Tipos de cifragem

- Os algoritmos de critpografia podem ser categorizados em dois grupos:
  - Cifras de fluxo
  - Cifras de bloco

Tipos de cifragem

Algoritmos de cifragem de fluxo

Algoritmos de cifragem de fluxo

- São algoritmos que convertem imediatamente um símbolo (bit, byte ou caractere) do texto simples em um símbolo do texto cifrado.
- A cifragem é feita símbolo por símbolo. A medida que os bytes do texto simples vão sendo submetidos como entrada ao algoritmo de criptografia, estes são imediatamente convertidos para um valor cifrado.

Tipos de cifragem

Algoritmos de cifragem de bloco

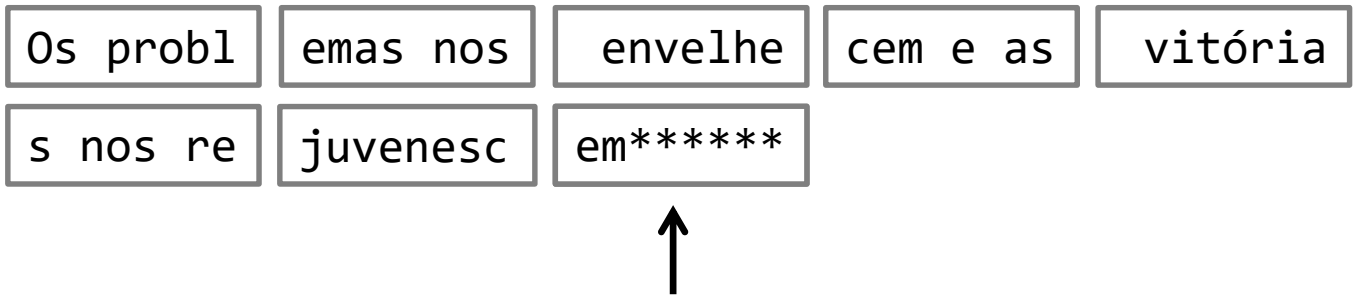
Algoritmos de cifragem de bloco

- O texto simples é dividido em blocos de tamanho fixo
- O algoritmo cifra bloco por bloco

Exemplo – texto para cifrar:

Os problemas nos envelhecem e as vitórias nos rejuvenescem

Tamanho do bloco – 8 bytes



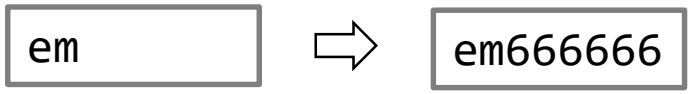
Tipos de cifragem

Algoritmos de cifragem de bloco

Existem alguns esquemas para definição do preenchimento.

O mais conhecido é **PKCS#5***:*

- Preenche o último bloco com bytes cujo valor é igual à quantidade de bytes faltantes para preencher o bloco.
- Exemplo: bloco de 8 bytes



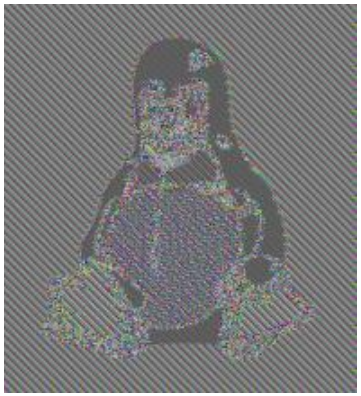
- Quando o último bloco não precisa de preenchimento, ainda assim é gerado um bloco adicional.

Modos de operação das cifras de bloco

Determina como o algoritmo opera sobre os blocos. Pode ser:

- **Livro de Código Eletrônico** - Eletronic CodeBook (**ECB**)
  - Os blocos são cifrados de forma independente um dos outros
  - Um mesmo bloco pode aparecer no texto simples várias vezes. Em todas estas vezes, será encriptado da mesma forma
    - Torna fácil um agente inferir análises por repetição de blocos.

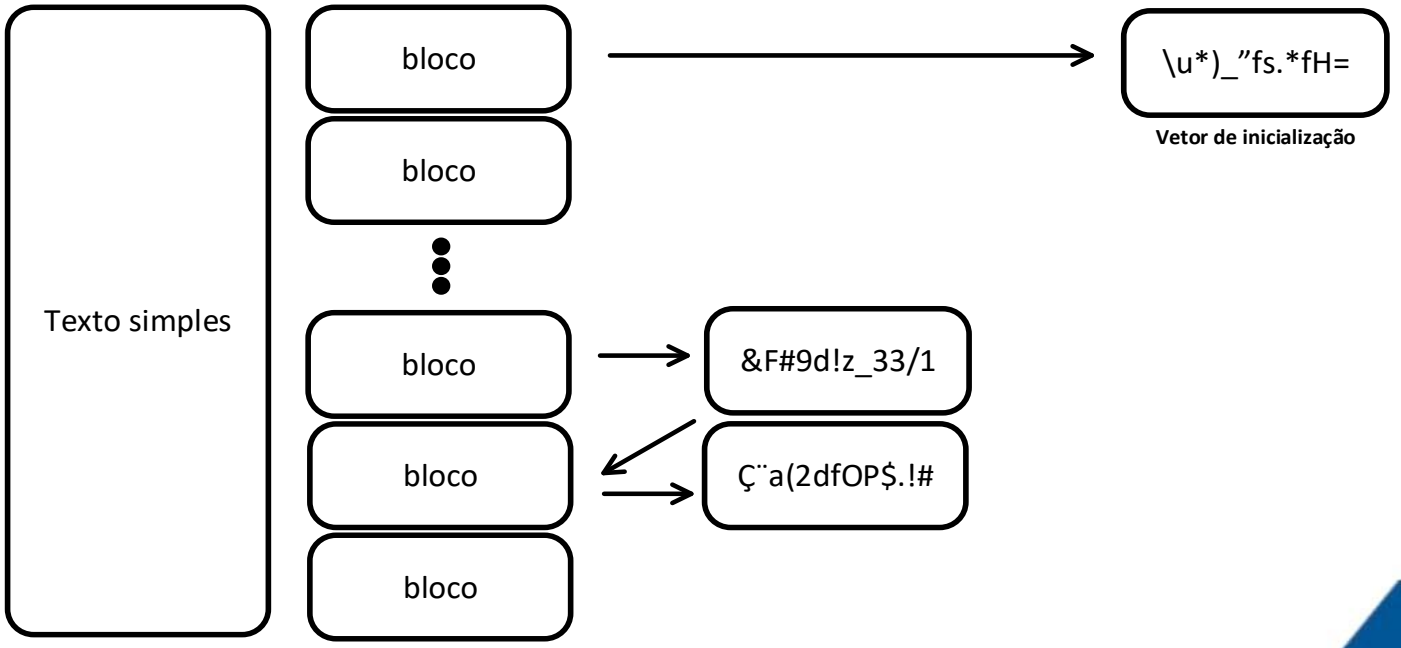
Texto simples



Texto cifrado

Modos de operação das cifras de bloco

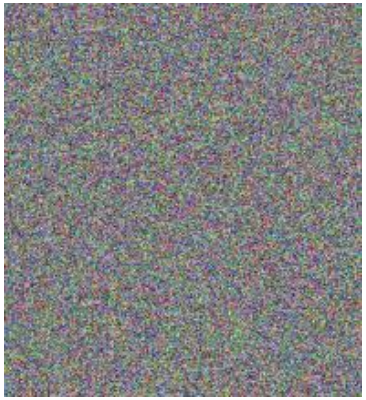
- **Cifragem de blocos por encadeamento –** *Cipher Chaining Block* **(*CBC*)**
  - O algoritmo utiliza o resultado da cifragem do bloco anterior como entrada para cifrar o próximo bloco



Modos de operação das cifras de bloco

- **Encadeamento de blocos cifrados – *Cipher Chaining Block* (*CBC*)**

Texto simples



Texto cifrado

Modos de operação das cifras de bloco

- Além de ECB e CBC, também existem:
  - Modo de feedback cifrado (CFB)
  - Feedback de Saída (OFB)
  - Propagando encadeamento e blocos cifrados (PCBC)

Características de um bom algoritmo de criptografia

- **Difusão**
  - Pequenas alterações no texto simples devem causar grande alteração no texto cifrado

- **Confusão**
  - Deve adotar mecanismos de transformação que ocorra de forma irregular e complexa

Diferenças entre os tipos de cifra

- **Cifras de fluxo**:
  - Mais rápido para cifrar

- **Cifras de bloco:**
  - Alta difusão
  - Imune à inserção de símbolos
  - Sujeito a propagação de erros (no caso do CBC). Um erro irá afetar a decriptação dos demais blocos
  - Mais lento para cifrar