# Cifras de Bloco

Fabrício Steinle Amoroso
Gustavo Henrique Stahl
Rafael Mendes Costa
Vinícius de Paula Pilan

# Criptografia

- Um modo de manter a privacidade sobre os seus dados para manter uma comunicação segura entre quem manda e quem recebe uma mensagem
- Isso pode ser feito de diversos modos
  - Desde traduzindo o texto para outra idioma, americanos e o Navajo na Primeira Guerra Mundial
  - Embaralhar as letras seguindo um padrão, Espartanos e as cítala
  - Cifra de substituição, como a de Júlio César que movia as letras da frase
    - Desvantagem: ao pegar a letra mais comum de uma língua é possível ir decifrando a mensagem
    - O livro dos códigos, Simon Singh: cifras de substituição estão obsoletas
    - Cifra de Vigenere, impede a análise de frequência
  -

# Criptografia

- O avanço da era da informação fez com que as pessoas precisassem cada vez mais de um ambiente seguro
- Hoje em dia criptografia a base de chaves tem tomado bastante abrangência
  - Chaves com 2^2048, grandeza 10^616
  - Processador comum 238 bi de instruções por segundo
- Uso de chave pública e privada
  - Pública: espécie de caixa de correio
  - Privada: chave da caixa de correio
- Chave, Encriptografia e Decriptografia

# Cifra de Bloco - O que é

- São cifras de chave simétricas
  - Usam a mesma chave criptográfica para encriptação e decriptação
- Convertem texto simples em texto cifrado bloco a bloco
  - Bloco: agrupamentos de bits de tamanho fixo
- Tem alta difusão
- É mais lenta do que uma cifra de fluxo
  - Cifra de fluxo: converte texto simples em cifrado símbolo a símbolo

# Cifra de Bloco - Como funciona

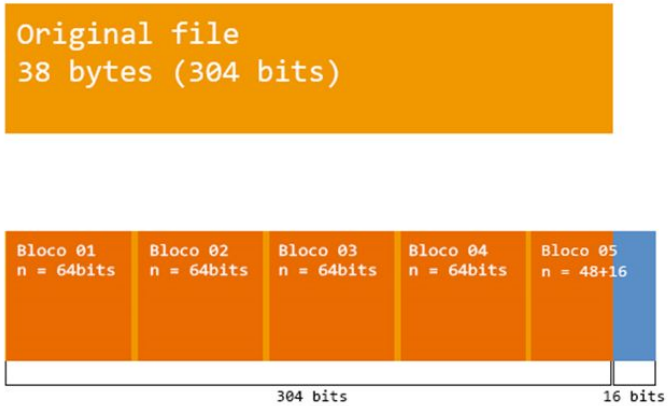
➔ Tamanho do bloco (n): deve ser fixo, geralmente 64 ou 128 bits.

**Problema:** caso o tamanho da mensagem total não seja múltiplo de n, blocos não podem ter o mesmo tamanho **a princípio.**

**Solução:** adicionar algum símbolo de ajuste ao arquivo para que seu tamanho se iguale a um múltiplo de n.

# Cifra de Bloco - Como funciona

Ex: Adicionando 16 bits no último bloco de um arquivo com tamanho total de 304 bits (n = 64bits):



# Cifra de Bloco - Como funciona

- **Algoritmo de encriptação (E):** recebe o bloco simples e o converte em texto cifrado de acordo com uma determinada chave K

- $E_K (P) = (K, P) = C$
  - K: chave de tamanho k
  - P: bloco não encriptado (purotexto) – cadeia de bits
  - C: cadeia de bits (bloco) encriptado (cifrotexto)
  - n: tamanho de P e consequentemente de C

# Cifra de Bloco - Como funciona

- **Algoritmo de decriptação (D):** recebe o bloco cifrado e o converte em texto simples de acordo com uma determinada chave K.

- $D_K (C) = D(K, C) = P$
  - K: chave de tamanho k
  - P: bloco não encriptado (purotexto) – cadeia de bits
  - C: cadeia de bits (bloco) encriptado (cifrotexto)
  - n: tamanho de P e consequentemente de C

# Cifra de Bloco - Modos de operação

Para que o funcionamento explicado seja aplicável em mensagens com vários blocos, foram desenvolvidos alguns modos de operação da cifra de bloco

Neste trabalho serão abordados apenas dois dos mais conhecidos:

- ➔ **Modo de operação Electronic Code Book (EBC)**
- ➔ **Modo de operação Cipher Block Chaining (CBC)**

# Cifra de Bloco - Modos de operação

➔ **Electronic Code Book (EBC):**

- Encriptação:
  1. Dividir a mensagem em blocos
  2. Aplicar o algoritmo E em cada bloco separadamente
  3. Concatenar os resultados.

- Decriptação:
  1. Dividir a mensagem em blocos
  2. Aplicar o algoritmo D em cada bloco separadamente
  3. Concatenar os resultados.

**Problema:** Se houver repetição de blocos, o texto cifrado será igual para ambos - pode gerar padrão de repetição e identificação da chave.

# Cifra de Bloco - Modos de operação

➔ **Cipher Block Chaining (CBC):**

Possível solução para o problema do EBC. Cada bloco cifrado fica dependente de todos os blocos de texto simples processados até o momento.

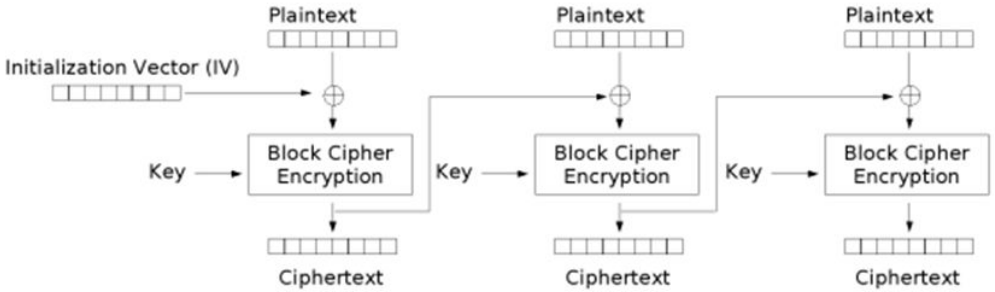
A cada bloco de texto simples é aplicada uma função XOR junto com o bloco cifrado anterior antes do texto ser criptografado.

Para encriptar o primeiro bloco deve-se utilizar junto um **vetor de inicialização V**:

- Idealmente deve ser aleatório, imprevisível e descartável

# Cifra de Bloco - Modos de operação

➔ **Cipher Block Chaining (CBC) - Encriptação:**




Cipher Block Chaining (CBC) mode encryption

Para todo i >= 1:

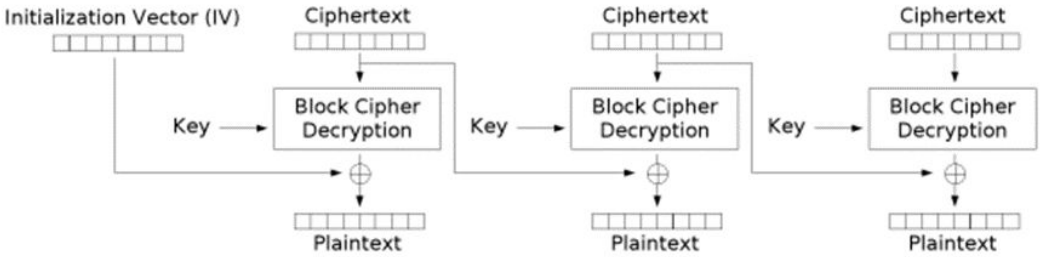
$C_i = E_k (P_i \text{ XOR } C_{i-1})$

Se i = 0 (primeiro bloco):

$C_i = E_k (P_i \text{ XOR } V)$

# Cifra de Bloco - Modos de operação

➔ **Cipher Block Chaining (CBC) - Decriptação:**




Cipher Block Chaining (CBC) mode decryption

Para todo i >= 1:

$P_i = D_k (C_i)$ XOR $C_{i-1}$

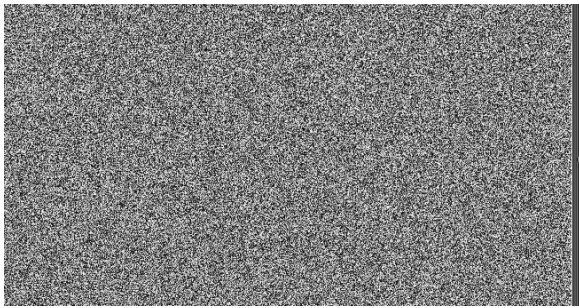
Se i = 0 (primeiro bloco):

$P_i = D_k (C_i)$ XOR V

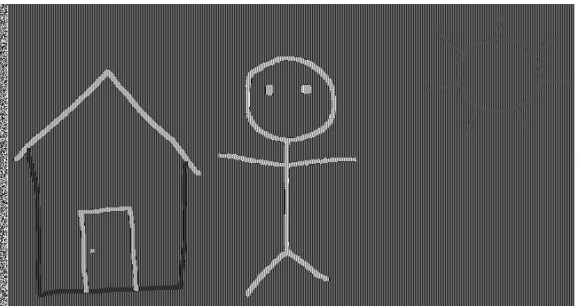
# Exemplo da cifra de bloco

```
def cipher_xor_ecm(phrase_block, key, BLOCK_BYTES, KEY_BYTES):
    cipher = phrase_block
    for bshift_n in range(max(BLOCK_BYTES//KEY_BYTES, 1)):
        cipher ^= key << BYTE * KEY_BYTES * bshift_n
    return cipher
```

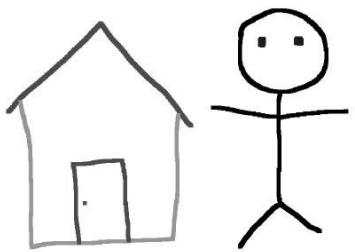
# Exemplo da cifra de bloco



Cipher block chaining



Electronic codebook mode



Original

# DES (Data Encryption Standard)

- **64-bits plaintext** (block size) -> **64-bits ciphertext**
- **Key size** pode ser de **64-bits**
- Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis.
- Criptografia utilizando o algoritmo DES pode ser quebrado facilmente devido a suas vulnerabilidades serem conhecidas. 3DES(Triple DES) é uma variação mais segura de DES.
- Criado pela IBM na década de 70

# AES (Advanced Encryption Standard)

- **128-bits plaintext** (block size) -> **128-bits ciphertext**
- **Key size** pode ser de **128-bits**, **192-bits**, e **256-bits**
- **No known crypt-analytical attacks against AES** but side channel attacks against AES implementations possible. Biclique attacks have better complexity than brute force but still ineffective.
- AES é mais seguro que DES e é "*de facto world standard*".
- Algoritmo que substituiu o DES (1999)

# DES (Data Encryption Standard)

- 16 rounds de operações
- São eles:
  - Expansion,
  - XOR operation with round key,
  - Substitution and
  - Permutation

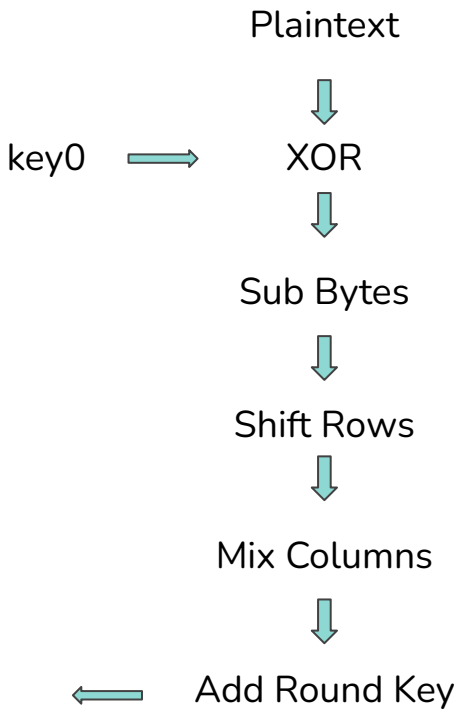
# AES (Advanced Encryption Standard)

- Rounds:
  - 10(128-bits)
  - 12(192-bits)
  - 14(256-bits)
- São eles:
  - Byte Substitution,
  - Shift Row,
  - Mix Column e
  - Round Key Addition (xor)

} Permutation

# AES Deep Dive

**Round:**

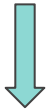



128 - 10 rounds
192 - 12 rounds
256 - 14 rounds

# AES Deep Dive

Plaintext 16 bytes

| B0 | B1 | B2 | B3 | B4 | … | | | | | | | | | B16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|



| B0 | B4 | B8 | B12 |
|---|---|---|---|
| B1 | B5 | B9 | B13 |
| B2 | B6 | B10 | B14 |
| B3 | B7 | B11 | B15 |

# AES Deep Dive

Byte Substitution a partir de uma função definida (mapeamento)

Não é possível um byte ser substituído por ele mesmo, necessariamente será diferente (se começou com um 15, não termina com 15)

| | | | |
|---|---|---|---|
| B0 | B4 | B8 | B12 |
| B1 | B5 | B9 | B13 |
| B2 | B6 | B10 | B14 |
| B3 | B7 | B11 | B15 |

| | | | |
|---|---|---|---|
| S(B0) | S(B4) | S(B8) | S(B12) |
| S(B1) | S(B5) | S(B9) | S(B13) |
| S(B2) | S(B6) | S(B10) | S(B14) |
| S(B3) | S(B7) | S(B11) | S(B15) |

# AES Deep Dive

Shift Rows

Cada coluna se move para a esquerda 0, 1, 2 ou 3 vezes

| | | | |
|---|---|---|---|
| S(B0) | S(B4) | S(B8) | S(B12) |
| S(B1) | S(B5) | S(B9) | S(B13) |
| S(B2) | S(B6) | S(B10) | S(B14) |
| S(B3) | S(B7) | S(B11) | S(B15) |

| | | | | |
|---|---|---|---|---|
| S(B0) | S(B4) | S(B8) | S(B12) | ← 0 |
| S(B5) | S(B9) | S(B13) | S(B1) | ← 1 |
| S(B10) | S(B14) | S(B2) | S(B6) | ← 2 |
| S(B15) | S(B3) | S(B7) | S(B11) | ← 3 |

# AES Deep Dive

Mix Columns

Multiplica-se cada coluna por uma matriz de multiplicação (in order to diffuse / espalhar)

| | | | |
|---|---|---|---|
| S(B0) | S(B4) | S(B8) | S(B12) |
| S(B5) | S(B9) | S(B13) | S(B1) |
| S(B10) | S(B14) | S(B2) | S(B6) |
| S(B15) | S(B3) | S(B7) | S(B11) |

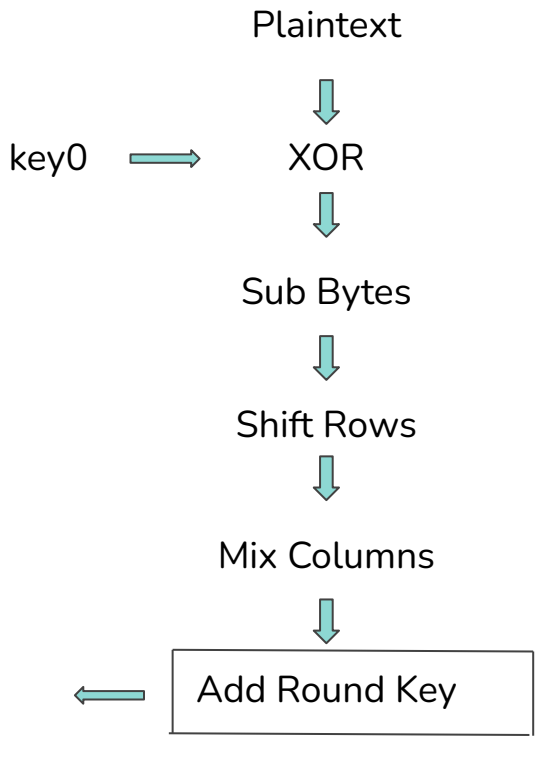
| | | | |
|---|---|---|---|
| S(B0) | | | |
| S(B5) | | | |
| S(B10) | | | |
| S(B15) | | | |

X

| | | | |
|---|---|---|---|
| 2 | 3 | 1 | 1 |
| 1 | 2 | 3 | 1 |
| 1 | 1 | 2 | 3 |
| 3 | 1 | 1 | 2 |

# AES Deep Dive

**Round:**




**128 - 10 rounds**
**192 - 12 rounds**
**256 - 14 rounds**

# Vantagens e Desvantagens

Vantagens

- High diffusion:
  - As informações de um texto de símbolos é difundida para outros vários símbolos de textos de cifras
- Immunity to tampering:
  - Dificuldade de inserir símbolos sem ser detectado
- Melhor aproveitado quando o tamanho dos dados é sabido
- Cada bloco pode ser transformado em uma cifra de fluxo com CFB,CBC

# Vantagens e Desvantagens

Desvantagens

- Demora de encriptação
  - É necessário acumular um bloco inteiro de informações antes de pode encripta-lo
- Erro de propagação
  - Um erro em um símbolo pode corromper todo um bloco de encriptação
- Geralmente requerem mais memória

# Referências


WIKIPÉDIA. **Cifra de bloco**. Disponível em: <https://pt.wikipedia.org/wiki/Cifra_de_bloco>. Acesso em: 29 junho 2022.

PROJETO DE REDES. **Cifras em Bloco e Cifras de Fluxo**. Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_cifras_em_bloco_cifras_de_fluxo.php>. Acesso em: 29 junho 2022.

SERAFIM, VINICIUS DA SILVEIRA. **Introdução à Criptografia: Cifras de Fluxo e Cifras de Bloco**. Brasil, v. 1, ago/2012. Disponível em: <http://www.serafim.eti.br/academia/recursos/Roteiro_05-Cifras_de_Fluxo_e_Bloco.pdf>. Acesso em: 29 junho 2022.

WIKIPÉDIA. **Modo de operação (criptografia)**. Disponível em: <https://pt.wikipedia.org/wiki/Modo_de_opera%C3%A7%C3%A3o_(criptografia)>. Acesso em: 29 junho 2022.

CRYPTOID. **O que é uma cifra de bloco e como ela funciona para proteger seus dados?**. Disponível em: <https://cryptoid.com.br/criptografia/o-que-e-uma-cifra-de-bloco-e-como-ela-funciona-para-proteger-seus-dados/>. Acesso em: 29 junho 2022.

**AES Explained (Advanced Encryption Standard) - Computerphile**. 1 vídeo (14 min e 13 segundos). Publicado pelo canal Computerphile. Disponível em: <https://www.youtube.com/watch?v=O4xNJsjtN6E>. Acesso em: 28 jun. 2022.

GEEKSFORGEEKS. **Difference between AES and DES ciphers**. Disponível em: <https://www.geeksforgeeks.org/difference-between-aes-and-des-ciphers/> Acesso em: 28 jun. 2022.