Criptografia

Introdução à criptografia simétrica moderna

Roadmap

- Cenário básico
- O problema de distribuição de chaves
- Protocolo Diffie e Hellman
- O algoritmo DES
- O algoritmo AES

Universidade Federal do Ceará
Campus de Crateús

Ciência da Computação
Sistemas de Informação

emerson@crateus.ufc.br

Criptografia simétrica

Introdução

- A **criptografia simétrica** é conhecida também por **criptografia de chave secreta**.
- Esse método de cifra utiliza a **mesma chave** para cifrar e decifrar uma mensagem.
- O emissor e o receptor concordam em utilizar uma determinada chave e então a compartilham entre eles.

Compartilhamento seguro

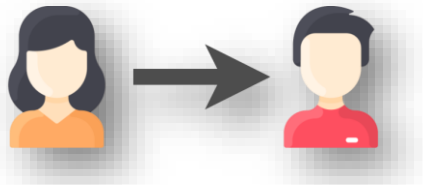
- O compartilhamento da chave precisa ser seguro, do contrário, todo o processo criptográfico seria em vão.
- Observe que é necessário um canal de comunicação para o compartilhamento da chave secreta **diferente** do canal utilizado para transmitir a mensagem criptografada.

- Assim, nasce um dos grandes problemas da criptografia, conhecido como o **problema da distribuição de chaves.**

Criptografia simétrica

Cenário básico

- Em geral, um processo de **criptografia simétrica** pode ser representado pelo **cenário** a seguir:



- Suponha que Alice deseja enviar uma mensagem **confidencial** a Bob.

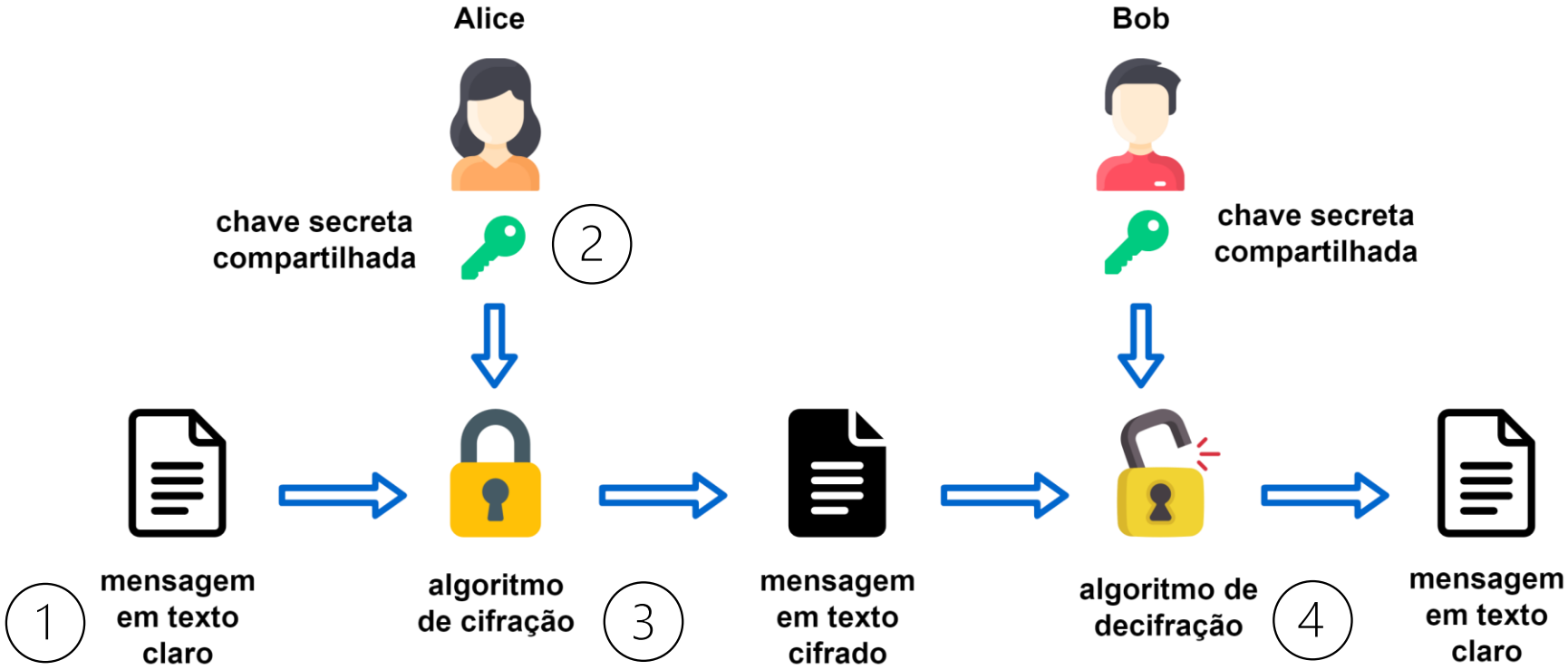
- Alice sabe que o canal de comunicação **não é seguro**, portanto a mensagem a ser enviada será criptografada.

- Alice compartilha uma **chave secreta** com Bob. Considere que a chave foi compartilhada em um momento anterior.

Criptografia simétrica

Cenário básico

- O esquema de criptografia simétrica utilizado por Alice e Bob precisa de quatro elementos básicos: **(1) mensagem; (2) chave; (3) algoritmo de cifração, (4) algoritmo de decifração.**



O problema de distribuição de chaves

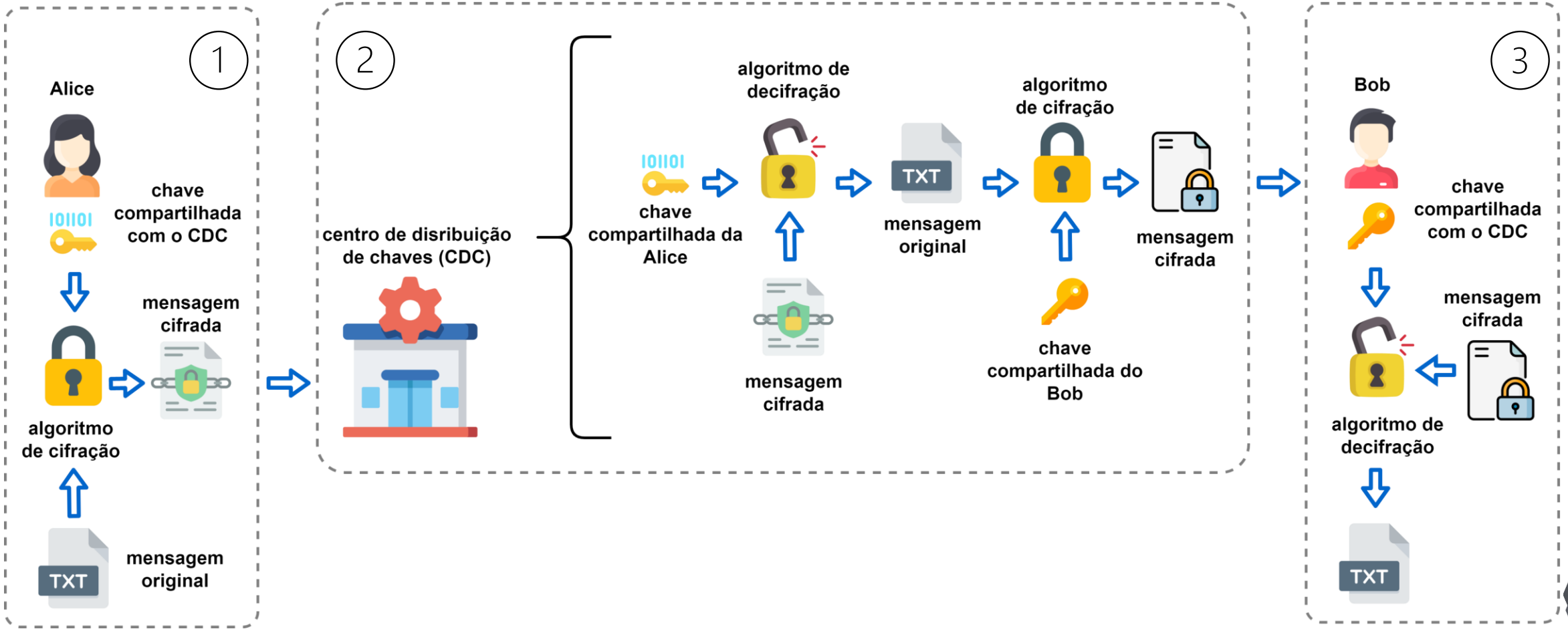
- Claramente, o grande desafio desse método é como **compartilhar** a chave secreta de forma segura entre o emissor e o receptor da mensagem.

- A maneira mais natural de compartilhar essa chave seria estabelecer uma comunicação utilizando um **outro canal** considerado seguro ou um **encontro pessoal privado**.

- Outra maneira é fazer uso de um **centro de distribuição de chaves**, com o qual os usuários compartilham sua chave secreta.

Criptografia simétrica

Distribuição de chave usando uma terceira parte confiável



Distribuição de chave usando uma terceira parte confiável

1. Suponha que Alice deseja enviar uma mensagem para Bob, então ela cifra a mensagem usando sua chave secreta e a envia ao centro de distribuição de chaves (CDC).

2. O CDC, conhecendo todas as chaves secretas, decifra a mensagem usando a chave de Alice, e então a cifra novamente usando a chave de Bob e envia a mensagem cifrada com a nova chave para Bob.

O CDC passa a ter conhecimento de todas as mensagens secretas.

3. Agora, Bob decifra a mensagem usando sua chave secreta, que também é compartilhada com o CDC.

Protocolo Diffie e Hellman (DH)

- Para resolver o problema de distribuição de chave, Diffie e Hellman (1976) apresentaram um método no qual duas pessoas podem produzir uma **chave secreta compartilhada** através da troca de informações públicas.
- Esta técnica ficou conhecida como **protocolo de troca de chave Diffie-Hellmam**.

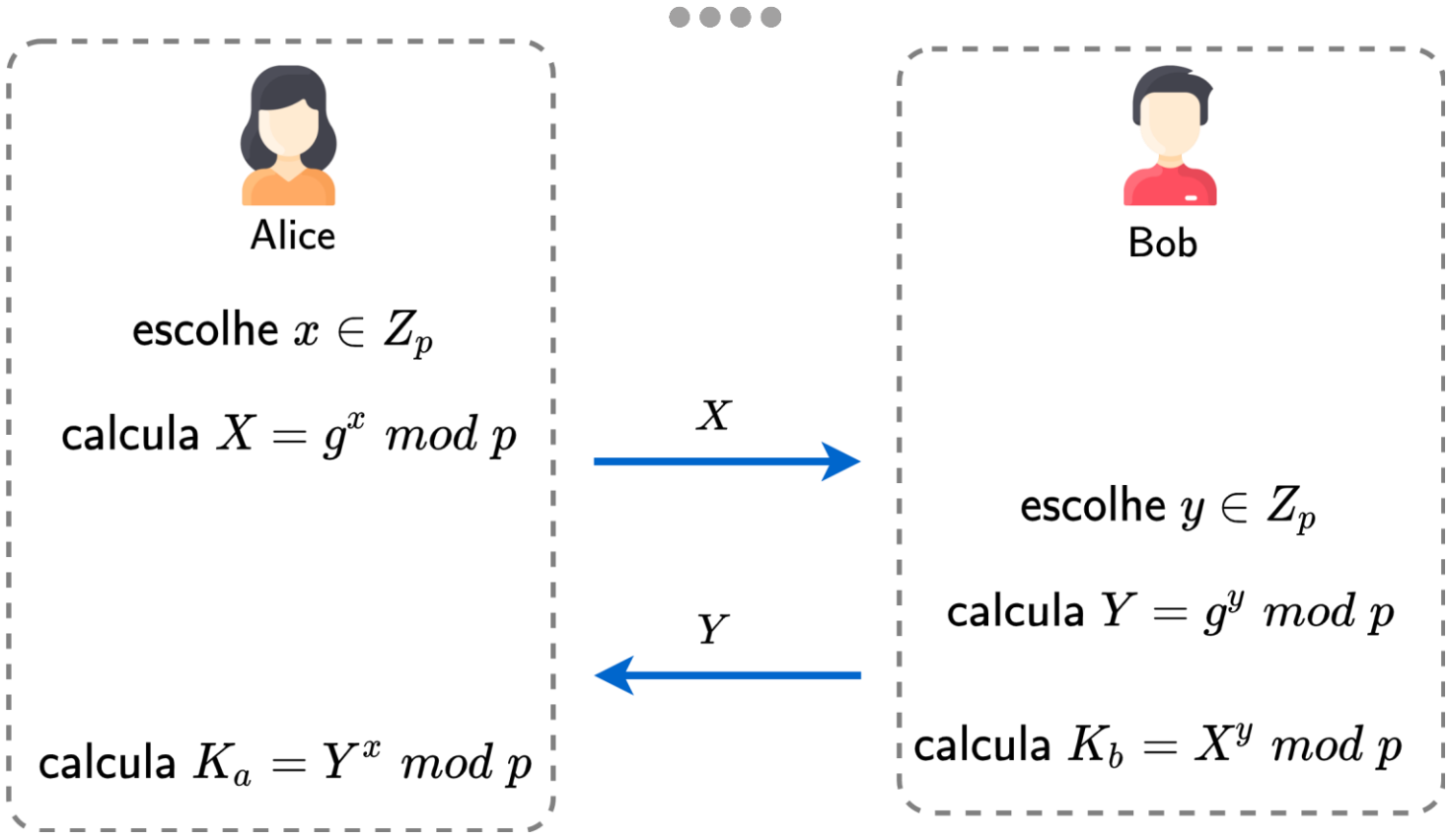
Observação

O protocolo não é em si um criptossistema, ele é utilizado para **gerar** e **compartilhar** a chave de modo seguro quando se pretende fazer uso de um sistema criptográfico simétrico.

Protocolo Diffie e Hellman (DH)

1. **Alice** e **Bob** concordam em usar um número primo $\boldsymbol{p}$ e como base $\boldsymbol{g}$. Tanto $\boldsymbol{p}$ como $\boldsymbol{g}$ são públicos.
2. **Alice** escolhe um inteiro secreto $\boldsymbol{x} \in \boldsymbol{Z_p}$, e usa para calcular $\boldsymbol{X = g^x \ mod \ p}$. Então envia $\boldsymbol{X}$ para Bob.
3. **Bob** escolhe um inteiro secreto $\boldsymbol{y} \in \boldsymbol{Z_p}$, e usa para calcular $\boldsymbol{Y = g^y \ mod \ p}$. Então envia $\boldsymbol{Y}$ para Alice.
4. **Alice** calcula a chave secreta secreto $\boldsymbol{K_a = Y^x \ mod \ p}$
5. **Bob** calcula a chave secreta $\boldsymbol{K_b = X^y \ mod \ p}$

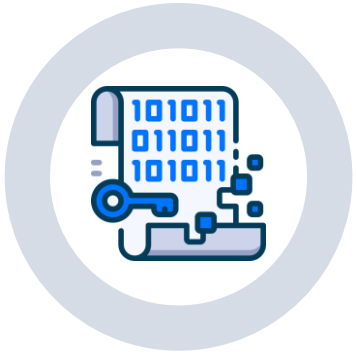
Protocolo Diffie e Hellman (DH)



Observe que Alice e Bob calculam uma chave secreta comum, $\boldsymbol{K_a = K_b}$, como

$$\boldsymbol{K_a = (g^y)^x = (g^x)^y = g^{xy} \ mod \ p = K_b}$$

Data Encryption Standard (DES)



DES *é um algoritmo de criptografia simétrica que foi desenvolvido na década de 1970 pelo projetado pela IBM para ser adotado como* ***padrão*** *nos EUA para informações comerciais.*

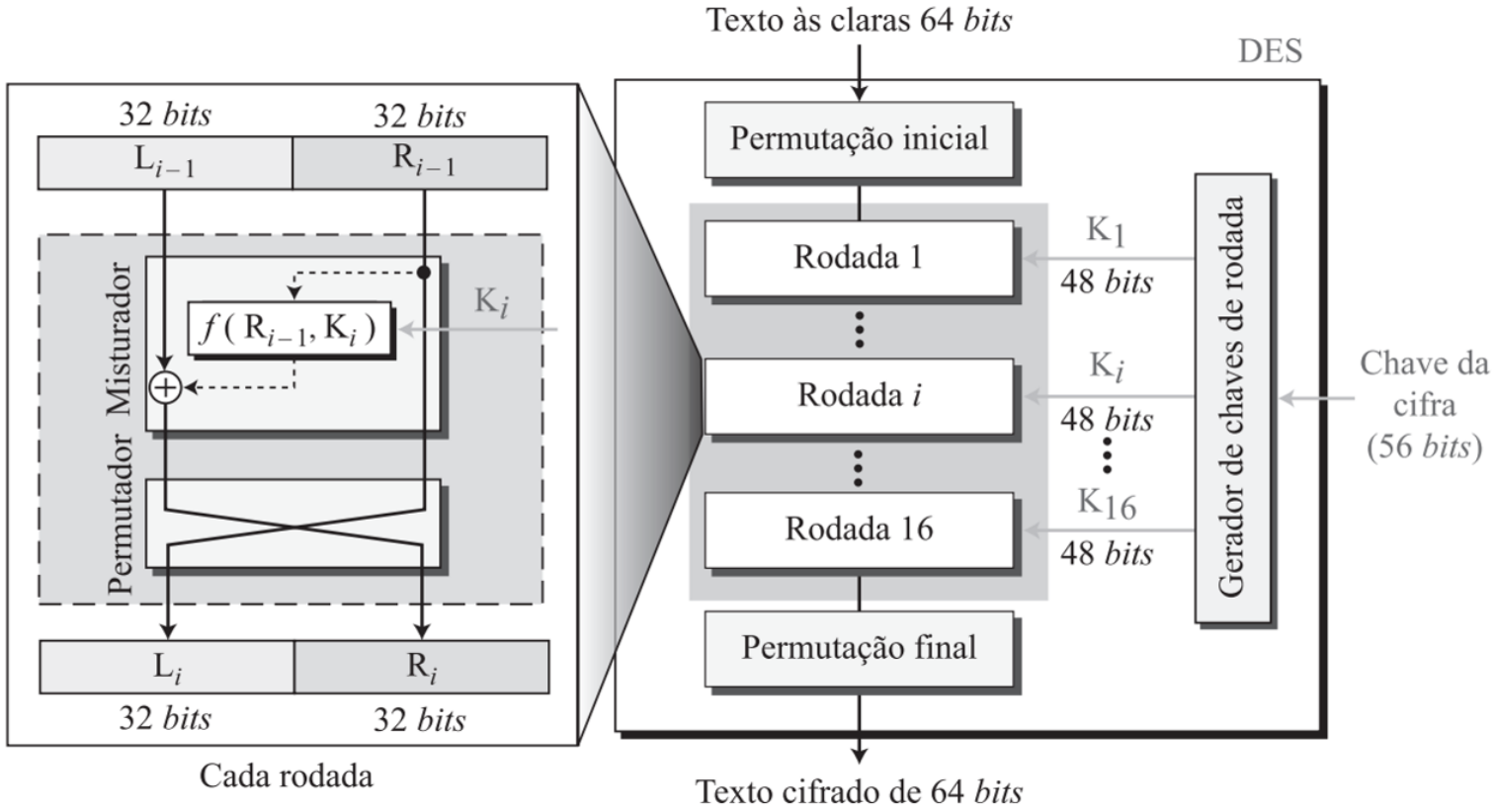
- Foi um avanço científico significativo no sentido de ter sido o **primeiro** criptossistema cujo conhecimento se tornou público: até então todos os algoritmos eram **secretos**.

- Ou seja, a segurança do DES não se baseia no conhecimento do algoritmo mas apenas no **conhecimento da chave secreta.**

Data Encryption Standard (DES)

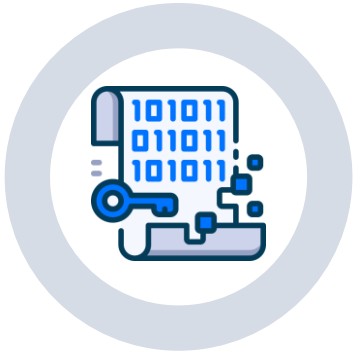
Cifração

- O **DES** processa um texto claro de **64 bits** e cria um texto cifrado de **64 bits.**
- A função espera uma **chave de 64 bits** como entrada. No entanto, **apenas 56 desses bits** são usados.

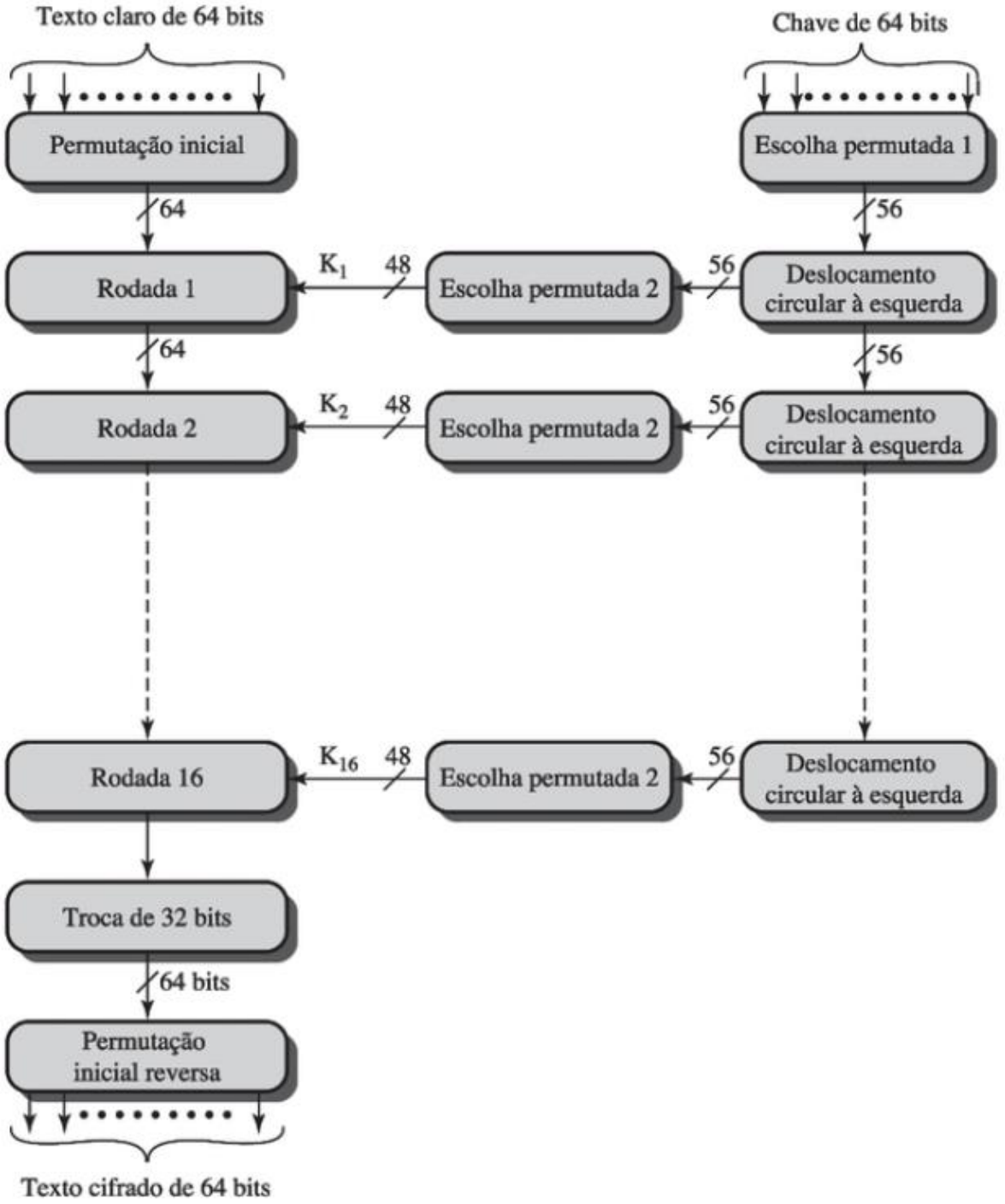


Data Encryption Standard (DES)

Cifração



- O processo acontece em três etapas:
  - **Permutação inicial**
  - **Rodadas**
  - **Permutação final**



Permutação inicial

- A tabela de permutação inicial (IP) do algoritmo DES é uma permutação dos 64 bits do bloco de dados de entrada, que reorganiza os bits de acordo com um esquema pré-determinado.

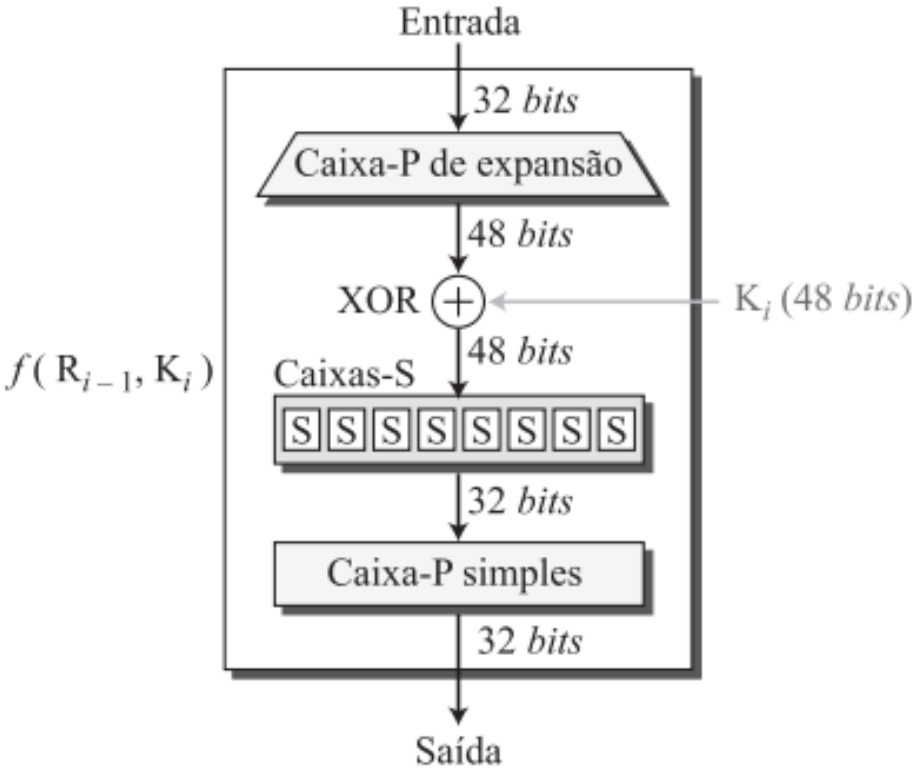
j-sai	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$j-ent$	58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	8
j-sai	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$j-ent$	62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
j-sai	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$j-ent$	57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
j-sai	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
$j-ent$	61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

*Na tabela, **j-ent** representa a posição do j-ésimo bit no bloco de entrada, e **j-sai** representa a posição do j-ésimo bit no bloco de saída.*

Rodadas

- São 16 rodadas da mesmo função. A saída da décima sexta rodada consiste em 64 bits em que as metades esquerda e direita da saída são trocadas para produzir a pré-saída.

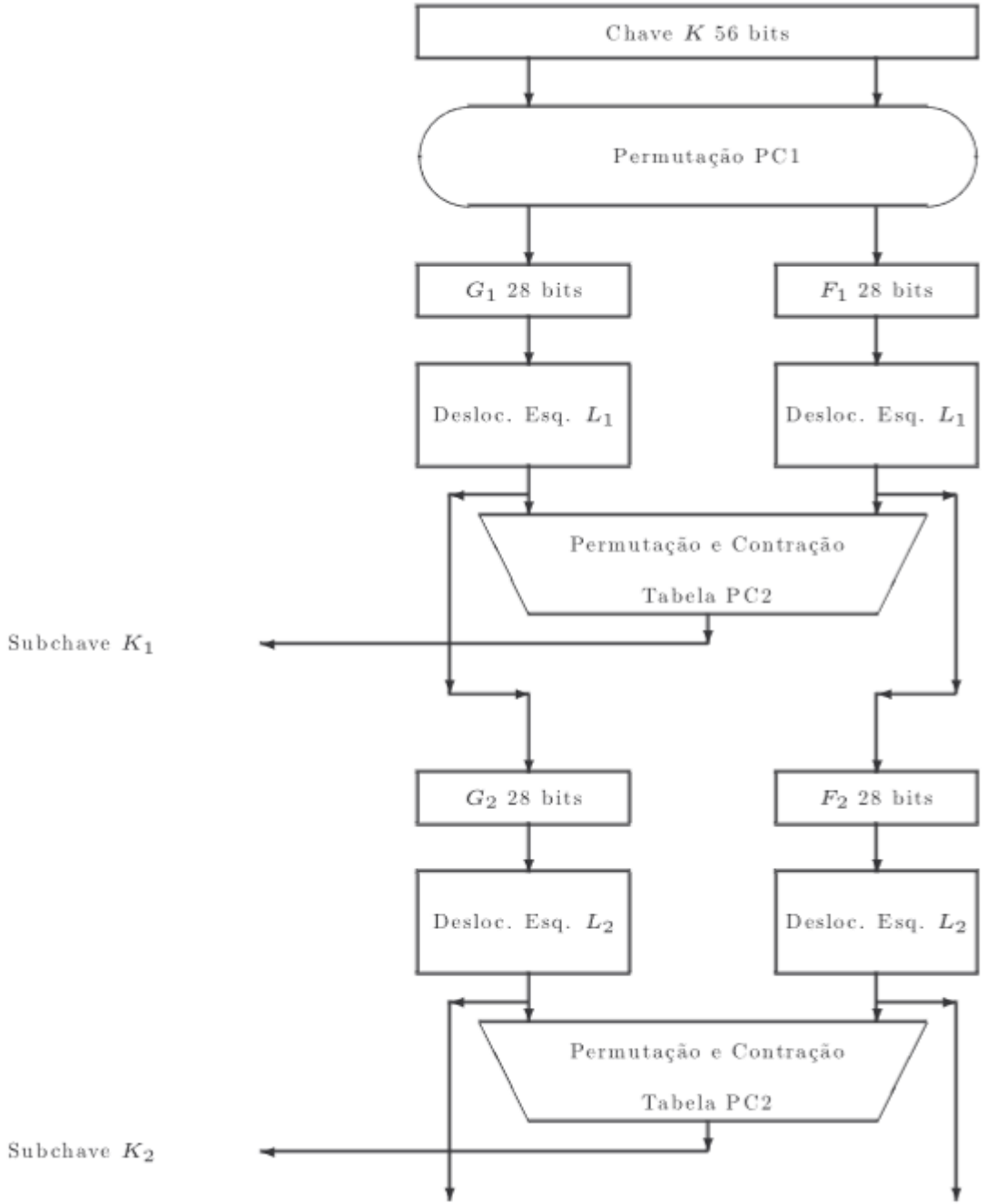
- **Função DES**
  - A função DES aplica uma chave de 48 bits aos 32 mais à direita para produzir uma saída de 32 bits.
  - Essa função é composta por quatro seções:
    - **Uma caixa-P de expansão,**
    - **Uma função que adiciona a chave da rodada**
    - **Um grupo de caixas-S**
    - **Uma caixa-P simples**



Data Encryption Standard (DES)

Rodadas

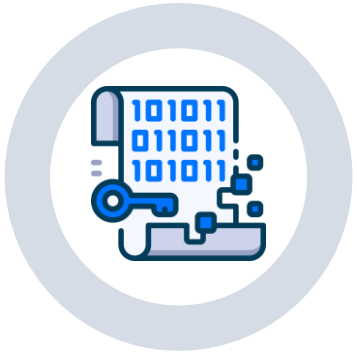
- **Geração de subchaves**
  - O gerador de chaves de rodada cria 16 chaves de 48 bits a partir de uma chave de 56 bits.
  - No entanto, a chave da cifra é normalmente fornecida como uma chave de 64 bits na qual os 8 bits adicionais são **descartados** antes do início do processo de geração de chaves.



Data Encryption Standard (DES)

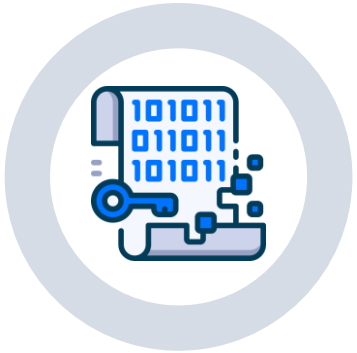
- **Para consultar as tabelas do DES consulte:**
  - TERADA, Routo. **Segurança de dados.** Editora Blucher, 2008. E-book. ISBN 9788521215400. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788521215400/

Advanced Encryption Standard (AES)



- Em 1997, o *National Institute for Standards e Technology* (**NIST**), dos Estados Unidos, fez uma chamada pública para um substituto do algoritmo DES.
- O AES é uma **cifra de blocos** que opera sobre blocos de 128 bits.
- Foi concebido para ser usado com chaves de **128**, **192** ou **256** bits de comprimento, com cifras conhecidas como:
  - $\boldsymbol{AES-128}$, $\boldsymbol{AES-192}$ e $\boldsymbol{AES-256}$.
- No inicio de 2010, o **AES-256** foi amplamente considerado como a melhor escolha para um criptossistema simétrico de proposito geral.

Rodadas AES



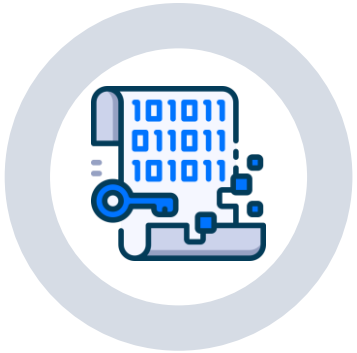
- O processo de cifração AES é feita em 10 rodadas.
- Cada rodada executa uma transformação em um *array* de 128 bits, chamado **estado**.
- O estado inicial $\boldsymbol{X_0}$ é o $\boldsymbol{XOR}$ do texto puro $\boldsymbol{P}$ com uma chave $\boldsymbol{K}$:

$$\boldsymbol{X_0 = P \oplus K}$$

A rodada $\boldsymbol{i}$ recebe o estado $\boldsymbol{X_{i-1}}$ como entrada e produz o estado $\boldsymbol{X_i}$. O texto cifrado $\boldsymbol{C}$ é a saída da rodada final: $\boldsymbol{C = X_{10}}$.

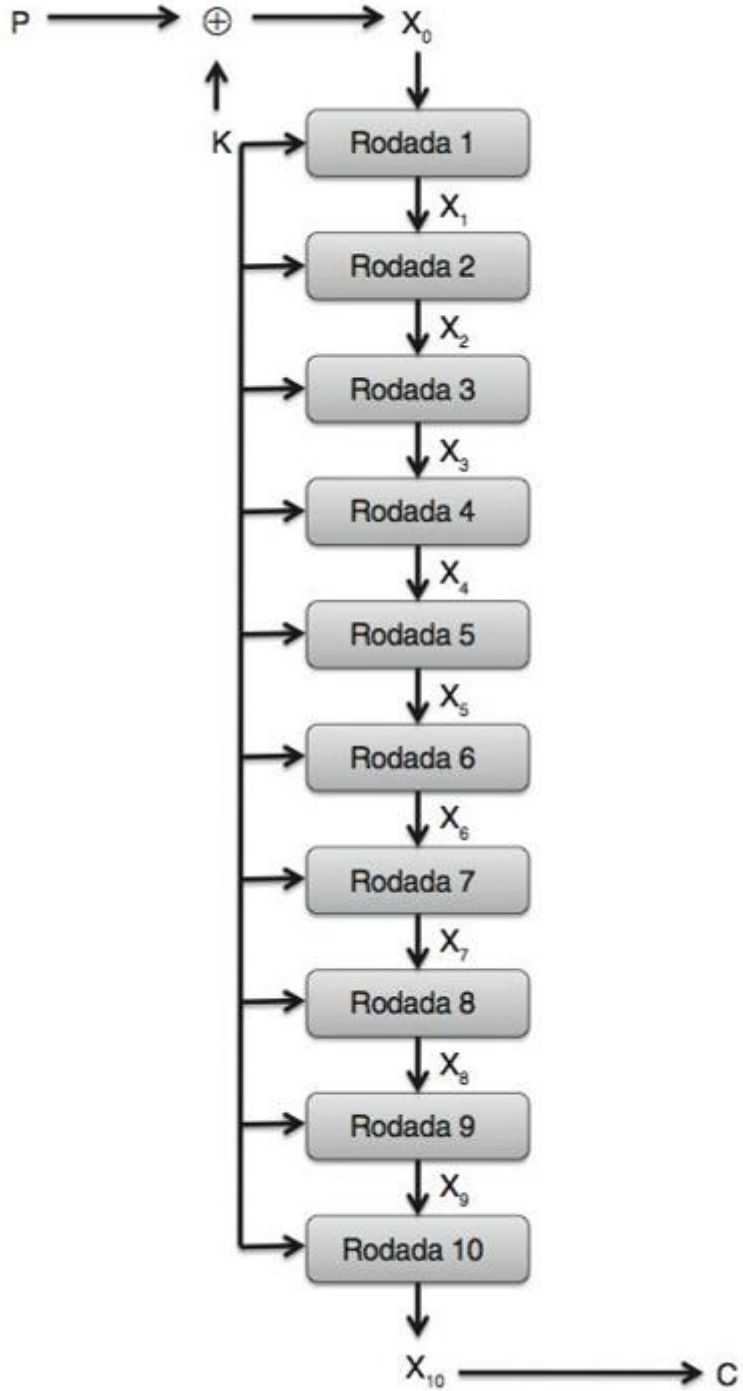
Advanced Encryption Standard (AES)

Rodadas AES



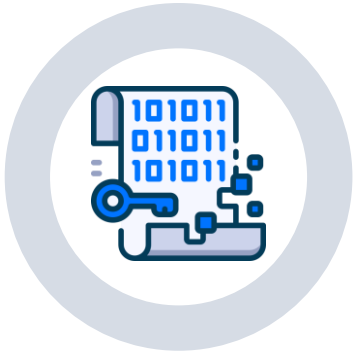
Cada rodada é construída com quatro passos básicos:

1. **Um passo de substituição S-box**
2. **Um passo de permutação**
3. **Um passo de multiplicação de matriz.**
4. **Um passo XOR com uma chave de rodada derivada da chave de cifração de 128 bits**



Advanced Encryption Standard (AES)

AES simplificado



O Professor Edward Schaefer da Universidade de Santa Clara (EUA) construiu uma versão **didática** e **simplificada** do AES chamada S-AES.

Ela é útil para uma melhor compreensão do AES.

Para detalhes veja URL:

http://www.rose-hulman.edu/~holden/Preprints/s-aes.pdf

Fim!

[Aula 07] Introdução à criptografia simétrica moderna