

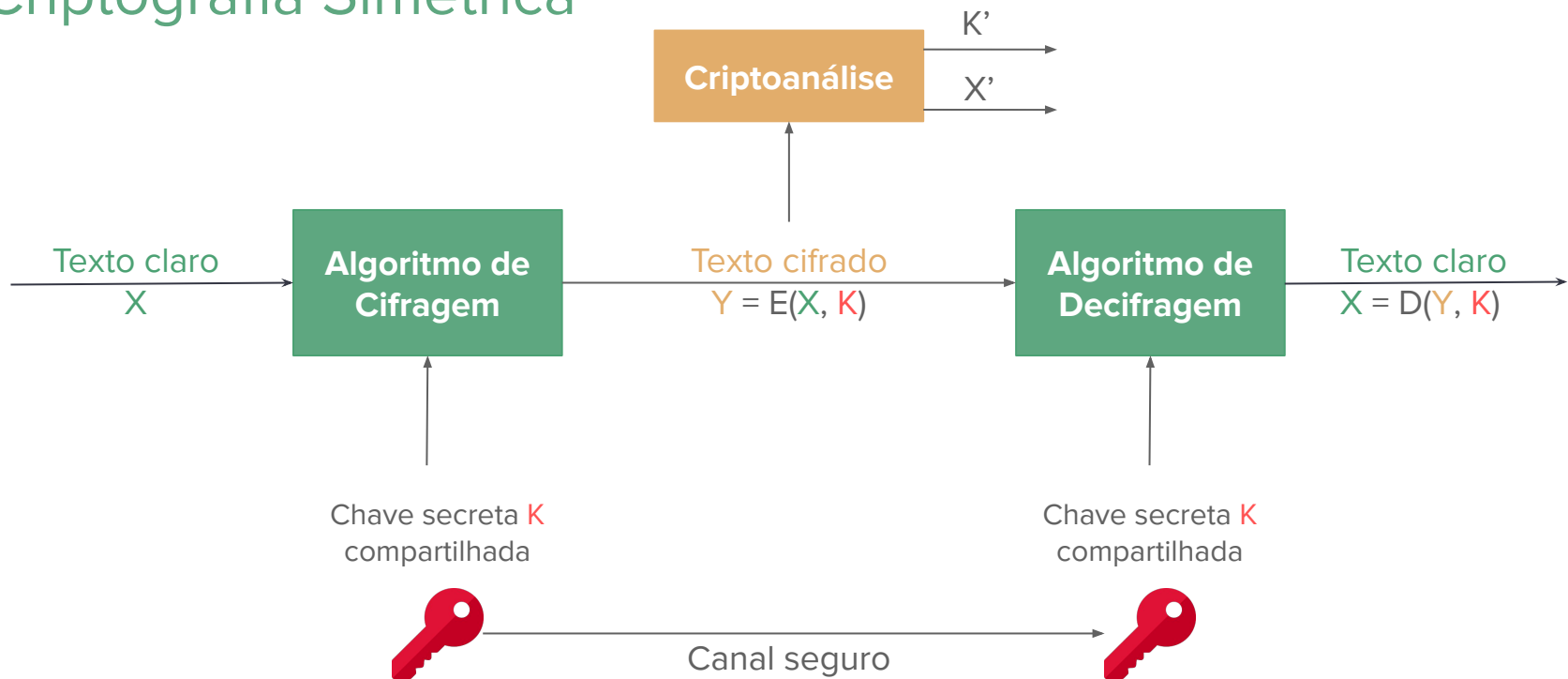
Criptografia Aplicada

Criptografia Simétrica - DES e AES

Sumário

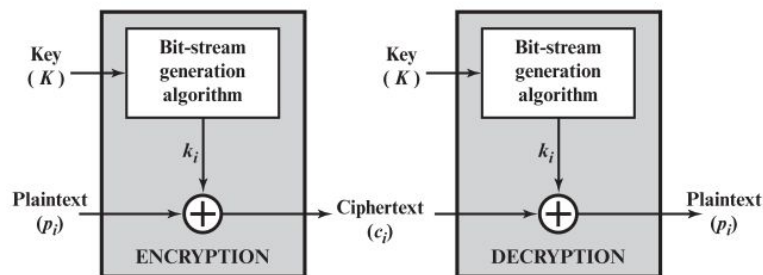
- Conceitos básicos
- DES
- AES
- Criptografia simétrica na prática

Criptografia Simétrica

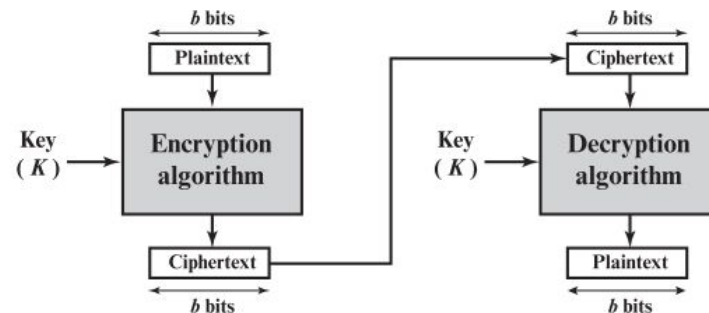


Definições básicas

- Existem dois tipos de criptografia simétrica:
 - Cifras de fluxo (stream)
 - Cifras de bloco



(a) Stream cipher using algorithmic bit-stream generator



(b) Block cipher

Definições básicas

- Queremos evitar que o texto cifrado carregue informações estatísticas do texto claro
 - como distribuição de frequência de letras do texto claro, ou letras ou palavras que provavelmente fazem parte do texto claro;
 - caso contrário, criptoanálise poderia deduzir a chave, ou parte dela.
- Métodos para dissipar informações estatísticas:
 - Difusão
 - Confusão
- **Difusão:** dissipar a estrutura estatística entre texto claro e texto cifrado
 - cada dígito do texto claro afeta o valor de vários dígitos do texto cifrado;
 - diagrama de frequências é mais equilibrado, difícil deduzir a chave utilizada;
 - conseguimos difusão ao aplicar **permutações** repetidamente.
- **Confusão:** dissipar a estrutura estatística entre texto cifrado e valor da chave
 - adiciona complexidade em como a chave foi usada para produzir o texto cifrado;
 - difícil deduzir a chave;
 - conseguimos confusão ao aplicar algoritmos de **substituição** complexos.

Definições básicas

- Cifras de bloco modernas incorporam uma sequência de **permutações** e **substituições**
- Geralmente são iterativas:
 - possuem uma sequência de n *rounds*
 - existe um *key schedule* que produz n *subchaves* k_i através da chave k
 - cada round possui uma *função* que recebe k_i e um estado e produz o próximo estado
 - o estado inicial é o *texto claro* e o estado final depois dos n *rounds* é o *texto cifrado*
 - a decifragem é feita usando uma *função inversa*.
- Vamos estudar a fundo duas cifras de bloco modernas:
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)

Definições básicas

- **Criptanálise linear:** tenta construir equações lineares que relacionam os bits da mensagem, cifra e chave.
 - Ou seja, tenta encontrar bits que não funcionam de maneira “aleatória”.
- **Criptanálise diferencial:** estuda como as diferenças na entrada resultam em diferenças na saída.
 - São estudados os XORs de duas entradas e de suas respectivas saídas para descobrir as chaves utilizadas.
- Estes ataques são probabilísticos e recuperam a chave dados pares de texto claro e texto cifrado suficientes.
- Esquemas criptográficos modernos devem evitar estes ataques.

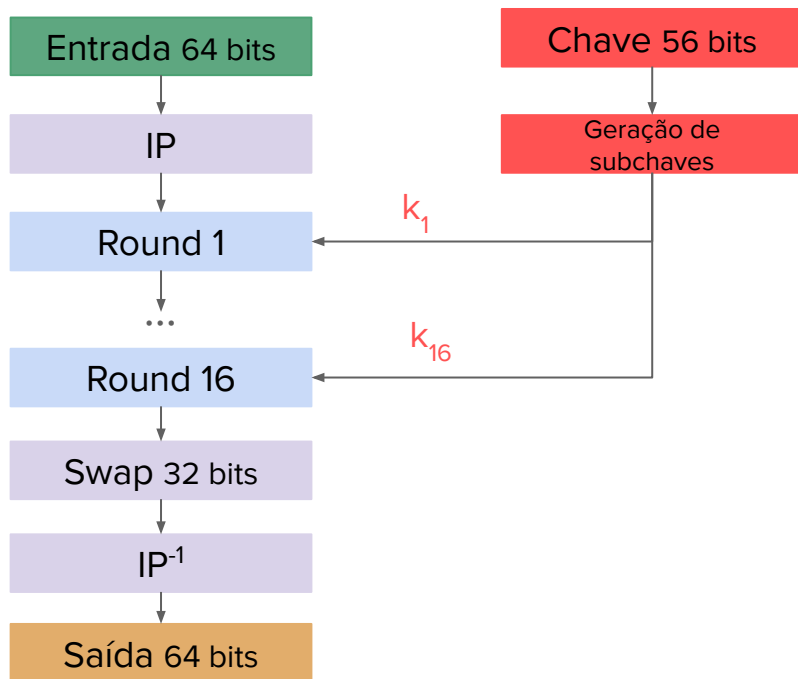
Sumário

- Conceitos básicos
- **DES**
- AES
- Criptografia simétrica na prática

DES – Data Encryption Standard (1977)

- Cifra simétrica de bloco.
- Desenvolvido pela IBM
 - modificação do sistema Lucifer (1971);
 - baseado em uma rede de Feistel.
- Adotado como padrão pelo NIST em 1977.
- Esperava-se que seria um padrão por 10-15 anos, mas durou muito mais
 - Revisado a cada 5 anos, última revisão em 1999;
 - substituído pelo AES em 2002;
 - não é mais indicado o seu uso.

DES – Data Encryption Standard (1977)



- Entrada dividida em blocos de 64 bits
- Chave k de 56 bits com geração de subchaves k_1, \dots, k_{16} de 48 bits cada
- Permutação inicial (IP) que rearranja os bits da entrada
- 16 rounds de uma mesma função (com substituições e permutações)
- *Swap* dos primeiros 32 bits (esquerda) com os últimos 32 bits (direita).
- Permutação final (IP^{-1}) que é o inverso da IP e gera a cifra de 64 bits.

DES – Data Encryption Standard (1977)

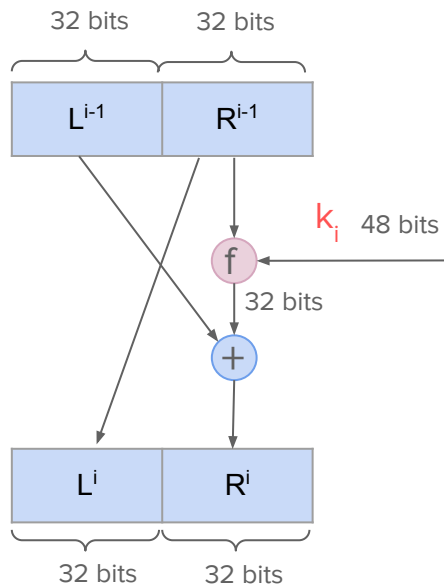


Figura: Um *round* do DES

- Cada *round* recebe um estado de entrada, dividido em duas partes: L^{i-1} e R^{i-1} .
- Gera o próximo estado, composto por duas partes: L^i e R^i .
- A figura ao lado mostra um *round*
 - $L^i = R^{i-1}$
 - $R^i = L^{i-1} \oplus f(R^{i-1}, k_i)$
- A permutação inicial IP gera o primeiro estado $L^0 R^0$.
- A permutação IP^{-1} recebe como entrada o estado $R^{16} L^{16}$
 - note que o *swap* troca $L^{16} R^{16}$ por $R^{16} L^{16}$

DES – Data Encryption Standard (1977)

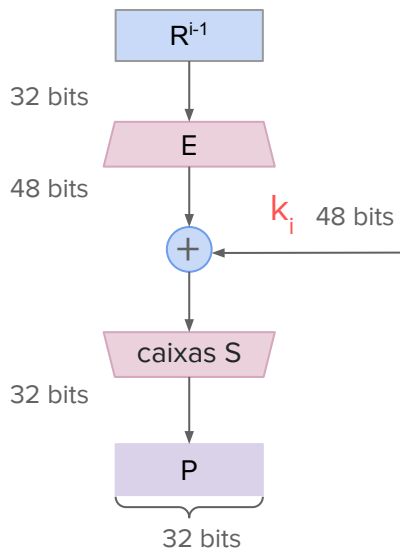


Figura: Função f do DES

- A função f recebe como entrada:
 - R^{i-1} com 32 bits e k_i com 48 bits
- A função E faz permutação e expande R^{i-1} e gera uma saída de 48 bits;
- XOR é aplicado entre a saída de E e k_i , produzindo um resultado de 48 bits;
- esse resultado é a entrada das caixas S :
 - elas recebem 48 bits e retornam 32
 - fazem substituição
 - fundamentais para a segurança do sistema, muito resistentes à ataques diferenciais
- Permutação final retorna 32 bits.

DES – Segurança

- A maior crítica do DES é o tamanho do espaço de chaves 2^{56}
- Ataque de força bruta
 - em 1977 já existia a possibilidade de um chip que testa 10^6 chaves por segundo
 - uma máquina com 10^6 chips poderia buscar o espaço de chaves todo em um dia
 - essa máquina teria um valor estimado (na época) de US\$20 milhões
 - em 1998 foi construída a máquina *DES Cracker*
 - capaz de buscar 88 bilhões de chaves por segundo
 - custo de US\$250.000, encontrou uma chave DES em 56 horas
 - atualmente, o <https://crack.sh/> consegue fazer busca exaustiva em 26 horas usando 48 FPGAs
- Criptoanálise Linear e Diferencial
 - Linear é mais eficiente, implementada em 1994
 - usa 2^{43} pares de texto plano e cifra
 - 40 dias para gerar os pares, 10 dias para encontrar a chave

Sumário

- Conceitos básicos
- DES
- **AES**
- Criptografia simétrica na prática

AES - Advanced Encryption Standard

- Cifrador de bloco para substituir o DES
- Competição em 2001, Chamada em 1997
 - 21 algoritmos, 15 candidatos, 5 finalistas, Rijndael vencedor
- Candidatos avaliados de acordo com os seguintes critérios:
 - segurança
 - eficiência computacional
 - características do algoritmo e implementação
- Não usa redes de Feistel
- Padronizado no FIPS 197

AES - Advanced Encryption Standard

- Suporte a chaves de 128, 192 e 256 bits
- Blocos de 128 bits
- Número de *rounds* dependente do tamanho da chave

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

Imagem: W. Stallings. *Cryptography and network security*. Cap 6.2

AES - Overview

- Blocos de 128 bits são representados como matrizes de bytes 4 x 4
- A chave é utilizada para criar $n+1$ subchaves de 128 bits (16 bytes) cada
- Cada *round*, com exceção do último, consiste de 4 transformações:
 - SubBytes, ShiftRows, MixColumns, e AddRoundKey
- O último round consiste de apenas três transformações
 - importante para que a cifra seja reversível

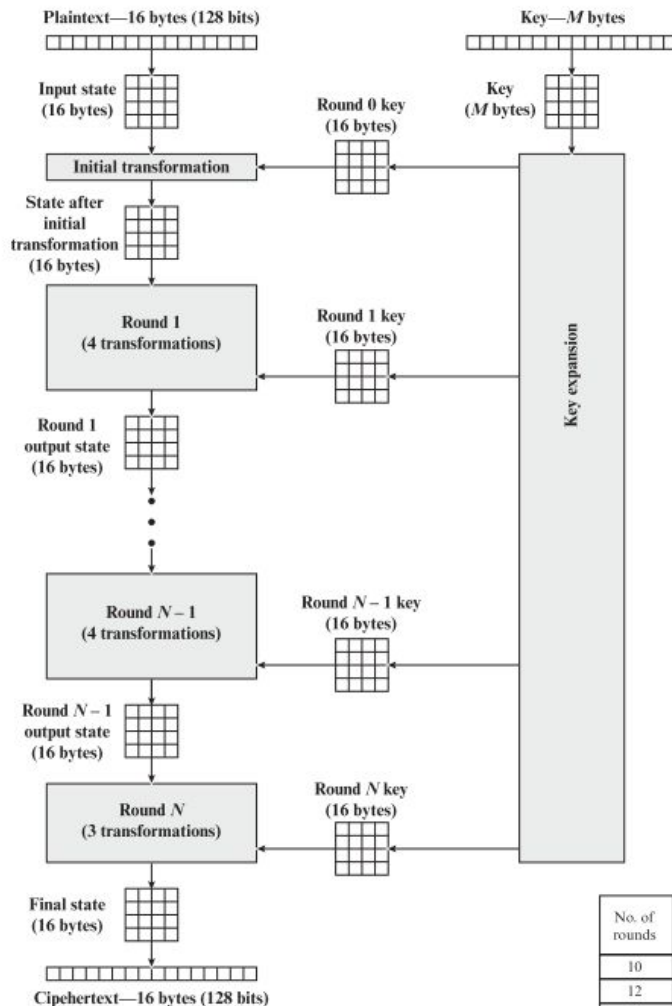


Figure 6.1 AES Encryption Process

AES - Rounds

- **SubBytes:** usa uma caixa S para fazer substituições byte a byte
- **ShiftRows:** permutação simples
- **MixColumns:** substituição nas colunas através de uma transformação linear
- **AddRoundKey:** XOR do estado com a subchave
- Cada transformação é facilmente reversível
 - existe uma função inversa para cada uma das 3 primeiras transformações
 - AddRoundKey é revertido ao fazer o XOR com a subchave novamente

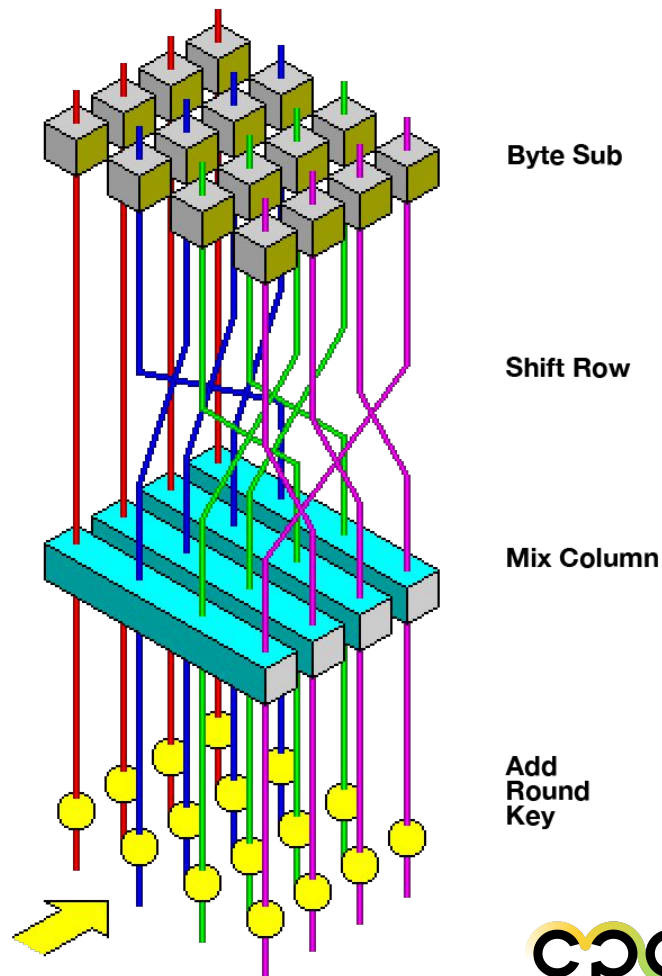
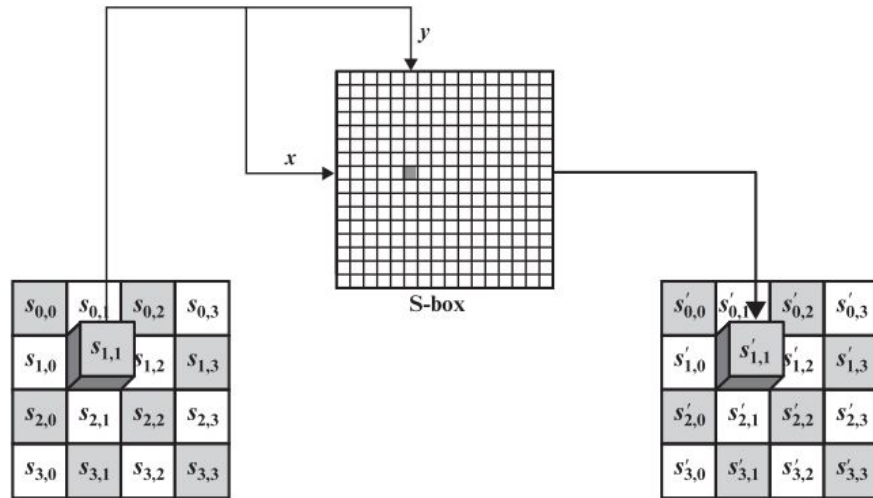


Imagem: <https://tinyurl.com/AES-round>

AES - SubBytes

- S-box é uma tabela de 16 x 16 bytes
- Cada byte de um estado é mapeado para um novo byte de acordo com a tabela
 - os 4 bits mais à esquerda determinam a linha da caixa S e os 4 bits mais à direita determinam a coluna
- Existem 2 caixas S
 - uma para a cifragem
 - e sua correspondente inversa para decifragem



(a) Substitute byte transformation

AES - ShiftRows

- Permutações simples nas linhas:
 - A primeira linha do estado não é alterada
 - Na segunda linha, é feito um *shift* de 1 byte para a esquerda de forma circular
 - Na terceira linha, é feito um *shift* de 2 bytes para a esquerda de forma circular
 - Na quarta linha, é feito um *shift* de 3 bytes para a esquerda de forma circular
- Existe também a transformação *InvShiftRows*, que faz *shifts* na direção oposta
 - utilizada para decifragem

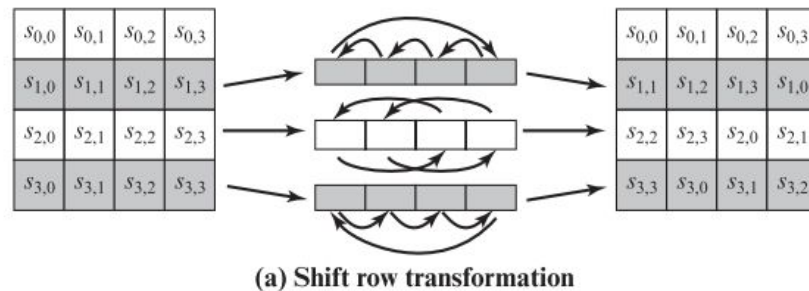


Imagem: W. Stallings. *Cryptography and network security*. Cap 6.3

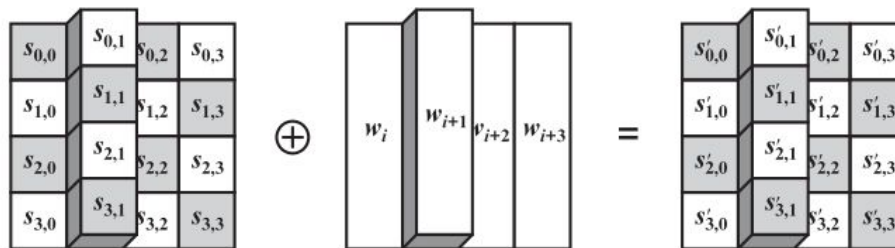
AES - MixColumns

- Multiplicação de uma coluna do estado por uma matriz pré-determinada
- Cada elemento (byte) de uma coluna é mapeado para outro com base em uma função (multiplicação e somas) que considera todos os 4 bytes daquela coluna
- Implementação prática baseada em XORs
- Existem também uma outra matriz utilizada para a decifragem (InvMixColumns)

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

AES - AddRoundKey

- XOR do estado com uma subchave do *round* (ambos de 128 bits)
- A operação é feita coluna por coluna ou byte por byte
- Ao refazer o XOR com a mesma subchave, conseguimos inverter a operação
 - já que $s \oplus k_i \oplus k_i = s$



(b) Add round key transformation

Imagem: W. Stallings. *Cryptography and network security*. Cap 6.3

AES - Cifragem e Decifragem

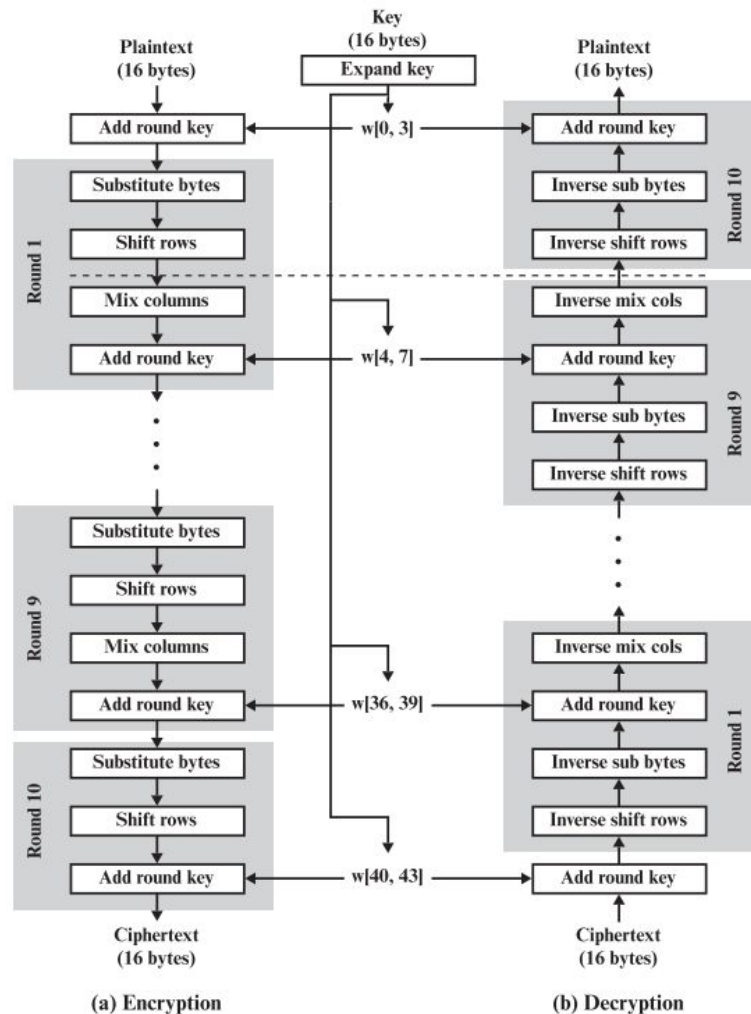


Figure 6.3 AES Encryption and Decryption

AES - Segurança

- AES é seguro contra todos os ataques conhecidos hoje em dia
- Vários aspectos do seu design foram incorporados para ajudar na segurança de ataques específicos
 - As operações feitas internamente nas caixas S garantem uma segurança contra ataques lineares e diferenciais
 - a transformação linear da etapa de MixColumns faz com que seja muito difícil encontrar ataques lineares e diferenciais
- Aparentemente, nenhum ataque "geral" no AES consegue ser significativamente mais rápido que o ataque de força bruta
 - O mais eficiente é o **biclique attack**, publicado em 2011, que reduz a complexidade de uma busca exaustiva por um fator de 4 ou 5
- Existem alguns ataques na geração de subchaves, que obtiveram sucesso apenas em variações do AES que usam menos *rounds*.
 - **related-key attack** conseguiram obter chaves em tempo 2^{39} em um AES de 9 *rounds*.

AES - eficiência

- Implementação eficiente em software
 - utiliza operações simples e bem definidas
 - implementações geralmente utilizam técnicas de otimização
- Implementação eficiente em hardware
 - projetadas para alto desempenho e eficiência energética
 - mais rápidas que as implementações em software
 - utilizam circuitos dedicados para realizar as operações
 - populares em dispositivos com recursos limitados, como IoT

Sumário

- Conceitos básicos
- DES
- AES
- **Criptografia simétrica na prática**

Aplicações

- Garantia de confidencialidade em redes Wi-Fi
- Navegação cifrada entre navegadores e servidores no protocolo HTTPS
- Cifragem de dados armazenados na nuvem com [Dropbox](#) e [Google Cloud](#)
- Segurança na comunicação entre usuário e servidor remoto em protocolos VPN
- Criptografia ponta-a-ponta na proteção de mensagens trocadas pelo WhatsApp e Signal
- entre muitos outros.

Fontes: [\[1\]](#)[\[2\]](#)

Futuro do AES

- Computadores quânticos serão capazes de quebrar alguns criptossistemas utilizados hoje em dia
 - Algoritmo de Shor é capaz de quebrar algoritmos de criptografia assimétrica (RSA e ECC)
 - Algoritmo de Grover pode reduzir a segurança de algoritmos simétricos pela metade
- Acredita-se que o AES ainda estará seguro contra ataques de computadores quânticos
 - AES com chave de 256 bits teria a segurança equivalente ao AES de 128 bits

Atividade: cifrando mensagens

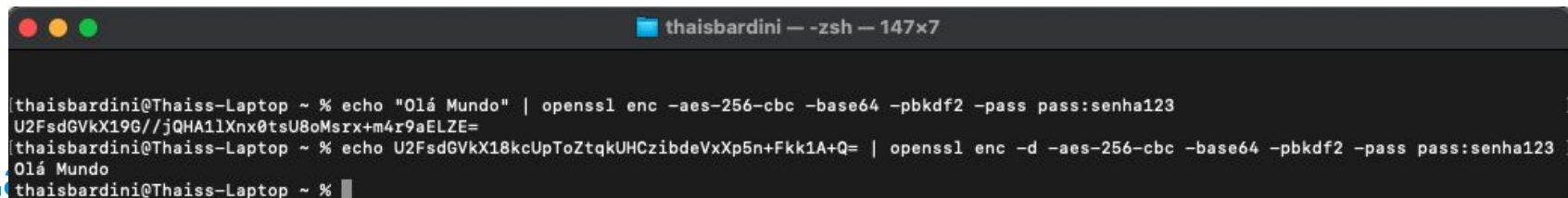
- Vamos praticar utilizando o openssl:

```
echo "msg a ser cifrada" | openssl enc -aes-256-cbc -base64 -pbkdf2 -pass pass:senha
```

- Agora decifre a mensagem cifrada acima usando:

```
echo texto-cifrado | openssl enc -d -aes-256-cbc -base64 -pbkdf2 -pass pass:senha
```

- Se você cifrar duas vezes a mesma mensagem com a mesma senha, o que acontece?



```
thaisbardini — zsh — 147x7

[thaisbardini@Thaiss-Laptop ~ % echo "Olá Mundo" | openssl enc -aes-256-cbc -base64 -pbkdf2 -pass pass:senha123
U2FsdGVkX19G//jQHA1lXnx0tsU8oMsrx+m4r9aELZE=
[thaisbardini@Thaiss-Laptop ~ % echo U2FsdGVkX18kcUpToZtqkUHCzibdeVxXp5n+Fkk1A+Q= | openssl enc -d -aes-256-cbc -base64 -pbkdf2 -pass pass:senha123
Olá Mundo
[thaisbardini@Thaiss-Laptop ~ % ]
```

Resumo

- Conceitos básicos
 - cifra de fluxo x cifra de bloco
 - difusão x confusão
 - criptoanálise linear x diferencial
- DES
 - chave de 56 bits, blocos de 64 bits
 - 16 rounds com substituições e permutações
- AES
 - chaves de 128, 192 e 256 bits, blocos de 128 bits
 - 10, 12 ou 14 rounds
 - substituiu o DES

Referências

- W. Stallings. *Cryptography and network security*. 7a edição.
 - Capítulos 4.1, 4.2, 4.3, 4.4, 6.2, 6.3, 7.2, 7.3, 7.4, 7.5, 7.6
- D. Stinson e M. Paterson. *Cryptography: Theory and Practice*. 4a edição.
 - Capítulos 4.1, 4.5, 4.6
- Joachim von zur Gathen. *CryptoSchool*. 1a edição.
 - Capítulo 2.2
- Buchanan, William J (2023). AES (Advanced Encryption Standard). Asecuritysite.com. <https://asecuritysite.com/aes/>
- Buchanan, William J (2023). DES, 3DES and Feistel ciphers. Asecuritysite.com. <https://asecuritysite.com/des/>