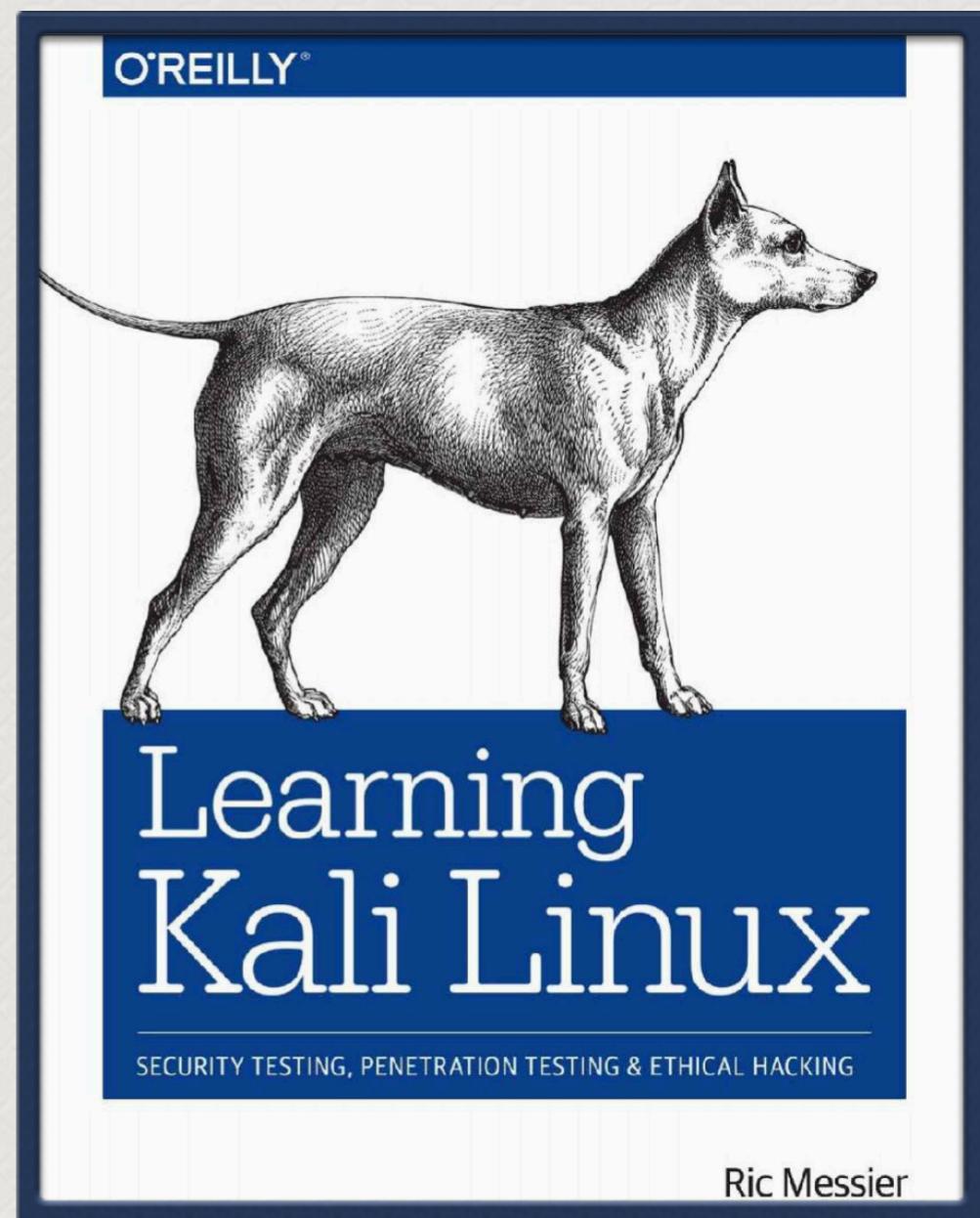
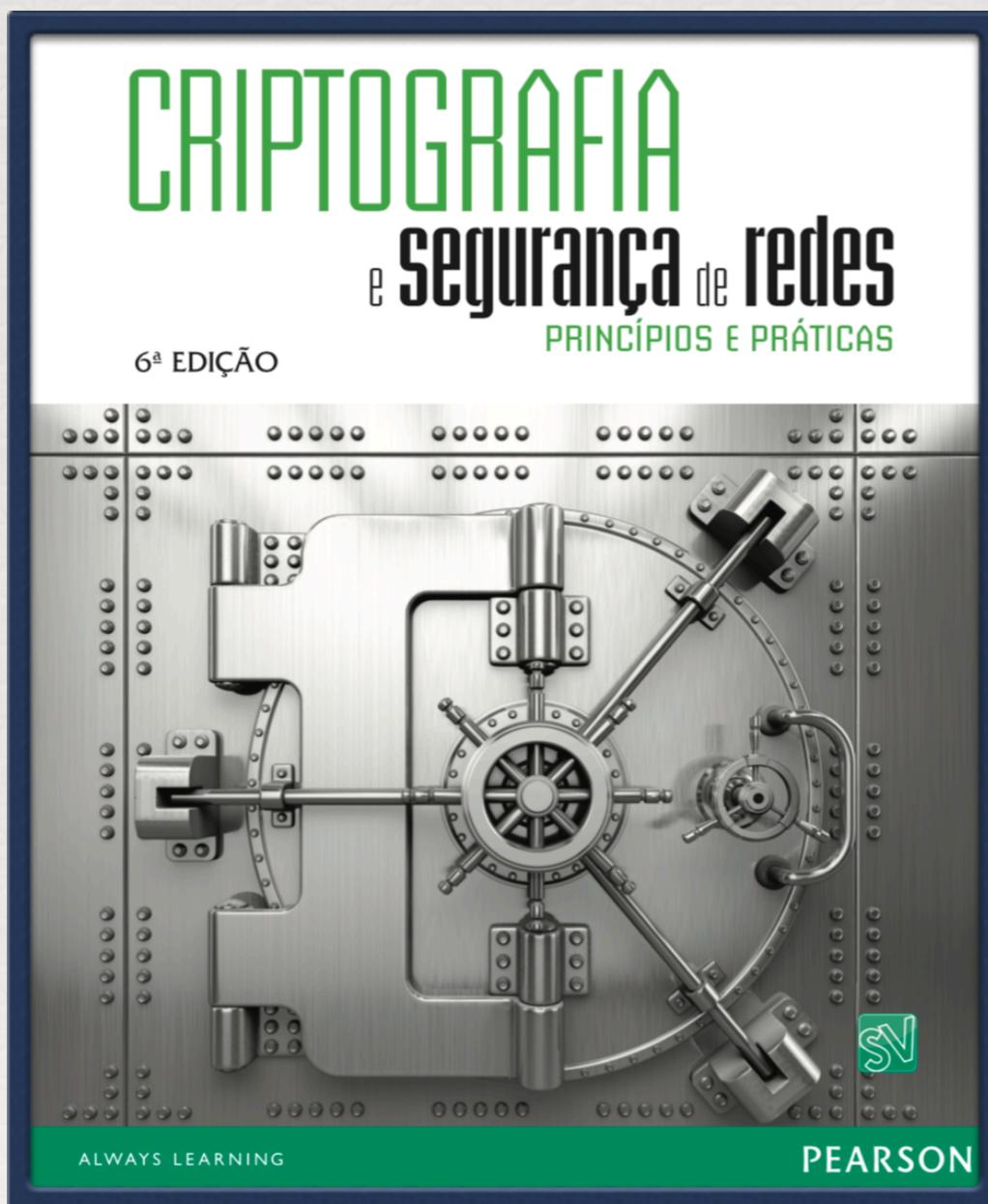
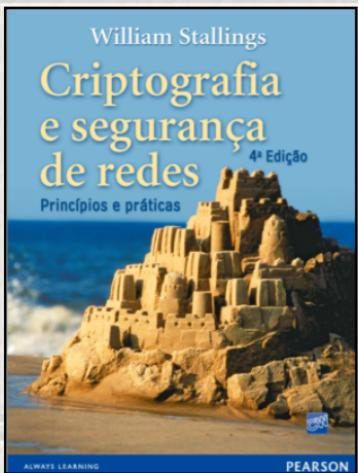


Segurança e Auditoria de Sistemas

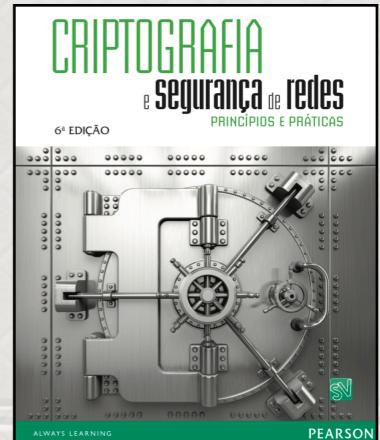
Rafael Vieira Coelho

Livros



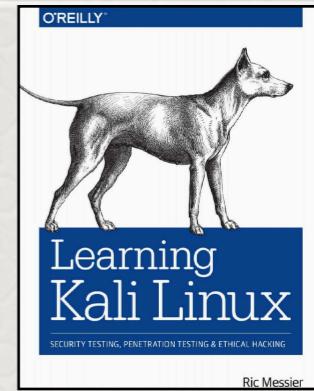


Criptografia e Segurança de Redes: Princípios e Práticas 6ª Edição

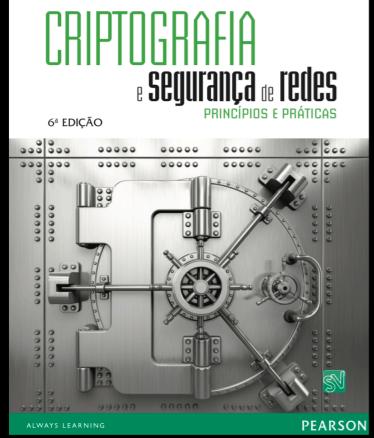


1. Introdução e Técnicas Clássicas de Criptografia (cap. 1 e 2)
- 2. Cifras de Bloco e DES (cap. 3)**
3. AES (cap. 5)
4. Cifras Assimétricas (Chave Pública) (cap. 9 e 10)
5. Funções de Hash (cap. 11)
6. Autenticação de Mensagens (cap. 12)
7. Assinaturas Digitais (cap. 13)
8. Gerenciamento e Distribuição 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 3

3.1 ESTRUTURA TRADICIONAL DE CIFRA DE BLOCO

Cifras de fluxo e cifras de bloco

Motivação para a estrutura de cifra de Feistel

Cifra de Feistel

3.2 DATA ENCRYPTION STANDARD

Encriptação DES

Decriptação DES

3.3 UM EXEMPLO DO DES

Resultados

Efeito avalanche

3.4 A FORÇA DO DES

Uso de chaves de 56 bits

Natureza do algoritmo DES

Ataques de temporização

3.5 PRINCÍPIOS DE PROJETO DE CIFRA DE BLOCO

Número de rodadas

Projeto da função F

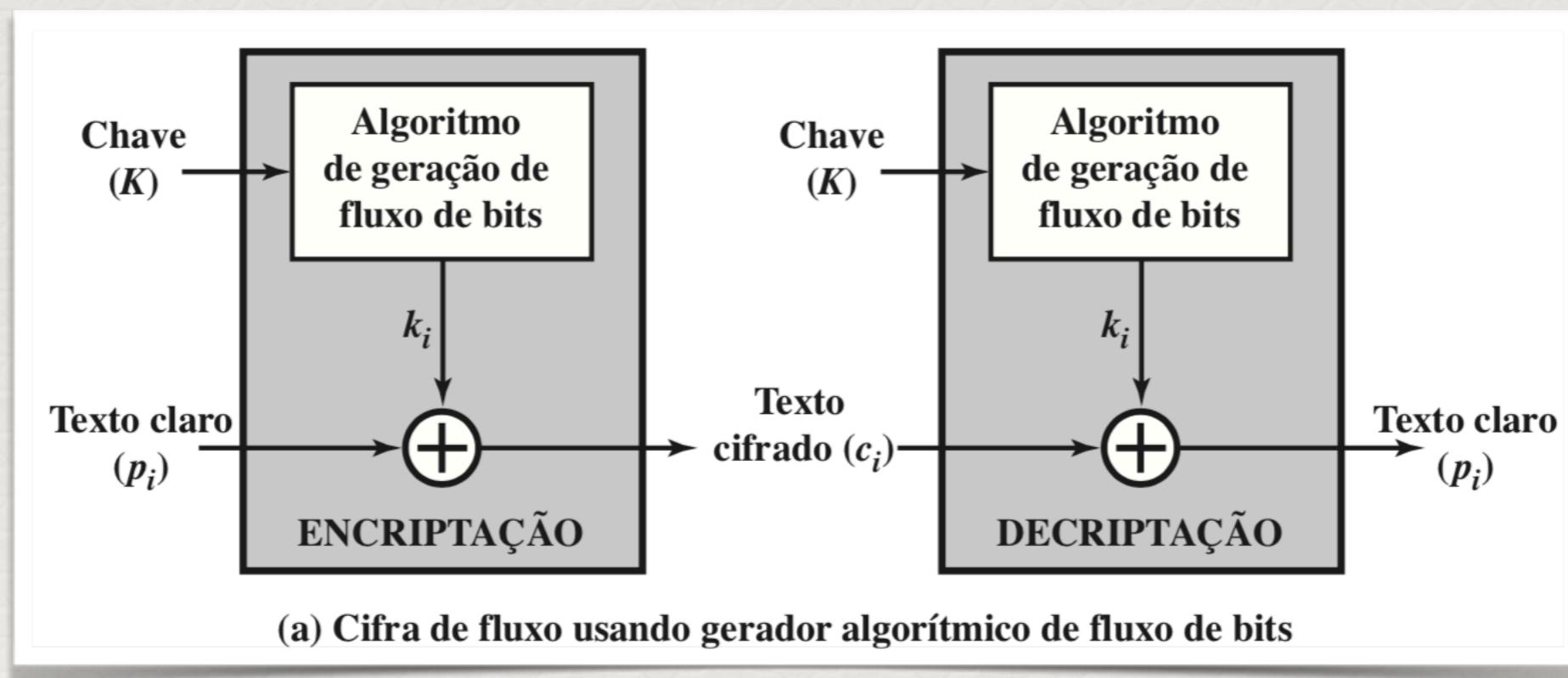
Algoritmo de escalonamento de chave

3.1 Estrutura Tradicional de Cifra de Bloco

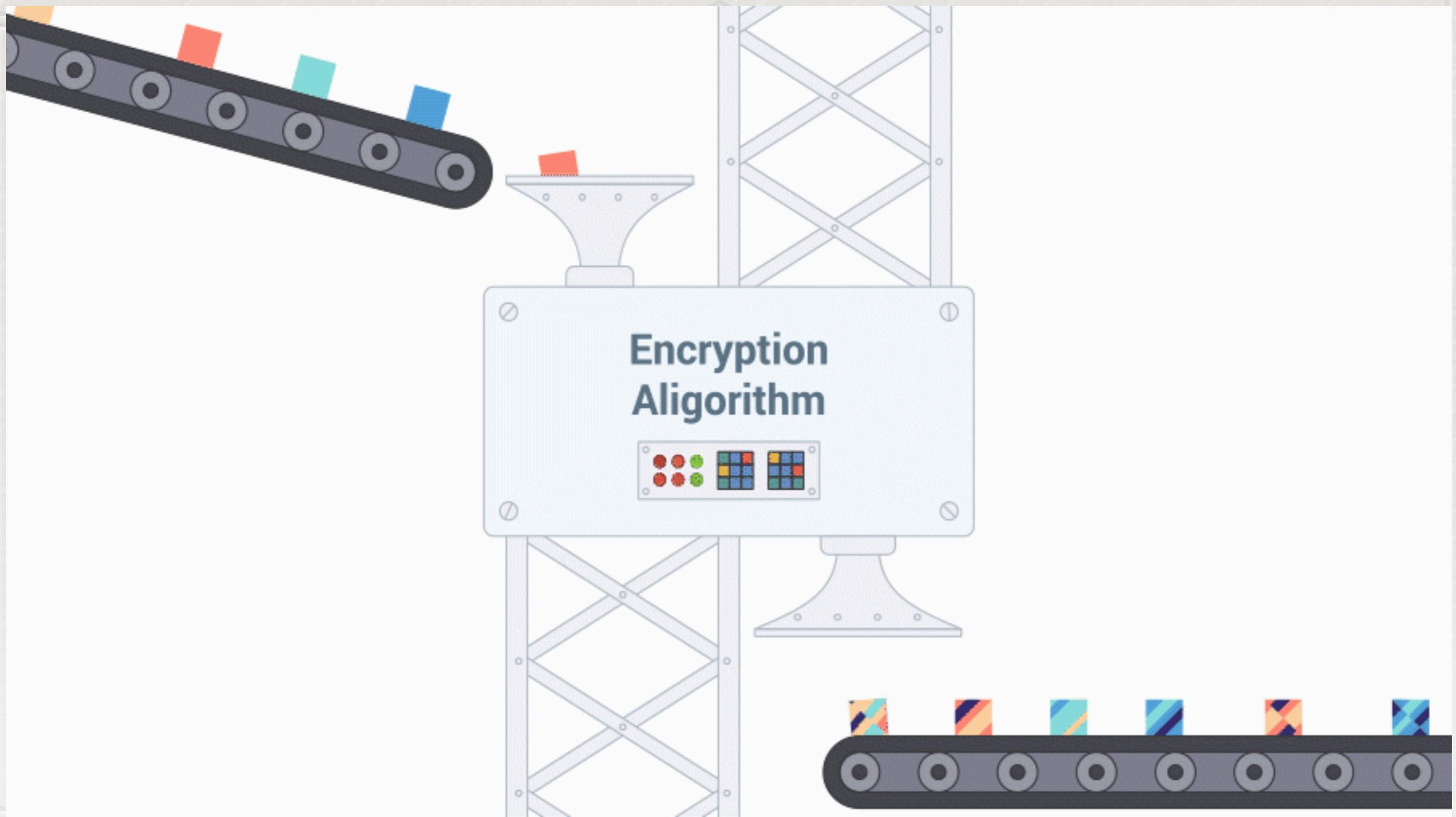
- ◆ O objetivo desta aula é ilustrar os princípios das cifras simétricas modernas.
- ◆ Para essa finalidade, focalizaremos a cifra simétrica mais utilizada: o Data Encryption Standard (DES).

Cifras de Fluxo

- ✿ **Cifra de fluxo** é aquela que encripta um fluxo de dados digital um *bit* ou um *byte* por vez. Ex: Vigenère.

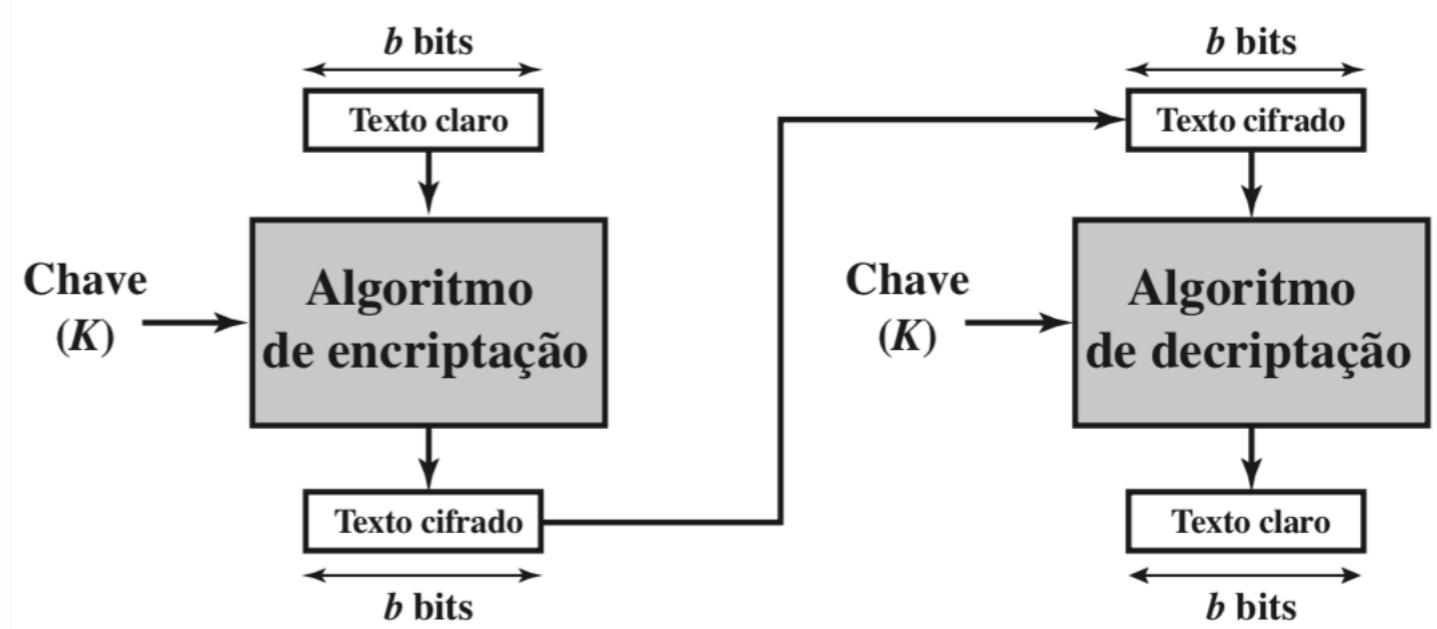


- ◆ **Cifra de fluxo** é aquela que encripta um fluxo de dados digital um *bit* ou um *byte* por vez. Ex: Vigenère.



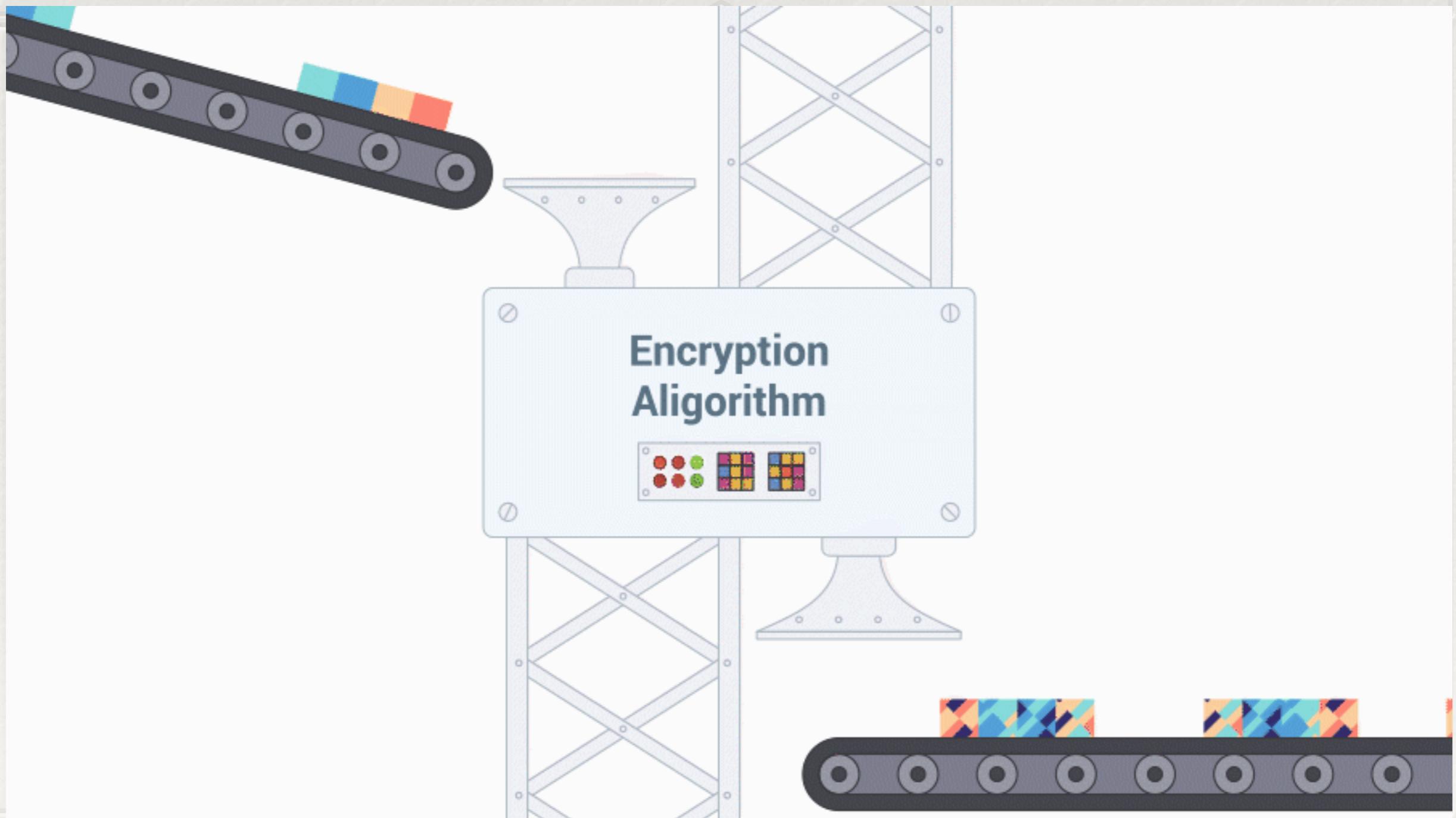
Cifras de Bloco

- **Cifra de bloco** é aquela em que um bloco de texto claro é tratado como um todo e usado para produzir um de texto cifrado com o mesmo tamanho (bloco de bits).
- Normalmente, um tamanho de bloco de 64 ou 128 *bits* é utilizado.
- Assim como a cifra de fluxo, os dois usuários compartilham uma chave de encriptação simétrica.



(b) Cifra de bloco

- ◆ **Cifra de bloco** é aquela em que um bloco de texto claro é tratado como um todo e usado para produzir um de texto cifrado com o mesmo tamanho (bloco de bits).



Cifra de Bloco

- * Tendo o bloco de texto claro/cifrado de n bits, existem 2^n diferentes blocos de texto claro possíveis
- * Cifras de bloco podem ajudar a esconder o tamanho real da mensagem que está sendo enviada pois cada bloco tem tamanho fixo.
- * Se o tamanho do bloco for maior que a mensagem que será enviada, a mesma é completada com conteúdo aleatório.
- * No entanto, usam mais memória e são mais lentos que cifras de fluxo.

Cifra de Feistel

- * O protocolo definido nas cifras de Feistel originaram as cifras de bloco.
- * Feistel propôs a execução de duas ou mais cifras simples em sequência, de tal forma que o resultado ou produto final seja criptograficamente mais forte do que qualquer uma das cifras componentes.
- * A essência da técnica é desenvolver uma cifra de bloco com um tamanho de chave de k bits e de bloco de n bits, permitindo um total de 2^k transformações possíveis, em vez de $2^n!$ transformações disponíveis com a cifra de bloco ideal.

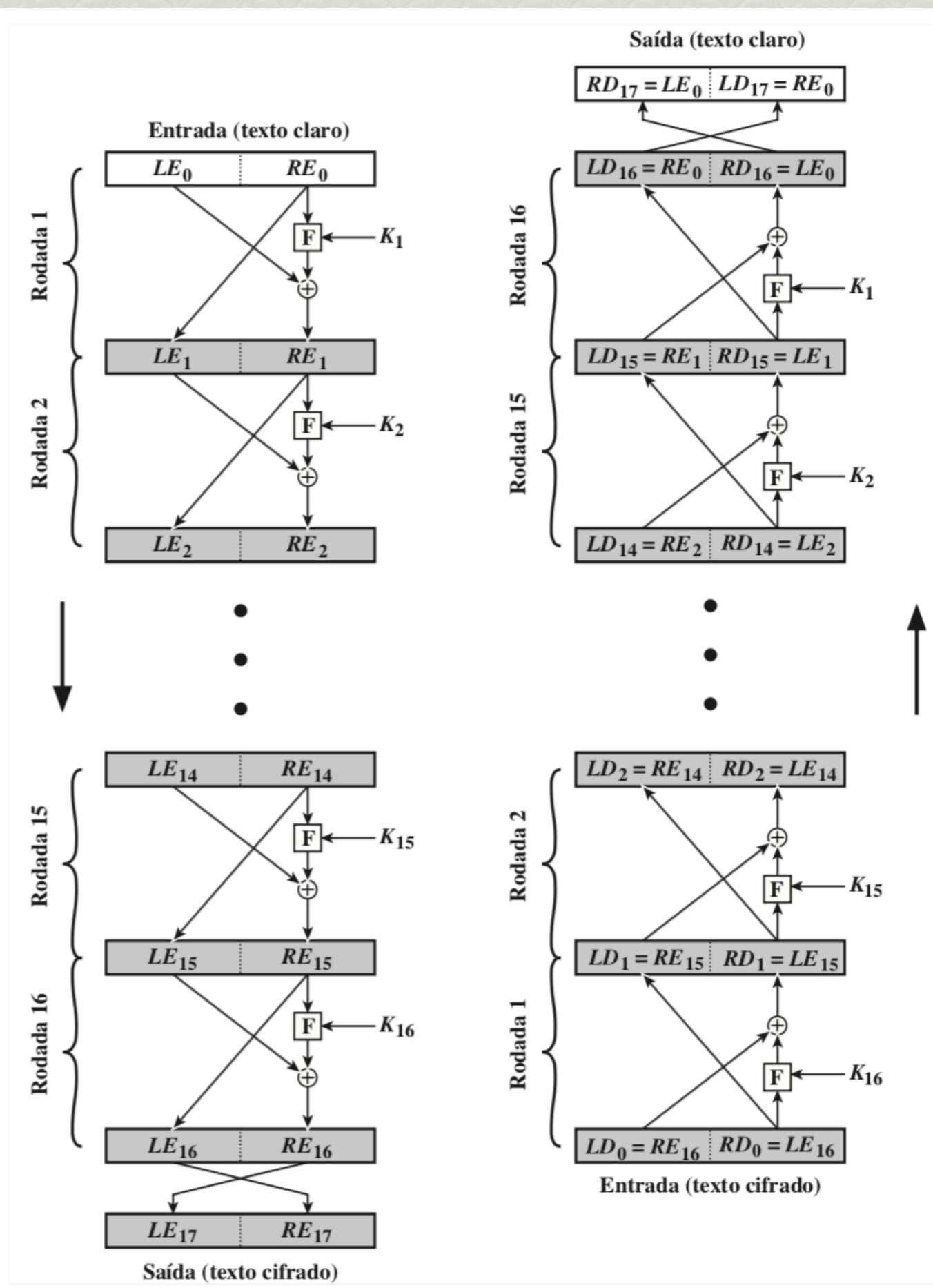
Cifra de Feistel

Em particular, Feistel propôs o uso de uma cifra que alterna substituições e permutações, nas quais esses termos são definidos da seguinte forma:

- * **Substituição:** cada elemento de texto claro ou grupo de elementos é substituído exclusivamente por um elemento ou grupo de elementos de texto cifrado correspondente.
- * **Permutação:** uma sequência de elementos de texto claro é substituída por uma permutação dessa sequência. Ou seja, nenhum elemento é acrescentado, removido ou substituído na sequência, mas a ordem em que os elementos aparecem nela é mudada.

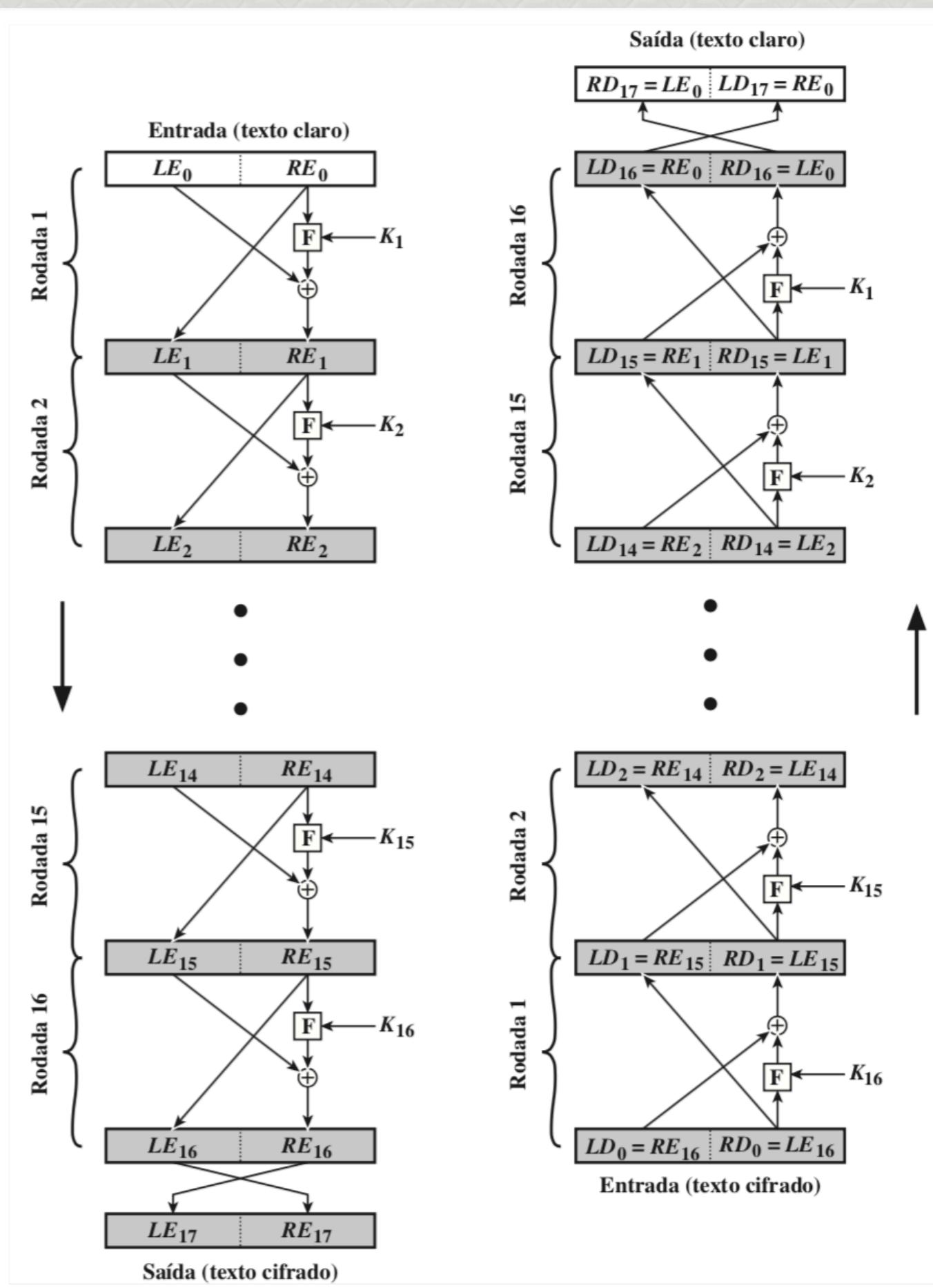
Cifra de Feistel

- * O lado esquerdo da Figura 3.3 representa a estrutura proposta por Feistel.
- * As entradas do algoritmo de encriptação são um bloco de texto claro de tamanho $2w$ bits e uma chave K .
- * O bloco do texto claro é dividido em duas metades, L_0 e R_0 . As duas metades dos dados passam por n rodadas de processamento, e depois se combinam para produzir o bloco do texto cifrado.
- * Cada rodada i possui como entradas L_{i-1} e R_{i-1} , derivadas da rodada anterior, assim como uma subchave K_i derivada do K geral.



Cifra de Feistel

- * Todas as rodadas têm a mesma estrutura.
- * Uma **substituição** é realizada na metade esquerda dos dados. Isso é feito aplicando-se uma *função F* à metade direita dos dados, e depois, a operação lógica de ou-exclusivo entre a saída dessa função e a metade esquerda dos dados.
- * A função F tem a mesma estrutura geral para cada rodada, mas é parametrizada pela subchave da rodada K_i .



Parâmetros de uma Cifra de Feistel

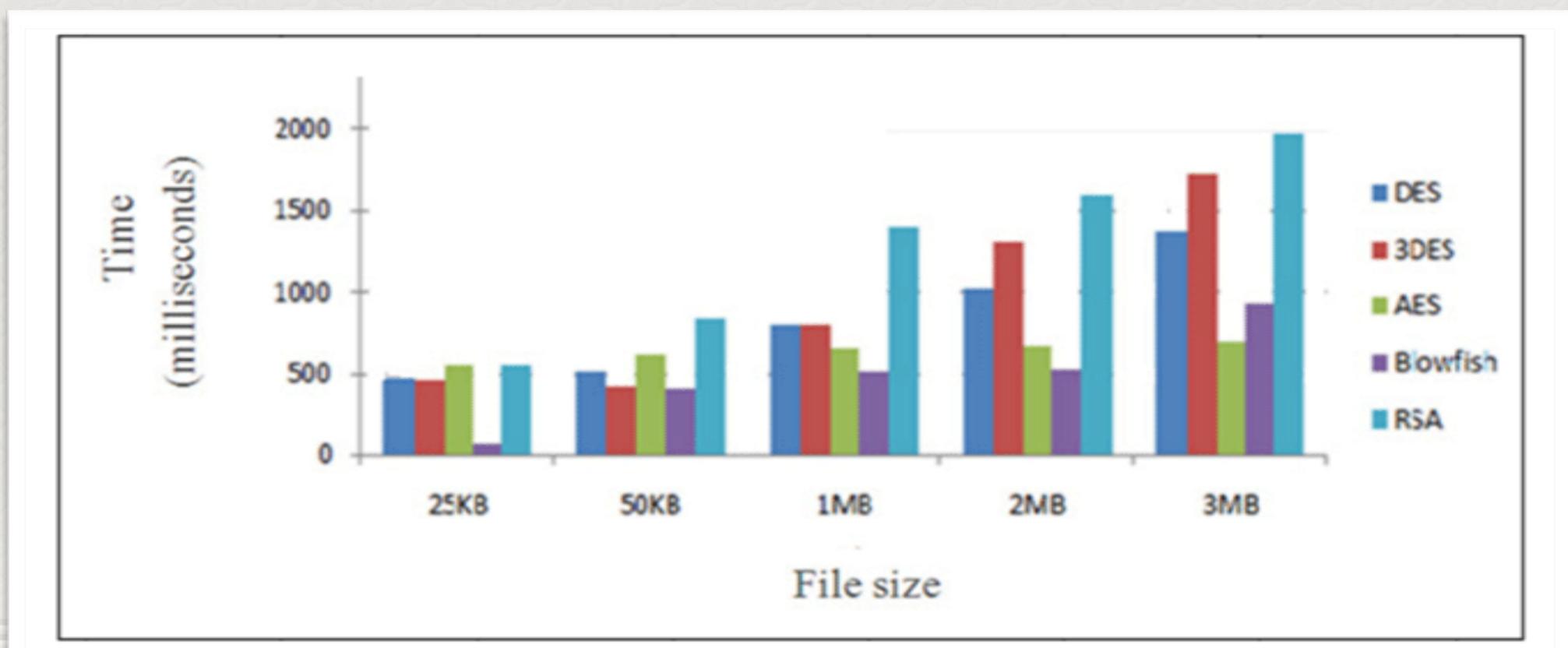
- * **Tamanho de bloco:** tamanhos de bloco maiores significam maior segurança (mantendo as outras coisas iguais), mas velocidade de encriptação/decriptação reduzida para determinado algoritmo. O AES usa um tamanho de bloco de 256 bits.
- * **Tamanho de chave:** tamanho de chave maior significa maior segurança, mas pode diminuir a velocidade de encriptação/decriptação. Maior segurança é obtida pela maior resistência a ataques de força bruta e maior confusão.

Parâmetros de uma Cifra de Feistel

- * **Número de rodadas:** a essência da cifra de Feistel é que uma única rodada oferece segurança inadequada, mas várias proporcionam maior segurança. Um tamanho típico é de 16 rodadas.
- * **Algoritmo de geração de subchave:** maior complexidade nesse algoritmo deverá levar a maior dificuldade de criptoanálise.
- * **Função F:** maior complexidade geralmente significa maior resistência à criptoanálise.

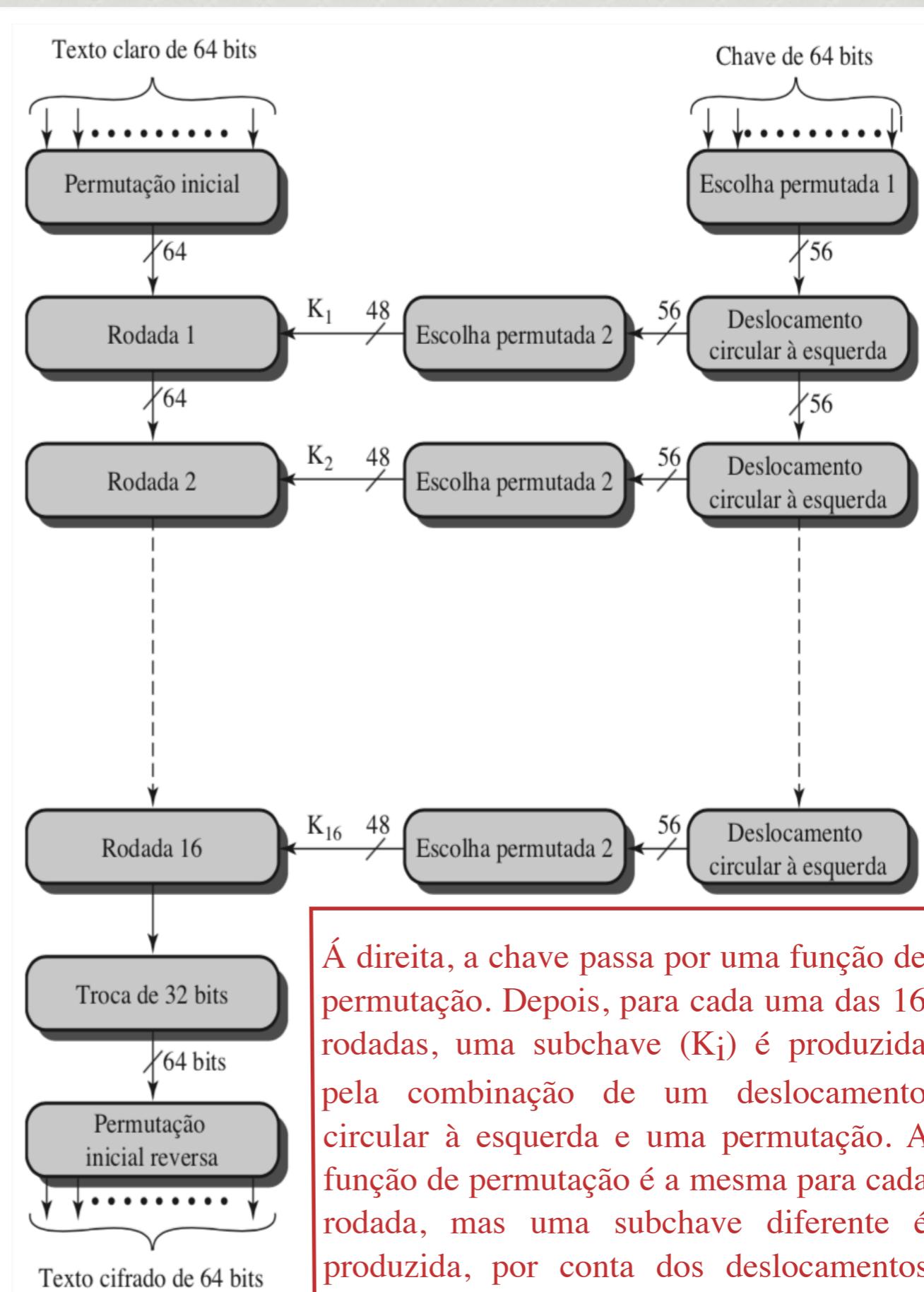
3.2 Data Encryption Standard

- * DES foi adotado em 1977 pelo National Bureau of Standards, agora National Institute of Standards and Technology (NIST), como Federal Information Processing Standard 46.
- * Até a introdução do advanced encryption standard (AES), em 2001, o data encryption standard (DES) era o esquema de encriptação mais utilizado.



Encriptação DES

- * Na esquerda, podemos ver que o processamento do texto claro prossegue em três fases.
 1. O texto claro de 64 bits passa por uma permutação inicial para reorganizar os bits a fim de produzir a *entrada permutada*.
 2. Ocorrem 16 rodadas da mesma função, que envolve funções de permutação e substituição.
 3. A saída da última (décima sexta) rodada baseia-se em 64 bits que são uma função do texto claro de entrada e da chave.
 4. As metades esquerda e direita da saída são trocadas para produzir a pré-saída.
 5. Finalmente, a pré-saída é passada por uma permutação, que é o inverso da função de permutação inicial, a fim de produzir o texto cifrado de 64 bits.



Á direita, a chave passa por uma função de permutação. Depois, para cada uma das 16 rodadas, uma subchave (K_i) é produzida pela combinação de um deslocamento circular à esquerda e uma permutação. A função de permutação é a mesma para cada rodada, mas uma subchave diferente é produzida, por conta dos deslocamentos

3.3 Exemplo do DES

Texto claro:	02468aceeca86420
Chave:	0f1571c947d9e859
Texto cifrado:	da02ce3a89ecac3b

IP - permutação inicial

K - chave (key)

L - esquerda (left)

R - direita (right)

A última linha mostra os valores da esquerda e da direita após a permutação inicial inversa. Esses dois valores combinados formam o texto cifrado.

<i>Rodada</i>	<i>K_i</i>	<i>L_i</i>	<i>R_i</i>
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	bad22845
2	0a31293432242318	bad22845	99e9b723
3	23072318201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	c11bf09
9	04292a380c341f03	c11bf09	887fb06c
10	2703212607280403	887fb06c	600f7e8b
11	2826390c31261504	600f7e8b	f596506e
12	12071c241a0a0f08	f596506e	738538b8
13	300935393c0d100b	738538b8	c6a62c4e
14	311e09231321182a	c6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP ⁻¹		da02ce3a	89ecac3b

3.4 A Força do DES

- * Tempo médio exigido para uma busca exaustiva no espaço de chaves.

Tamanho de chave (bits)	Cifra	Número de chaves alternativas	Tempo exigido a 10^9 decriptações/s	Tempo exigido a 10^{13} decriptações/s
56	DES	$2^{56} \approx 7,2 \times 10^{16}$	$2^{55} \text{ ns} = 1,125 \text{ ano}$	1 hora
128	AES	$2^{128} \approx 3,4 \times 10^{38}$	$2^{127} \text{ ns} = 5,3 \times 10^{21} \text{ anos}$	$5,3 \times 10^{17} \text{ anos}$
168	Triple DES	$2^{168} \approx 3,7 \times 10^{50}$	$2^{167} \text{ ns} = 5,8 \times 10^{33} \text{ anos}$	$5,8 \times 10^{29} \text{ anos}$
192	AES	$2^{192} \approx 6,3 \times 10^{57}$	$2^{191} \text{ ns} = 9,8 \times 10^{40} \text{ anos}$	$9,8 \times 10^{36} \text{ anos}$
256	AES	$2^{256} \approx 1,2 \times 10^{77}$	$2^{255} \text{ ns} = 1,8 \times 10^{60} \text{ anos}$	$1,8 \times 10^{56} \text{ ano}$
26 caracteres (permutação)	Monoalfabético	$2! = 4 \times 10^{26}$	$2 \times 10^{26} \text{ ns} = 6,3 \times 10^9 \text{ anos}$	$6,3 \times 10^6 \text{ anos}$

Tarefas

1. Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?
2. O que é uma cifra de produto?
3. Qual é a diferença entre difusão e confusão no contexto criptográfico?
4. Que parâmetros e escolhas de projeto determinam o algoritmo real de uma cifra de feistel?
5. Pesquise e explique o efeito avalanche em um algoritmo de encriptação (não esqueça de colocar as referências).
6. Analise o código pydes.py e explique o seu funcionamento (classes, funções, etc). <https://github.com/RobinDavid/pydes>