Criptografia

Cifras de blocos

Roadmap

- Princípios de cifra de bloco
- Esquema geral de uma cifra de bloco
- Definição e problemas sobre a chave
- Cifra de Feistel

Universidade Federal do Ceará
Campus de Crateús

Ciência da Computação
Sistemas de Informação

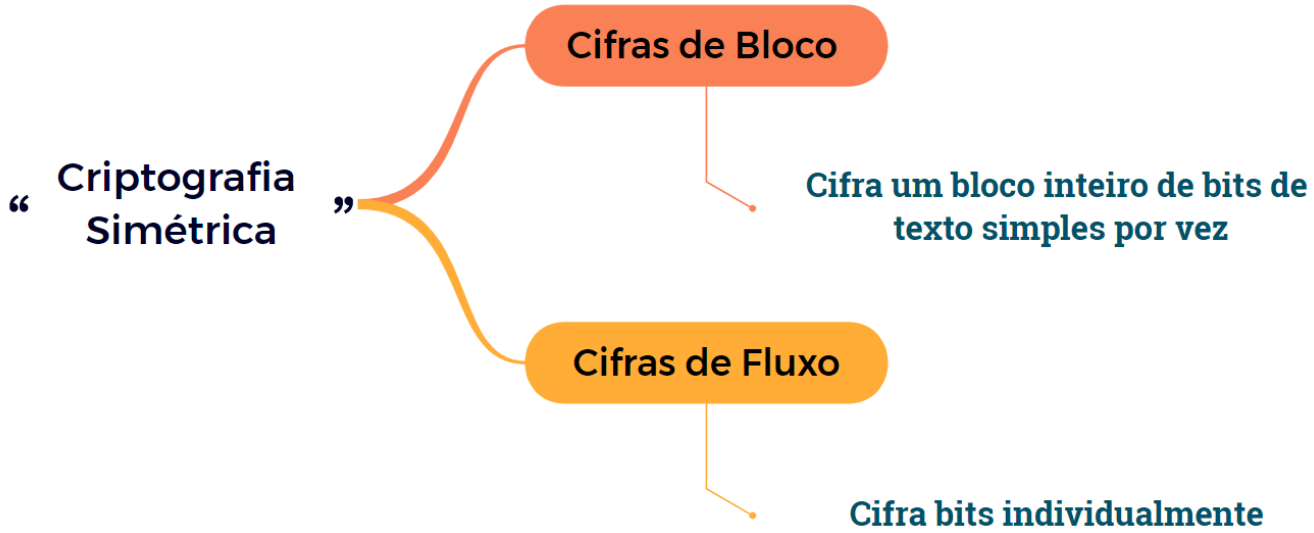
emerson@crateus.ufc.br

Cifras de blocos

Introdução

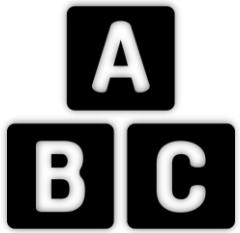
- Todas as cifras clássicas, ou seja, anteriores a 1970, são de **natureza simétrica** e compartilham alguns princípios com as cifras modernas.

> *A criptografia simétrica é aquela em que tanto o **emissor** quanto o **receptor** utilizarem a mesma chave para cifrar e decifrar uma mensagem. É conhecida também como **criptografia de chave secreta**.*

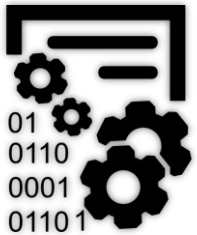


Cifras de blocos

Introdução



- As cifras de chave simétrica tradicionais estudadas até agora são cifras **orientadas a caracteres**.



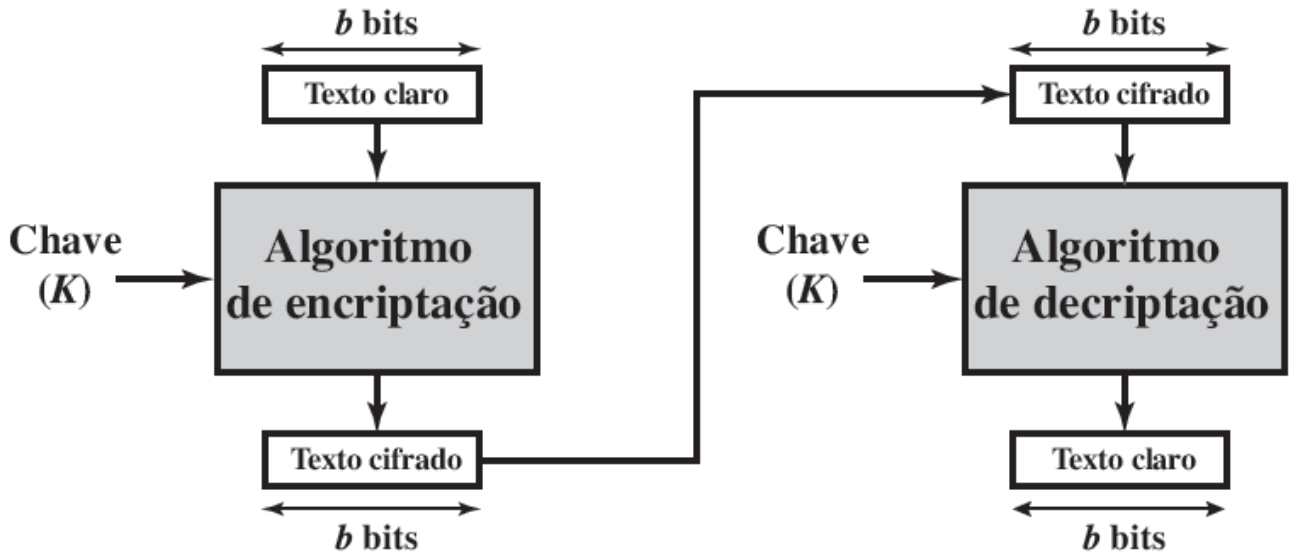
- Com o surgimento do computador, passamos a precisar de cifras **orientadas a *bits***.

- A razão é que a informação a ser cifrada não envolve apenas texto; pode também envolver números, gráficos, **áudio** e dados de **vídeo**.

Cifra de bloco

*Uma **cifra de bloco** é aquela em que um bloco de texto claro é tratado como um todo e usado para produzir um bloco de texto cifrado de igual comprimento.*

- Normalmente, um tamanho de bloco de **64** ou **128** bits é usado.



Cifra de bloco

Notação

- ***Algoritmo de cifração*** (E).
  - Recebe uma chave, K, e um bloco de texto simples, P, e produz um bloco de texto cifrado, C.
  - Denotamos o processo de cifração como:

$$C = E(K, P).$$

- ***Algoritmo de decifração*** (D).
  - É o inverso do algoritmo de cifração e decifra uma mensagem para o texto simples original, P.
  - Denotamos o processo de decifração como:

$$P = D(K, C) .$$

O algoritmo de decifração deve ser o inverso do algoritmo de cifração

Cifra de bloco

Princípios de cifra de bloco

1. Uma cifra de bloco opera sobre um bloco de texto claro de n *bits* para produzir um bloco de texto cifrado de n *bits*.

2. Existem 2^n blocos de texto claro possíveis e 2^n blocos de texto cifrado de comprimento n.

3. Para a transformação ser **reversível**, cada bloco deve produz um bloco de texto cifrado exclusivo.

4. Se a mensagem tiver menos do que n *bits*, devem ser adicionados ***bits* de enchimento** (*padding*) para completar um bloco.

5. Se a mensagem tiver mais do que n *bits*, ela deve ser dividida em blocos de n *bits* e os bits de enchimento devem ser adicionado ao último bloco.

Cifra de bloco

Esquema geral de uma cifra de bloco

Cifras de blocos modernas são cifras de ***substituição*** *quando observamos um bloco inteiro.*

No entanto, cifras de bloco modernas não são projetadas como uma unidade única.

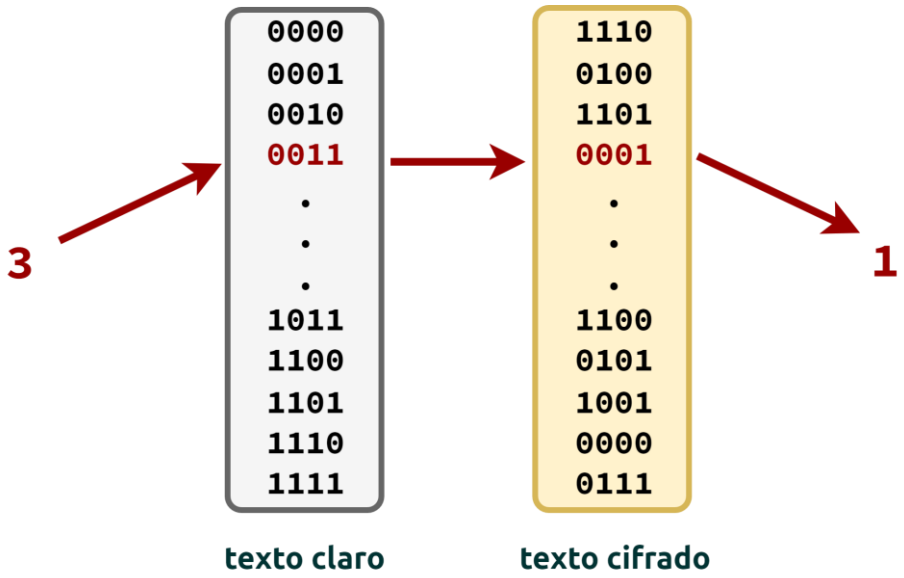
Uma cifra de bloco moderna é projetada como uma ***combinação*** *de unidades de* ***transposição*** *e unidades de* ***substituição****.*

Esquema geral de uma cifra de bloco

Demonstração

- Considere uma cifra de substituição geral para $n = 4$ (blocos de 4 *bits*).

- Uma entrada de 4 *bits* corresponde um dos 16 blocos de entrada possíveis.
- Cada bloco de entrada é mapeado pela cifra de substituição para **um** dos 16 blocos de saída possíveis.
- No entanto, o **texto cifrado** ao lado é apenas uma das permutações possíveis.
- Ou seja, há $2^n!$ transformações possíveis.



Cifra de bloco

Qual é a chave?

Nesse esquema, escolher uma chave significa selecionar uma permutação entre as $\mathbf{2^n!}$ *permutações possíveis.*

Essa permutação é então usada para cifrar os blocos de texto simples.

Como escolher a permutação

- Poderíamos tentar **enumerar** todas as permutações e, em seguida, selecione aleatoriamente um índice (esse índice seria a **chave**).
- Assim, precisamos de $\mathbf{log_2(2^n!)}$ bits para armazenar a chave.

> *Para um comprimento de bloco* $\boldsymbol{n = 64}$ *bits, precisaríamos de aproximadamente* $\mathbf{2^{67}}$ *bytes para armazenar uma única chave.*

Cifra de bloco

Qual é a chave?

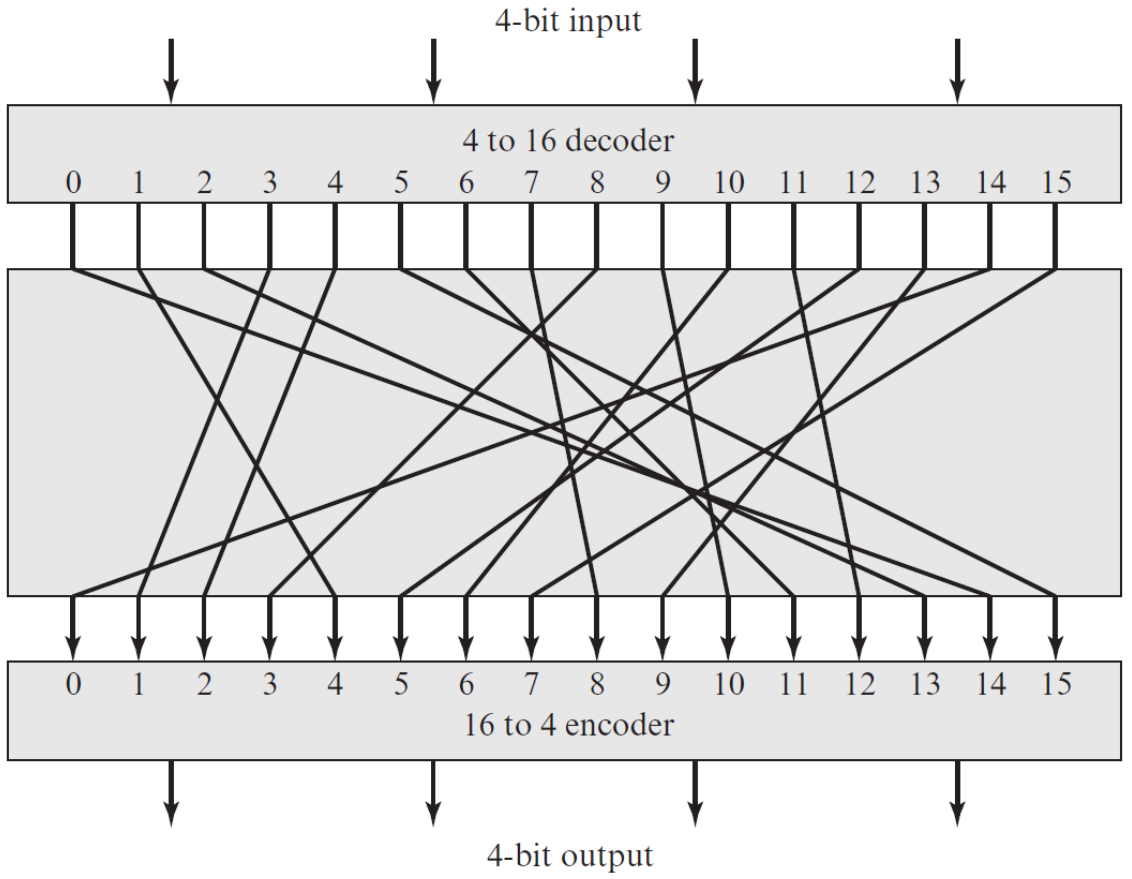
Quando o mapeamento é a chave

- Considere cifra em que $n = 4$.
- O mapeamento pode ser definido pelos valores na segunda linha que mostra o **valor do texto cifrado** para cada **texto claro.**

Nesse caso, o tamanho da chave necessário é $(4\ bits) * (16\ linhas) = 64\ bits$.

Em geral, para uma cifra de bloco ideal de n *bits, o tamanho da chave* $n * 2^n$ *bits.*

Para um bloco de 64 bits, é necessário é $64 * 2^{64} = 2^{70}$



Esquema geral de uma cifra de bloco

Demonstração

Mapeamento de cifração

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
C	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111

Texto cifrado: `0001 0011 0101 0111`

Mapeamento de decifração

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
C	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
P	1110	0011	0100	1000	0001	1100	1010	1111	0111	1101	1001	0110	1011	0010	0000	0101

Texto claro: `0011 1000 1100 1111`

Cifra de bloco

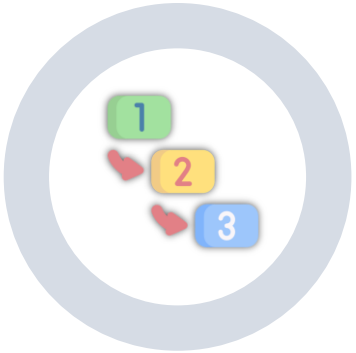
Qual é a chave?

- Esta é a forma mais geral de cifra de bloco, pois permite o número **máximo de mapeamentos** criptográficos do **bloco de texto simples** — está é a **cifra de bloco ideal**.

- *Porém, a cifra de bloco ideal não é **prática** do ponto de vista de implementação e desempenho.*

- Ao considerar essas dificuldades, Feistel (*matemático e criptógrafo alemão)* apontou que é necessário uma aproximação do sistema ideal de cifras de bloco para n grande.

A cifra de Feistel

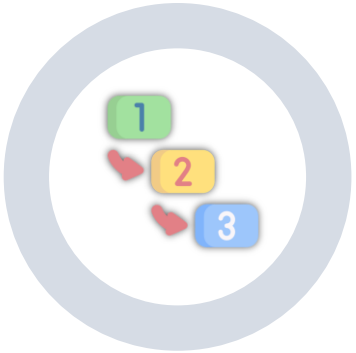


- Muitos algoritmos de cifra de bloco simétricos em uso atual são baseados em uma estrutura conhecida como **cifra de bloco de Feistel.**
- Feistel propôs que podemos aproximar a cifra de bloco ideal utilizando o conceito de uma **cifra de produto**.

> ***Cifra de produto*** *é 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.*

- Em particular, **Feistel** propôs o uso de uma cifra que alterna **substituições** e **permutações.**

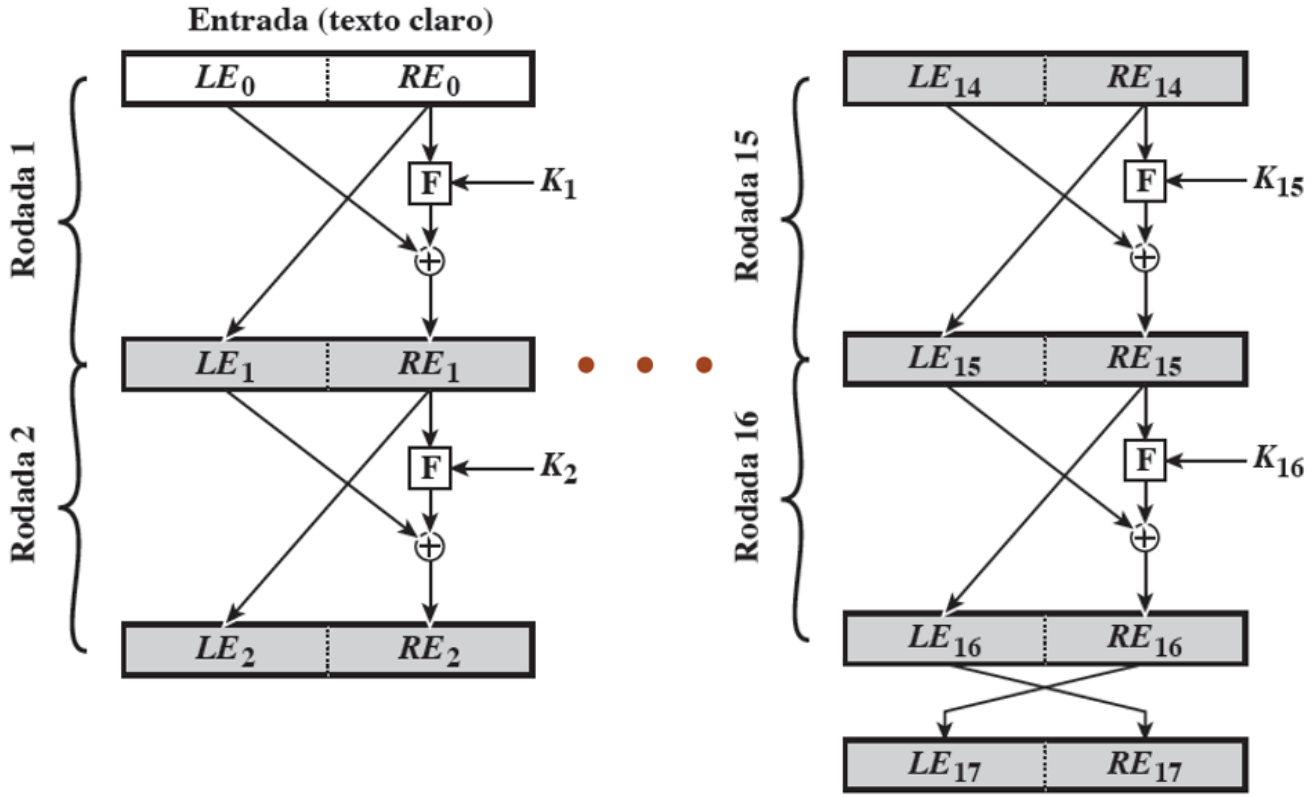
A cifra de Feistel



- A essência da técnica de Feistel é:
- Restringir o conjunto das permutações a um subconjunto extremamente pequeno de $\mathbf{2^k}$ permutações.
- $\boldsymbol{k}$ *é o tamanho da chave* — tipicamente na faixa de 56 a 256 bits.
  - *Com essa chave, há um total de* 2^k *transformações possíveis, em vez de* $\mathbf{2^n!}$ *transformações disponíveis com a cifra de bloco ideal.*

Estrutura da cifra de Feistel

- Divide o bloco de 64 bits em duas metades de 32 bits, L_0 e R_0.
- Cada rodada i possui como entradas L_{i-1} e R_{i-1}, que são derivadas da rodada anterior, assim como uma subchave K_i derivada do K geral.
- A **metade direita** é copiada para a próxima rodada inalterada e se torna L_i.
- Define R_i como $F(R_{i-1}, K_i) \oplus L_{i-1}$
  - Pense na função F como um gerador pseudoaleatório com os dois parâmetros de entrada R_{i-1} e K_i.



Parâmetros da cifra de Feistel

Tamanho de bloco

- Tamanhos de bloco maiores significam maior segurança, mas a velocidade de cifração/decifração é reduzida.
- Tradicionalmente, o tamanho de bloco de **64 bits** foi considerado uma escolha razoável e quase universal no projeto de cifras de bloco.
- Porém, o novo AES usa um tamanho de bloco de **128 bits**.

Parâmetros da cifra de Feistel

Tamanho de chave

- **Tamanho de chave** maior significa maior segurança, mas pode diminuir a velocidade de cifração/decifração.
- Maior segurança é obtida pela maior resistência a **ataques de força bruta.**
- Os tamanhos de chave de **64 bits ou menos** agora são em grande parte considerados inadequados, e **128 bits** tornou-se um padrão comum.

Parâmetros da 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.

Fim!

[Aula 03] Cifras de blocos