

Abstract geometric lines in the top left corner, consisting of several overlapping, irregular polygons and lines in a light brown color.

CIFRAS DE BLOCO

Gerência e Segurança de Redes

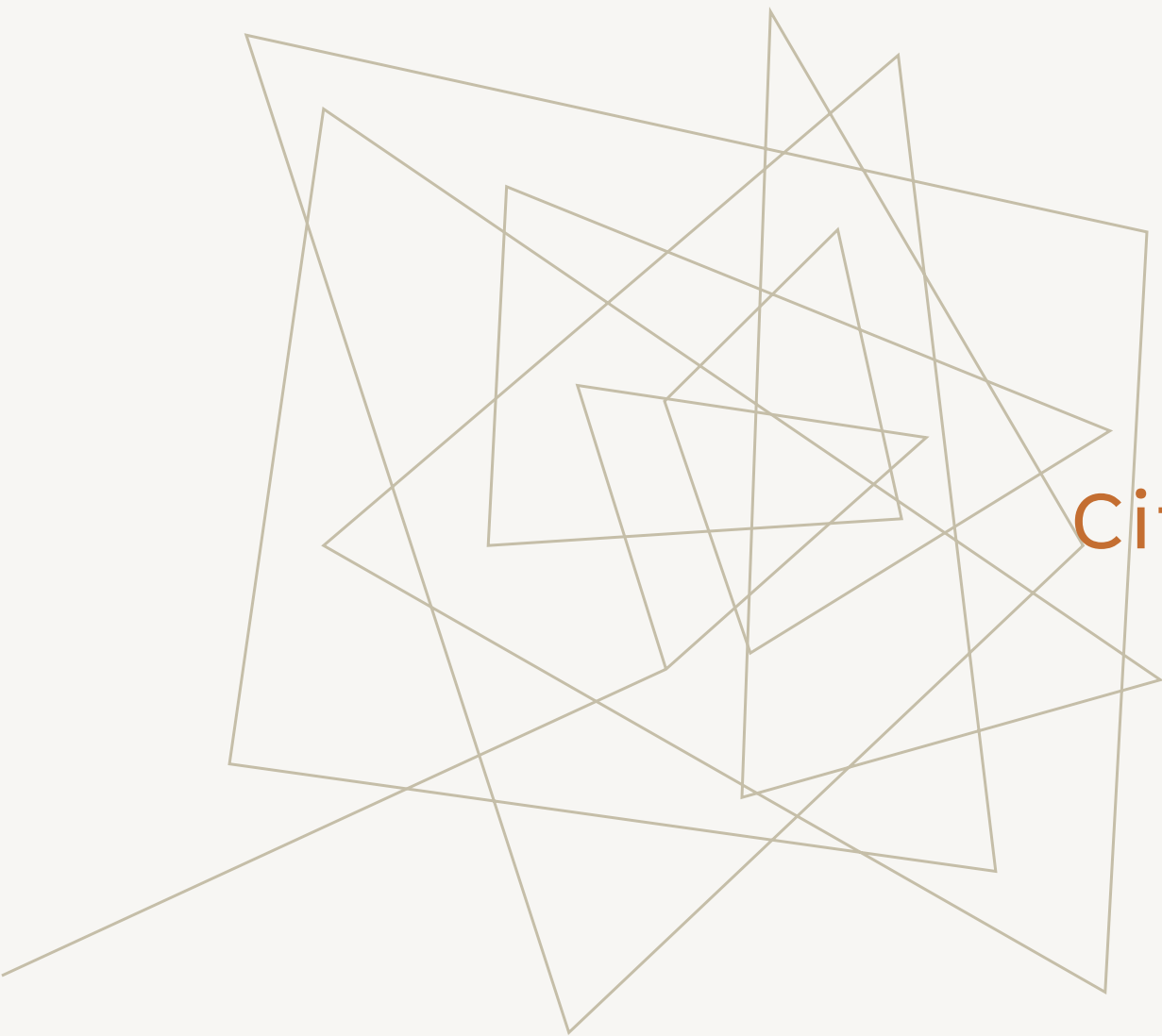
Objetivos de Aprendizagem

Distinguir cifras de bloco e de fluxo

Apresentar o *Data Encryption Standard*

Agenda

1. Cifras de fluxo e de bloco
2. Cifra de Feistel
3. DES
4. Modos de Operação
5. Open SSL



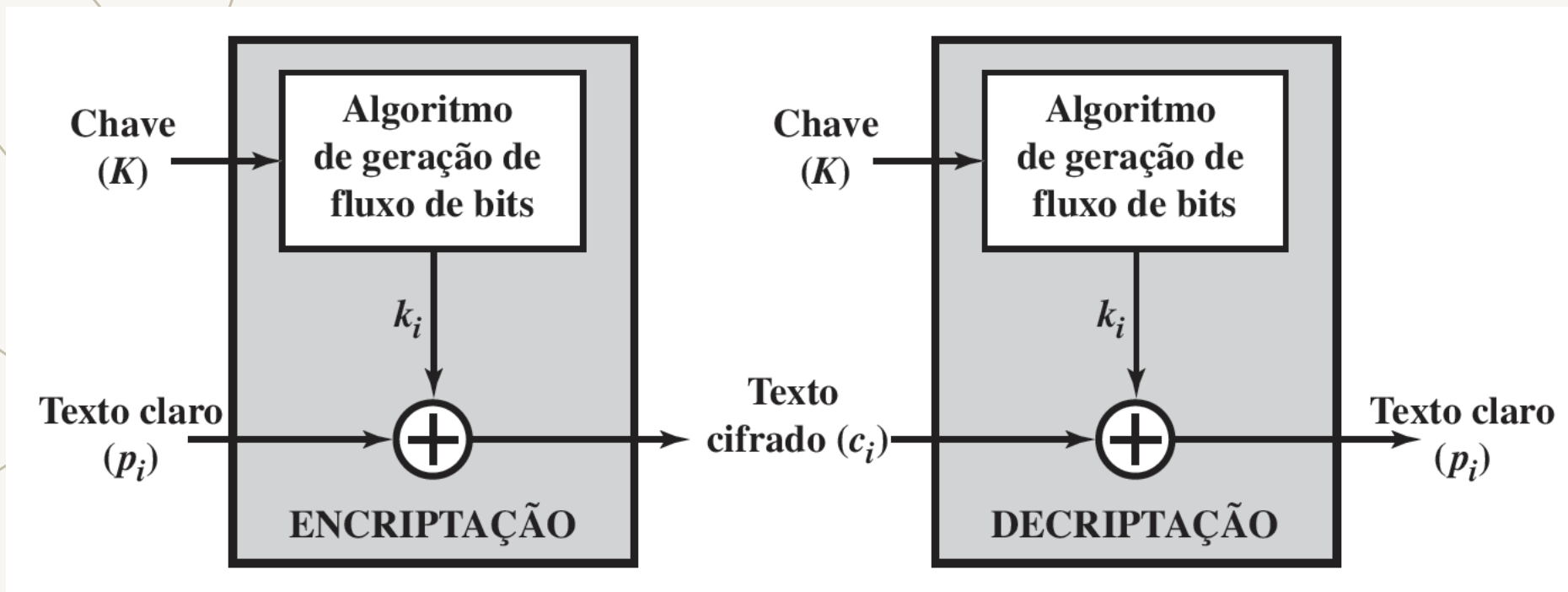
Cifras de Fluxo e de Bloco

Cifra de Fluxo

- Encripta um fluxo de dados digital bit a bit ou byte a byte
- O fluxo de chaves (k_i) tem o tamanho do fluxo de bits de texto claro (p_i)
- Para chaves aleatórias, a cifra é inquebrável (One Time Pad)
- Problema de compartilhamento de chaves

Cifra de Fluxo

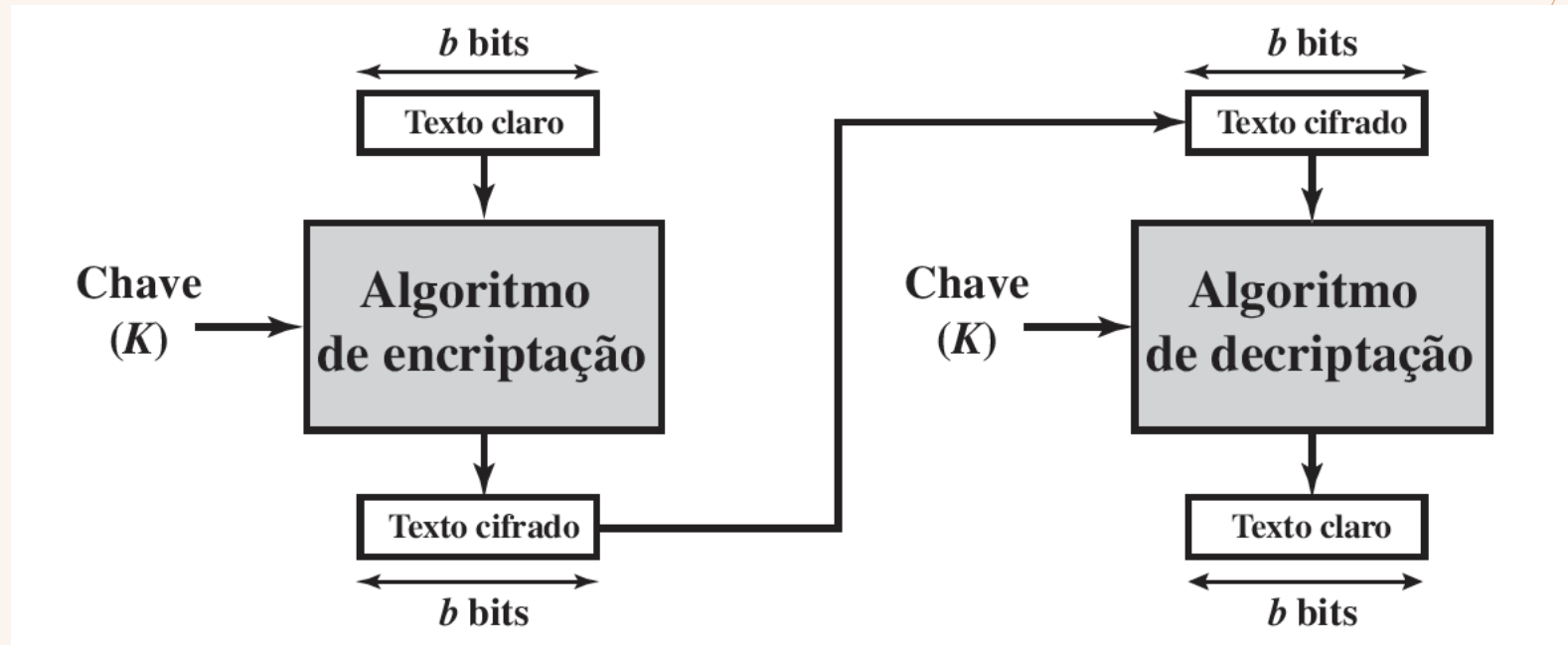
- Geração de fluxo de bits feita via função algorítmica no emissor e receptor
- O algoritmo é afetado pela chave
- O fluxo de bits deve ser criptograficamente forte



Cifra de Bloco

- O texto claro é tratado como um todo ou em partes de tamanho fixo
- Blocos de 64 ou 128 bits
- Emissor e receptor compartilham uma chave simétrica

Cifra de Bloco



Cifra de Bloco Ideal

- Para blocos de n bits 2^n blocos possíveis
- Existem $2^n!$ mapeamentos possíveis

Mapeamento reversível

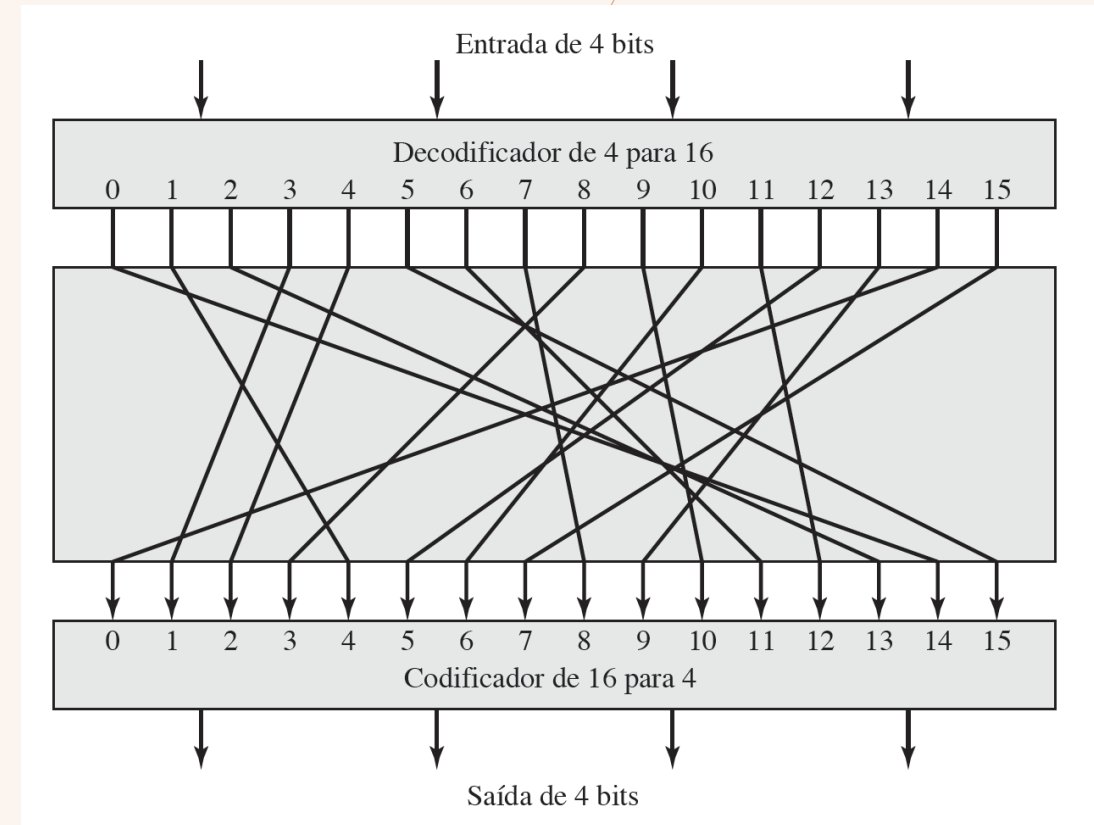
Texto claro	Texto cifrado
00	11
01	10
10	00
11	01

Mapeamento irreversível

Texto claro	Texto cifrado
00	11
01	10
10	01
11	01

Cifra de Bloco Ideal

- Cifra reversível
- Mapeamentos de encriptação e decríptação definidos por tabulação
- Exemplo, cifra de substituição com $n = 4$ bits



Cifra de Bloco Ideal

Texto claro	Texto cifrado
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

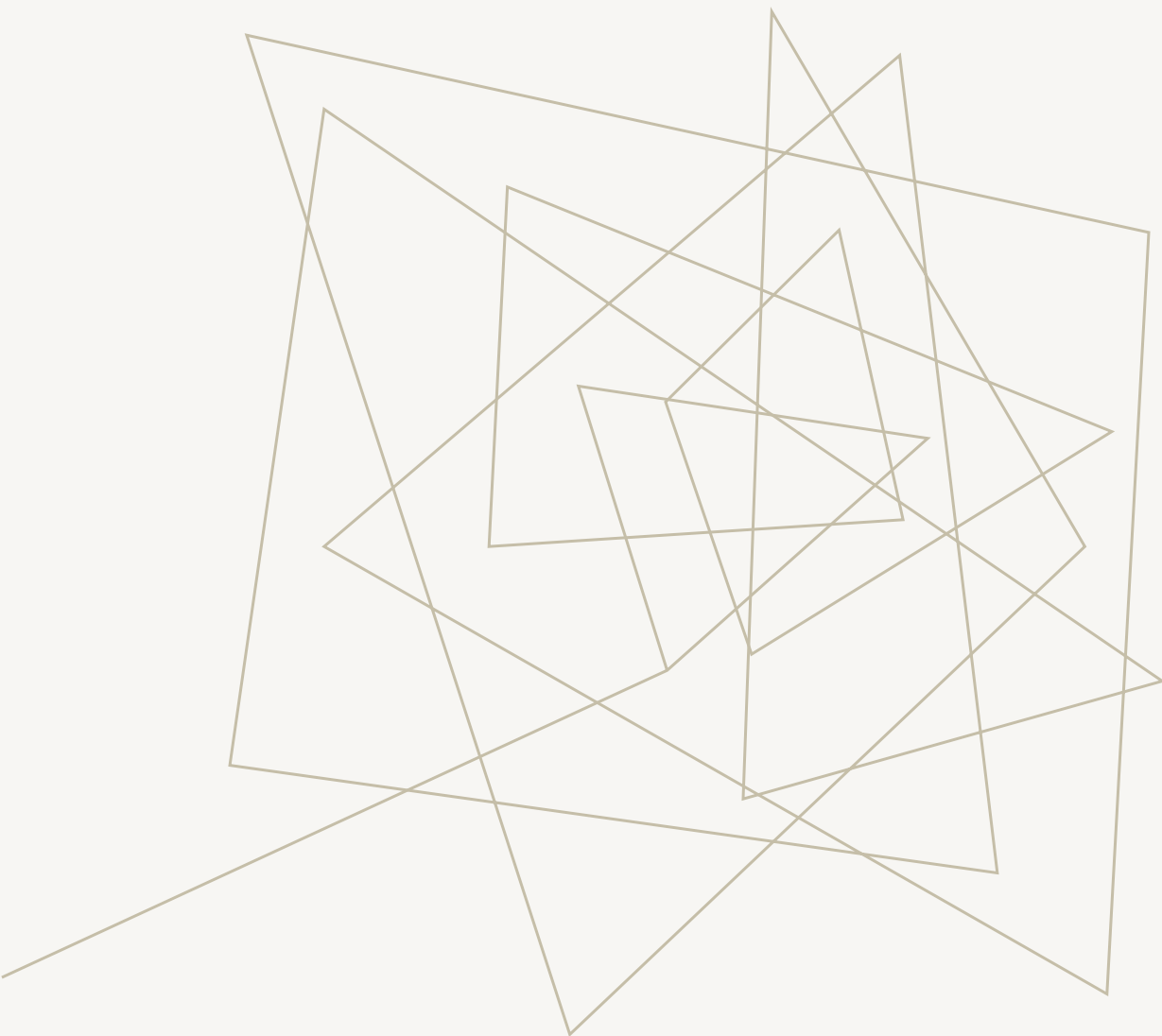
Texto cifrado	Texto claro
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

Fragilidades

- Para n pequeno a CFI equivale a cifra de substituição
Sujeita a análise estatística da texto
- Considerando n suficientemente grande e uma substituição reversível, as características estatísticas do texto são mascaradas
- Porém, uma cifra de bloco com n suficiente grande é **impraticável**

Fragilidades

- O mapeamento coincide com a própria chave
- Para o exemplo com 4 bits é necessário uma chave de 4 bits x 16 linhas = 64 bits
- Regra geral:
Tamanho de bloco: n
Tamanho da chave: $n \times (2^n)$



Cifra de Feistel

Cifra de Feistel

Conceito de uma cifra de produto, (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.

Cifra Feistel

- Cifra de bloco com chave de tamanho k bits + bloco de n bits
Transformações: 2^k
- Cifra de bloco ideal
Transformações: $2^n!$
- Alternância entre permutações e substituições

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 é modificada.**

Difusão x Confusão

- A cifra de Feistel é uma aplicação prática de uma proposta de *Claude Shannon* para uma cifra de produto que alterne funções de confusão e difusão
- Difusão e confusão são os ingredientes básicos para qualquer sistema criptográfico para frustrar a criptoanálise estatística

Difusão

- Dissipa a estrutura estatística do texto
- Cada dígito do texto claro afeta vários dígitos do texto cifrado
- Seja uma mensagem $M = m_1 + m_2 + m_3 + \dots$
- Cada letra y_n do texto cifrado é representado por

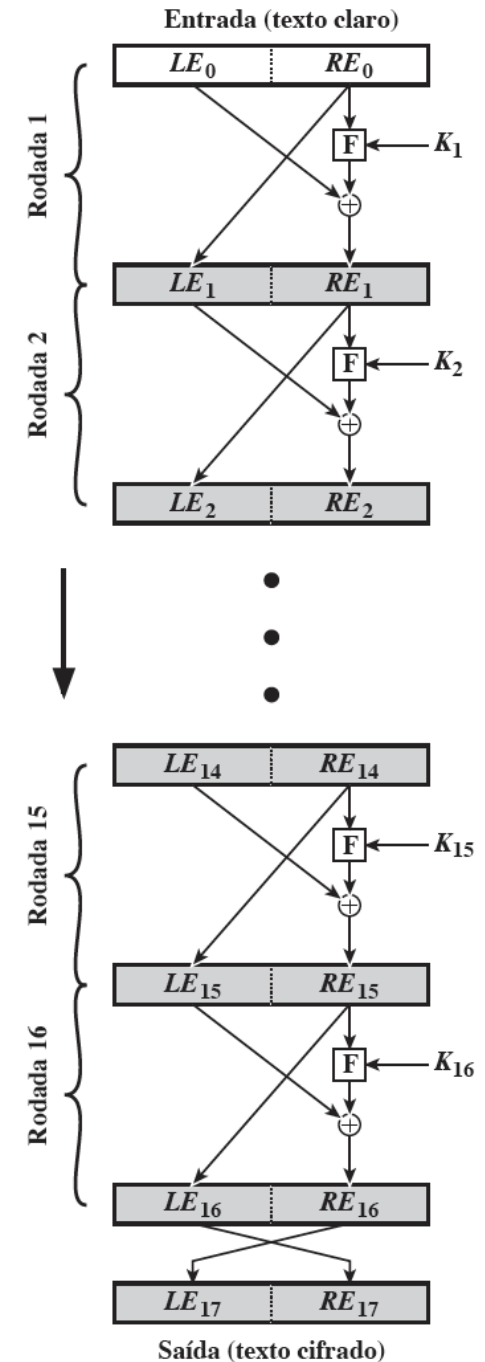
$$y_n = \left(\sum_{i=1}^k m_{n+i} \right) \bmod 26$$

Confusão

- Agrega complexidade ao relacionamento estatístico entre o texto claro e o texto cifrado
- Mesmo que o atacante tenha alguma ideia das estatísticas do texto a complexidade conferida pela confusão impede a dedução da chave

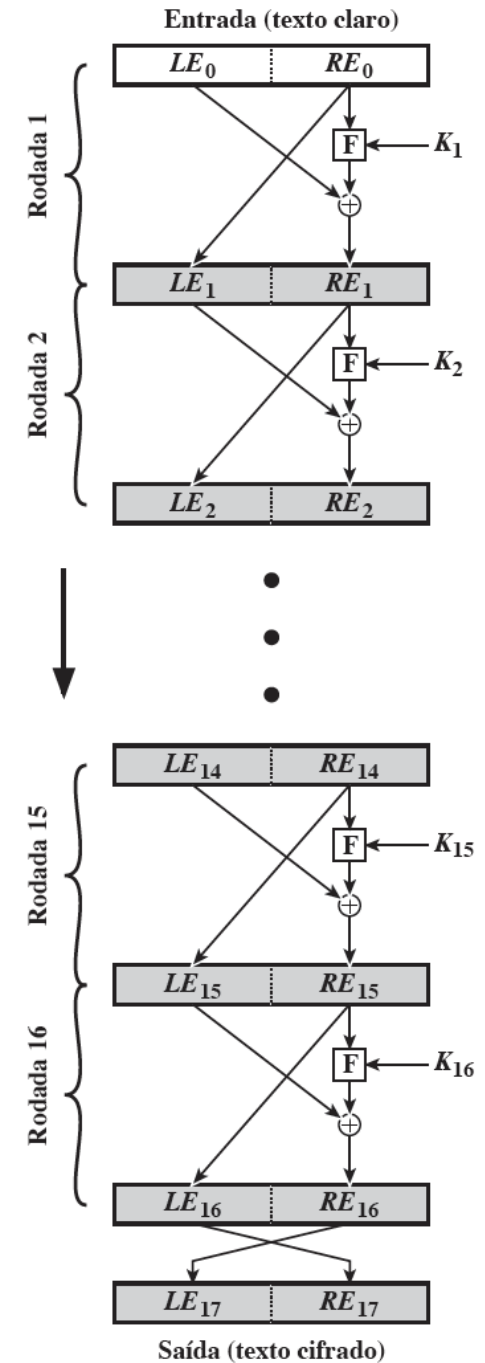
Cifra de Feistel

- **Entrada:**
Bloco de texto claro com $2w$ bits
Chave K
Dividido em LE_0 (Left) e RE_0 (Right)
- **Rodadas:**
 N rodadas
A chave é alterada a cada rodada
Permutação entre L e R
- **Saída:**
 LE_1 e RE_1 (alimentam a entrada próxima rodada)



Cifra de Feistel

- Função (F):
XOR



Parâmetros

- **Tamanho de bloco:**

Maior segurança com blocos maiores

Custo computacional

Blocos de 64 bits são razoáveis

- **Tamanho de chave:**

Maior segurança com chaves maiores

Custo computacional

- **Número de rodadas:**

Quanto mais rodadas maior segurança

Parâmetros

- Algoritmo de subchave e F:
Dificulta a criptoanálise

An abstract graphic on the left side of the slide, consisting of several overlapping, irregular polygons and lines in a light brown color. The shapes are nested and intersect, creating a complex, layered geometric pattern.

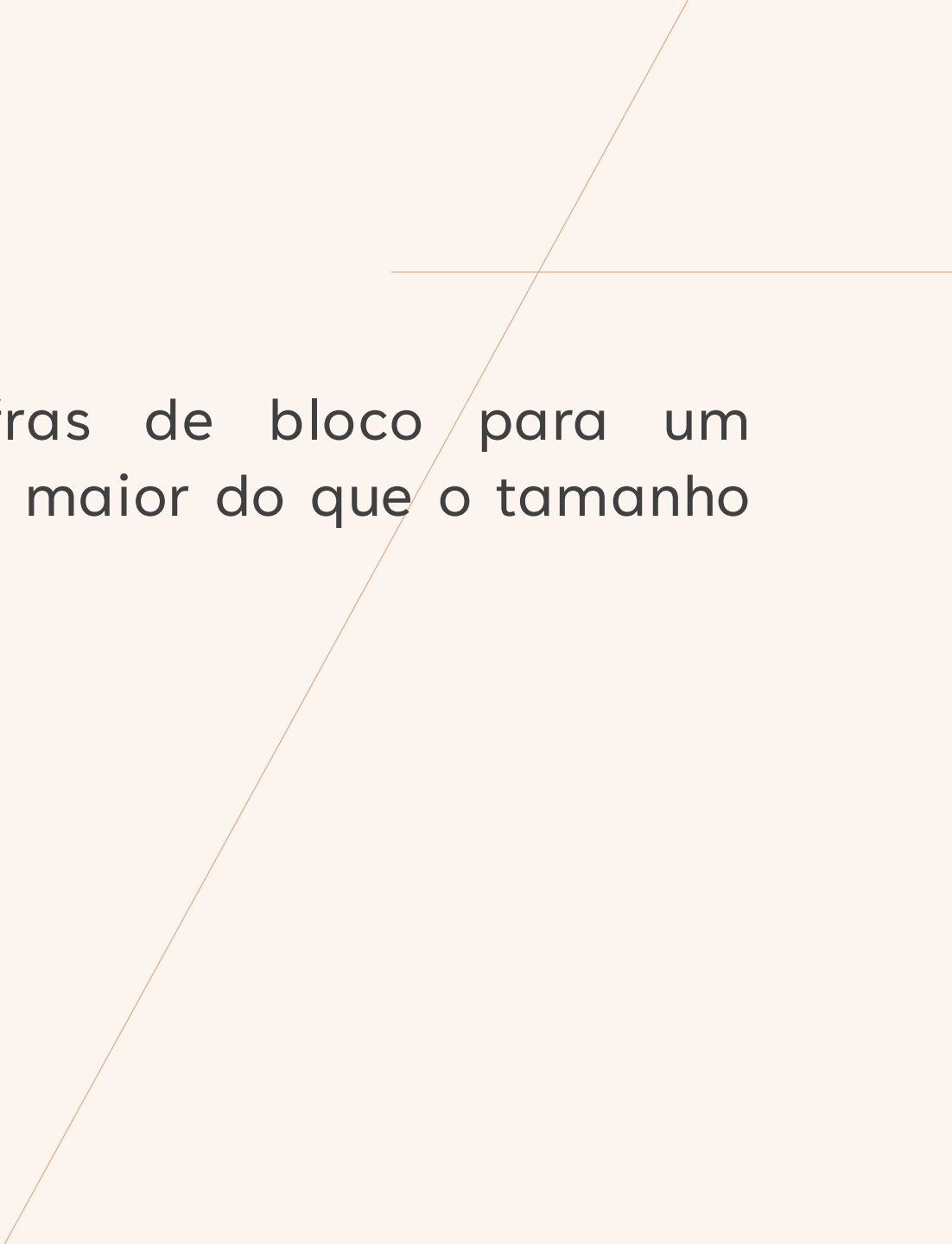
Data Encryption Standard

Data Encryption Standard

- Criptografia mais utilizada antes do AES (2001)
- Adotado pelo NIST em 1977
- Reafirmado em 1994
- Substituído pelo Triple DES em 1999
- Triple DES substituído pelo AES em 2001

Data Encryption Standard

- Blocos de dados de 64 bits
- Chave de 56 bits
- 16 rodadas



Como utilizar cifras de bloco para um conjunto de dados maior do que o tamanho do bloco?



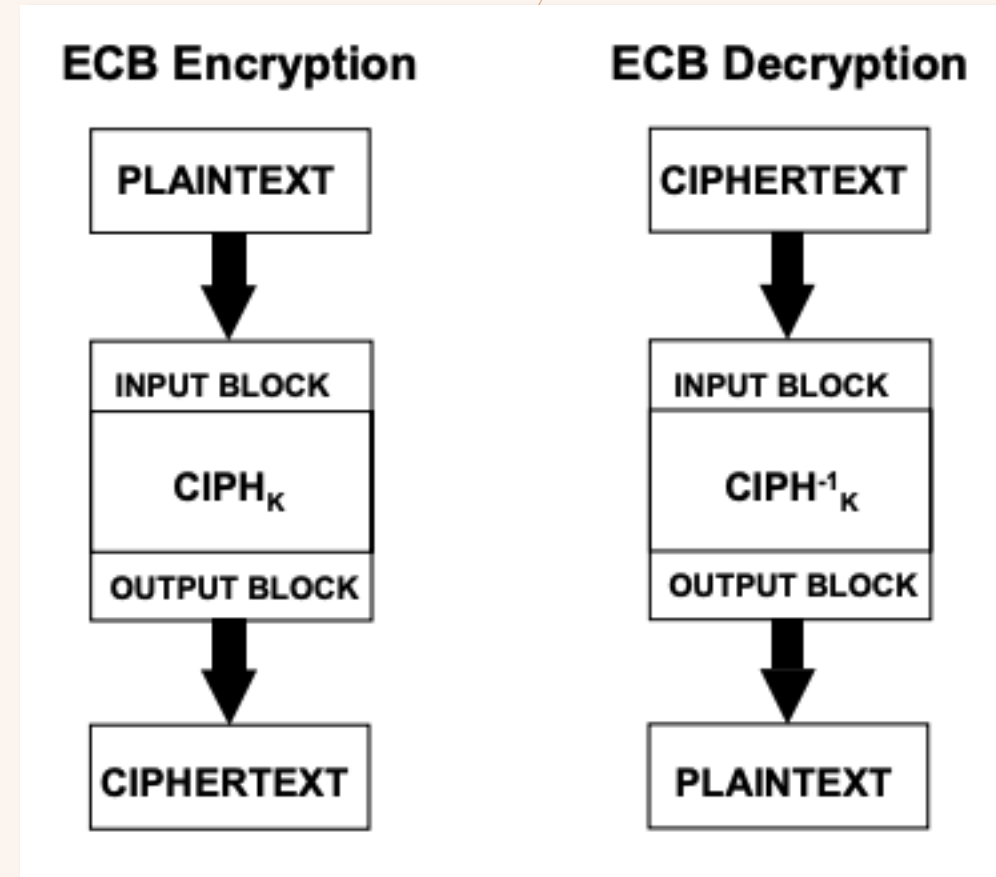
Modos de Operação

Modos de Operação

- Descrevem como aplicar os princípios de bloco a mensagens mais longas
- Existem diversos “modos” de operação
 - Electronic Codebook Mode (ECB)
 - Cipherblock Chaining Mode
 - Cipher Feedback Mode
 - Output Feedback Mode
 - Counter Mode

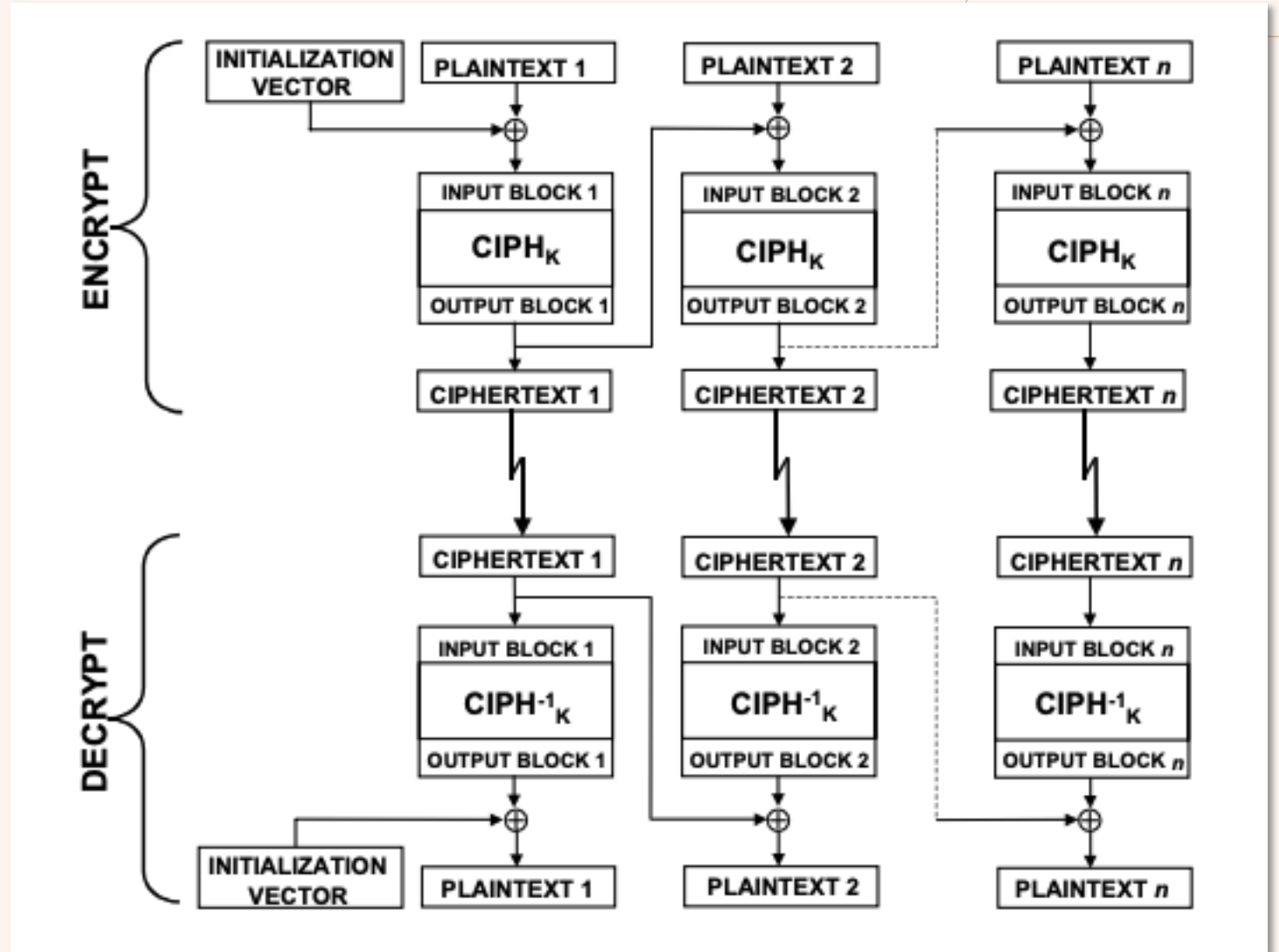
Electronic Codebook Mode

- ECB
- In ECB encryption, the forward cipher function is applied directly and independently to each block of the plaintext. The resulting sequence of output blocks is the ciphertext.
- In ECB encryption and ECB decryption, multiple forward cipher functions and inverse cipher functions can be computed in parallel
- Mensagens com tamanho múltiplo do tamanho do bloco
- Vulnerável a ataques, pois a mesma chave gera as mesmas cifras, sempre



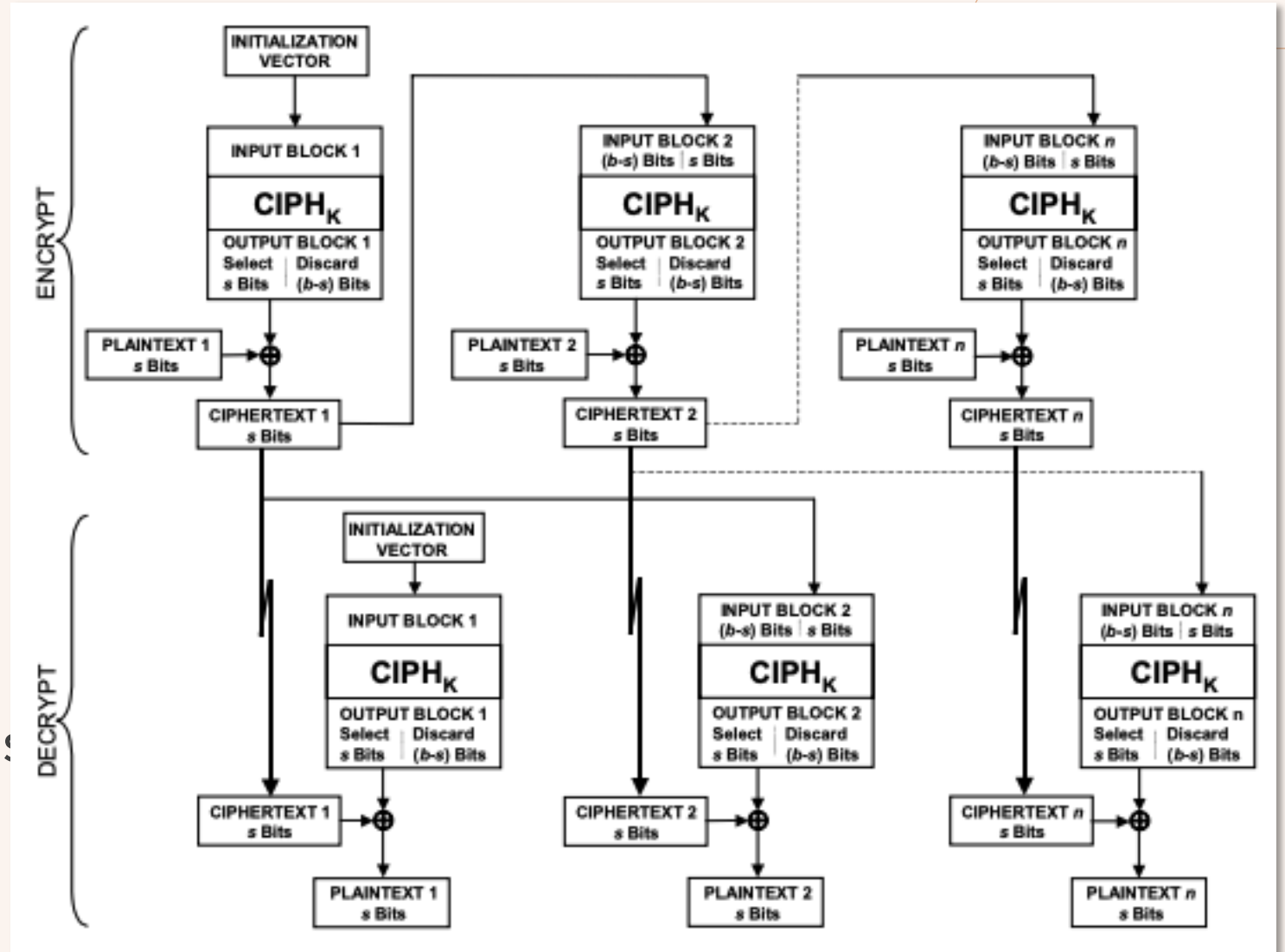
Cipher Block Chaining Mode

- CBC
- so the forward cipher operations cannot be performed in parallel.
- In CBC decryption, however, the input blocks for the inverse cipher
- function, i.e., the ciphertext blocks, are immediately available, so that multiple inverse cipher
- operations can be performed in parallel
- Um dos mais usados



Cipher Feedback Mode

- CFB
- Similar ao CBC, porém utilizado apenas uma fração do bloco cifrado como entrada do próximo bloco
- Criptografia não pode ser realizada em paralelo, mas a decriptografia sim

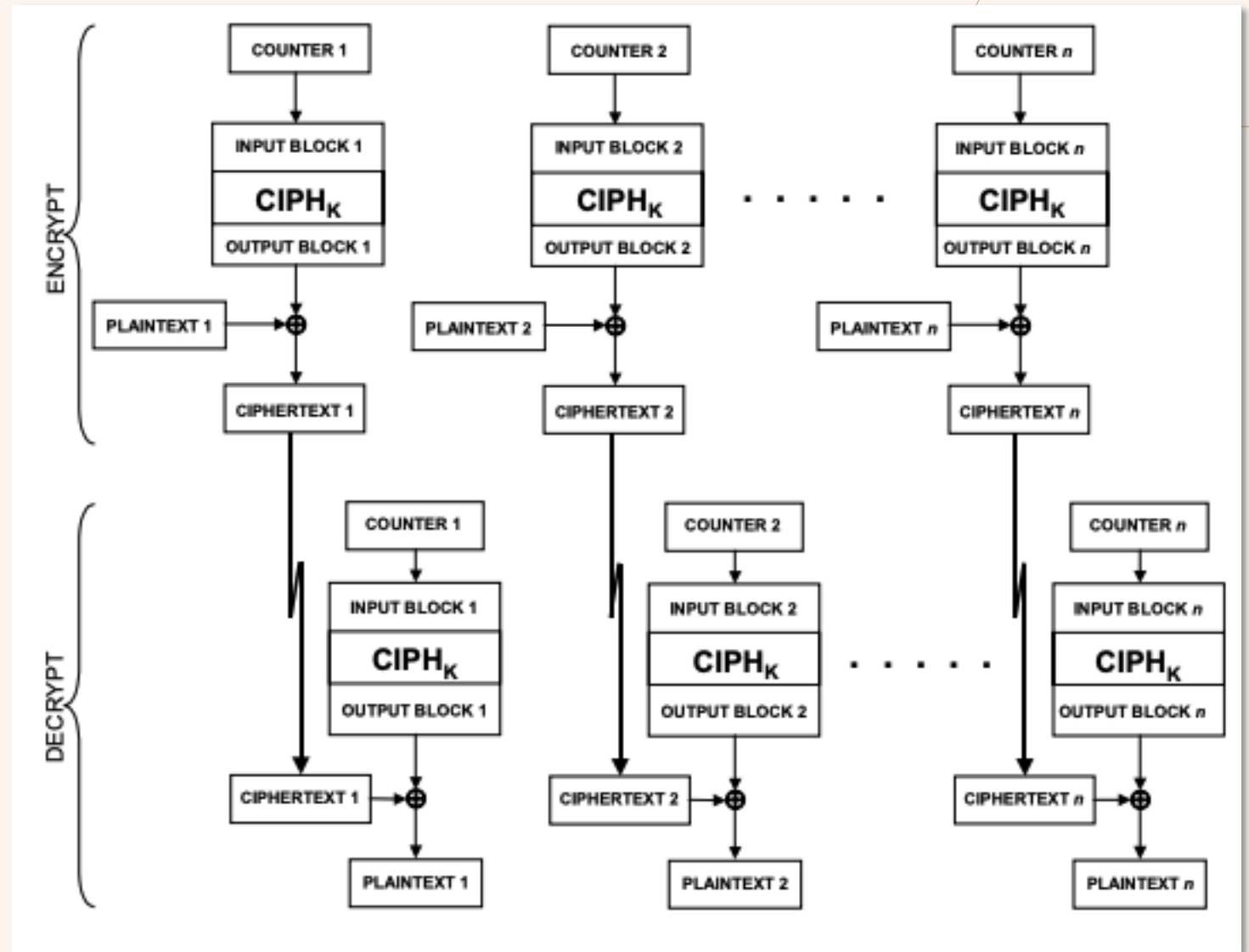


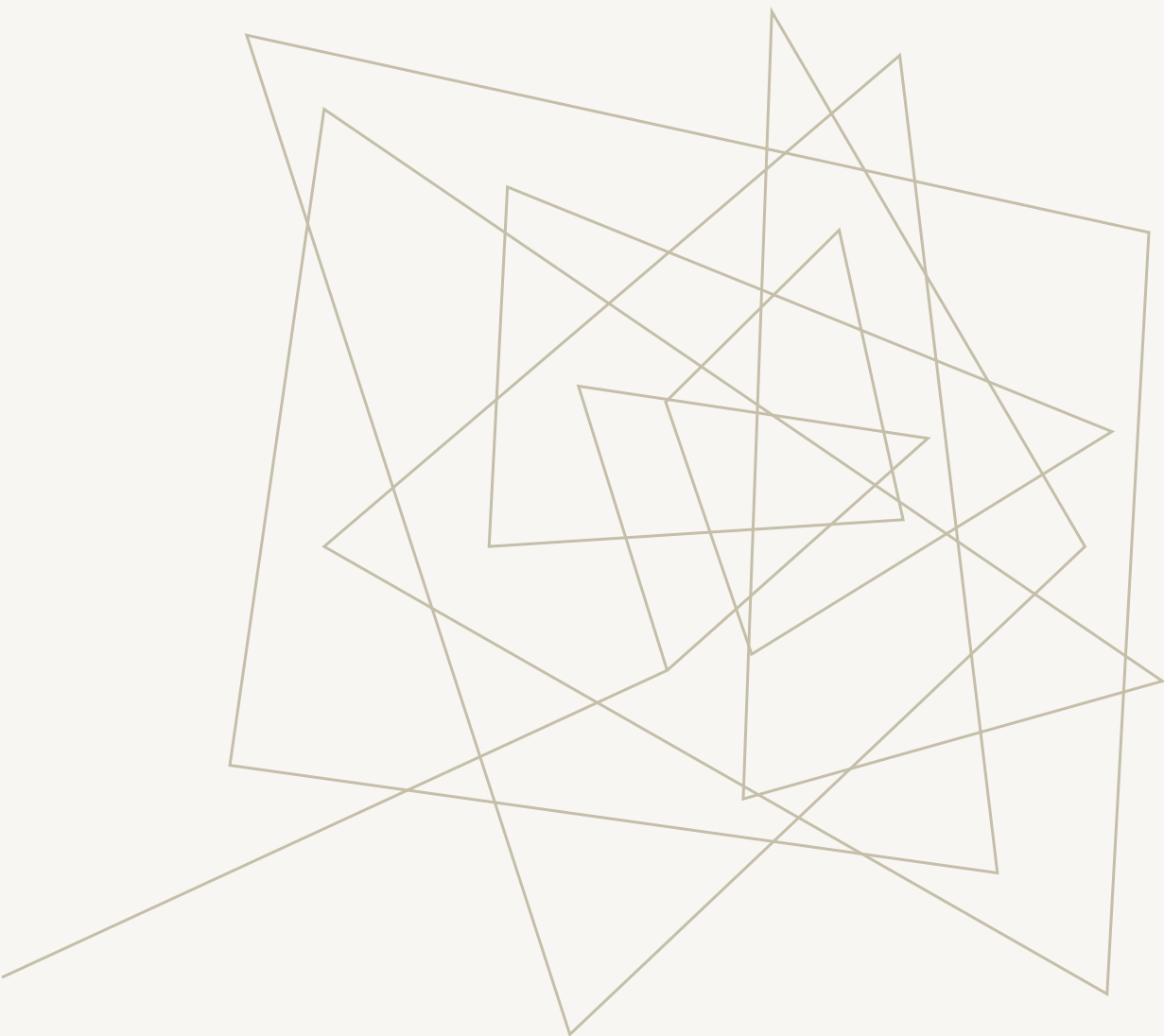
Output Feedback Mode

- Similar ao CFB
- Pequena diferença no tratamento do vetor de inicialização
- Pode ser usado como cifra de fluxo
- Mais resistente a erros de transmissão

Counter Mode

- CTR
- Utiliza contadores ao invés de vetor de inicialização
- Pode criptografar e decriptografar em paralelo





Open SSL

Open SSL

The OpenSSL Project develops and maintains the OpenSSL software - a robust, commercial-grade, full-featured toolkit for general-purpose cryptography and secure communication.

Open SSL

- Kit de ferramentas de criptografia (SSL/TLS)
- Versão 3.2.1
- `openssl version`

openssl help

Cipher commands (see the `enc` command for more details)

aes-128-cbc	aes-128-ecb	aes-192-cbc	aes-192-ecb
aes-256-cbc	aes-256-ecb	aria-128-cbc	aria-128-cfb
aria-128-cfb1	aria-128-cfb8	aria-128-ctr	aria-128-ecb
aria-128-ofb	aria-192-cbc	aria-192-cfb	aria-192-cfb1
aria-192-cfb8	aria-192-ctr	aria-192-ecb	aria-192-ofb
aria-256-cbc	aria-256-cfb	aria-256-cfb1	aria-256-cfb8
aria-256-ctr	aria-256-ecb	aria-256-ofb	base64
bf	bf-cbc	bf-cfb	bf-ecb
bf-ofb	camellia-128-cbc	camellia-128-ecb	camellia-192-cbc
camellia-192-ecb	camellia-256-cbc	camellia-256-ecb	cast
cast-cbc	cast5-cbc	cast5-cfb	cast5-ecb
cast5-ofb	des	des-cbc	des-cfb
des-ecb	des-ede	des-ede-cbc	des-ede-cfb
des-ede-ofb	des-ede3	des-ede3-cbc	des-ede3-cfb
des-ede3-ofb	des-ofb	des3	desx
rc2	rc2-40-cbc	rc2-64-cbc	rc2-cbc
rc2-cfb	rc2-ecb	rc2-ofb	rc4
rc4-40	seed	seed-cbc	seed-cfb
seed-ecb	seed-ofb	sm4-cbc	sm4-cfb
sm4-ctr	sm4-ecb	sm4-ofb	

openssl enc

```
[macbookpro:~ roberto1$ openssl enc -base64 -in f.txt -out f.enc
[macbookpro:~ roberto1$ cat f.enc
bGluaGEgMQpsaW5oYSAYCmxpbmhhIDUKCg==
[macbookpro:~ roberto1$ cat f.txt
linha 1
linha 2
linha 5

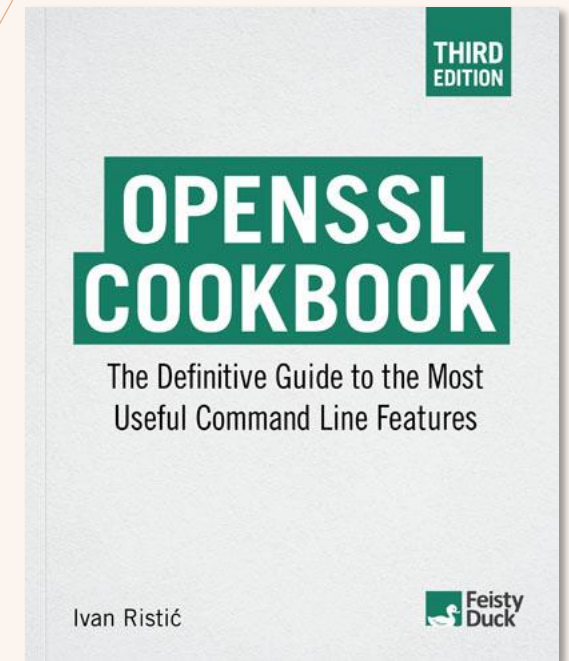
[macbookpro:~ roberto1$ openssl enc -d -base64 -in f.enc
linha 1
linha 2
linha 5

macbookpro:~ roberto1$ █
```

openssl enc -des

Referências

- <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf>
- <https://www.openssl.org/>
- <https://www.feistyduck.com/library/openssl-cookbook/online/>
- <https://wiki.openssl.org/index.php/Enc>



Referências

- **Capítulo 3.** Criptografia e Segurança de Redes. *William Stallings*. 6ª. Edição. Editora Pearson.



A series of thin, light brown lines forming an abstract geometric pattern in the top left corner of the slide. The lines intersect to create various triangular and polygonal shapes.

FIM

Prof. José Roberto Bezerra

jbroberto@ifce.edu.br

IFCE – *Campus* Fortaleza