CIFRAS DE BLOCO (AES)

Gerência e Segurança de Redes

Objetivos de Aprendizagem

Apresentar o *Advanced Encryption Standard*

Agenda

1. *Advanced Encryption Standard*
2. Open SSL

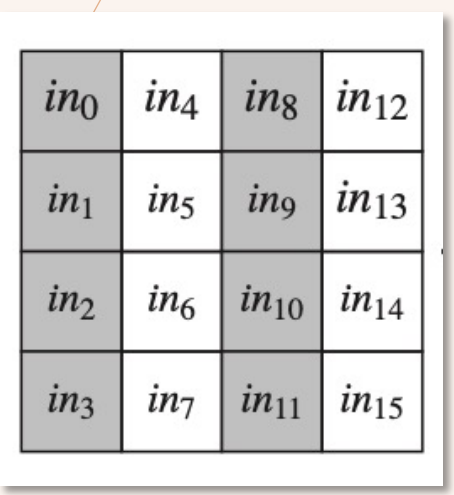
Advanced Encryption Standard

Advanced Encryption Standard

- Publicado pelo NIST em 2001 em substituição ao DES como padrão de cifra de bloco
- Complexidade bastante superior ao DES, RSA, etc
- Padrão atual para cifra de bloco

Características AES

- Blocos de 128 bits (16 bytes)
- O bloco de entrada é definido como uma matriz quadrada de bytes (4x4) chamado de ***State***
- Ao longo da execução *State* vai sendo modificado até no estágio final se tornar o texto cifrado



Características AES

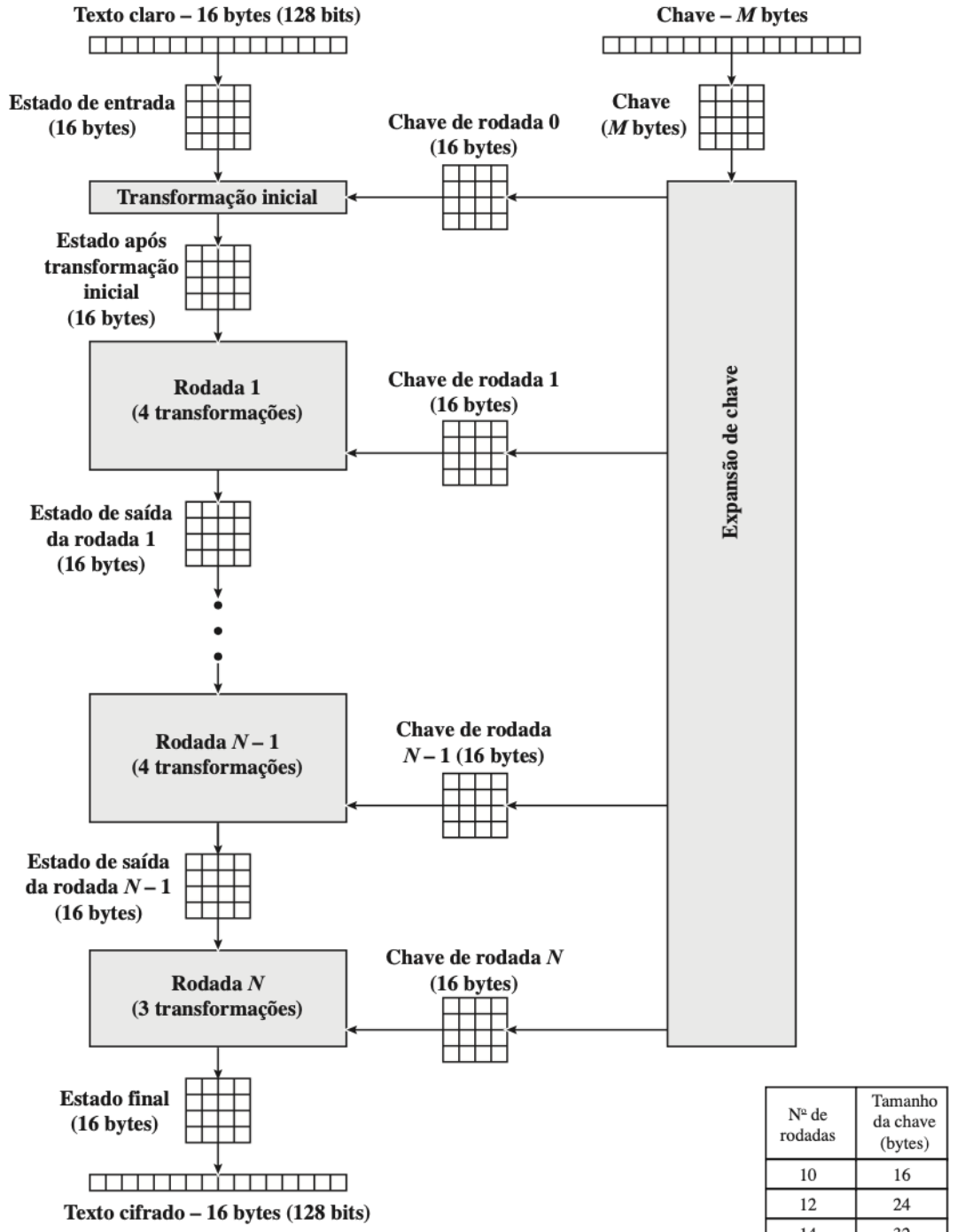
- Chave de 128, 192 ou 256 bits

  AES-128, AES-192 ou AES-256
- A chave também é vista como uma matriz quadrada de bytes (4x4)
- A chave passa por um processo de expansão passando a ser de 44 words de 4 bytes

Características AES

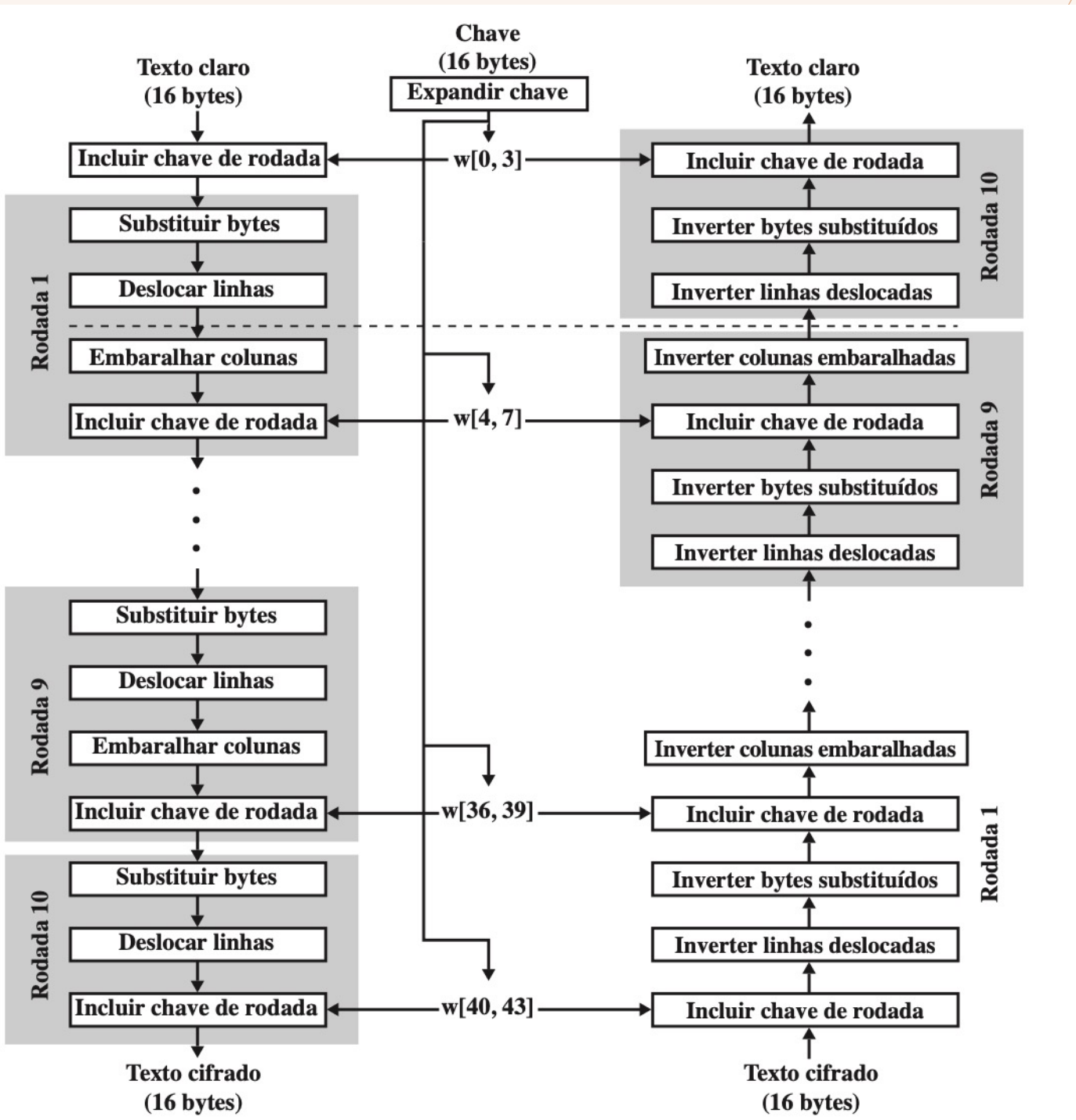
- A cifra é executada em diversas rodadas, segundo o tamanho da chave
  - 10 rodadas, chave de 16 bytes (128bits)
  - 12 rodadas, chave de 24 bytes (192bits)
  - 16 rodadas, chave de 32 bytes (256bits)
- Em cada rodada são aplicadas 4 funções de transformação
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey

Estrutura Geral AES



Nº de rodadas	Tamanho da chave (bytes)
10	16
12	24
14	32

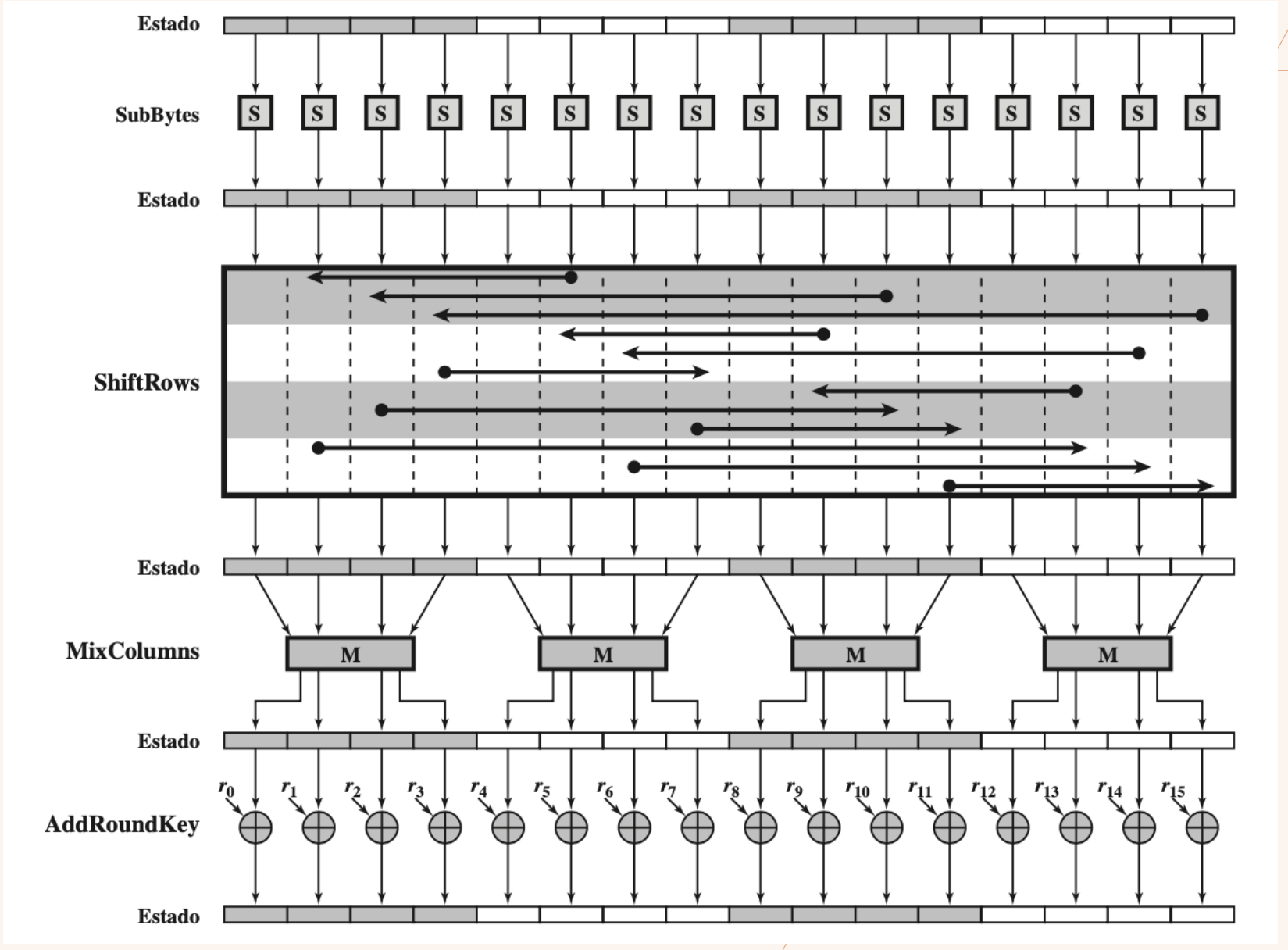
Estrutura Detalhada AES



Estrutura Detalhada

- A primeira rodada aplica *AddRoundKey* ao texto claro
- As 9 rodadas seguintes aplicam as 4 funções de transformação
- Apenas *AddRoundKey* utiliza-se da chave
- As outras funções acrescentam confusão, difusão e não linearidade

Rodada Individual

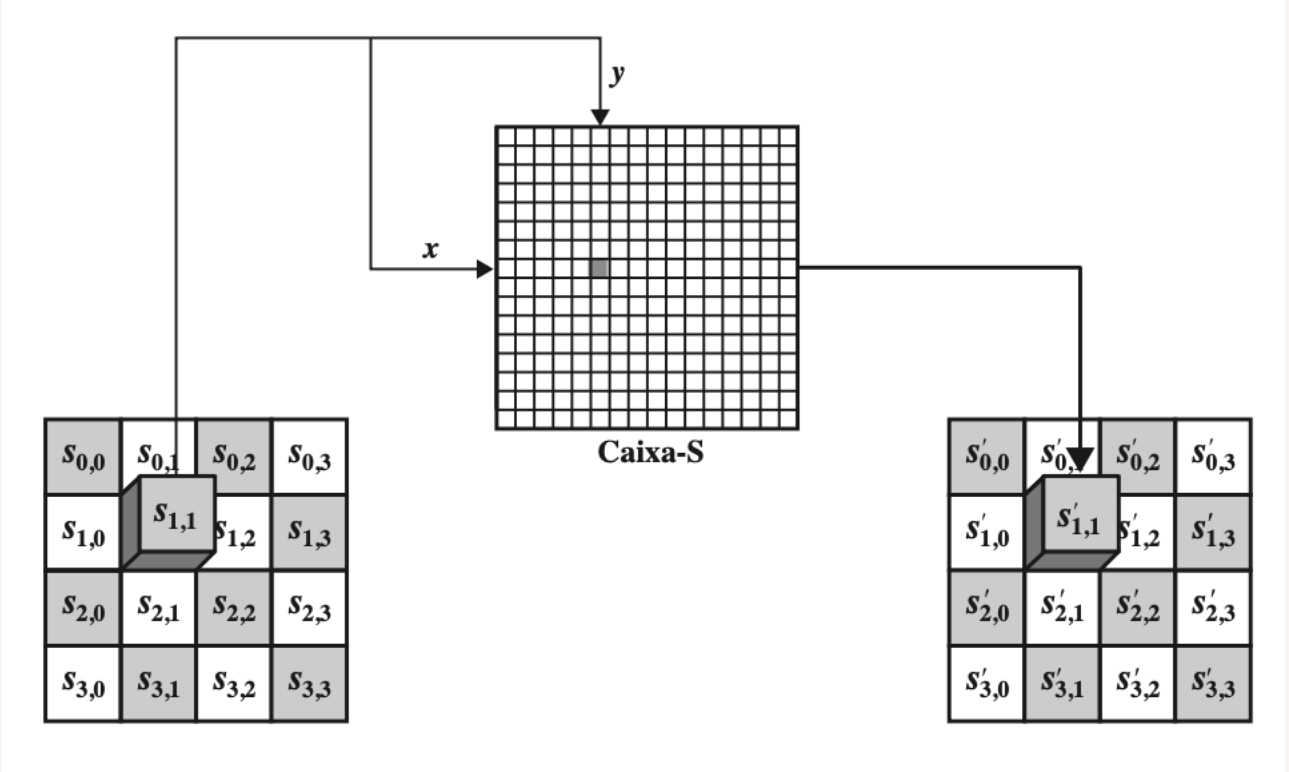


SubBytes

- Transformação de **substituição** de bytes
- Define uma matriz de 16x16 bytes (S-Box) para permutações de todos os valores de 8bits possíveis
- Cada byte de *State* é mapeado para um novo valor
- 4 bits a esquerda representam as linhas
- 4 bits a direita representam as colunas

SubBytes

- Por exemplo, o valor hexadecimal {95} referencia a linha 9, coluna 5 da S-box, que contém o valor {2A}.
- Logo, o valor {95} é mapeado para o {2A}



SubBytes

- S-Box é projetada para ser resistente a ataques de criptoanálise
- A saída não pode ser descrita como uma função matemática simples da entrada (não linear)
- S-Box é inversível, mas não é autoinversível

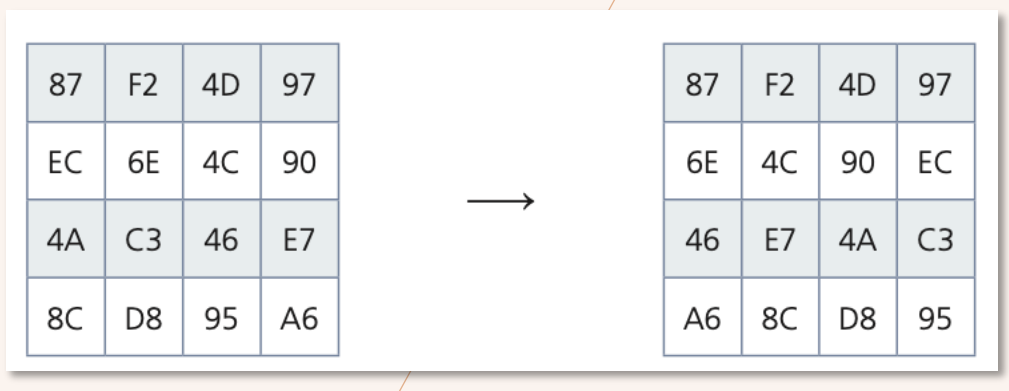
  Por exemplo, S-box({95}) = {2A}

  Mas, IS- box({95}) = {AD}

ShiftBytes

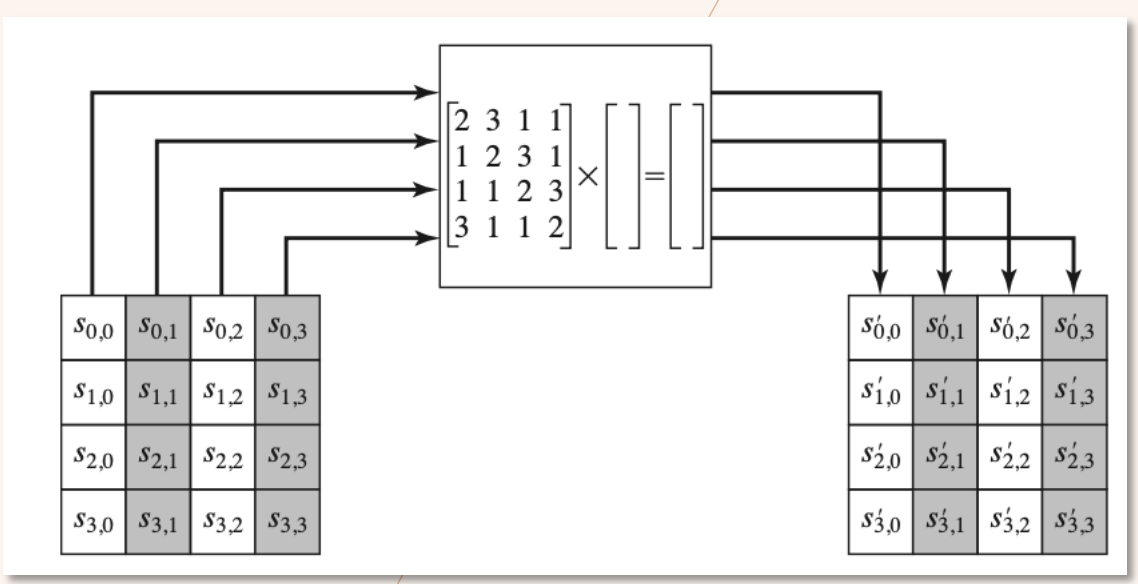
- Transformação de deslocamento de bytes
- Recebe o *State* como entrada

  Mantém 1ª linha intacta
  Desloca a 2ª linha 1 byte a esquerda
  Desloca a 3ª linha 2 bytes a esquerda
  Desloca a 4ª linha 3 bytes a esquerda
- Garante que os 4 bytes de uma coluna sejam espalhados em quatro colunas diferentes

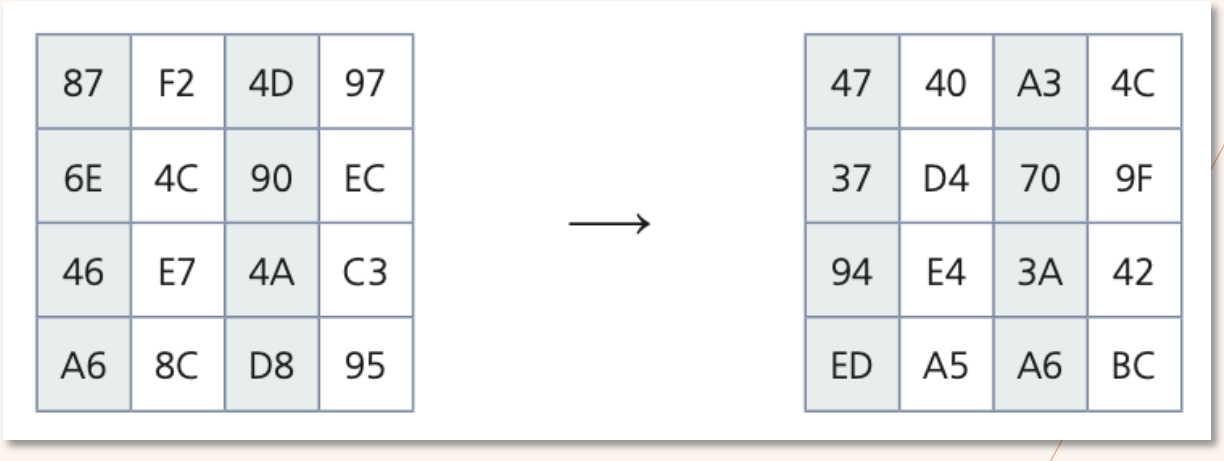


MixColumns

- Transformação de embaralhamento de colunas
- Opera sobre cada coluna de *State*
- Cada byte de uma coluna é mapeado para um novo valor que é determinado em função de **todos os quatro bytes nessa coluna**



MixColums



87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

→

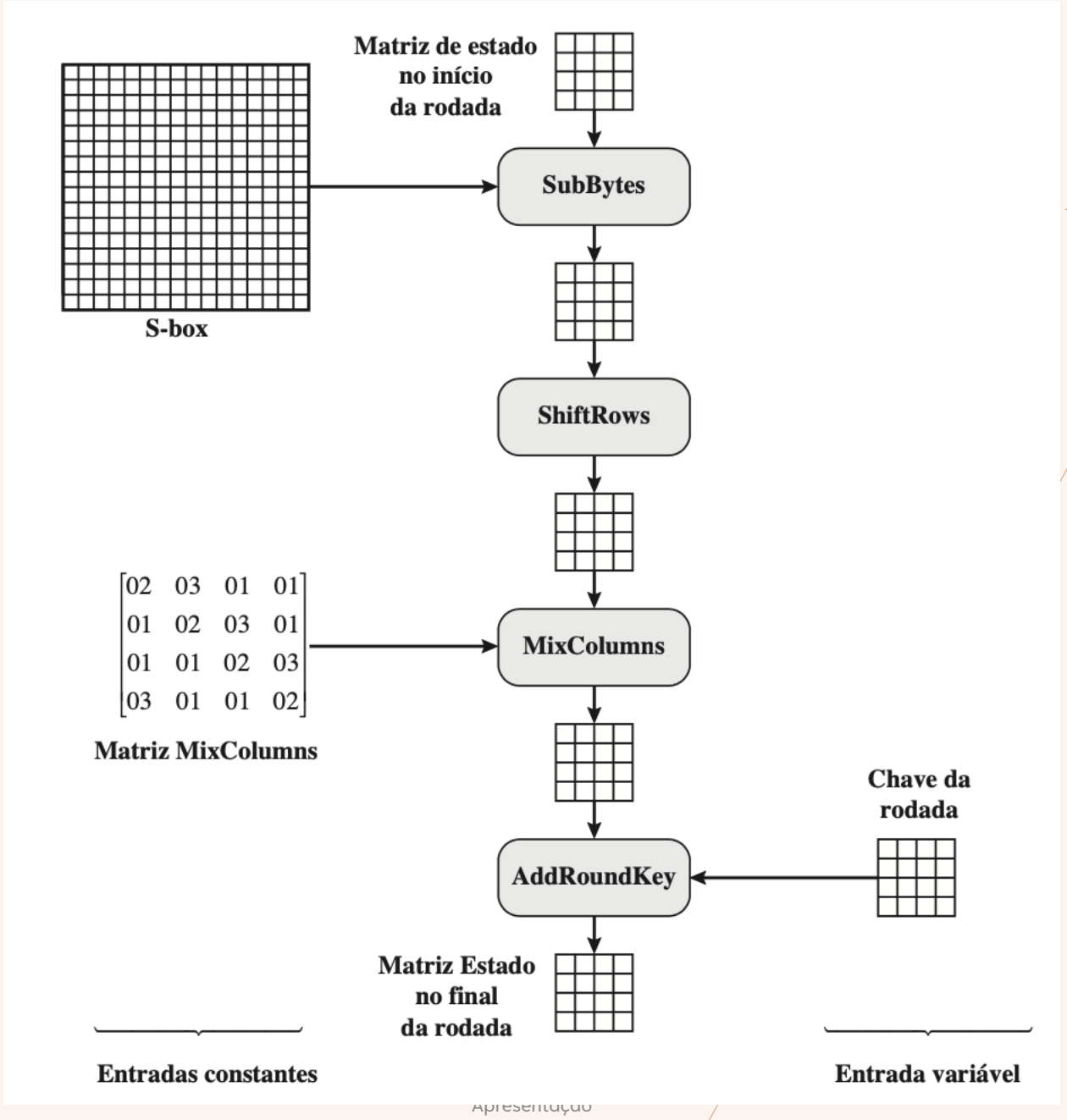
47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

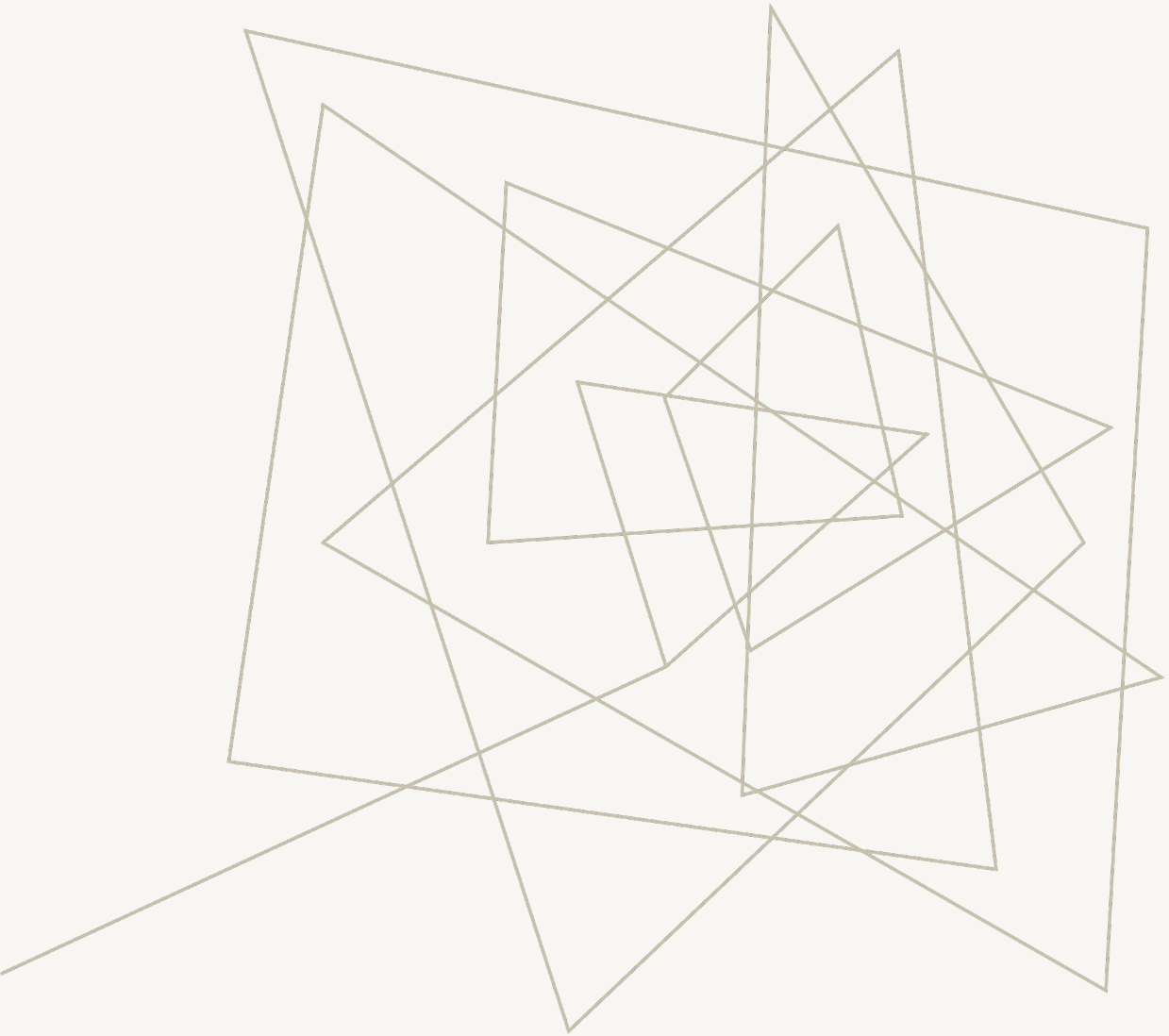
MixColumns

- Os coeficientes da matriz são baseados em um código linear que garante um bom embaralhamento entre os bytes de cada coluna
- A transformação de embaralhamento de colunas combinada com a de deslocamento de linhas garante que, após algumas rodadas, todos os bits da saída dependam de todos os bits da entrada.

AddRoundKey

- Transformação direta de adição de chave de rodada
- Os 128 bits de State passam por um XOR com os 128 bits da chave da rodada
- A transformação de adição de chave da rodada é a mais simples e afeta cada bit de Estado.
- A complexidade da expansão de chave da rodada, mais a dos outros estágios do AES, garantem a sua segurança.


Matriz de estado
no início
da rodada
SubBytes
S-box
ShiftRows
02 03 01 01
01 02 03 01
01 01 02 03
03 01 01 02
MixColumns
Matriz MixColumns
Chave da
rodada
AddRoundKey
Matriz Estado
no final
da rodada
Entradas constantes
Entrada variável



OpenSSL

OpenSSL

The OpenSSL Project develops and maintains the OpenSSL software - a robust, commercial-grade, full-featured toolkit for general-purpose cryptography and secure communication.

OpenSSL Help

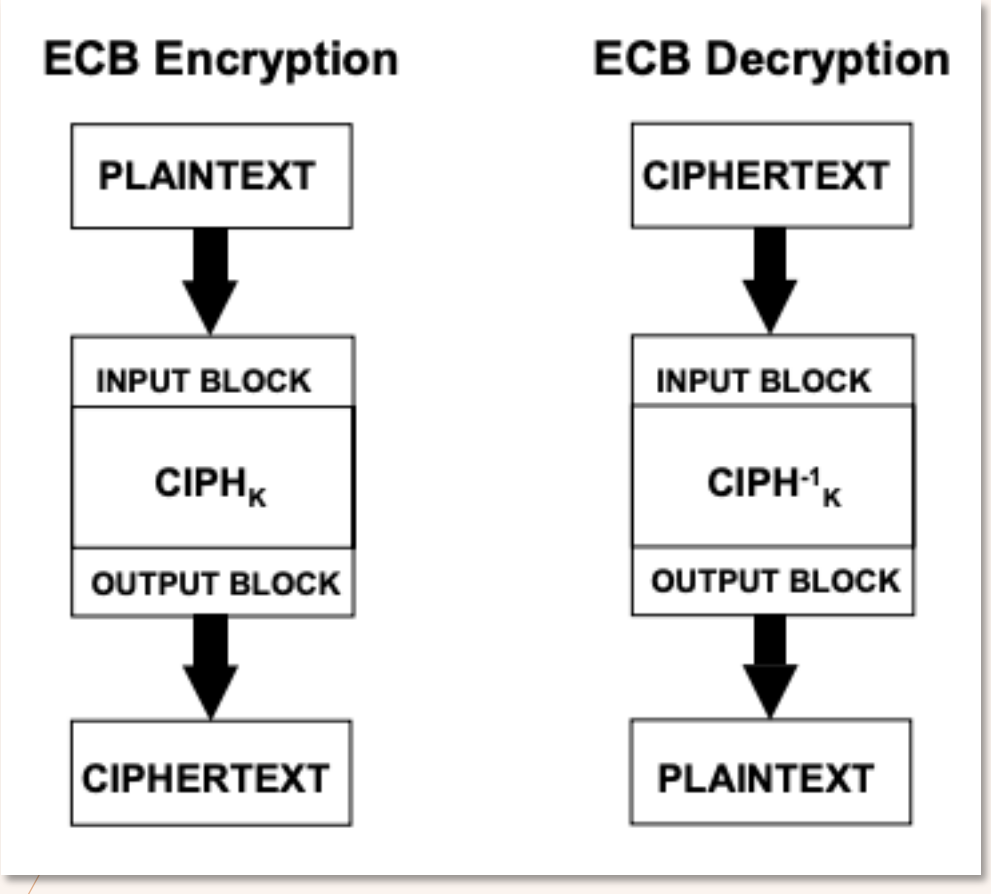
- Dentre os diversos comandos disponíveis **`openssl enc`** realiza a encriptação de arquivos
- Diversas cifras estão disponíveis **`openssl help`**

```
Cipher commands (see the `enc' command for more details)
aes-128-cbc        aes-128-ecb        aes-192-cbc        aes-192-ecb
aes-256-cbc        aes-256-ecb        base64             bf
bf-cbc             bf-cfb             bf-ecb             bf-ofb
camellia-128-cbc   camellia-128-ecb   camellia-192-cbc   camellia-192-ecb
camellia-256-cbc   camellia-256-ecb   cast               cast-cbc
cast5-cbc          cast5-cfb          cast5-ecb          cast5-ofb
chacha             des                des-cbc            des-cfb
des-ecb            des-ede            des-ede-cbc        des-ede-cfb
des-ede-ofb        des-ede3           des-ede3-cbc       des-ede3-cfb
des-ede3-ofb       des-ofb            des3               desx
rc2                rc2-40-cbc         rc2-64-cbc         rc2-cbc
rc2-cfb            rc2-ecb            rc2-ofb            rc4
rc4-40

dtel@MacBook-Pro-de-Adm ~ %
```

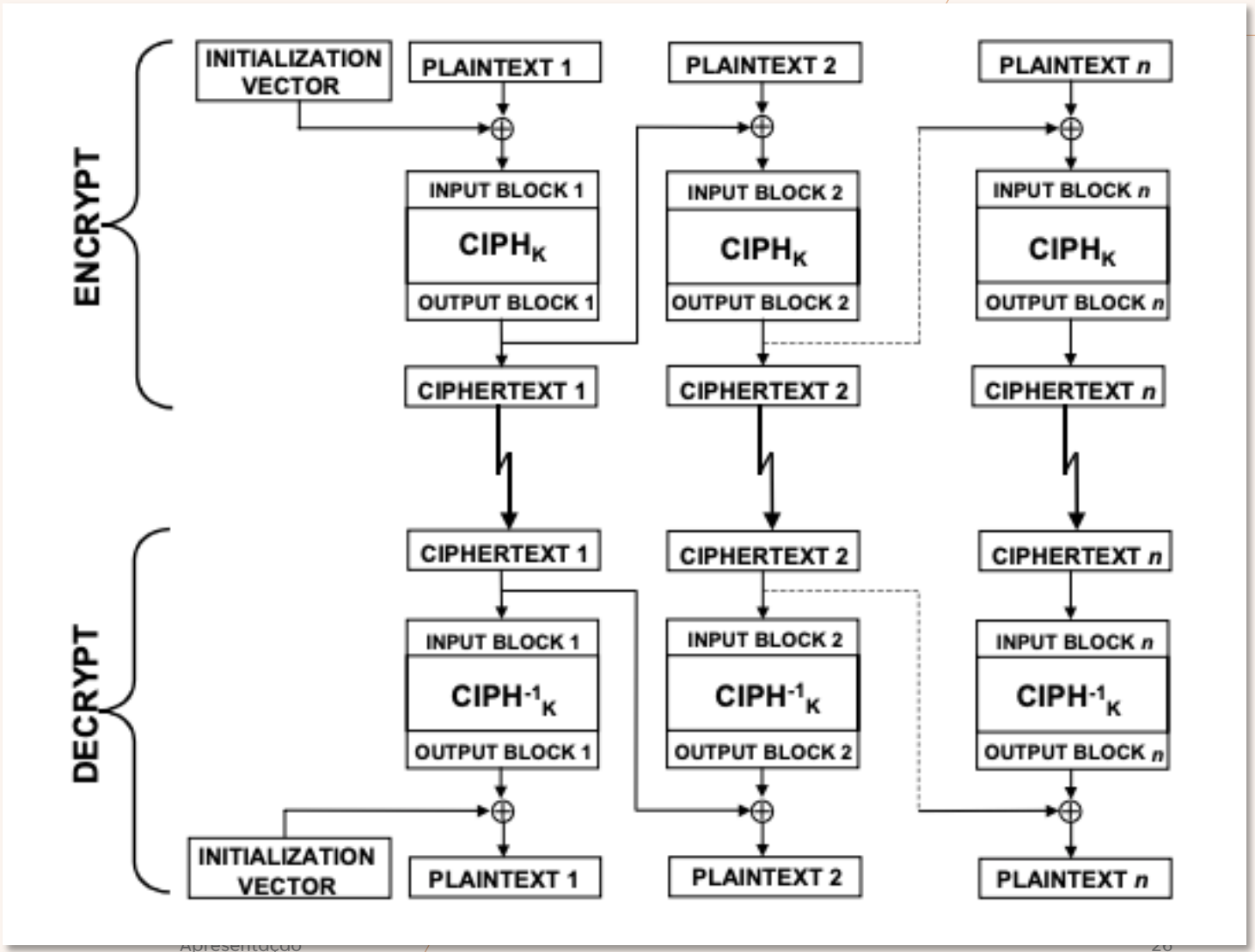
Electronic Codebook Mode

- ECB
- A encriptação é aplicada diretamente a cada bloco
- Encriptação e Decriptação podem acontecer em paralelo
- Mensagens com tamanho múltiplo do tamanho do bloco
- Vulnerável a ataques, pois a mesma chave gera as mesmas cifras, sempre



Cipher Block Chaining Mode

- CBC
- A operação de encriptação não pode ser realizada em paralelo
- Como na decriptação os blocos já disponibilizados simultaneamente, a operação de decriptação pode ocorrer em paralelo
- Um dos mais usados

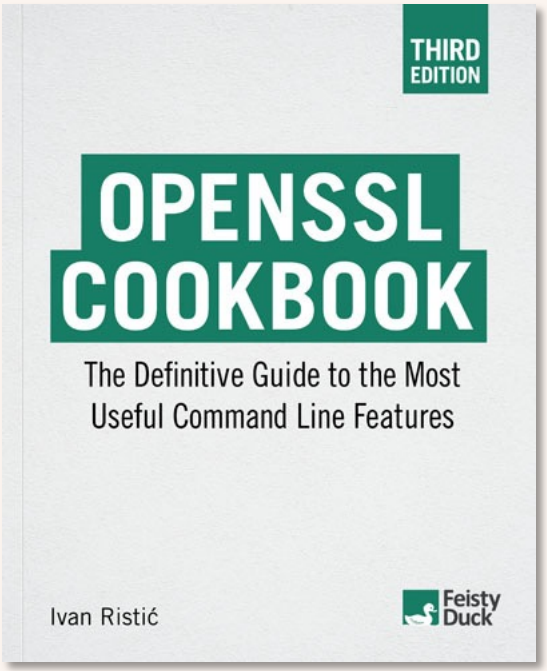


openssl enc aes-256-cbc

```
dtel@MacBook-Pro-de-Adm ~ % cat file.txt
Lorem ipsum dolor sit amet, consectetur efficitur.
dtel@MacBook-Pro-de-Adm ~ % openssl enc -aes-256-cbc -in file.txt -out file.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
dtel@MacBook-Pro-de-Adm ~ % cat file.enc
Salted__9?ε??Ω?h?x???Ai????Qm??W????j??ŗx?d?
                                        HT??|3^l?)G?U?MXv?WO???%
dtel@MacBook-Pro-de-Adm ~ % openssl enc -aes-256-cbc -base64 -in file.txt -out file.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
dtel@MacBook-Pro-de-Adm ~ % cat file.enc
U2FsdGVkX18ITn4wQT1eSqXgZGJgqDZ1LWM86wQUUQVLhkx8Igpv0lzdOSYFil0A
9qE9RAi3d6SosorAn9ZxWgI+/MitK0k5qvVROsUXtVo=
dtel@MacBook-Pro-de-Adm ~ %
```

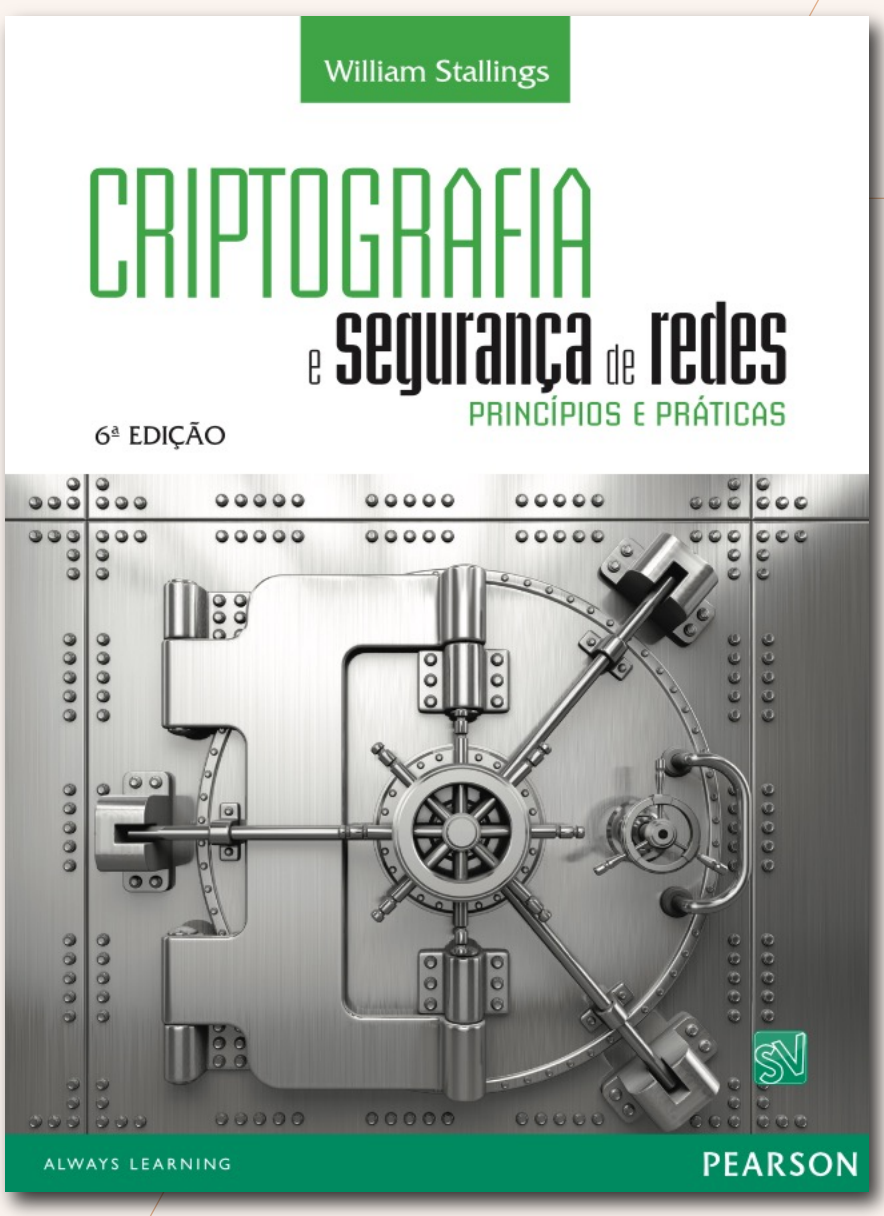
Referências

- https://www.openssl.org/
- https://www.feistyduck.com/library/openssl-cookbook/online/
- https://wiki.openssl.org/index.php/Enc



Referências

- **Capítulo 5**. Criptografia e Segurança de Redes. *William Stallings*. 6ª. Edição. Editora Pearson.



FIM

Prof. José Roberto Bezerra

jbroberto@ifce.edu.br

IFCE – *Campus* Fortaleza