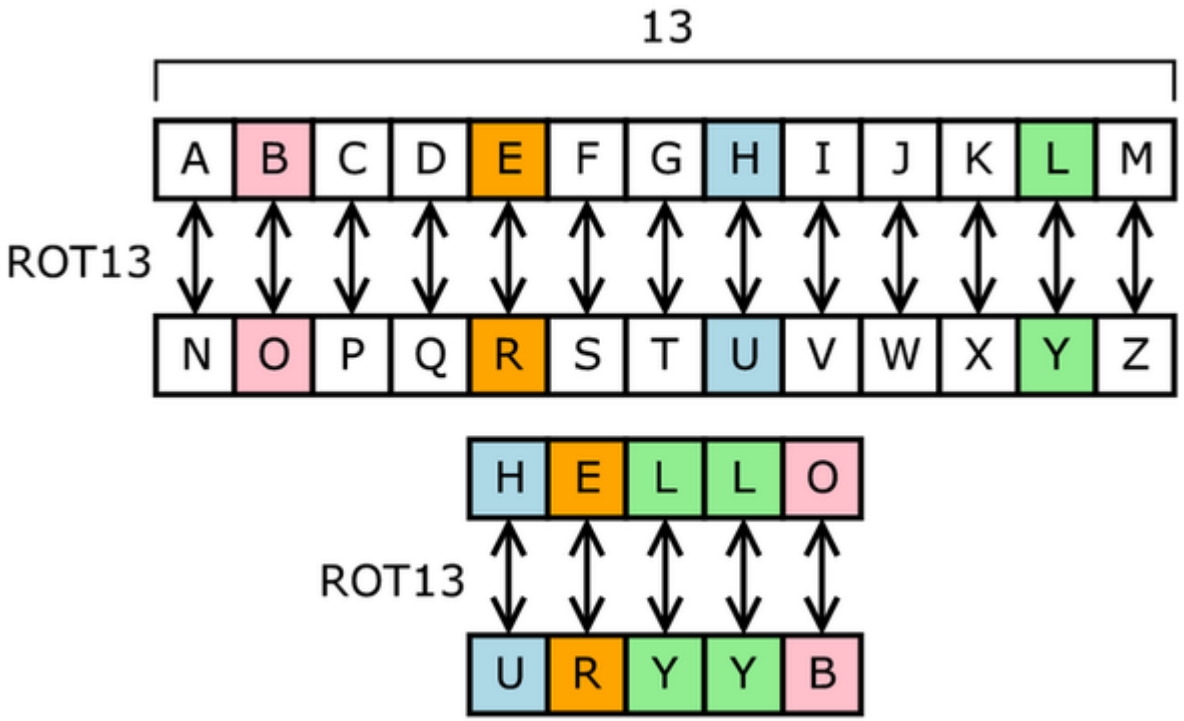
- Modificação na organização de um conjunto de valores
- Os valores são mapeados para outras posições
- Ex.:



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Por dentro das operações: Substituição

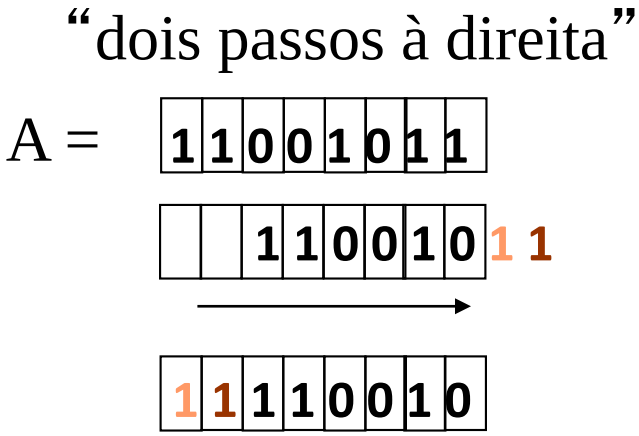
- Substituição de um conjunto de valores por outro
- Só funciona se as substituições forem variáveis e imprevisíveis



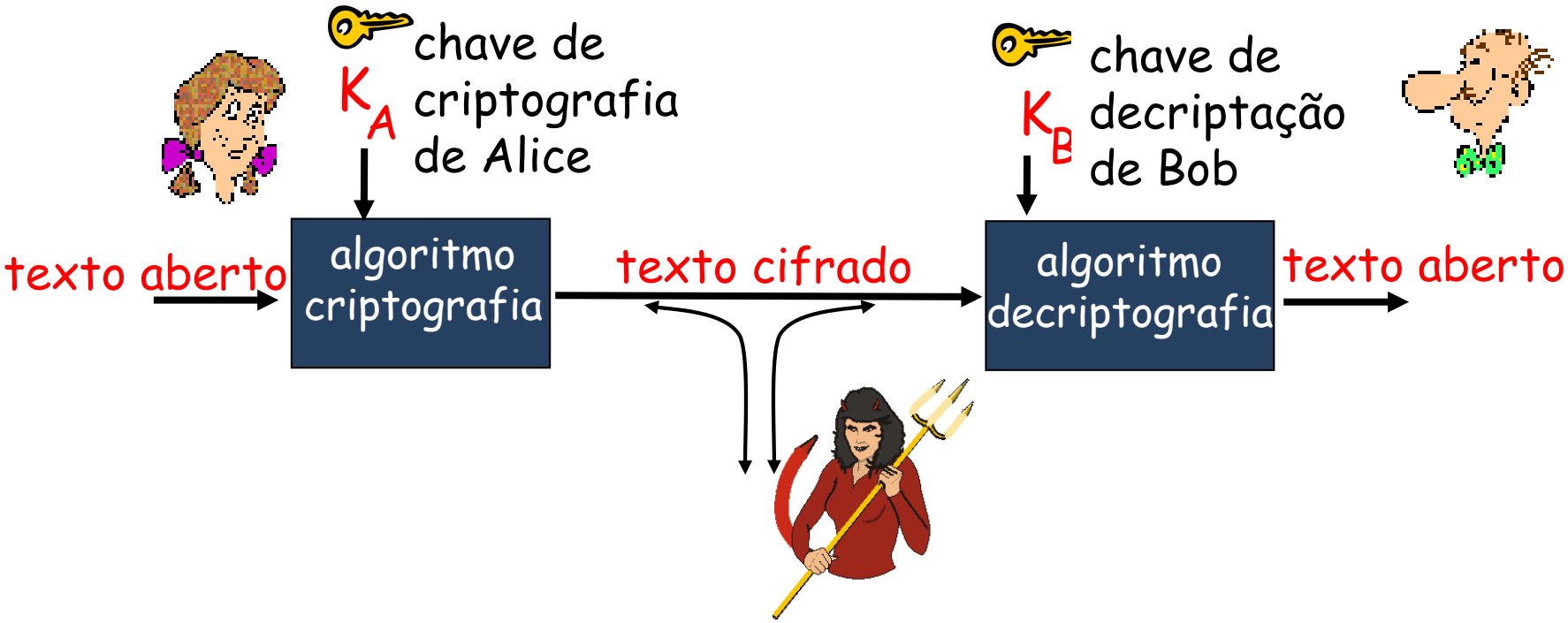
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Por dentro das operações: Rotação

- Deslocamento de bits (shift)
- Rotação circular (direita ou esquerda):
  - os bits mais extremos são movidos para o outro lado (se estão no fim, aparecem no início e vice-versa)
- Ex.: A >> 2 (rotação circular à direita)



A linguagem da criptografia



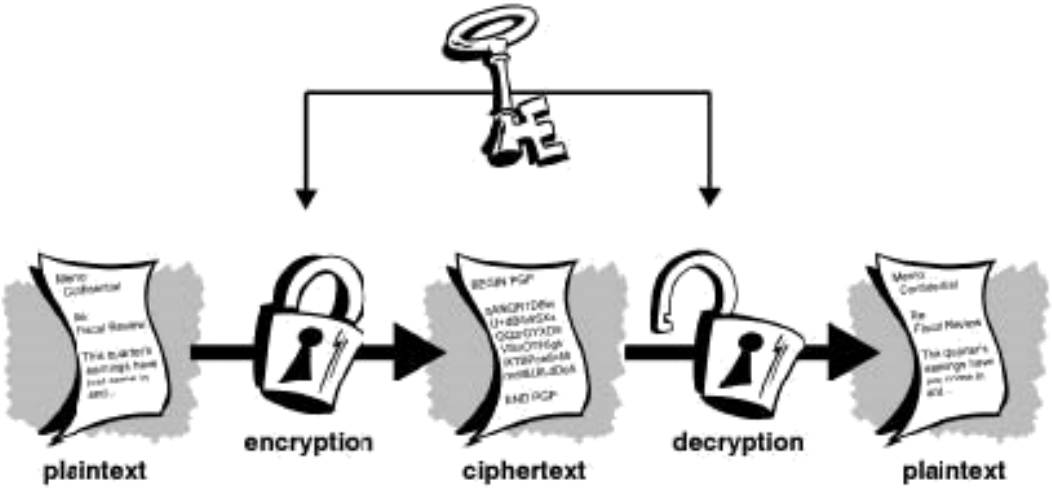
m mensagem em texto aberto

$K_A(m)$ texto cifrado, criptografado com chave K_A

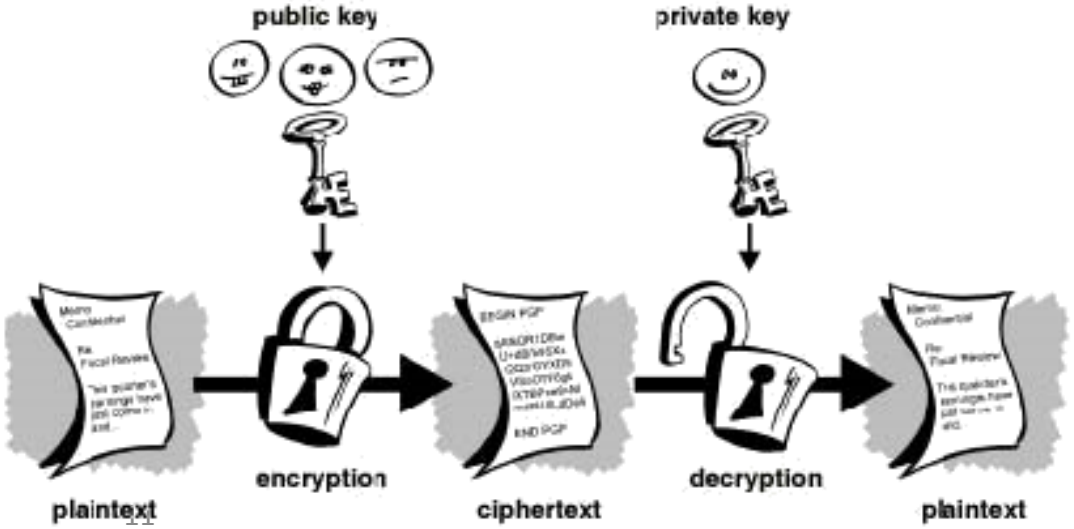
$m = K_B(K_A(m))$

Criptografia
Introdução

- Simétrica
  - envolve o uso de uma única chave

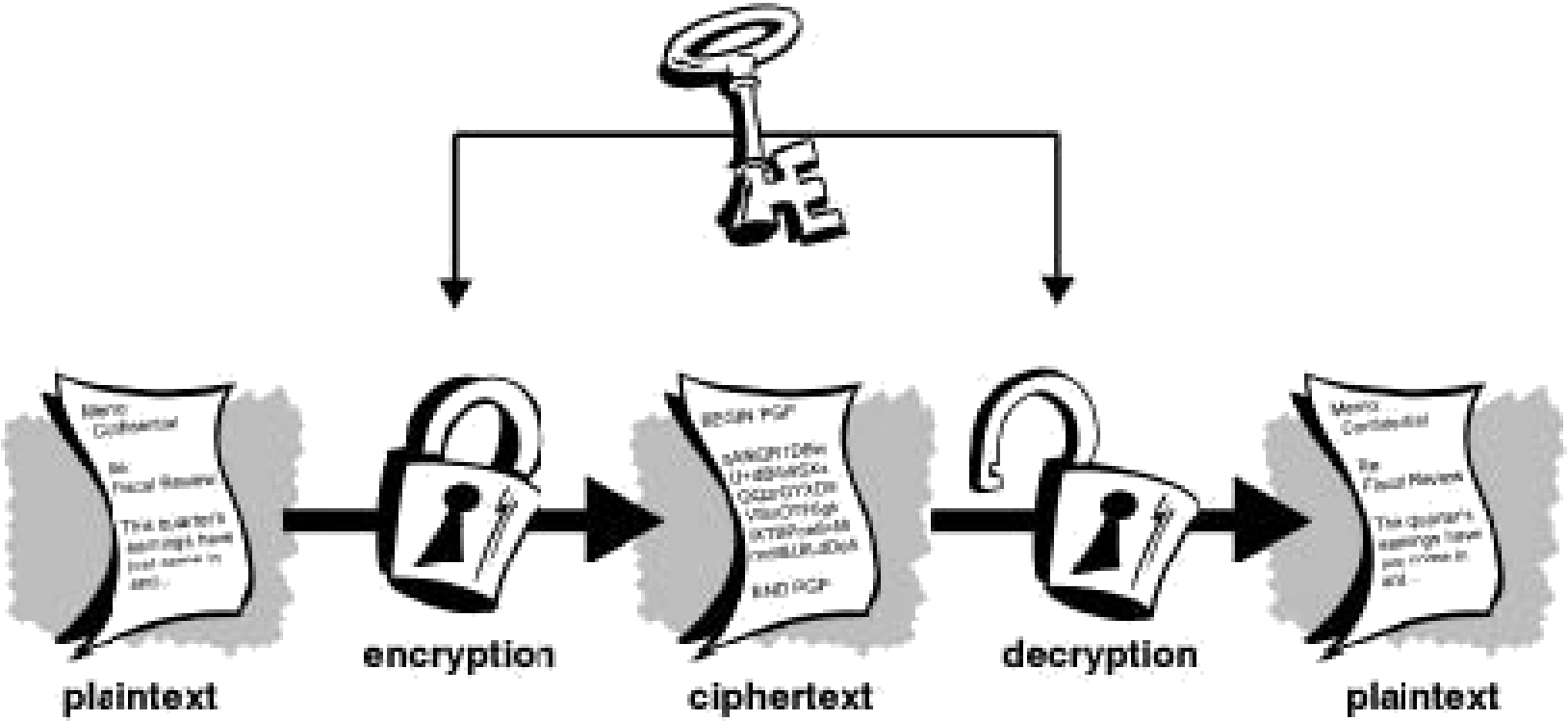


- Assimétrica
  - envolve o uso de um par de chaves



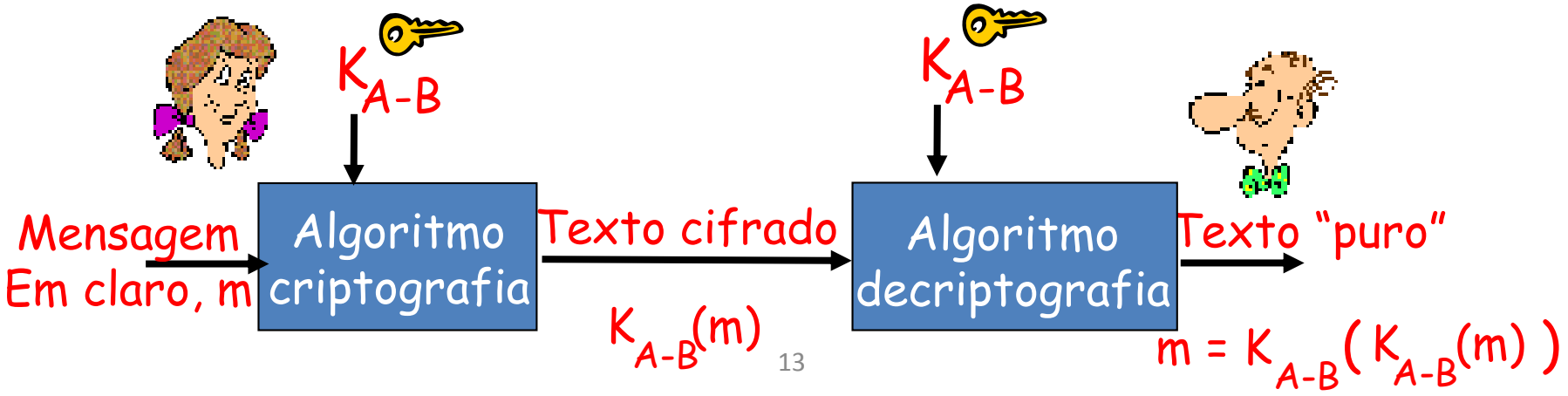
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
Criptografia Simétrica



Criptografia
Criptografia Simétrica

- Principal característica: utilização da mesma chave para cifrar/decifrar
- Outros nomes: (Criptografia ...)
  - Convencional, de chave única, de chave secreta



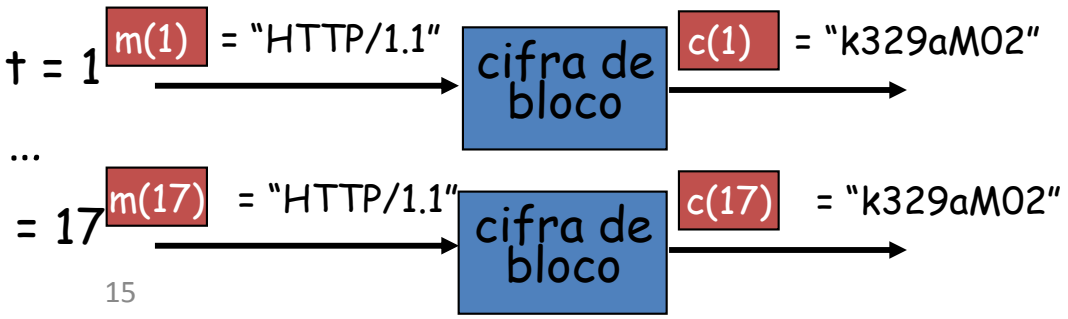
Criptografia
Criptografia Simétrica

- Algoritmos Simétricos
  - Quanto a manipulação de bits
    - Cifragem em bloco: trabalham sobre blocos
      - Quebram a mensagem de texto aberto em blocos de mesmo tamanho.
      - Criptografam cada bloco como uma unidade.
      - Quanto a chave
        - » Mesma chave: ECB (Electronic Codebook)
        - » Chave variável: CBC (Cipher Block Chaining), CFB (Cipher Feedback) e OFB (Output Feedback).
    - Cifragem em fluxo: trabalham bit-a-bit
      - Combinam cada bit da sequência de chaves com bit de texto aberto para obter bit de texto cifrado.
      - Vantagem está na rapidez.

Cifras de bloco

- Mensagem a ser criptografada é processada em blocos de k bits (ex.: blocos de 64 bits).
- Mapeamento 1-para-1 é usado para mapear bloco de k bits de texto aberto para bloco de k bits de texto cifrado
- Exemplo com k = 3:

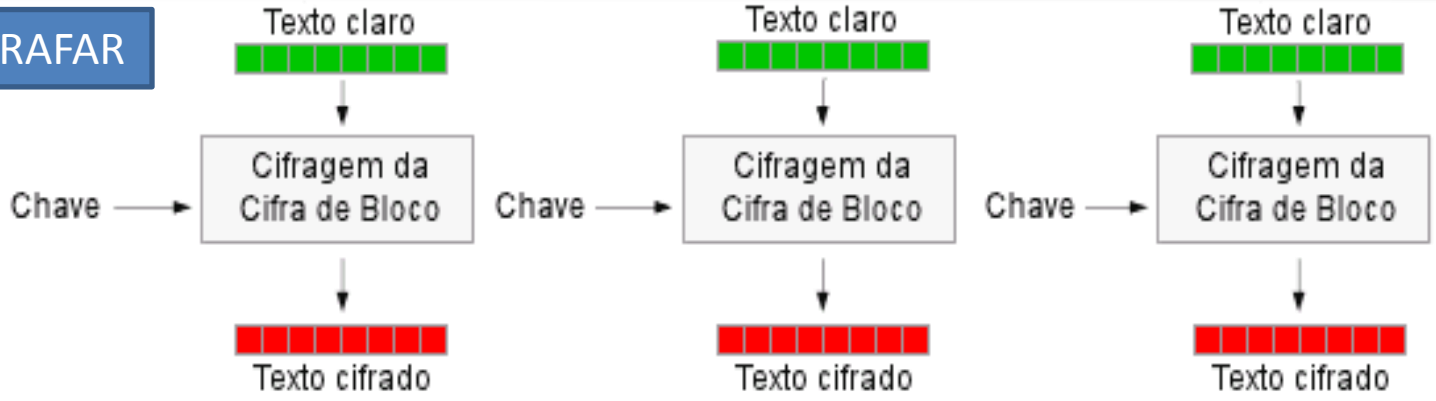
entrada	saída	entrada	saída
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001



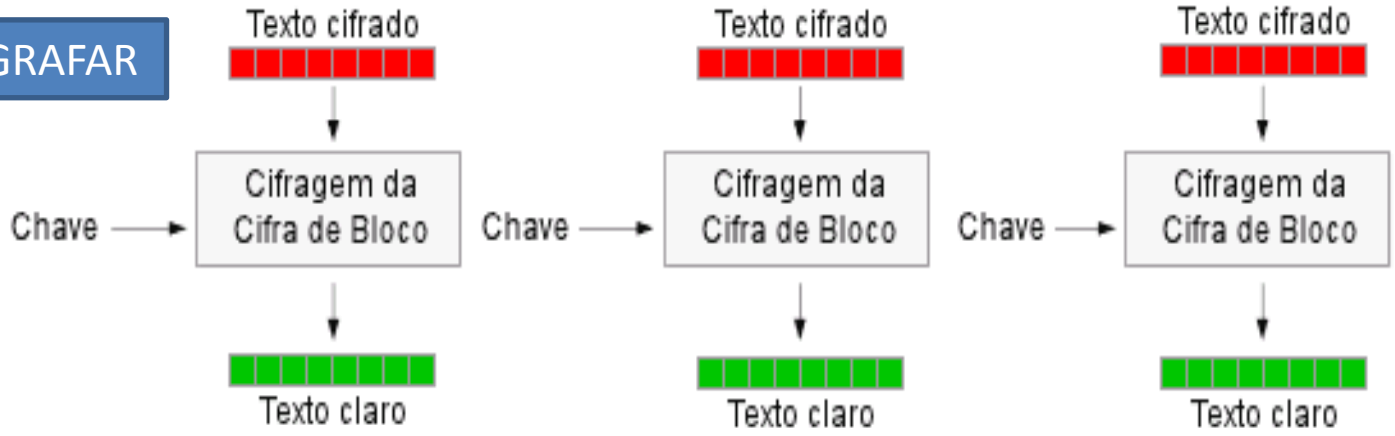
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
ECB (Electronic Codebook)

CRIPTOGRAFAR



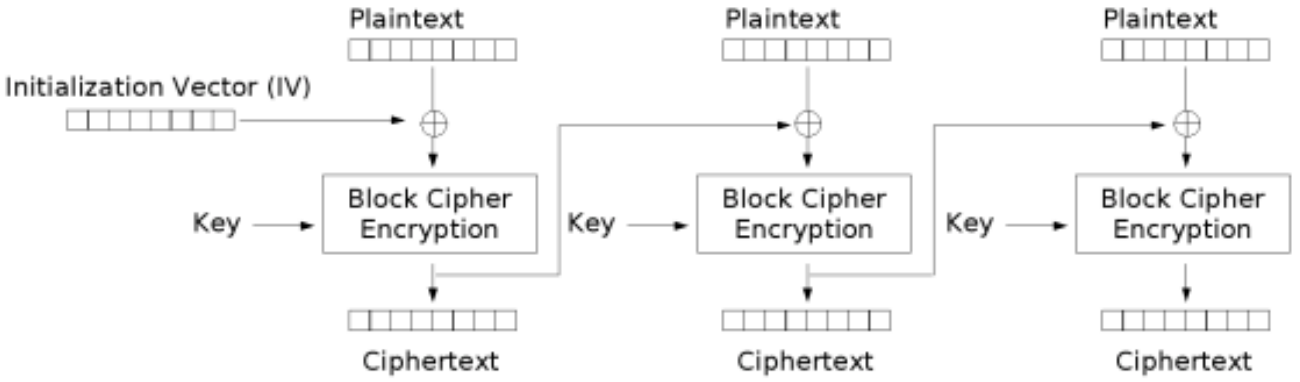
DECRIPTOGRAFAR



Problema: análise estatística fácil

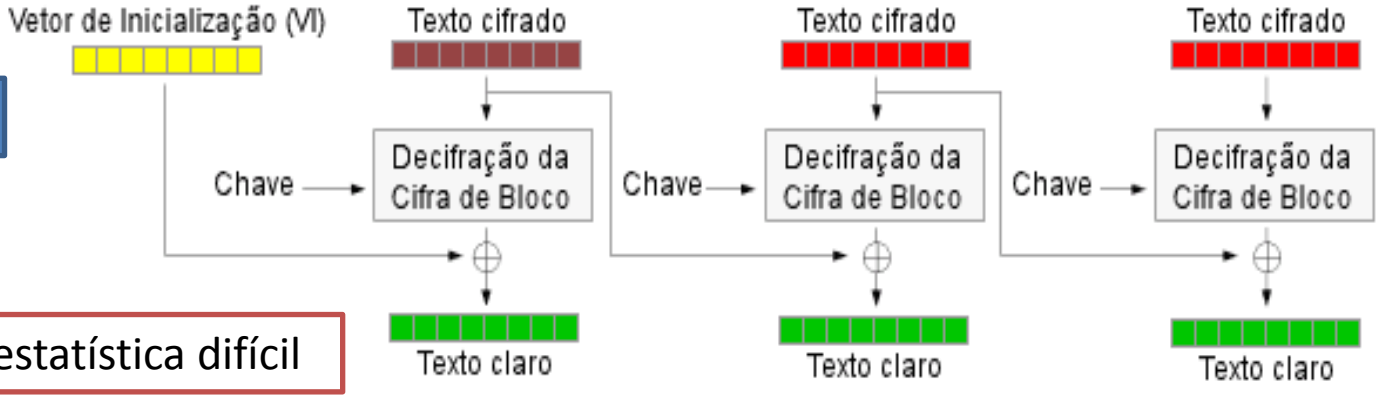
Criptografia
CBC (Cipher Block Chaining)

CRIPTOGRAFAR



Cipher Block Chaining (CBC) mode encryption

DECRIPTOGRAFAR



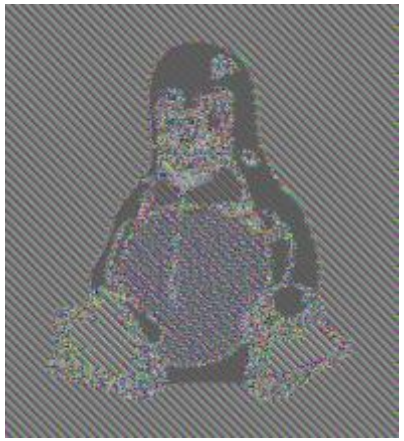
Vantagem: análise estatística difícil

Problema: propagação de erro

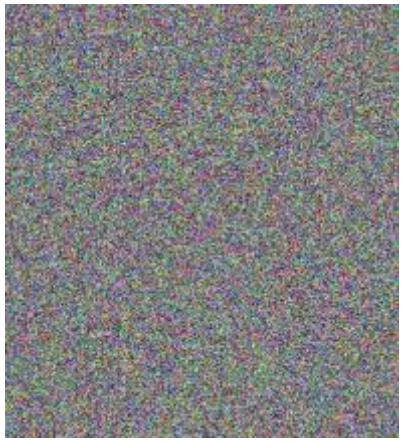
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
ECB x CBC

Original



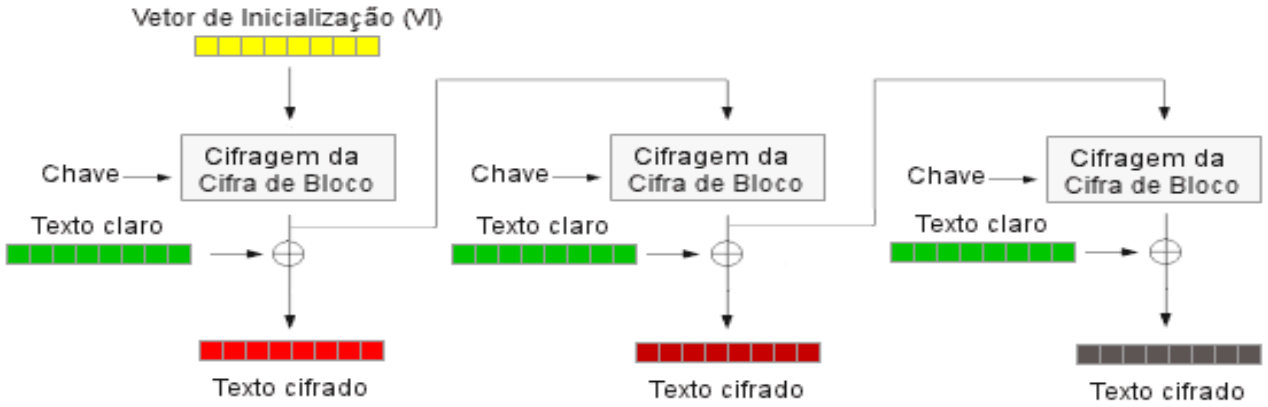
ECB
Modificada, mas com
padrões preservados.



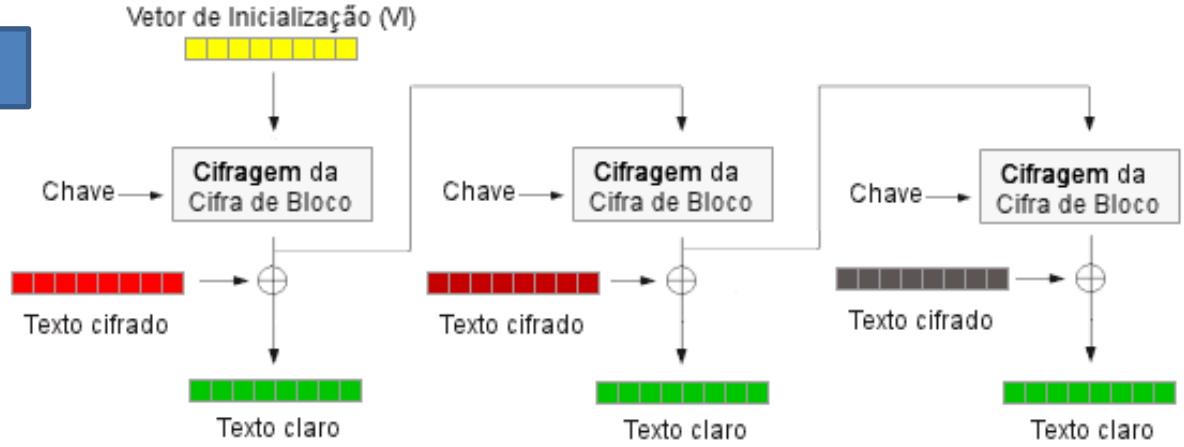
CBC
Ilegível

Criptografia
OFB – Output Feedback

CRIPTOGRAFAR



DECRIPTOGRAFAR

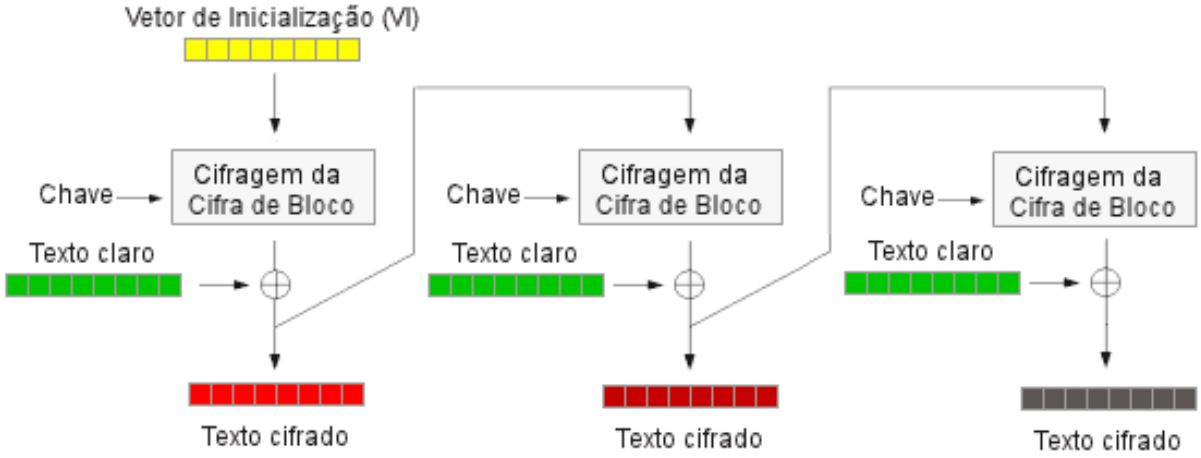


Não propaga erro

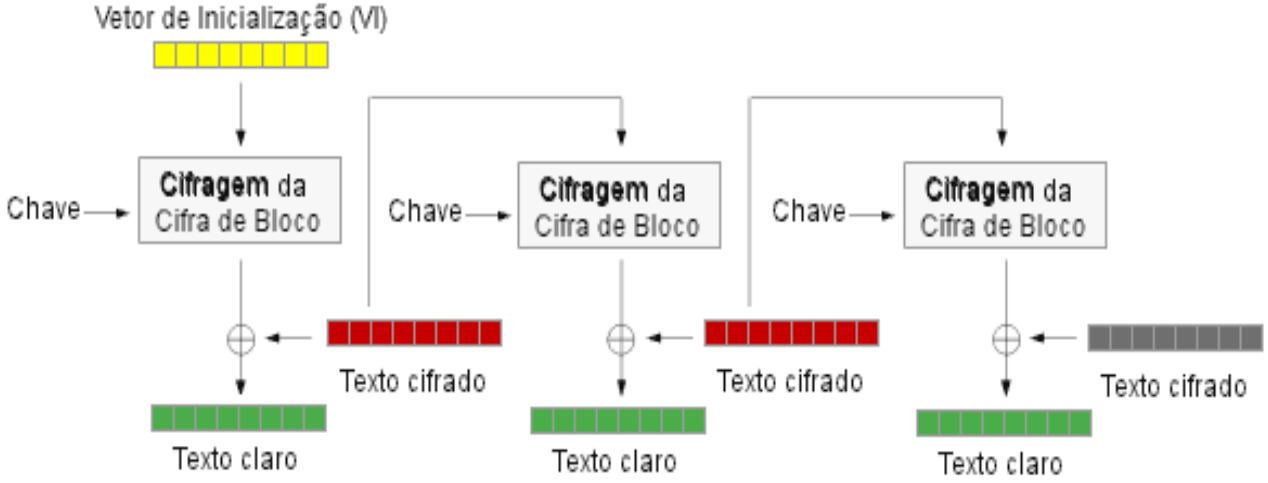
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia
CFB – Cipher Feedback

CRIPTOGRAFAR



DECRIPTOGRAFAR

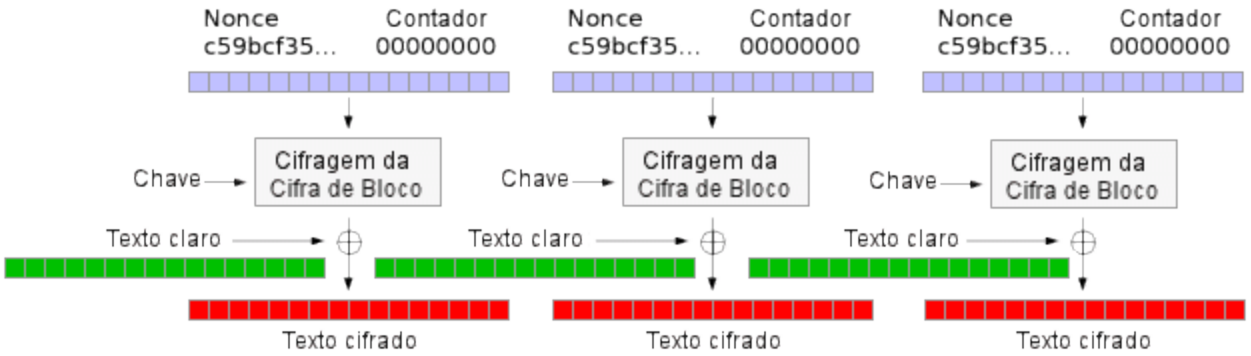


Problema: propagação de erro

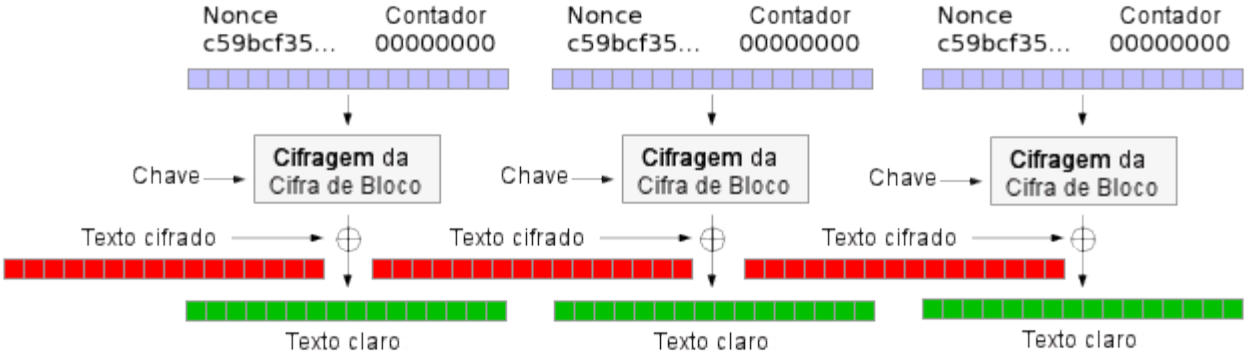
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia Counter

CRIPTOGRAFAR



DECRIPTOGRAFAR



Não propaga erro

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Fixação

- A operação lógica mais usada na criptologia é o _____, porque há reversibilidade. As três técnicas mais usadas são a _____, quando um bits é trocados por outros, a _____, onde onde apenas a posição dos bits é trocada, e o _____, onde alguns bits sequenciais são “empurrados”.
- A criptografia é chamada de _____ quando usa uma só chave, e _____ quando usa um par de chaves.

XOR
SUBSTITUIÇÃO
PERMUTAÇÃO
DESLOCAMENTO
SIMÉTRICA
ASSIMÉTRICA

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Fixação

- A criptografia simétrica pode ser de **BLOCO**, quando um número fixo de bits são criptografados por processo, ou de **FLUXO**, quando não há formação de um conjunto fixo.
- Cifras de bloco podem ser implementadas através de vários modelos, desde o **ECB**, onde há padrões criptológicos fáceis de quebra, ou **CBC** e **CFB**, que apesar de seguras, propagam erro, ou **OFB** e **COUNTER**, onde o erro não é propagado.