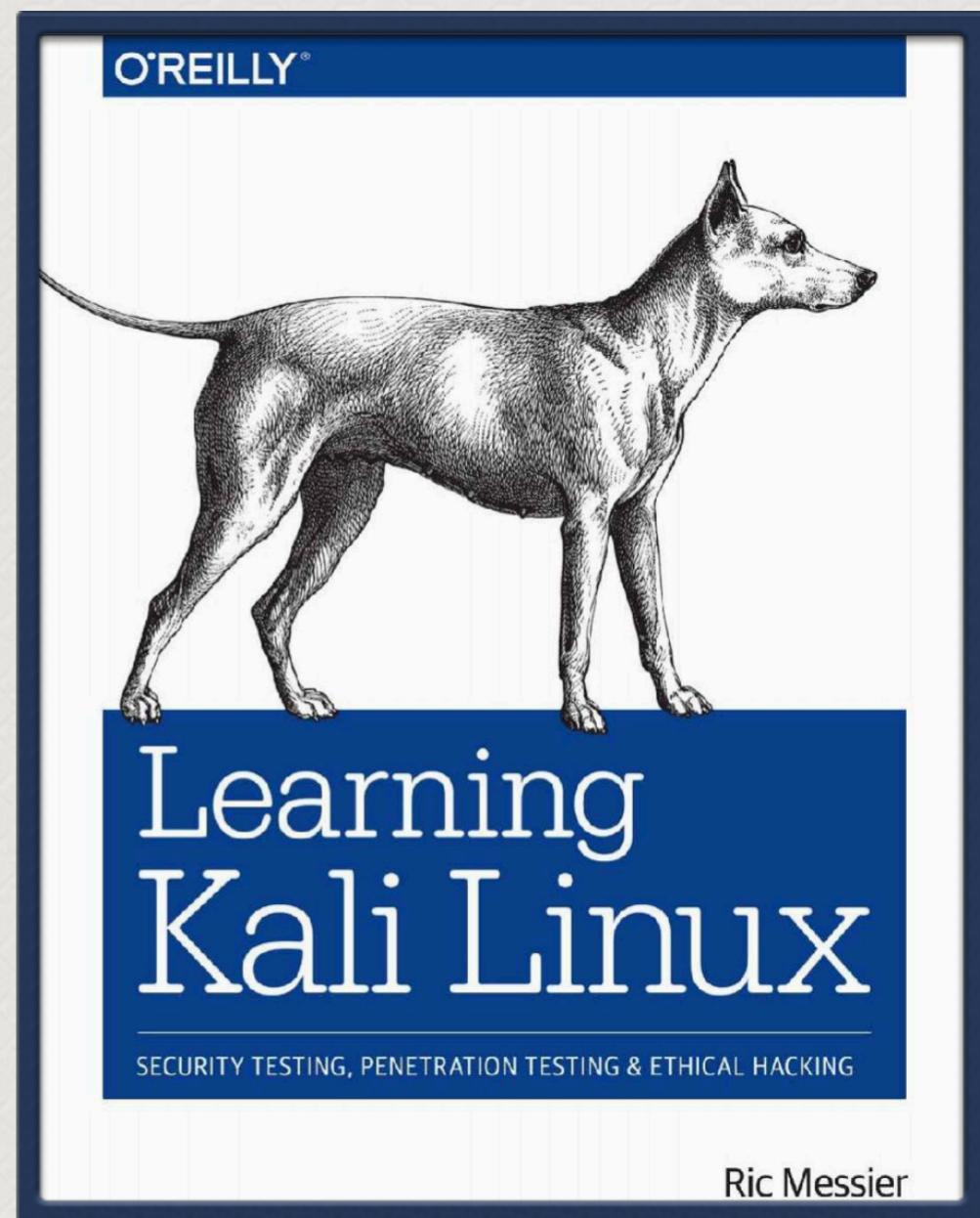
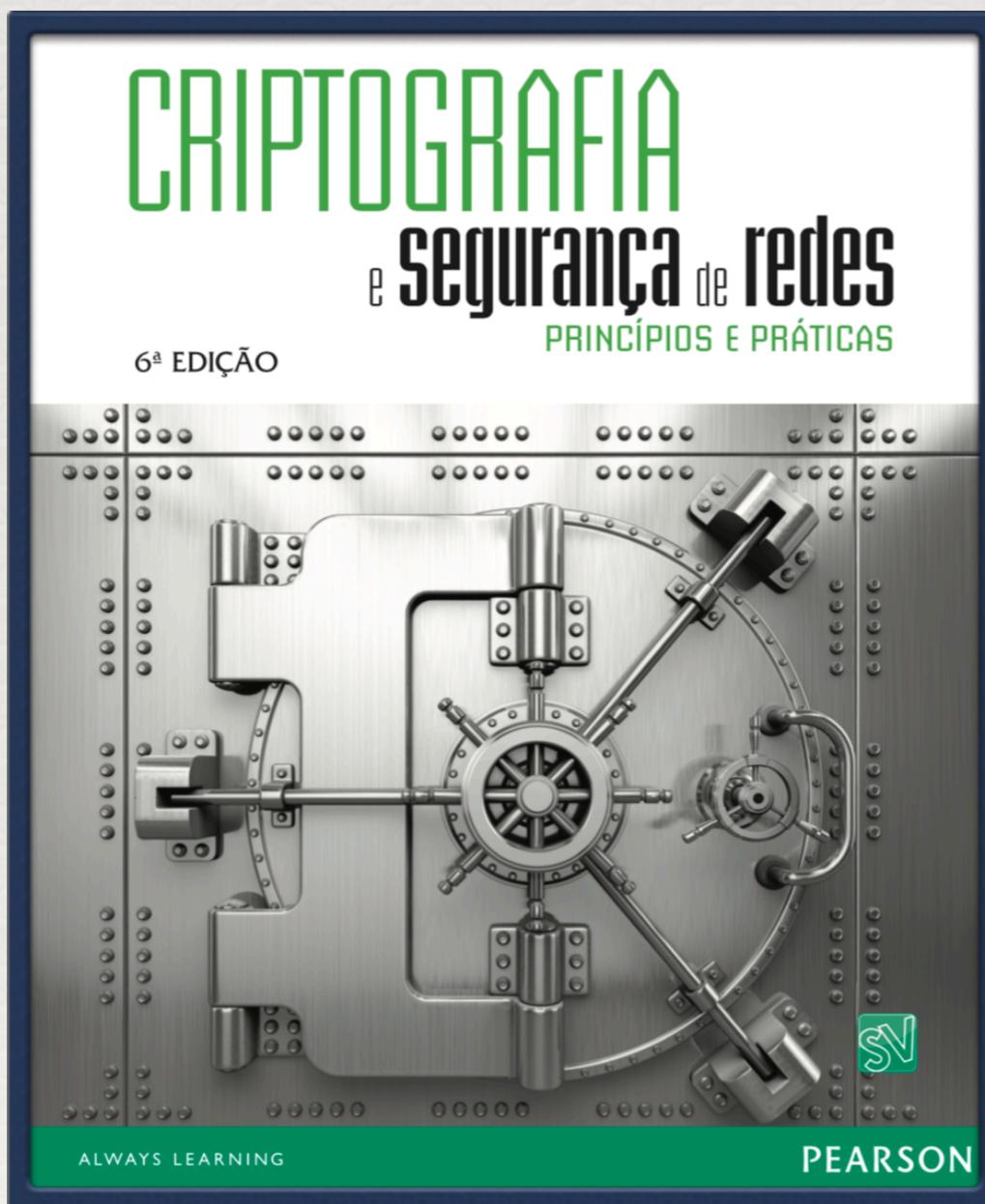
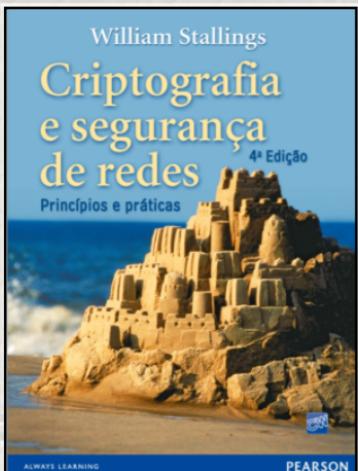


Segurança e Auditoria de Sistemas

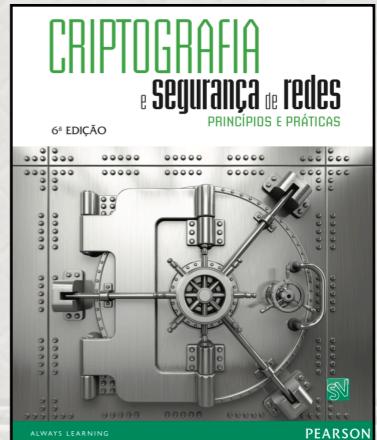
Rafael Vieira Coelho

Livros



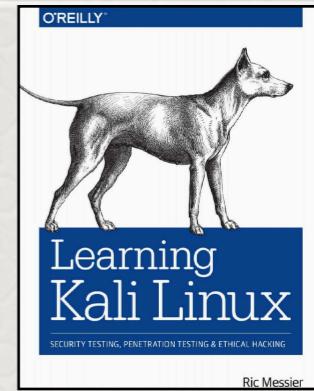


Criptografia e Segurança de Redes: Princípios e Práticas 6ª Edição



1. Introdução e Técnicas Clássicas de Criptografia (cap. 1 e 2)
2. Cifras de Bloco e DES (cap. 3)
- 3. AES (cap. 5)**
4. Cifras Assimétricas (Chave Pública) (cap. 9 e 10)
5. Funções de Hash (cap. 11)
6. Autenticação de Mensagens (cap. 12)
7. Assinaturas Digitais (cap. 13)
8. Gerenciamento e Distribuição de Chaves (cap. 14)
9. Controle de Acesso à Rede e Segurança na Nuvem (cap. 16)
10. Segurança na Camada de Transporte (cap. 17)
11. Segurança em Redes Wireless (cap. 18)
12. Segurança de e-mail (cap. 19)
13. Segurança de IP (cap. 20)
14. Intrusos (cap. 18 da 4 edição)
15. Software malicioso (cap. 19 da 4 edição)
16. Firewalls (cap. 20 da 4 edição)

Learning Kali Linux: Security Testing, Penetration Testing & Ethical Hacking



18. Kali Linux (introdução e ambientação) (cap. 1)
19. Segurança em Rede (cap. 2)
20. Reconhecimento (scanning) (cap. 3)
21. Vulnerabilidades (cap. 4)
22. Exploits (cap. 5)
23. Framework Metasploit (cap. 6)
24. Segurança em Rede Sem-Fio (cap. 7)
25. Segurança em Aplicações WEB (cap. 8)
26. Quebrando Senhas (cap. 9)
27. Aspectos Avançados (cap. 10)
28. Relatório (Análise Forense Digital) (cap. 11)

Capítulo 5

5.1 ARITMÉTICA DE CORPO FINITO

5.2 ESTRUTURA DO AES

Estrutura geral

Estrutura detalhada

5.3 FUNÇÕES DE TRANSFORMAÇÃO DO AES

Transformação subBytes

Transformação ShiftRows

Transformação MixColumns

Transformação AddRoundKey

5.4 EXPANSÃO DE CHAVE DO AES

Algoritmo de expansão de chave

Raciocínio

5.5 EXEMPLO DE AES

Resultados

Efeito avalanche

5.6 IMPLEMENTAÇÃO DO AES

Cifra inversa equivalente

Aspectos de implementação

Advanced Encryption Standard

- * No AES, todas as operações são realizadas em 8 bits.
- * As operações aritméticas de soma, multiplicação e divisão são feitas sobre o corpo finito $GF(2^8)$. Basicamente, um corpo é um conjunto no qual nós podemos somar, subtrair, multiplicar e dividir sem sair dele.

Polynomial: $x^6 + x^4 + x + 1$

Binary: 01010011

Polynomial: $(x^6 + x^4 + x + 1) + (x^7 + x^6 + x^3 + x) = x^7 + x^4 + x^3 + 1$

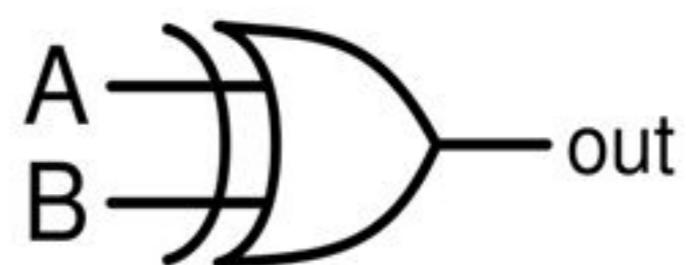
Binary: {01010011} + {11001010} = {10011001}

- * A aritmética nos coeficientes é calculada usando módulo 2. Isso é o mesmo que realizar a operação XOR.

Operação lógica XOR

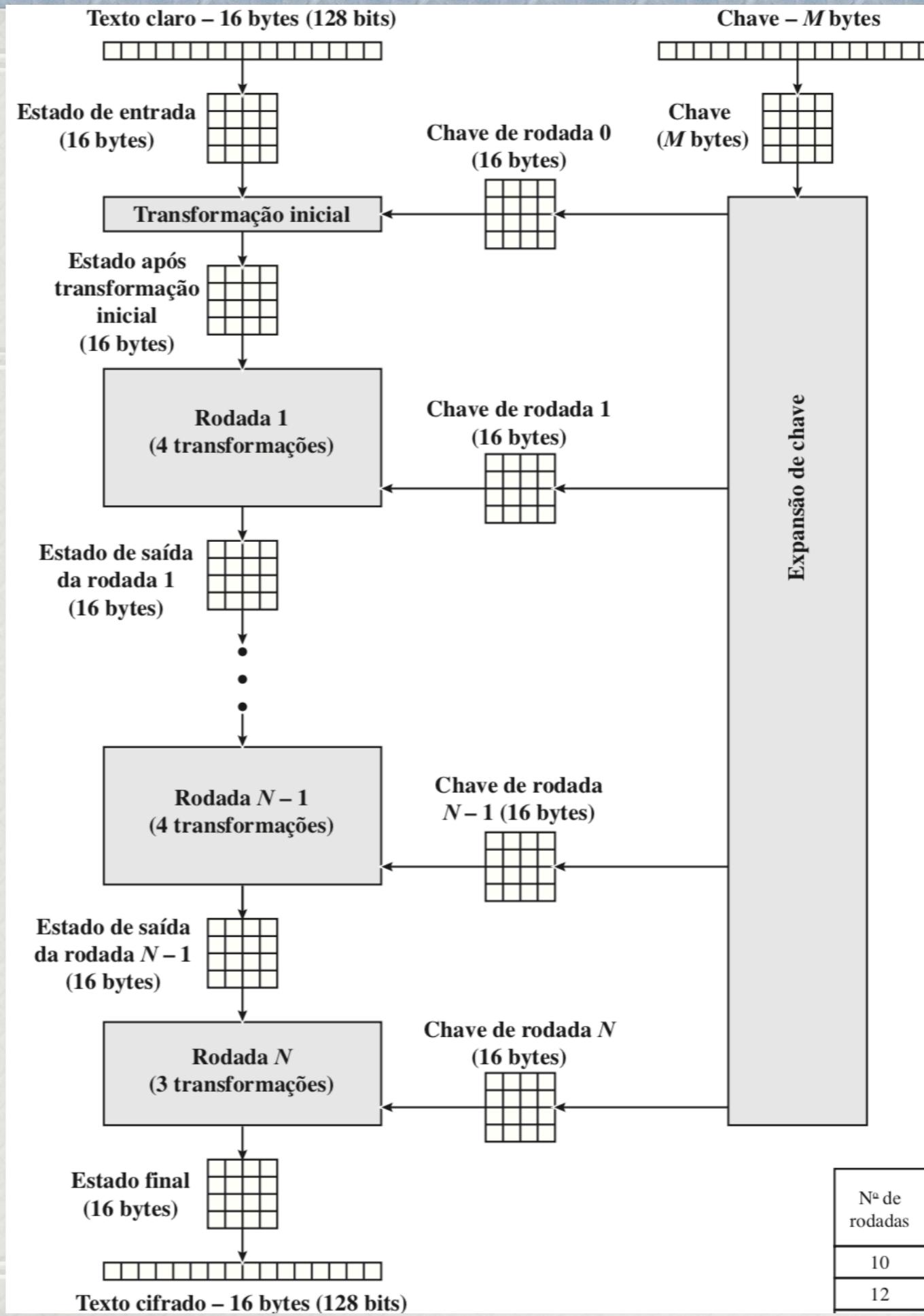
- Conceito
 - Produz um resultado verdade se somente uma de duas entradas for verdade.
 - A saída será verdade se os valores das entradas forem diferentes.
 - XOR = EXCLUSIVE OR.
- Exemplos
 - Se $A = 1$ e $B = 0$, então:
 $A \oplus B = 0$.
 - Se $A = 11001$ e $B = 11110$, então: $A \oplus B = 00111$.

Entrada		Saída
A	B	$X = A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0



5.2 Estrutura do AES

- * O algoritmo de encriptação utiliza um bloco de 16 bytes de texto claro como entrada e uma chave de M bytes, e produz um bloco de 16 bytes de texto cifrado como saída.
- * A rodada 0 é simplesmente de inclusão de chave;
- * Cada rodada conta com a função incluir chave, que utiliza os 16 bytes dela. A chave inicial é expandida, de modo que cada rodada utiliza uma chave de rodada distinta de M bytes.
- * Cada estágio é facilmente reversível. Funções inversas são usadas no algoritmo de decriptação.

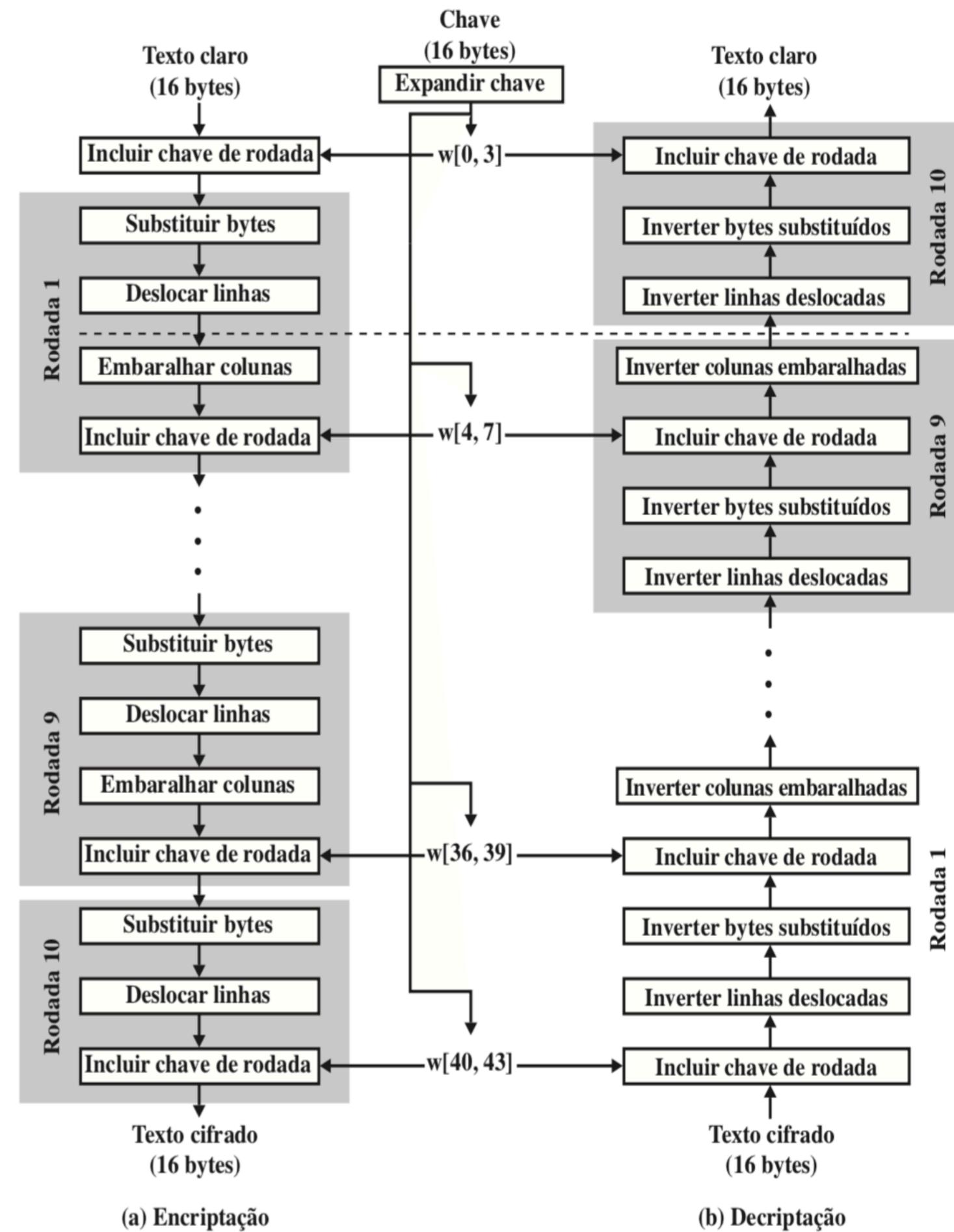


5.3 Funções de Transformação do AES

- * Quatro estágios diferentes são usados, um de permutação e três de substituição:

 1. **SubBytes**: substituição byte a byte do bloco
 2. **ShiftRows**: uma permutação simples
 3. **MixColumns**: uma substituição que utiliza aritmética sobre $GF(2^8)$
 4. **AddRoundKey**: um XOR bit a bit simples do bloco atual com uma parte da chave expandida

- * A cifra começa com um estágio AddRoundKey, seguido por nove rodadas, e cada uma inclui todos os quatro estágios, seguidas por uma décima rodada de três estágios.
- * Somente o estágio AddRoundKey utiliza a chave. Por esse motivo, a cifra começa e termina com ele. Qualquer outro estágio, aplicado no início ou no final, é reversível sem conhecimento da chave e, portanto, não impacta na segurança.
- * Podemos ver a cifra como operações alternadas de encriptação XOR



Parâmetros do AES

- * O AES não é uma estrutura Feistel.
- * Lembre-se de que, na estrutura Feistel clássica, metade do bloco de dados é usada para modificar a outra metade, e depois elas são invertidas.
- * Em vez disso, AES processa o bloco de dados inteiro como uma única matriz durante cada rodada usando substituições e permutação.

Tamanho da chave (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Tamanho do bloco de texto claro (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Número de rodadas	10	12	14
Tamanho da chave de rodada (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Tamanho da chave expandida (words/bytes)	44/176	52/208	60/240

Representação dos Dados no AES

$b_0 b_1 b_2 b_3$	$b_8 b_9 b_{10} b_{11}$
$b_4 b_5 b_6 b_7$	$b_{12} b_{13} b_{14} b_{15}$

Representação de bits

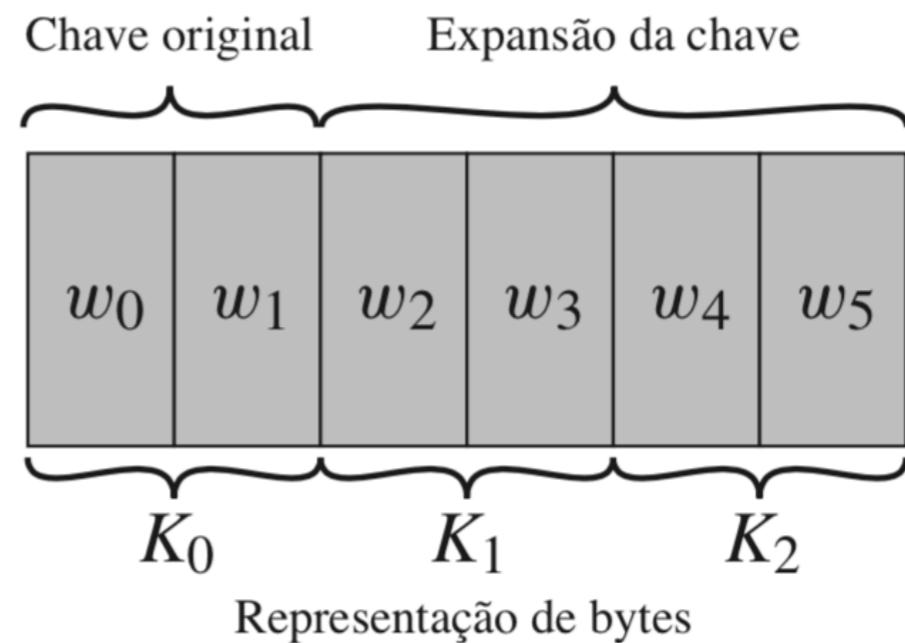
$S_{0,0}$	$S_{0,1}$
$S_{1,0}$	$S_{1,1}$

Representação de nibbles

(a) Matriz de estado

$k_0 k_1 k_2 k_3 k_4 k_5 k_6 k_7$	$k_8 k_9 k_{10} k_{11} k_{12} k_{13} k_{14} k_{15}$
-----------------------------------	---

Representação de bits



(b) Chave

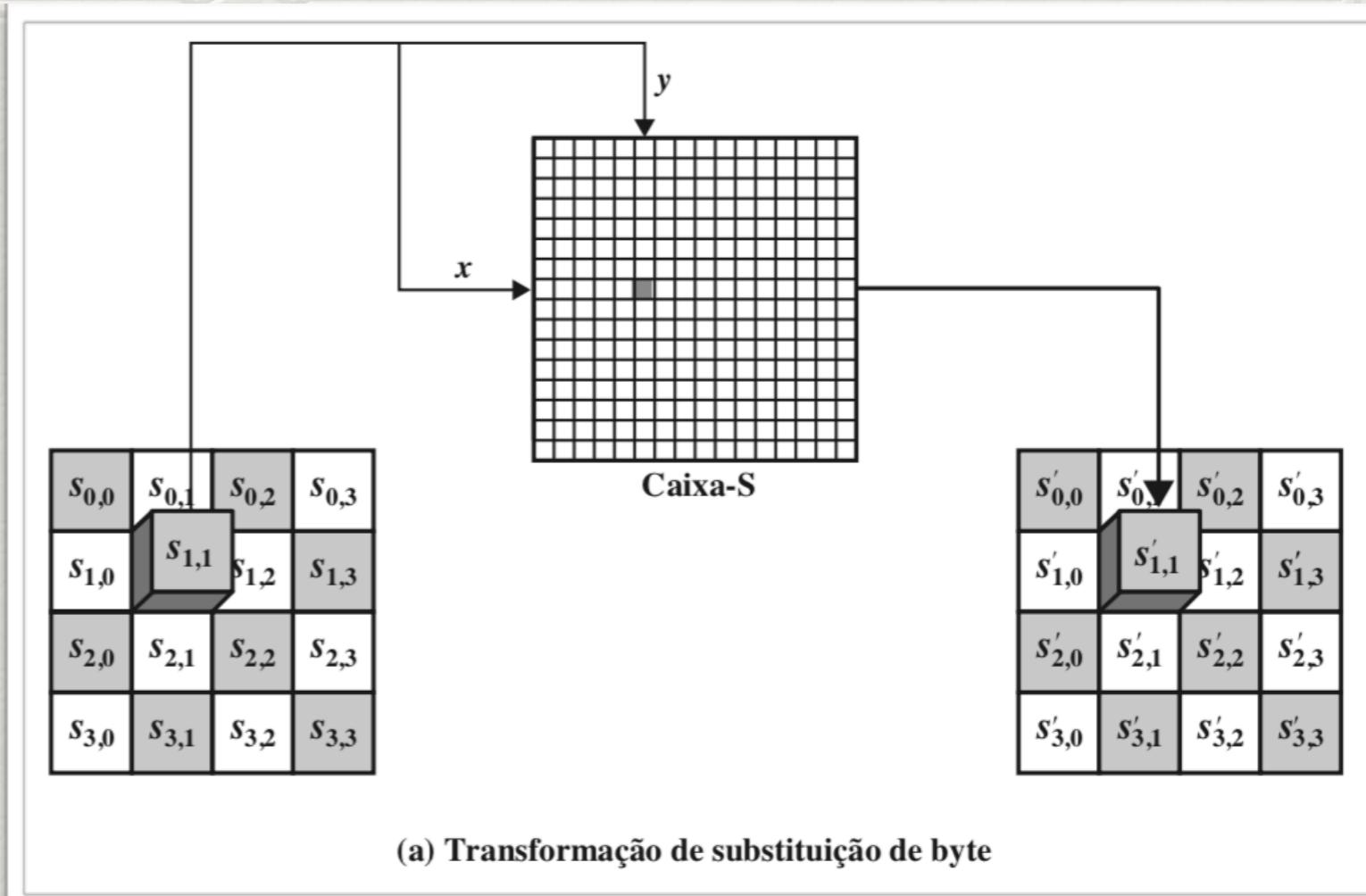
1. SubBytes

- * Cada byte individual de **Estado** é mapeado para um novo byte da seguinte maneira:

Os 4 bits mais à esquerda do byte são usados como um valor de linha e os 4 bits mais à direita, como um valor de coluna.

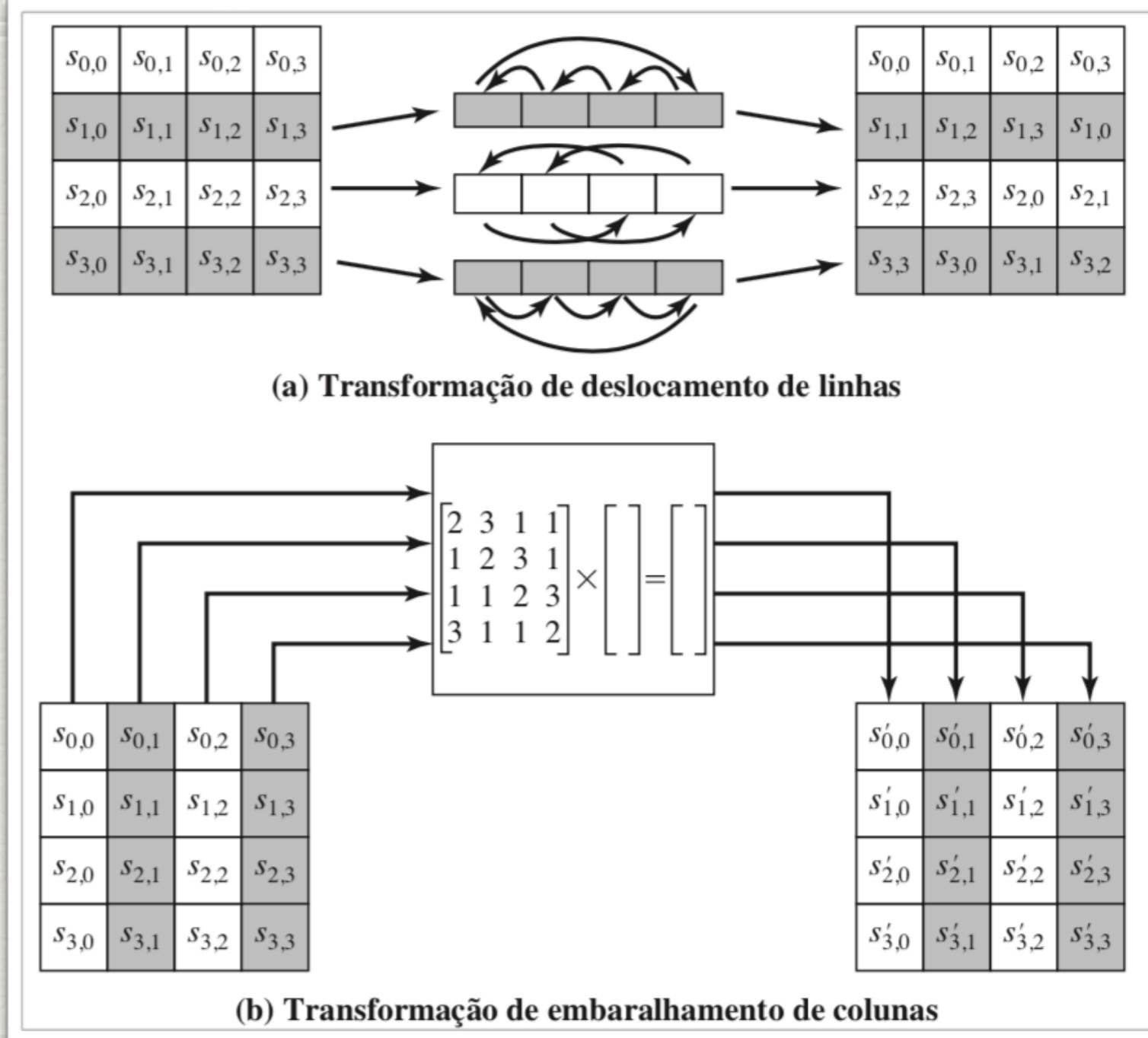
- * Esses valores de linha e coluna servem como índices para a S-box (matriz 16x16 bytes) a fim de selecionar um valor de saída de 8 bits.

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



2. ShiftRows

- * A primeira linha de **Estado** não é alterada.
- * Para a segunda linha, é realizado um deslocamento circular à esquerda por 1 byte.
- * Para a terceira linha, é feito um deslocamento circular à esquerda por 2 bytes.
- * Para a quarta linha, ocorre um deslocamento circular à esquerda por 3 bytes.



3. MixColumns

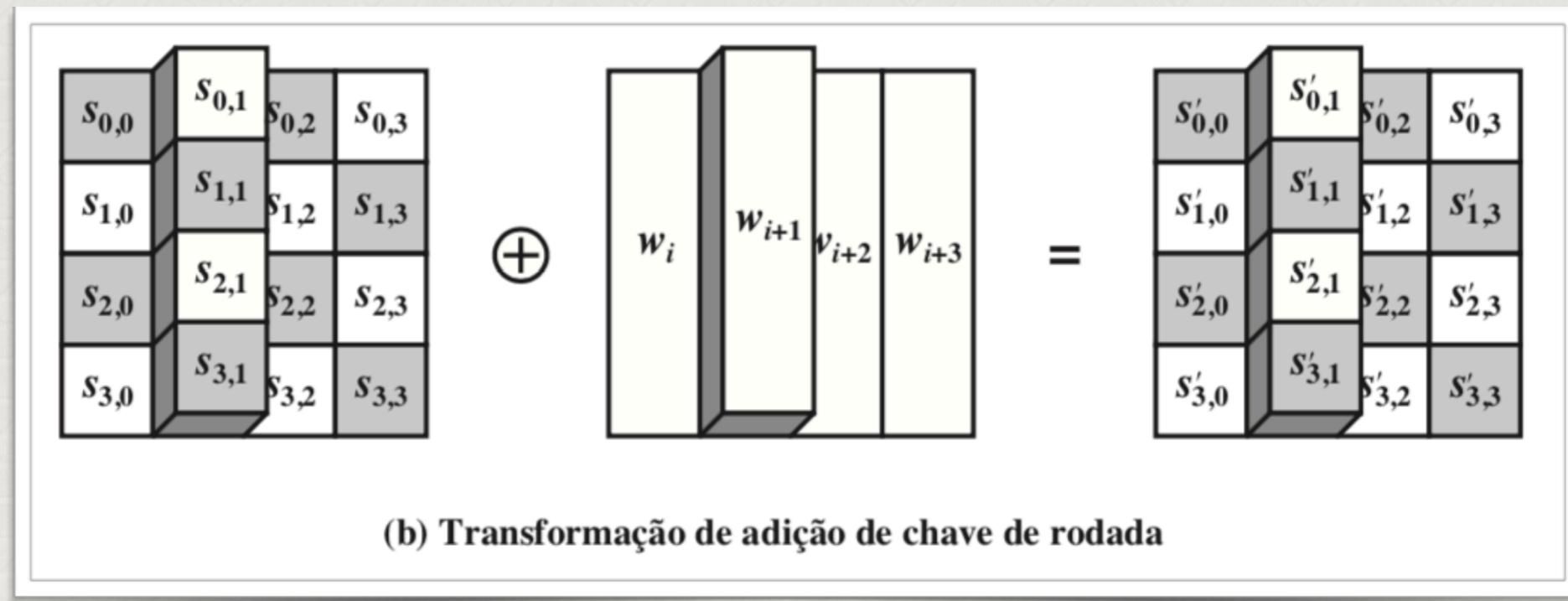
- * A multiplicação de um valor por x pode ser implementada como um deslocamento à esquerda por 1 bit seguido de um XOR bit a bit com (0001 1011), caso o bit mais à esquerda do valor original (antes do deslocamento) seja 1.

TRANSFORMAÇÕES DIRETA E INVERSA A transformação direta de embaralhamento de colunas, chamada MixColumns, opera sobre cada coluna individualmente. Cada byte de uma coluna é mapeado para um novo valor que é determinado em função de todos os quatro bytes nessa coluna. A transformação pode ser definida pela seguinte multiplicação de matriz sobre **Estado** (Figura 5.7b).

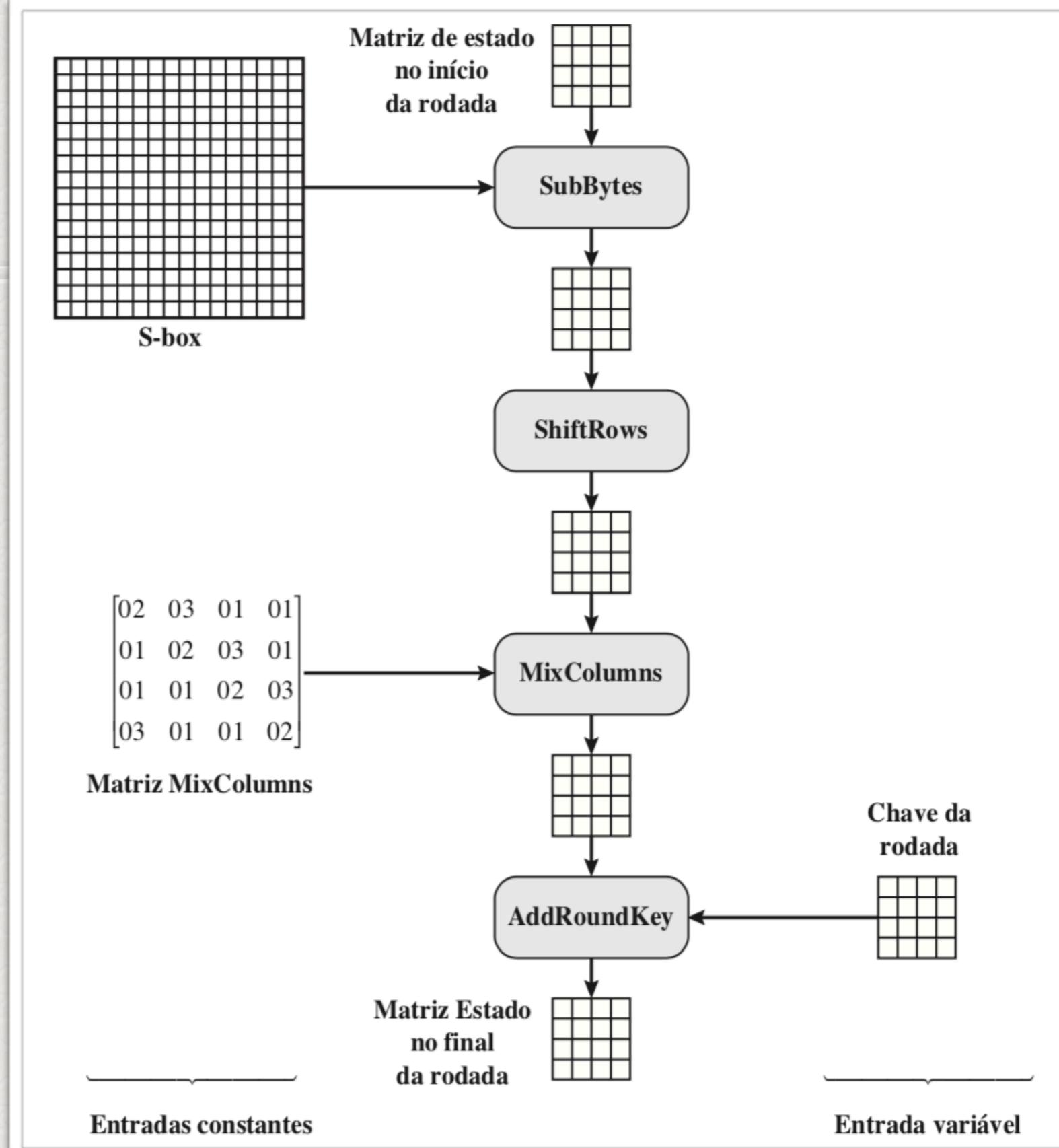
$$\begin{array}{cc|cc} & & & \\ \begin{array}{ccccc} 02 & 03 & 01 & 01 & s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ | & & & & s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ 01 & 02 & 03 & 01 & | & | & | & | \\ 01 & 01 & 02 & 03 & s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ 03 & 01 & 01 & 02 & s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{array} & = & \begin{array}{cccc} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{array} & (5.3) \end{array}$$

4. AddRoundKey

- * Os 128 bits de **Estado** passam por um XOR bit a bit com os 128 bits da chave da rodada.



Resumo de 1 Rodada do AES



5.4 Expansão da Chave AES

Os desenvolvedores do **Rijndael** criaram o algoritmo de expansão de chave para ser resistente a ataques criptoanalíticos conhecidos. A inclusão de uma constante dependente da rodada elimina a simetria, ou similaridade, entre as formas como as chaves da rodada são geradas em diferentes rodadas. Os critérios específicos que foram usados são os seguintes:

- * O conhecimento de uma parte da chave da cifra ou chave da rodada não permite o cálculo de muitos outros bits dela.
- * Uma transformação reversível [ou seja, o conhecimento de quaisquer Nk words consecutivas da chave expandida permite a regeneração da chave expandida inteira (Nk = tamanho da chave em words)].
- * Uso de constantes de rodada para eliminar simetrias.
- * Difusão de diferenças de chave de cifra nas chaves da rodada; ou seja, cada bit de chave afeta muitos bits de chave da rodada.

TAREFAS

1. Qual é a diferença entre rijndael e AES?
2. Descreva rapidamente o estágio SubBytes.
3. Descreva rapidamente o estágio Shiftrows.
4. Descreva rapidamente o estágio MixColumns.
5. Descreva rapidamente o estágio addroundKey.
6. Descreva rapidamente o algoritmo de expansão de chave.
7. Qual é a diferença entre o algoritmo de decriptação AES e a cifra inversa equivalente?
8. Analise e explique o código test-aes.py (<https://github.com/ricmoo/pyaes>).