Algoritmos e Estruturas de Dados III

11 - Criptografia

PUC Minas

Roteiro

- Introdução
  - Cifra de César
  - Cifra de substituição
  - Cifra de Vigenére
  - Cifras de transposição
  - Cifras das colunas
- Criptografia Simétrica
  - Cifras de Fluxo - One Time Pad
  - Cifras de Bloco
    - DES
    - 3DES ou TDES
    - AES
- Criptografia Assimétrica
  - RSA
  - Assinatura Digital
  - Certificado Digital

Roteiro

- **Introdução**
  - **Cifra de César**
  - **Cifra de Substituição**
  - **Cifra de Vigenére**
  - **Cifras de Transposição**
  - **Cifras das Colunas**
- Criptografia Simétrica
  - Cifras de Fluxo - One Time Pad
  - Cifras de Bloco
    - DES
    - 3DES ou TDES
    - AES
- Criptografia assimétrica
  - RSA
  - Assinatura Digital
  - Certificado Digital

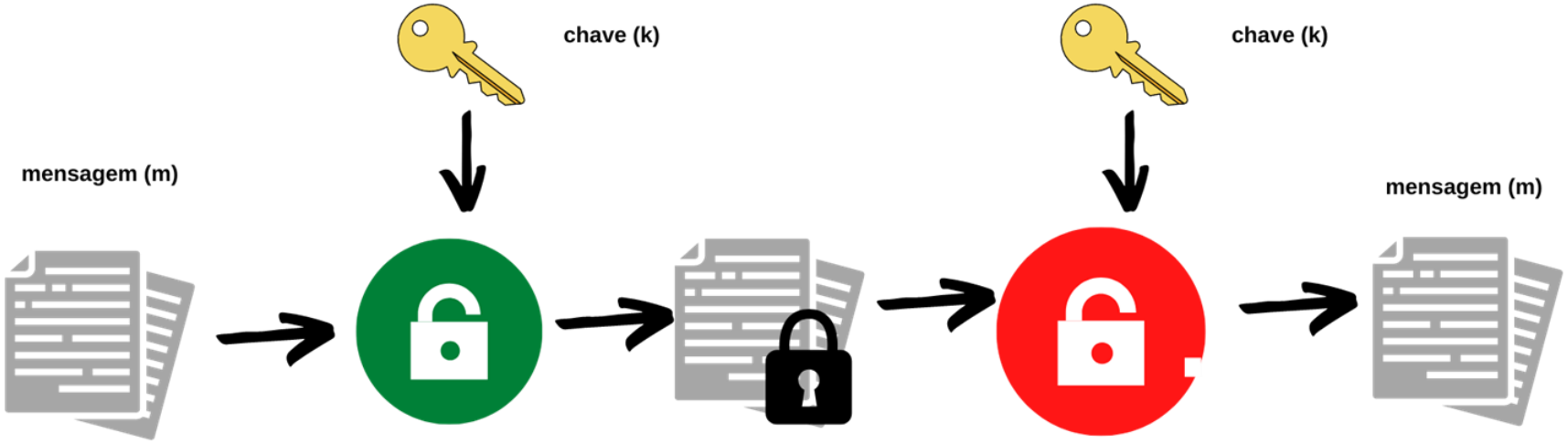
Introdução

PUC Minas

Criptografia

- Do grego: kryptós (escondido) + graphein (escrita)
- Substantivo feminino
    - 1. conjunto de princípios e técnicas empregadas para cifrar a escrita, **torná-la incompreensível para os que não tenham acesso às convenções combinadas**
    - 2. em operações políticas, diplomáticas, militares, criminais etc., modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções

Criptografia



Cifragem (ou encriptação)

Transformação do documento em algo incompreensível

c = E(k,m)

Decifragem (ou desencriptação)

Transformação do documento cifrado em sua versão original

m = D(k,c)

Criptografia - Cifragem

Cifragem é o processo de conversão de um texto claro para um código cifrado.

Decifragem é o processo contrário, de recuperar o texto original a partir de um texto cifrado.

Criptografia

- Geralmente, a criptografia refere-se à construção e análise de protocolos/algoritmos que impeçam terceiros, ou o público, de lerem mensagens privadas.

Criptografia

Muitos aspectos em **segurança da informação**, como: confidencialidade, integridade de dados, autenticação e não-repúdio são centrais à criptografia moderna.

Confidencialidade: Manter as informações privadas
Integridade de dados: Garantir que os dados não foram alterados
Autenticação: Estabelecer a identidade de um usuário ou sistema
Não-Repúdio: Impedir que uma pessoa negue ter feito uma operação ou enviado uma mensagem

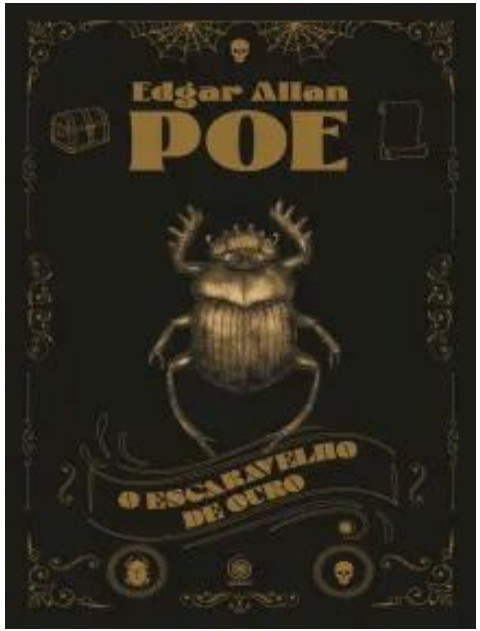
Os algoritmos criptográficos realizam uma ou mais operações, mas não todas. Assim, devem ser usados de forma combinada, se necessário.

Criptografia - Aplicações

- Comércio eletrônico
- Cartões de pagamento baseados em chip
- Moedas digitais
- Senhas de computadores
- Comunicações militares


Proteção de dados
Sigilo de dados armazenados localmente ou em algum servidor na nuvem, com acesso controlado
Comunicação *online*
Troca de mensagens sigilosas, com autenticação das partes envolvidas
Comércio eletrônico e *e-banking*
Segurança para comprador e vendedor, inclusive nas operações bancárias
Assinaturas digitais
Formalização de operações e negócios realizados por meios eletrônicos
Anonimato
Garantia do direito de anonimato e sigilo em determinadas operações

Criptografia - Origens



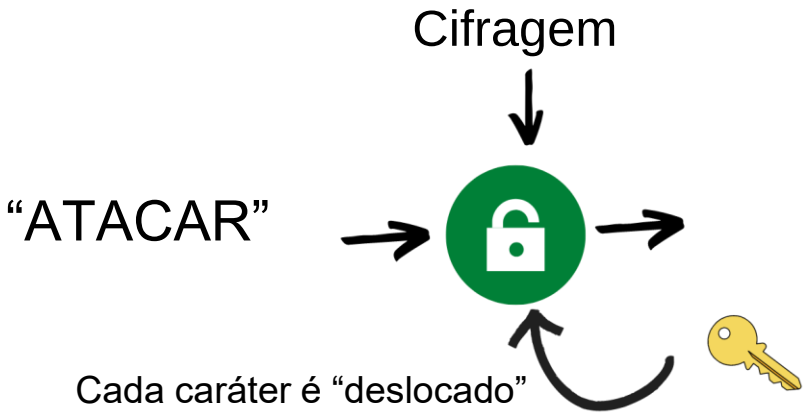
Um dos contos mais famosos de Edgar Allan Poe, "O Escaravelho de Ouro" é também uma espécie de aula prática de criptografia. Nele, conta-se a busca de um tesouro escondido, mas o fascínio do texto está muito mais nas explicações posteriores de William Legrand sobre **como decifrar uma mensagem secreta** do que na própria descoberta.

The Golden-Bug, 1842

https://www1.folha.uol.com.br/fsp/mais/fs0907200004.htm
https://ideiasesquecidas.com/2021/10/11/escaravelho-dourado-decifre-o-enigma-de-allan-poe-com-python/

Criptografia - Cifra de César

Homenagem a Júlio César (100 a.C. - 44 a.C.) que usava um alfabeto assim

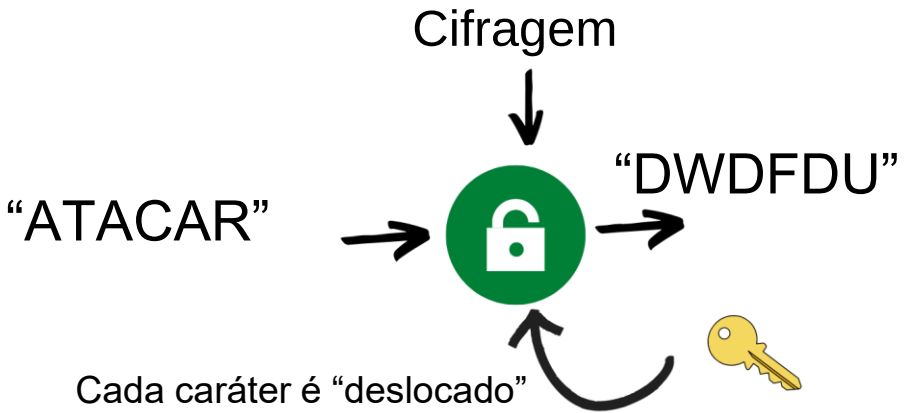


Cada caráter é “deslocado” três posições para frente (não há chave)

$E(x) = (x + 3) \bmod 26$

Criptografia - Cifra de César

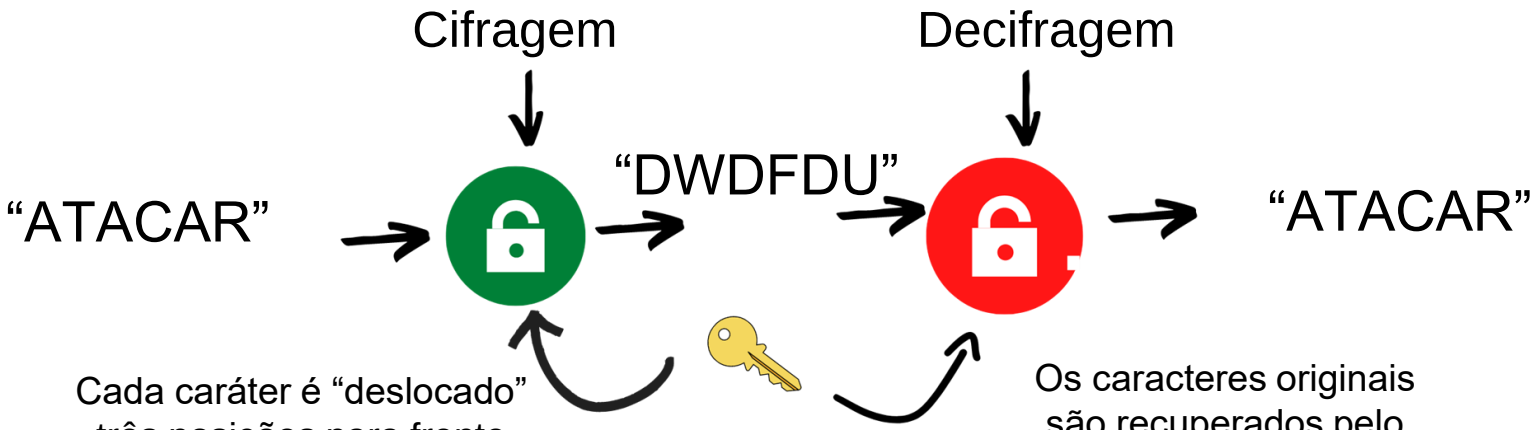
Homenagem a Júlio César (100 a.C. - 44 a.C.) que usava um alfabeto assim



$E(x) = (x + \mathbf{3}) \bmod 26$

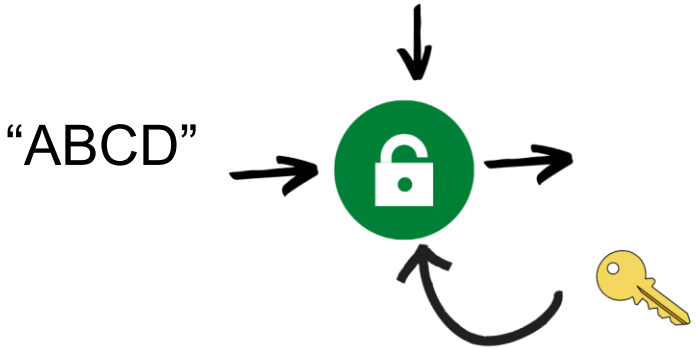
Criptografia - Cifra de César

Homenagem a Júlio César (100 a.C. - 44 a.C.) que usava um alfabeto assim



Criptografia - Cifras de Substituição

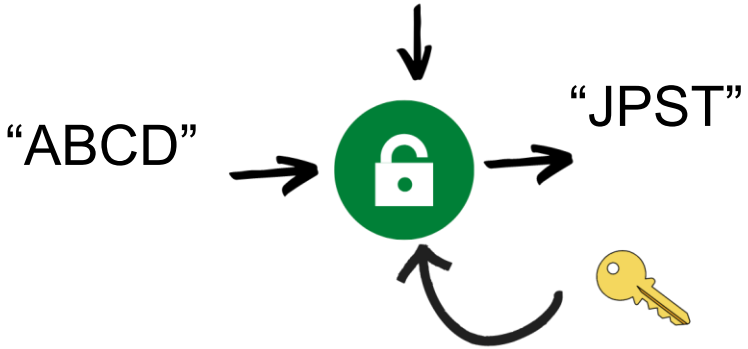
Cada símbolo é substituído por outro símbolo



Caracter Original	A	B	C	D	E	…	Z
Novo Caracter	J	P	S	T	V	…	

Criptografia - Cifras de Substituição

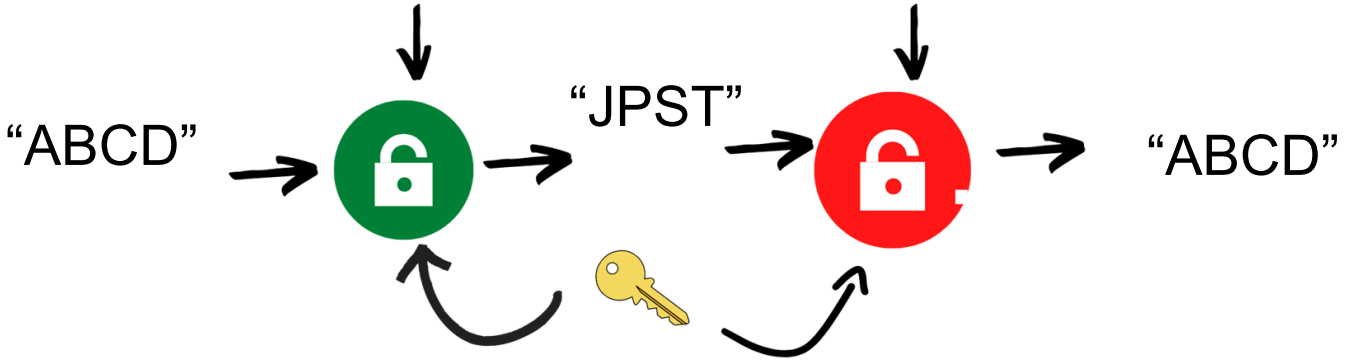
Cada símbolo é substituído por outro símbolo



Caracter Original	A	B	C	D	E	…	Z
Novo Caracter	J	P	S	T	V	…	

Criptografia - Cifras de Substituição

Cada símbolo é substituído por outro símbolo



Caracter Original	A	B	C	D	E	…	Z
Novo Caracter	J	P	S	T	V	…	

Criptografia - Cifra de Vigenére

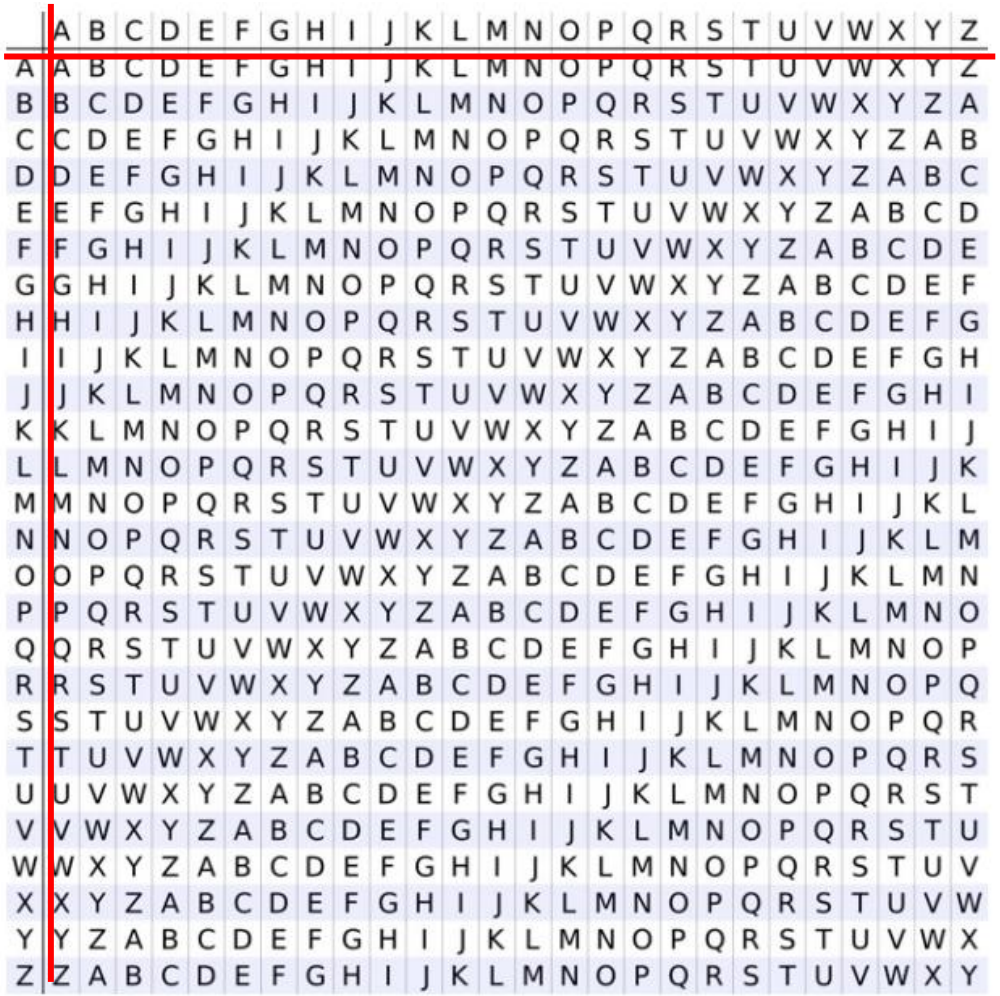
Inventada por Giovan Batista Belsa em 1553, apesar de ter sido atribuída durante muito tempo a Blaise de Vigenère.

Semelhante à Cifra de César, mas cada letra é deslocada um diferente número de posições, de acordo com uma senha.

Exemplo:

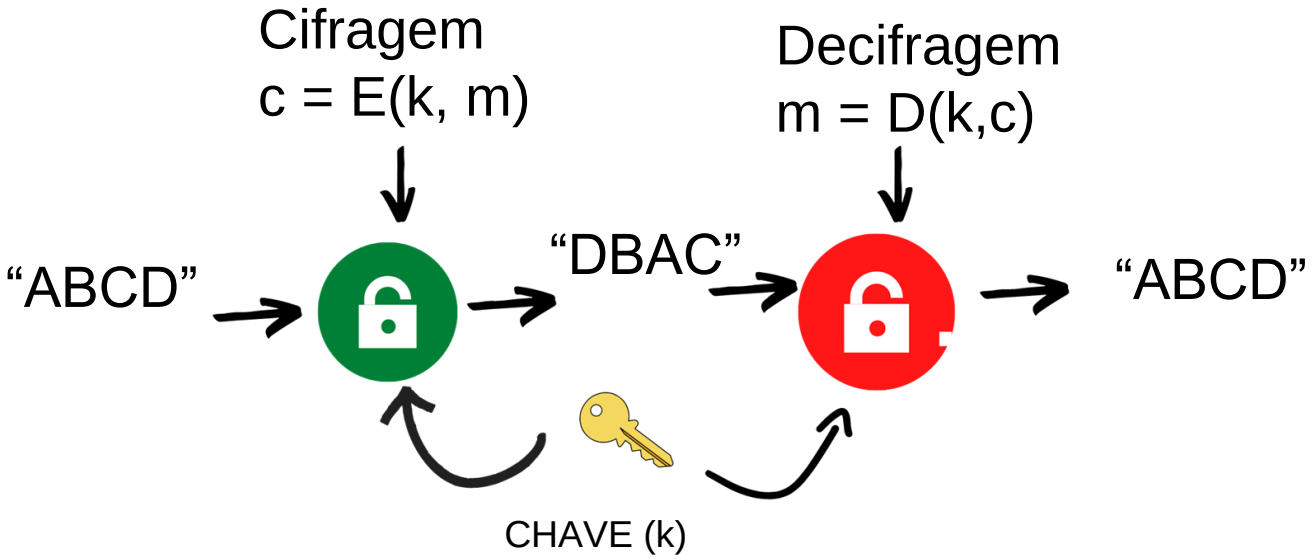
FIMDESEMANA (FIM DE SEMANA)
CAROCAROCAR (CARO)
HIDRGSUACNR

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



Criptografia - Cifras de transposição

Os símbolos são trocados de lugar



Posição original -> Nova posição

Criptografia - Cifras das Colunas

Cifra das colunas

A informação é escrita em uma matriz, linha a linha. Em seguida, as colunas são extraídas, na ordem dos valores dos caracteres da palavra chave.

Exemplo:

M = “**FIMDESEMANA**”

C	**A**	**R**	**O**
2	1	4	3
F	I	M	D
E	S	E	M
A	N	A	

“**ISNFEADMMEA**”

Criptografia - Enigma

A família Enigma de máquinas de cifragem, criadas pelos **Alemães a partir de 1918**, empregava três ou quatro rotores para fazerem a cifragem por substituição. A cada dia, a configuração deveria ser alterada.

Acredita-se que a decifragem das mensagens da Enigma ajudou a por fim à Segunda Guerra Mundial.

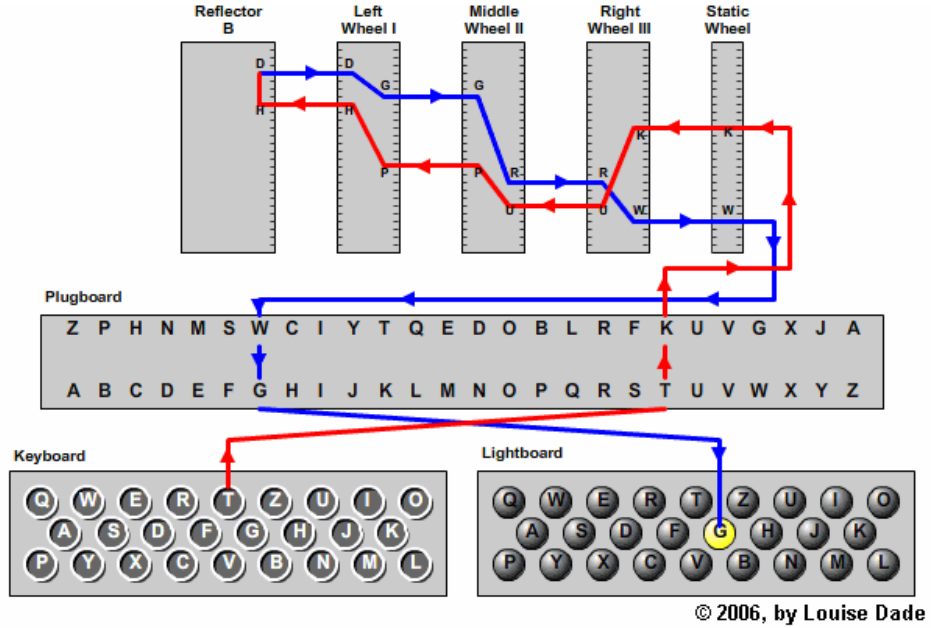
O **Enigma Machine Emulator** permite entender como as Enigmas funcionavam

https://www.101computing.net/enigma-machine-emulator/

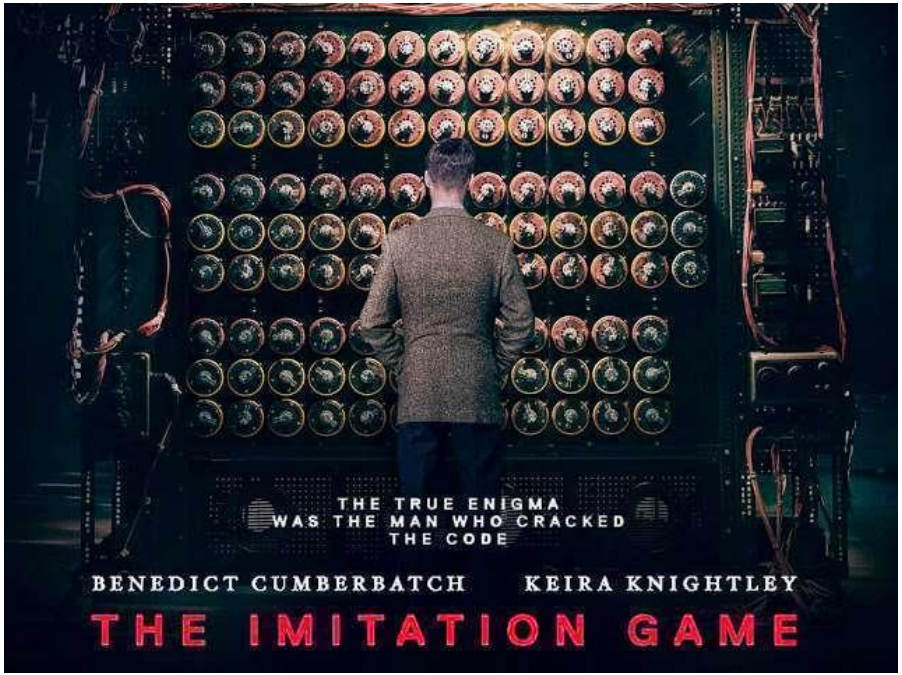
Criptografia - Enigma

Cada tecla era substituída pelo *plugboard* e depois embaralhada por meio de três rotores.

A configuração dos rotores e do *plugboard* era mudada diariamente.



Criptografia - Enigma



“Em 1939, a recém-criada agência de inteligência britânica MI6 recruta Alan Turing, um aluno da Universidade de Cambridge, para entender códigos nazistas, incluindo o "Enigma", que criptógrafos acreditavam ser inquebrável.

A equipe de Turing, incluindo Joan Clarke, analisa as mensagens de "Enigma", enquanto ele constrói uma máquina para decifrá-las.”

Tipos de Criptografia

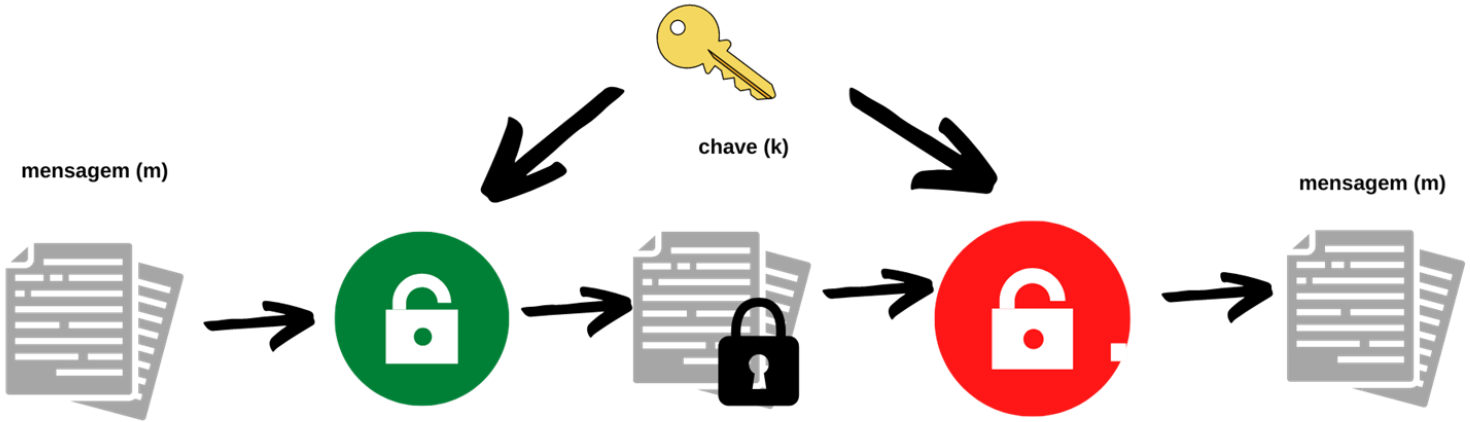
PUC Minas

Criptografia - Tipos

Criptografia simétrica – a mesma chave criptográfica é usada na cifragem e na decifragem.

Criptografia assimétrica – chaves diferentes são usadas na cifragem e na decifragem, mas, geralmente, o processo é bidirecional

Criptografia Simétrica



Cifragem (ou encriptação)

Transformação do documento em algo incompreensível

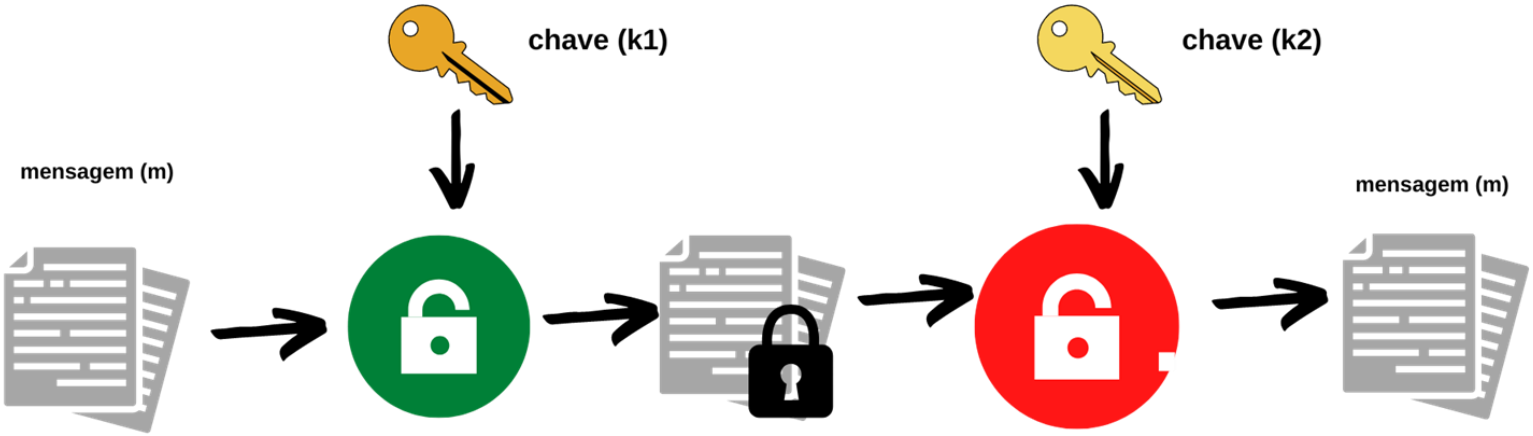
c = E(k,m)

Decifragem (ou desencriptação)

Transformação do documento cifrado em sua versão original

m = D(k,c)

Criptografia Assimétrica



Cifragem (ou encriptação)

Transformação do documento em algo incompreensível

c = E(k1,m)

Decifragem (ou desencriptação)

Transformação do documento cifrado em sua versão original

m = D(k2,c)

Roteiro

- Introdução
  - Cifra de César
  - Cifra de substituição
  - Cifra de Vigenére
  - Cifras de transposição
  - Cifras das colunas
- **Criptografia Simétrica**
  - Cifras de Fluxo - One Time Pad
  - Cifras de Bloco
    - DES
    - 3DES ou TDES
    - AES
- Criptografia assimétrica
  - RSA
  - Assinatura Digital
  - Certificado Digital

Criptografia Simétrica: Cifras de Fluxo e de Bloco

PUC Minas

Cifras

Cifras de fluxo (stream cipher) - A cifragem é feita **bit a bit** (ou símbolo a símbolo). Convertem imediatamente um símbolo do texto em claro em um símbolo do texto cifrado.

Ex.: Substituição simples

Cifras de bloco (block cipher) - A cifragem é feita em blocos, cada um contendo vários símbolos. Cifram um grupo de símbolos do texto em claro como um bloco.

Ex.: Transposição de colunas

Cifras de Fluxo

- Cifra de chave simétrica que combina os bits de um fluxo de bits (bitstream) com os bits de uma chave (keystream)
- A encriptação geralmente é feita por meio de uma simples operação XOR:

$$c = E(k,m) = k \oplus m$$

Tabela verdade:

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Roteiro

- Introdução
  - Cifra de César
  - Cifra de substituição
  - Cifra de Vigenére
  - Cifras de transposição
  - Cifras das colunas
- **Criptografia Simétrica**
  - **Cifras de Fluxo - One Time Pad**
  - Cifras de Bloco
    - DES
    - 3DES ou TDES
    - AES
- Criptografia assimétrica
  - RSA
  - Assinatura Digital
  - Certificado Digital

Criptografia Simétrica: Cifras de Fluxo

PUC Minas

Cifras de Fluxo - One Time Pad

- Desenvolvido em 1917 por Gilbert Vernam nos laboratórios da Bell, para cifrar fluxos.
- A **chave** é uma string de bits aleatória do mesmo tamanho da mensagem a ser criptografada.
- É **inquebrável** (matematicamente comprovado), desde que a chave seja realmente aleatória e mantida em segredo.

Cifras de Fluxo - One Time Pad

c = E(k,m) = k ⊕ m

Mensagem: 1000110
Chave: 1100011
Texto cifrado: 0100101

m = D(k,m) = k ⊕ c

Texto cifrado: 0100101
Chave: 1100011
Mensagem: 1000110

Cifras de Fluxo - One Time Pad

- O OTP requer chaves muito longas, difíceis de serem gerenciadas e mantidas em sigilo.

- Os algoritmos usam, portanto, um gerador de chaves pseudoaleatórias usando uma chave semente de 64, 128, 256 ou mais bits.

Cifras de Fluxo - One Time Pad

Embora realmente o método seja de criptografia inquebrável, seu uso é **impraticável** para muitos aplicativos modernos porque:

- A chave deve ter o mesmo tamanho da mensagem que está sendo enviada.
- A chave deve ser verdadeiramente aleatória.
- As chaves nunca devem ser reutilizadas.
- As chaves devem ser compartilhadas com segurança entre as partes remetente e receptora.
- Devido a essas condições, o uso de one-time pad em mídia digital é impraticável

Roteiro

- Introdução
  - Cifra de César
  - Cifra de substituição
  - Cifra de Vigenére
  - Cifras de transposição
  - Cifras das colunas
- **Criptografia Simétrica**
  - Cifras de Fluxo - One Time Pad
  - **Cifras de Bloco**
    - **DES**
    - **3DES ou TDES**
    - **AES**
- Criptografia assimétrica
  - RSA
  - Assinatura Digital
  - Certificado Digital

Criptografia Simétrica: Cifras de Bloco

PUC Minas

Cifras de Bloco

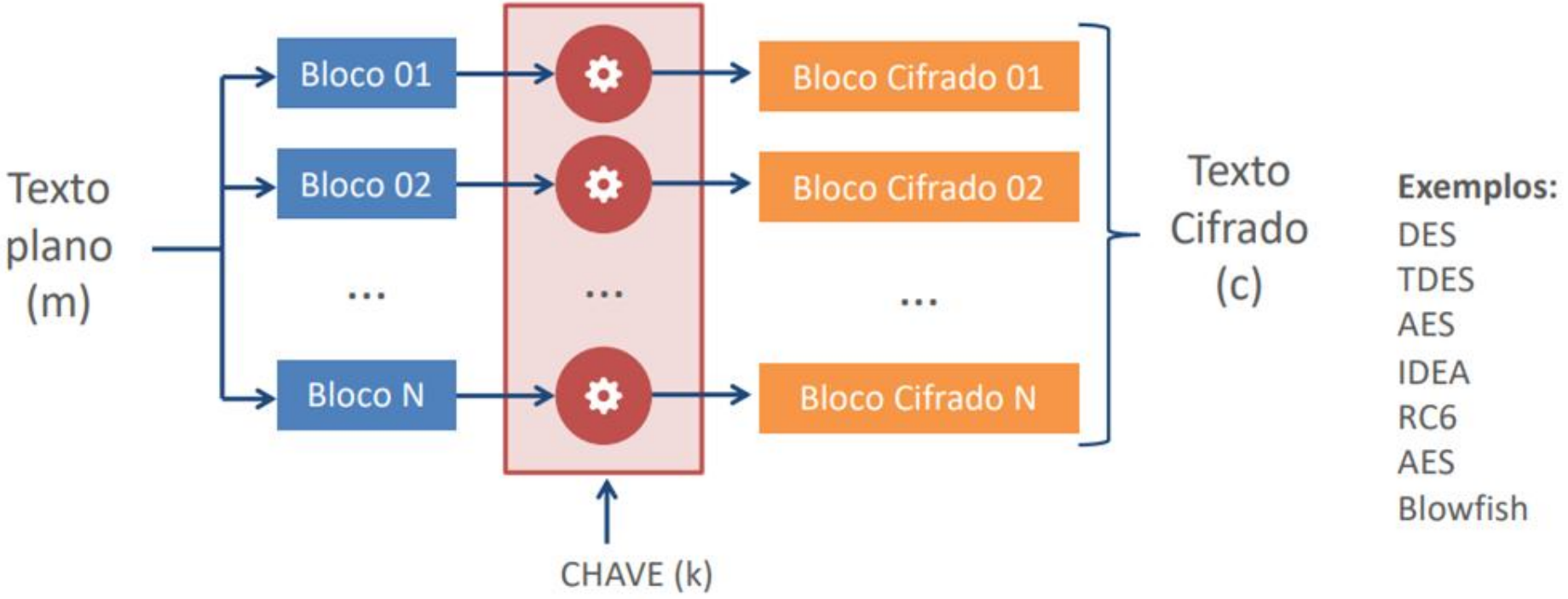
Cifra um conjunto de símbolos como um único bloco.

• O tamanho do bloco pode variar

(64 bits no DES, 128 bits no AES, etc.).

• Cada bloco é cifrado de forma independente.

Cifras de Bloco



Cifra de Blocos

Se o mesmo bloco se repetir, os blocos cifrados serão iguais, facilitando a percepção de um padrão.

• Para evitar isso, existem algumas técnicas como a realimentação, em que o bloco anterior é usado na cifragem do bloco atual

Cifra de Blocos

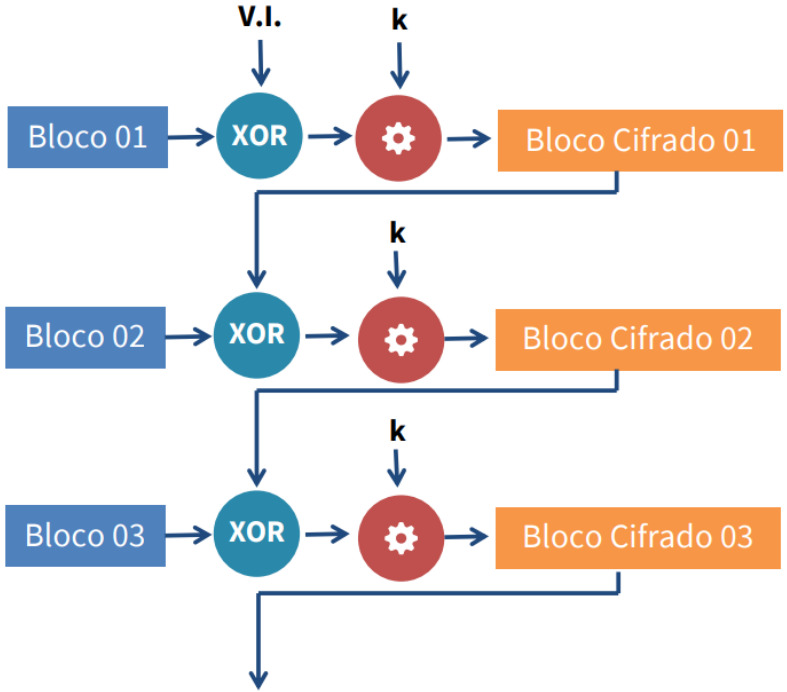
Se o mesmo bloco se repetir, os blocos cifrados serão iguais, facilitando a percepção de um padrão.

• Para evitar isso, existem algumas técnicas como a realimentação, em que o bloco anterior é usado na cifragem do bloco atual

  • Faz-se um XOR do bloco plano atual com o bloco cifrado anterior

  • Para o primeiro bloco (sem bloco anterior), é feito um XOR com um vetor de inicialização (V.I.)

Cifra de Blocos por encadeamento



DES

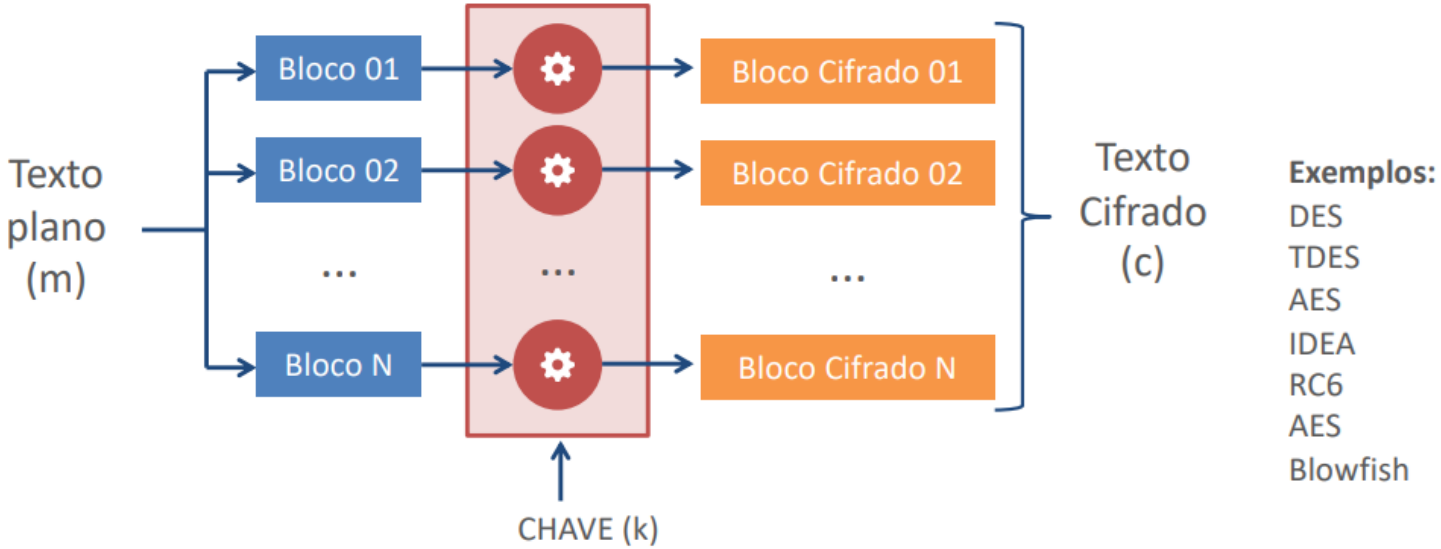
PUC Minas

Data Encryption Standard (DES)

Como é uma cifra de **bloco**, ele toma blocos de 64 bits e os cifra separadamente, usando 16 rodadas da estrutura de **Feistel** (comum em cifras de bloco).

Data Encryption Standard (DES)

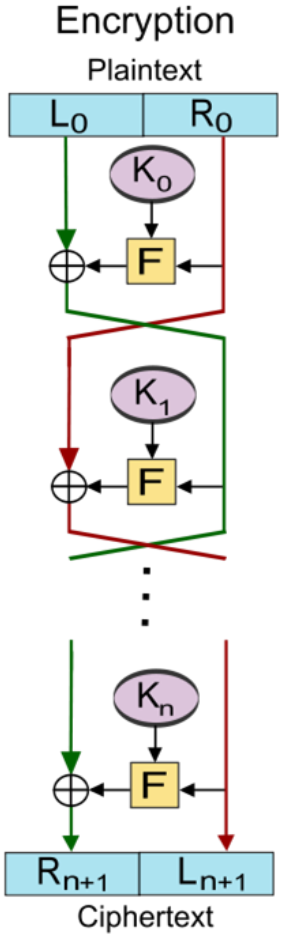
Como é uma cifra de **bloco**, ele toma blocos de 64 bits e os cifra separadamente, usando 16 rodadas da estrutura de **Feistel** (comum em cifras de bloco).



Cifra de Feistel

K -> subchaves para as rodadas 0 até n

L e R -> blocos do texto de mesmo tamanho

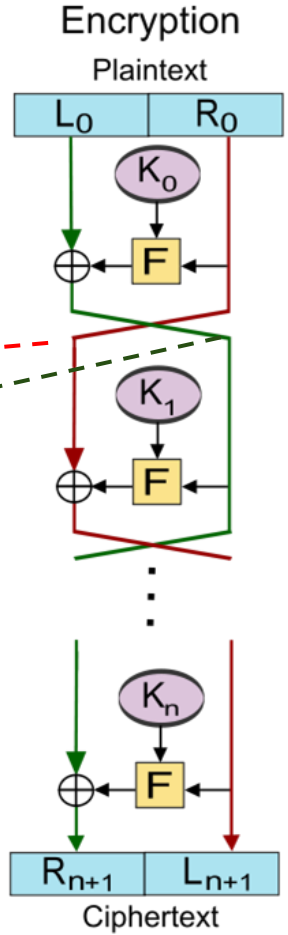


Cifra de Feistel

K -> subchaves para as rodadas 0 até n

L e R -> blocos do texto de mesmo tamanho

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i).$$

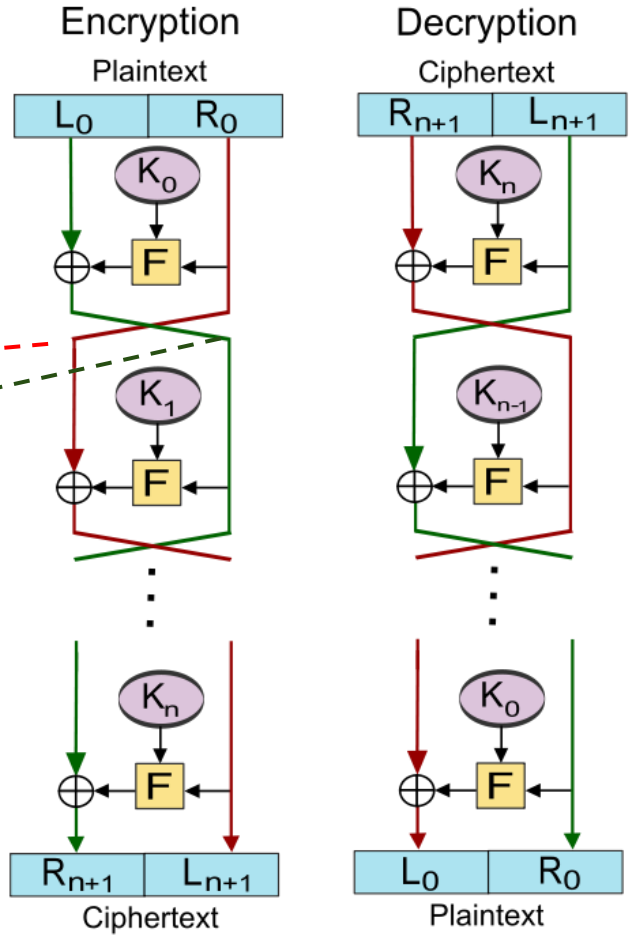


Cifra de Feistel

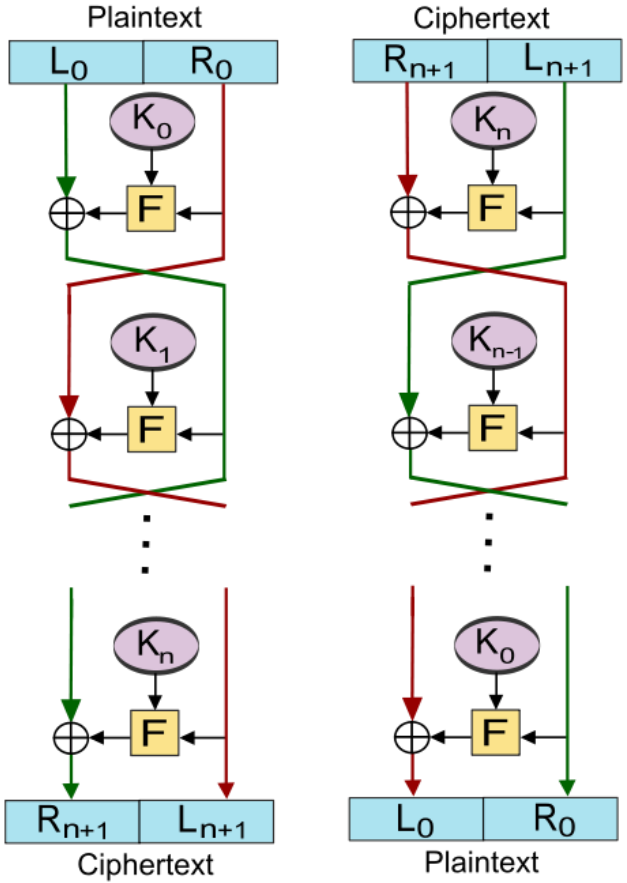
K -> subchaves para as rodadas 0 até n

L e R -> blocos do texto de mesmo tamanho

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i).$$

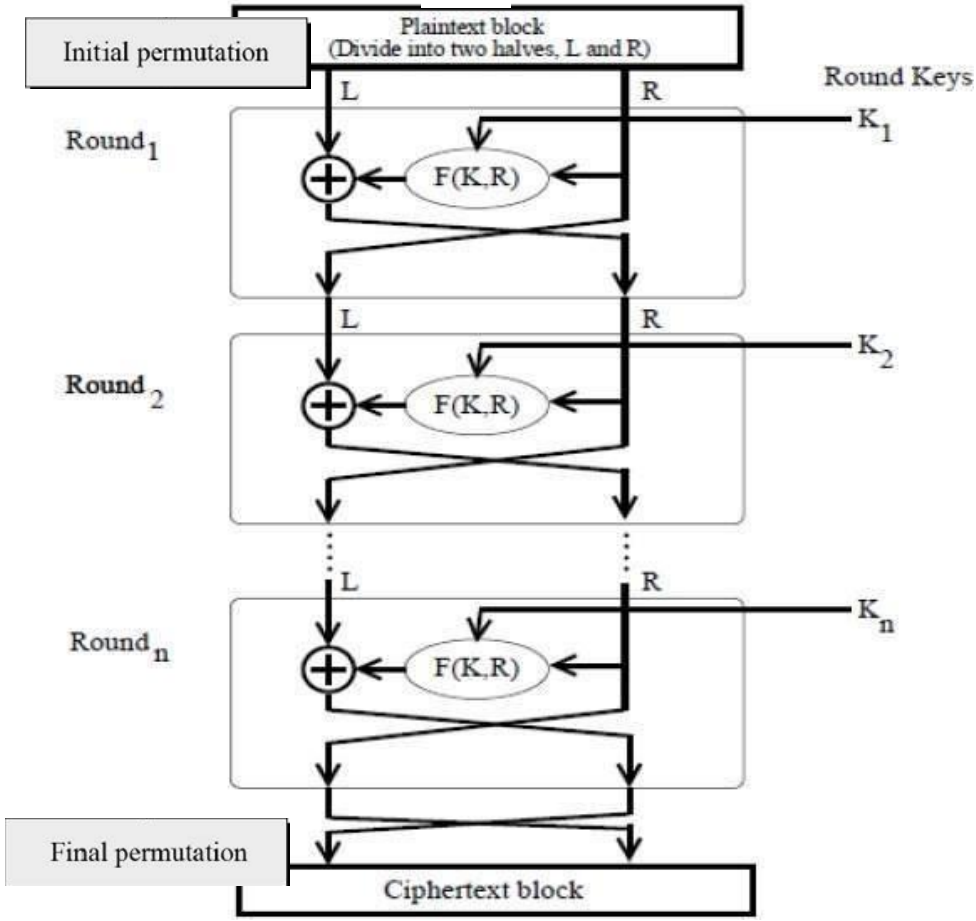


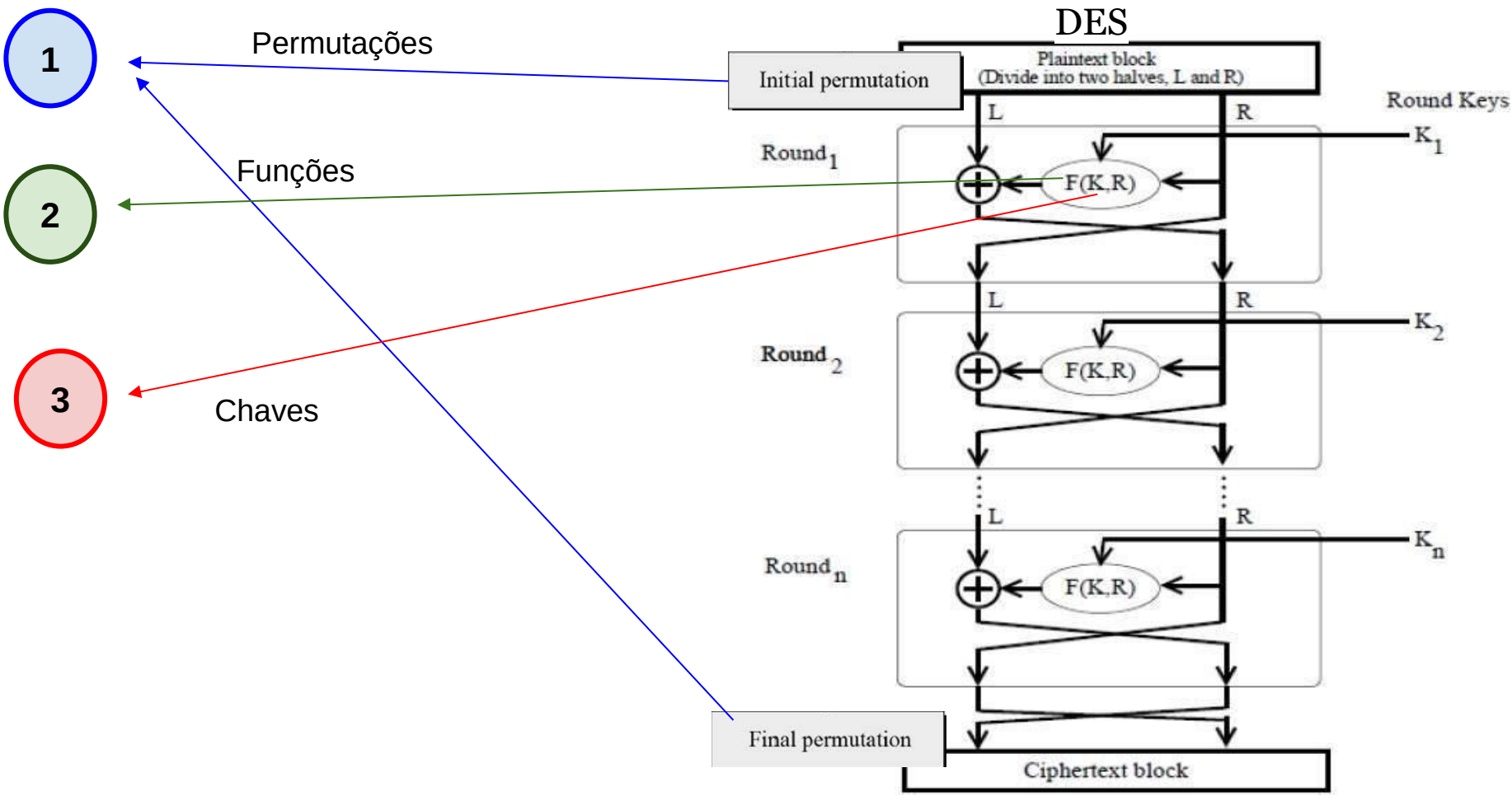
Cifra de Feistel



X

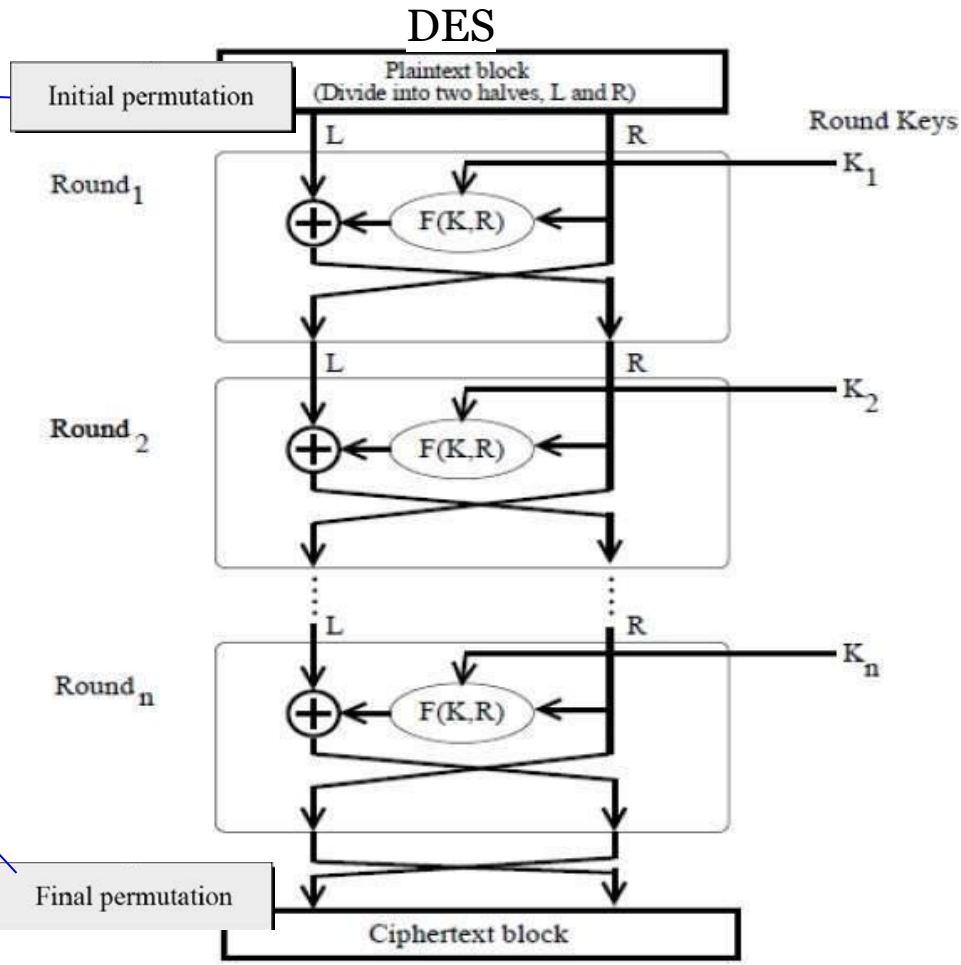
DES




1
Permutações
2
Funções
3
Chaves
DES
Initial permutation
Plaintext block
(Divide into two halves, L and R)
Round Keys
L
R
Round 1
F(K,R)
K1
Round 2
K2
Round n
Kn
Final permutation
Ciphertext block

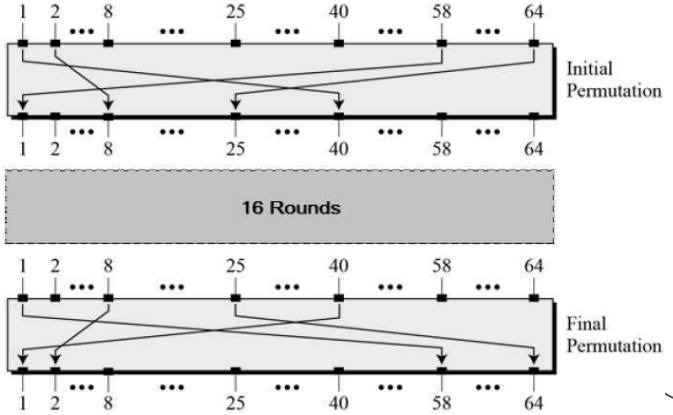
1

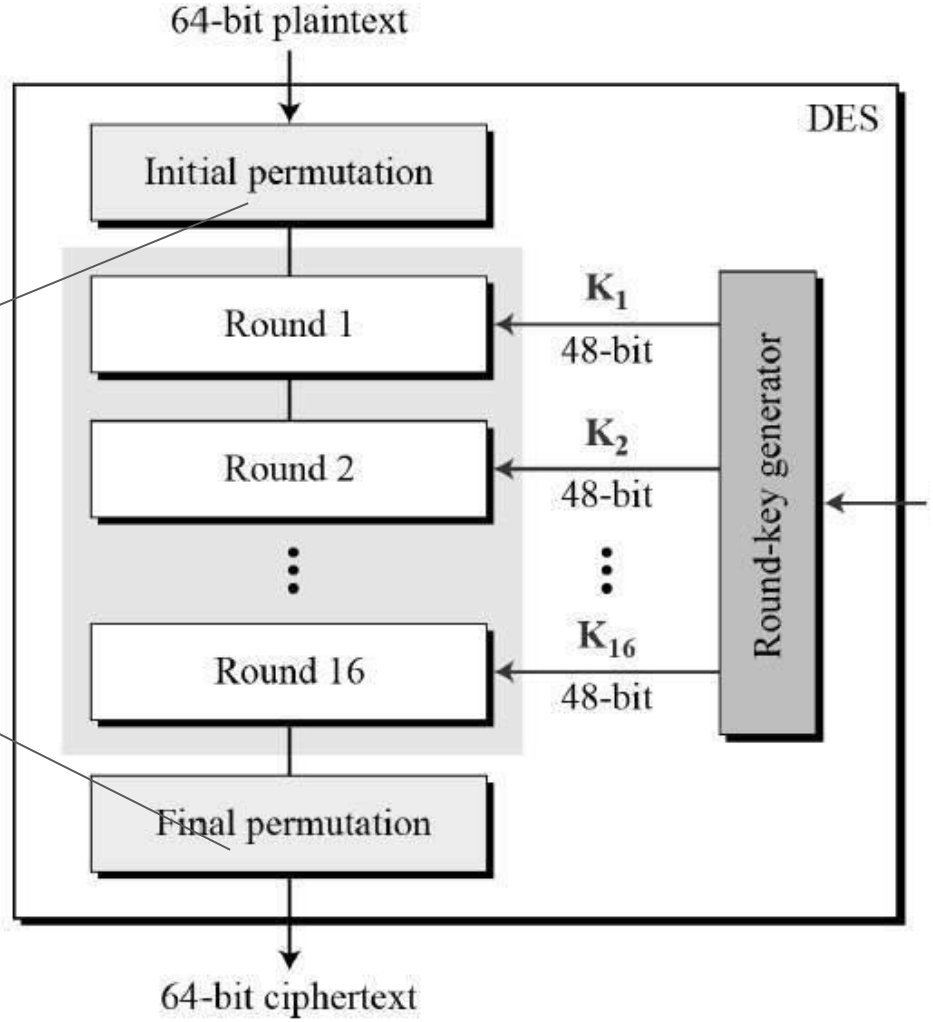
Permutações



1 PERMUTAÇÕES

apenas trocam os bits
de posição.

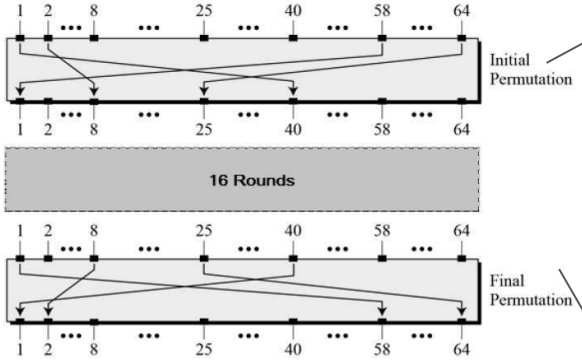


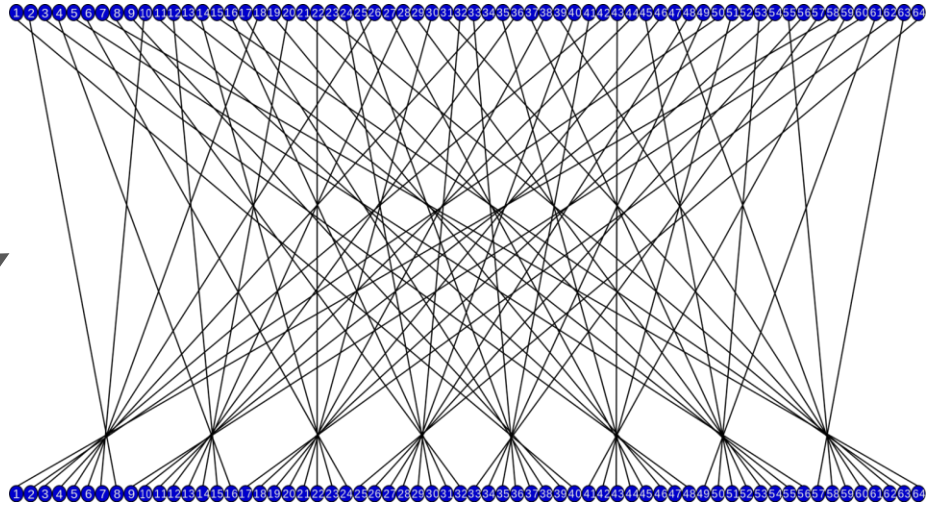


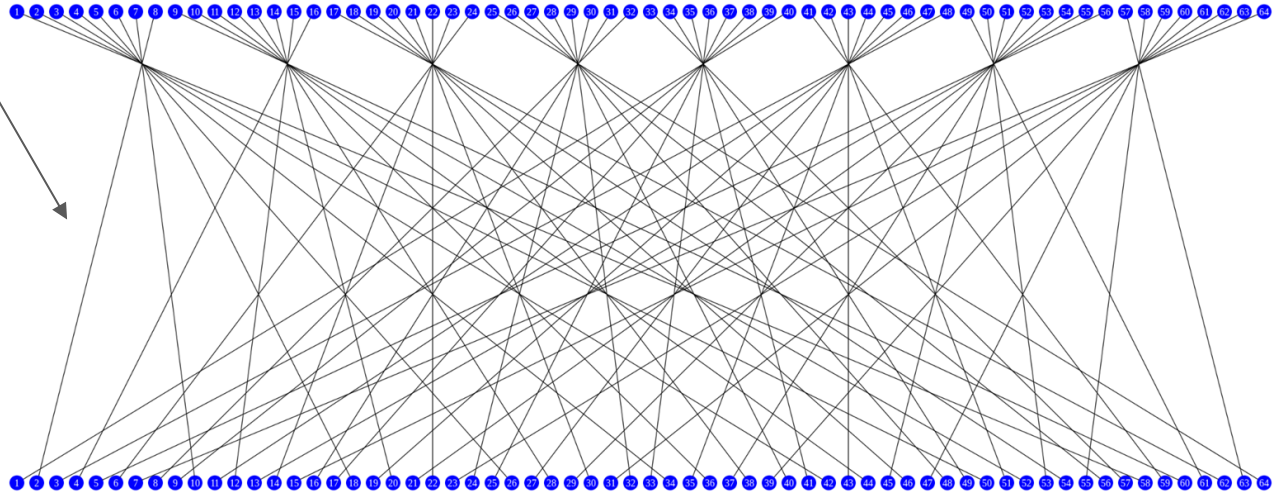
1

PERMUTAÇÕES

apenas trocam os bits
de posição.

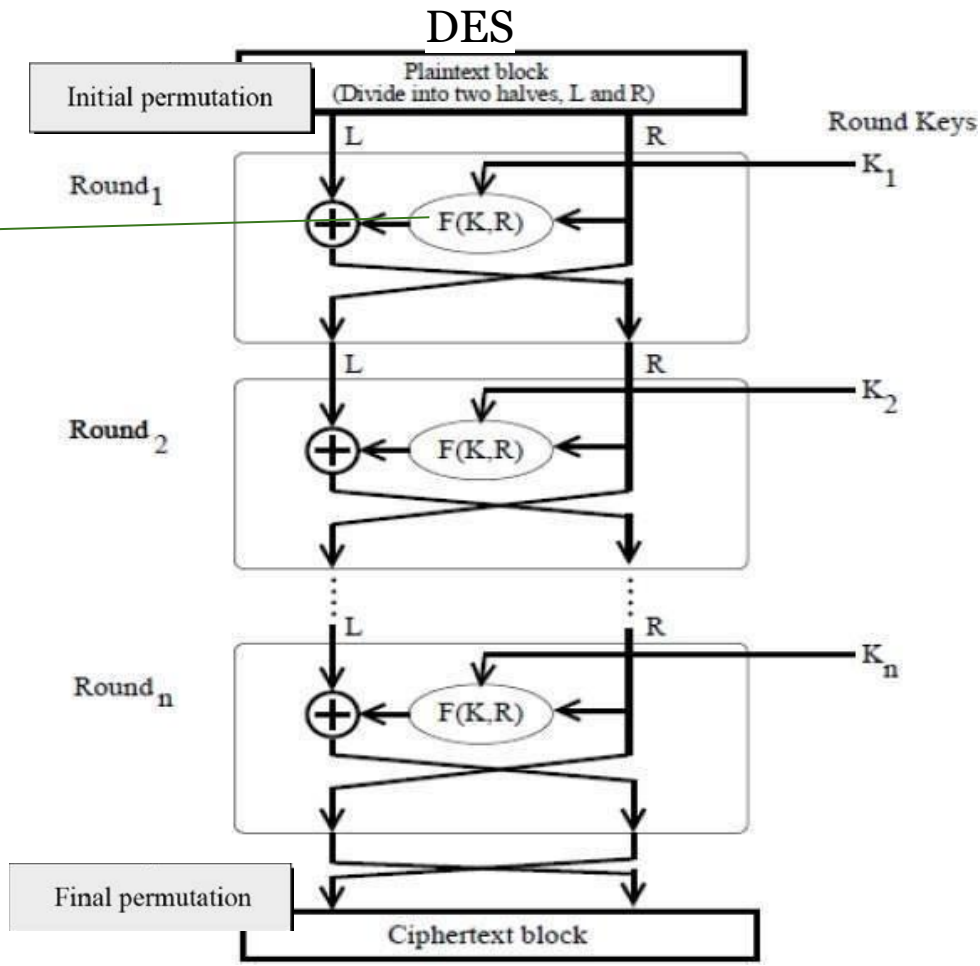






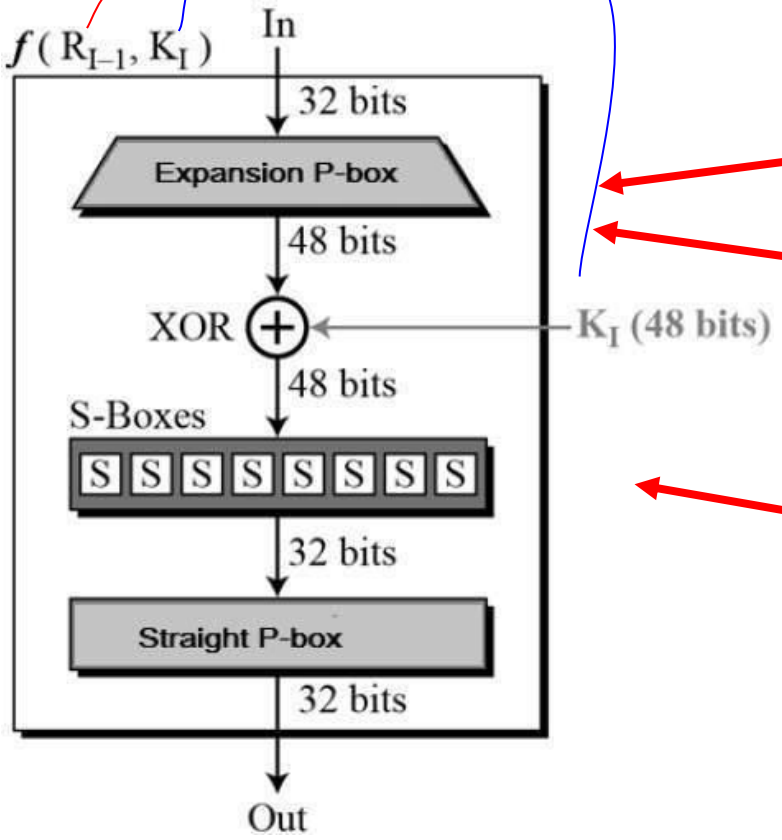
2

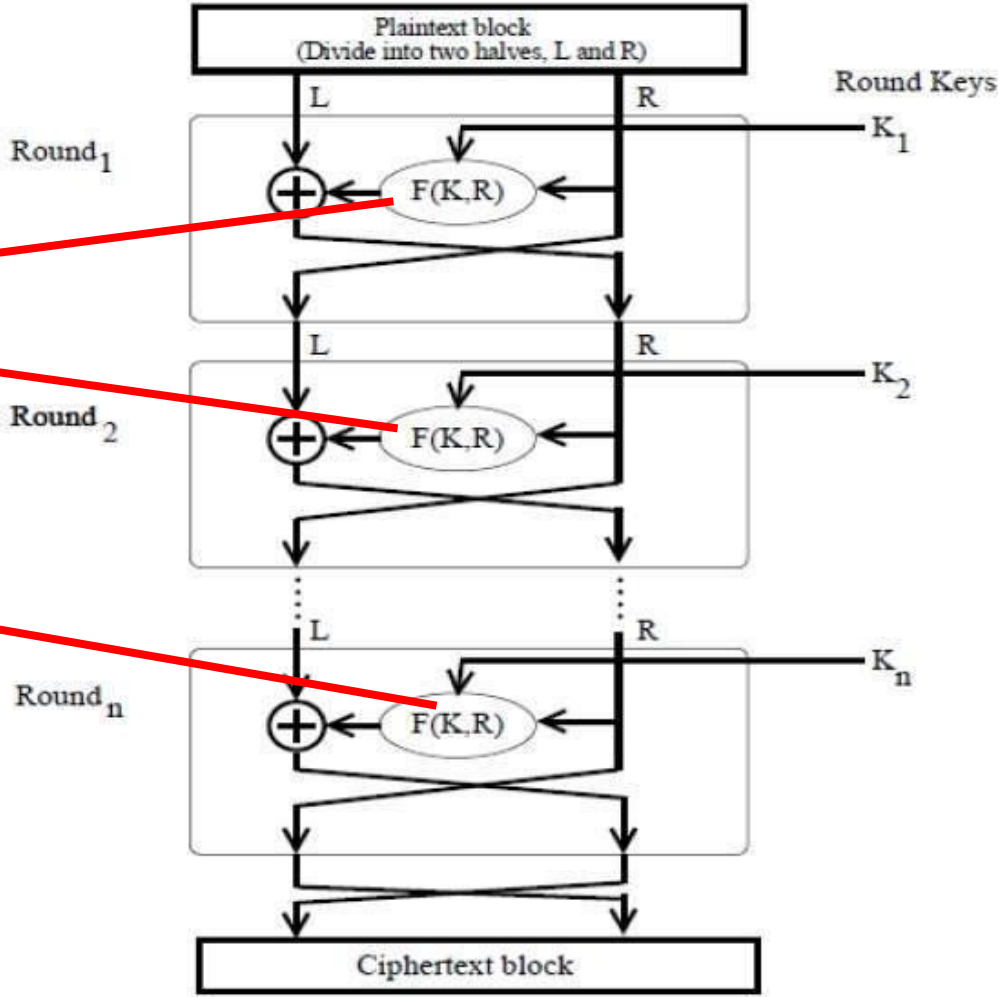
Funções


DES
Initial permutation
Plaintext block
(Divide into two halves, L and R)
Round Keys
L
R
Round 1
K1
F(K,R)
L
R
Round 2
K2
F(K,R)
L
R
Round n
Kn
F(K,R)
Final permutation
Ciphertext block

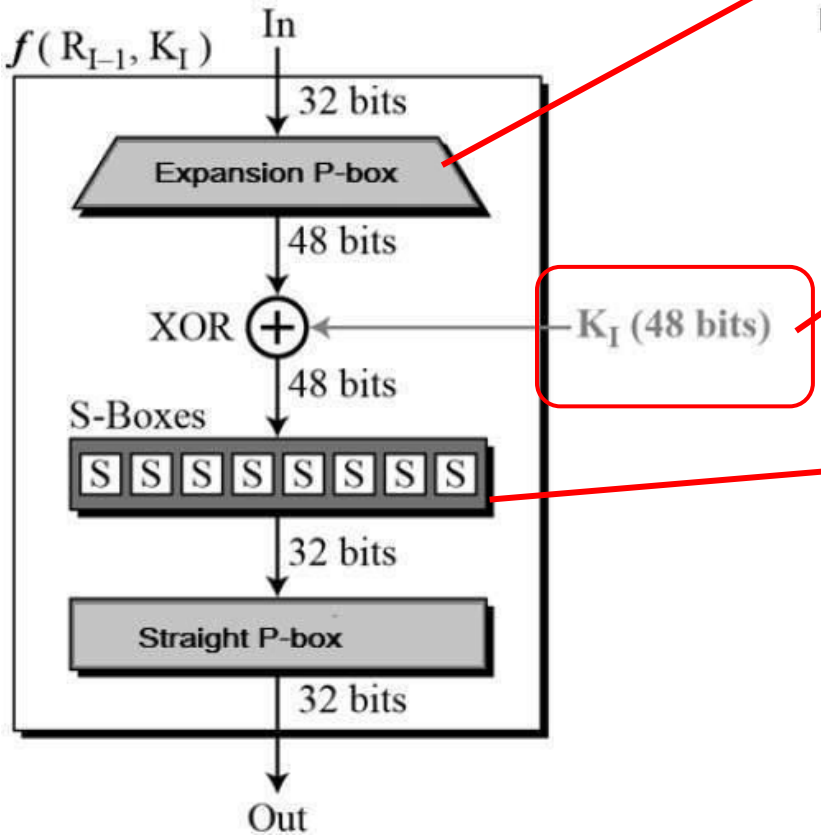
2

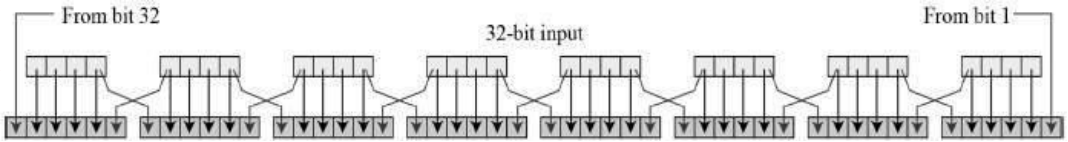
FUNÇÃO CRIPTOGRÁFICA



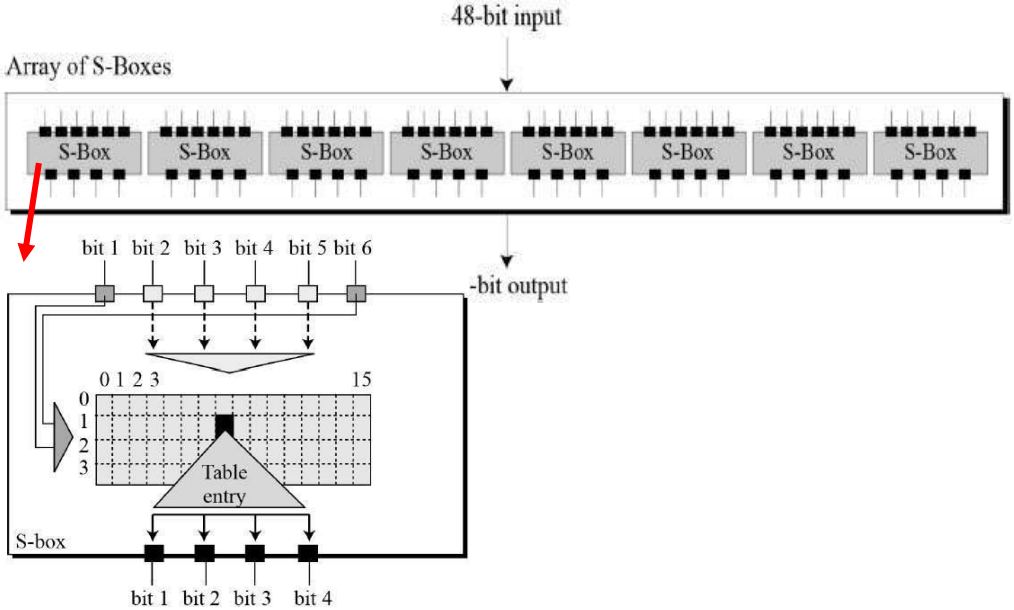


2 FUNÇÃO CRIPTOGRÁFICA



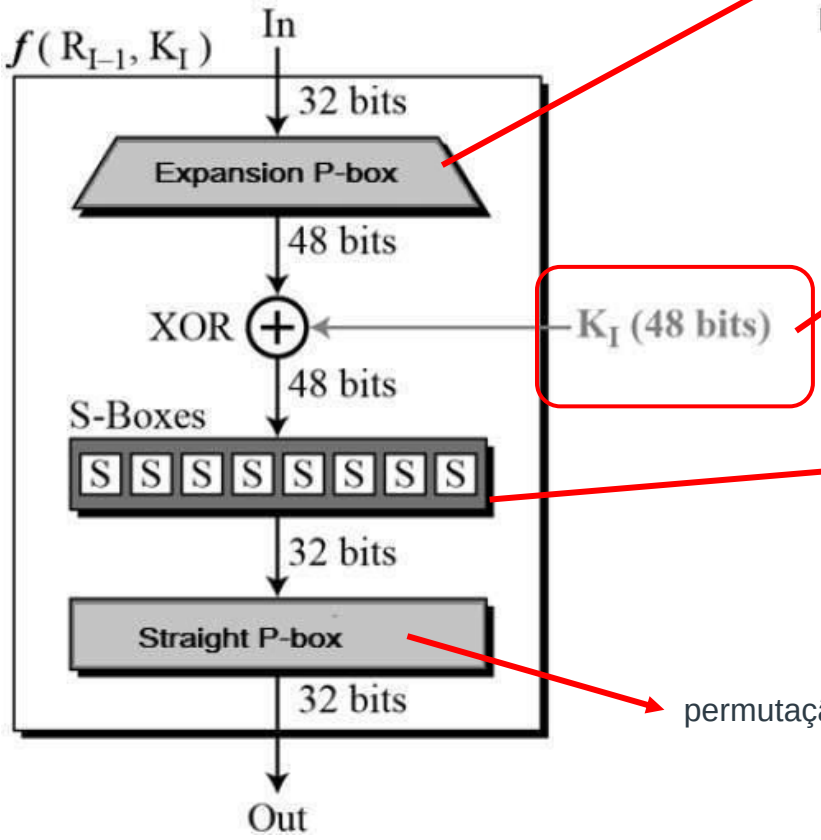


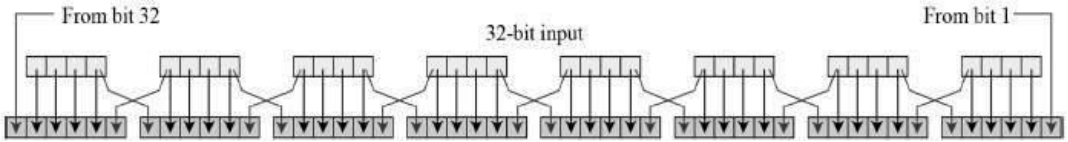
chave da rodada



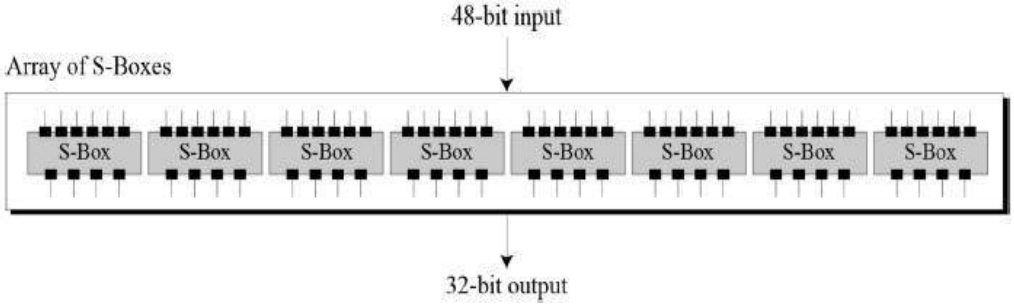
2

FUNÇÃO CRIPTOGRÁFICA





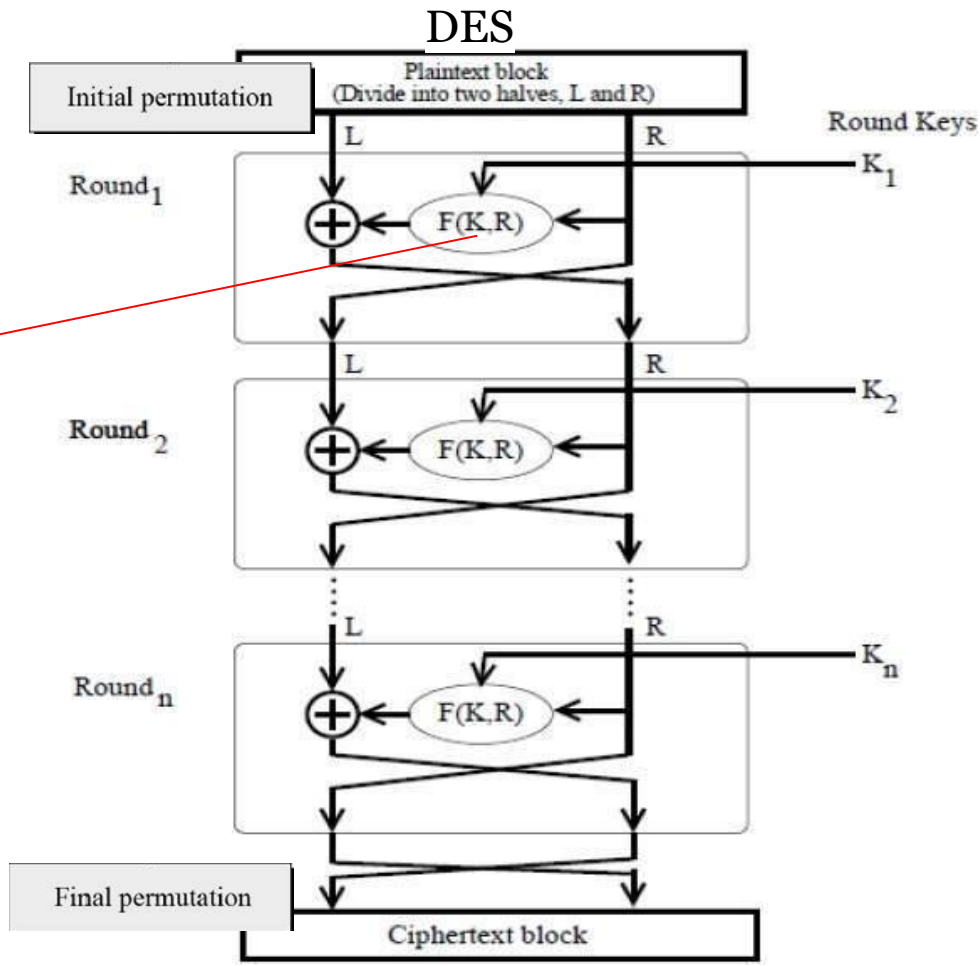
chave da rodada



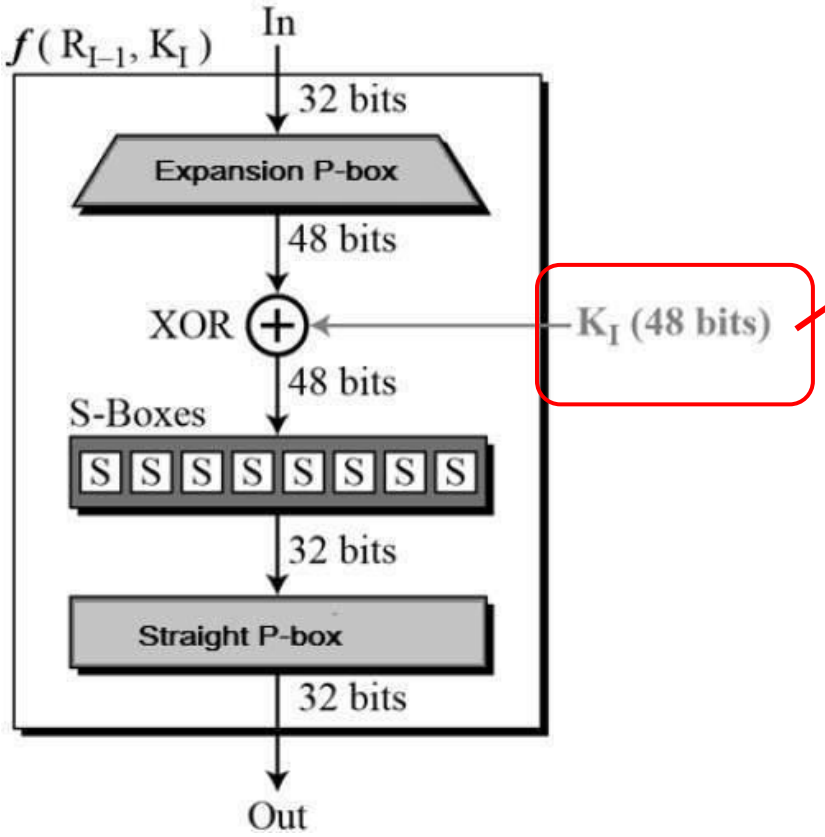
permutação

3

Chaves

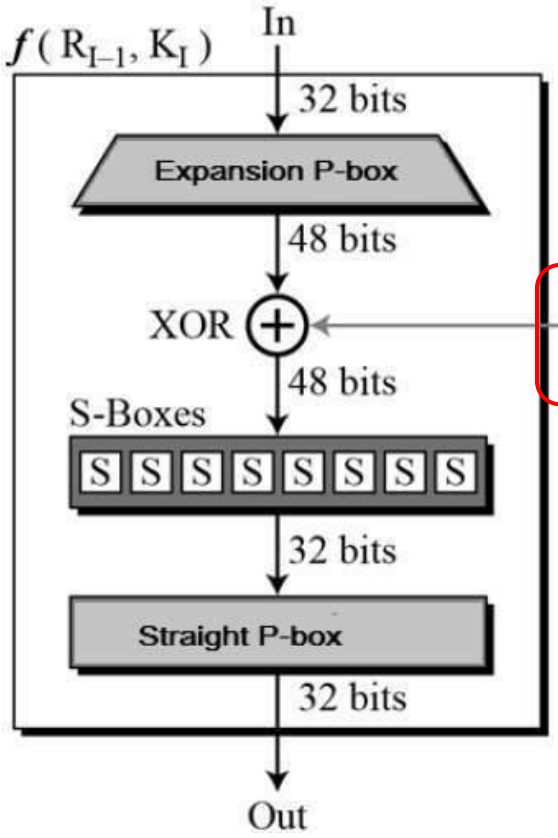

DES
Plaintext block
(Divide into two halves, L and R)
Initial permutation
Round Keys
L
R
Round 1
K1
F(K,R)
L
R
Round 2
K2
F(K,R)
L
R
Round n
Kn
F(K,R)
Final permutation
Ciphertext block

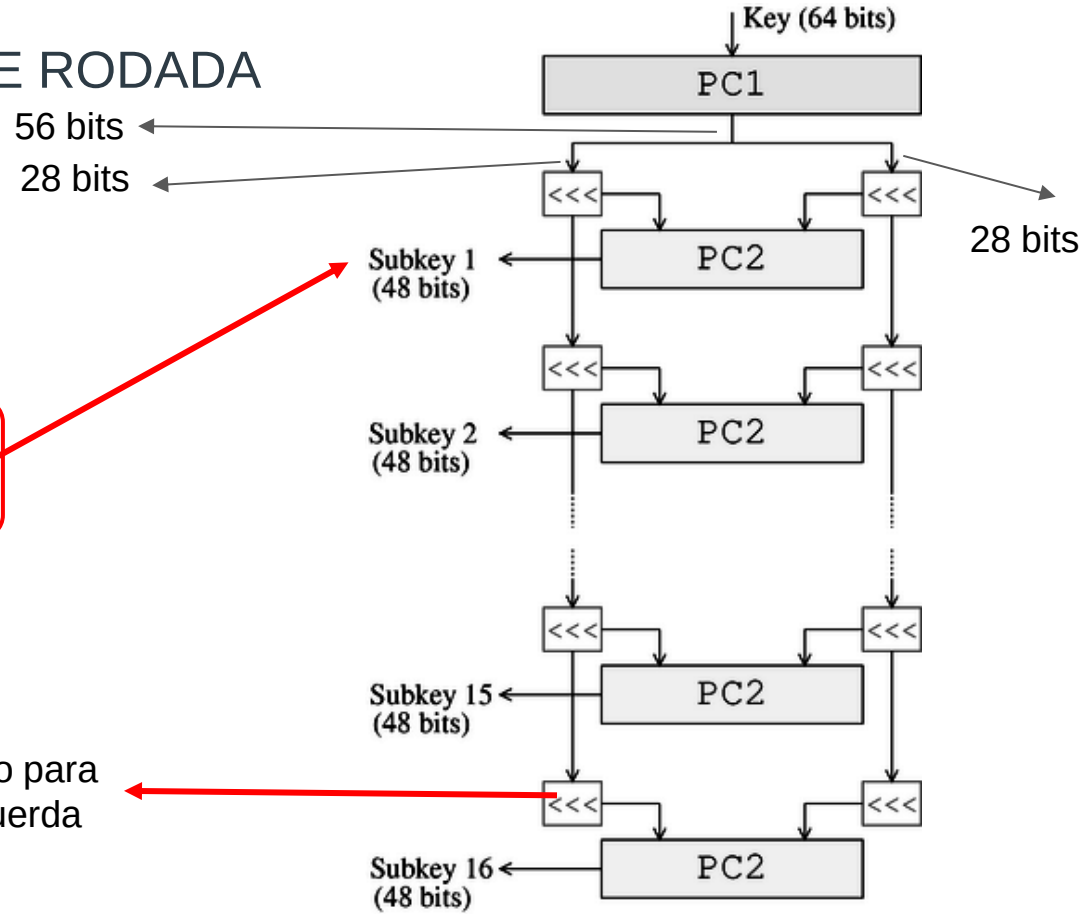
3 GERAÇÃO DAS CHAVES DE RODADA



chave da rodada

3 GERAÇÃO DAS CHAVES DE RODADA





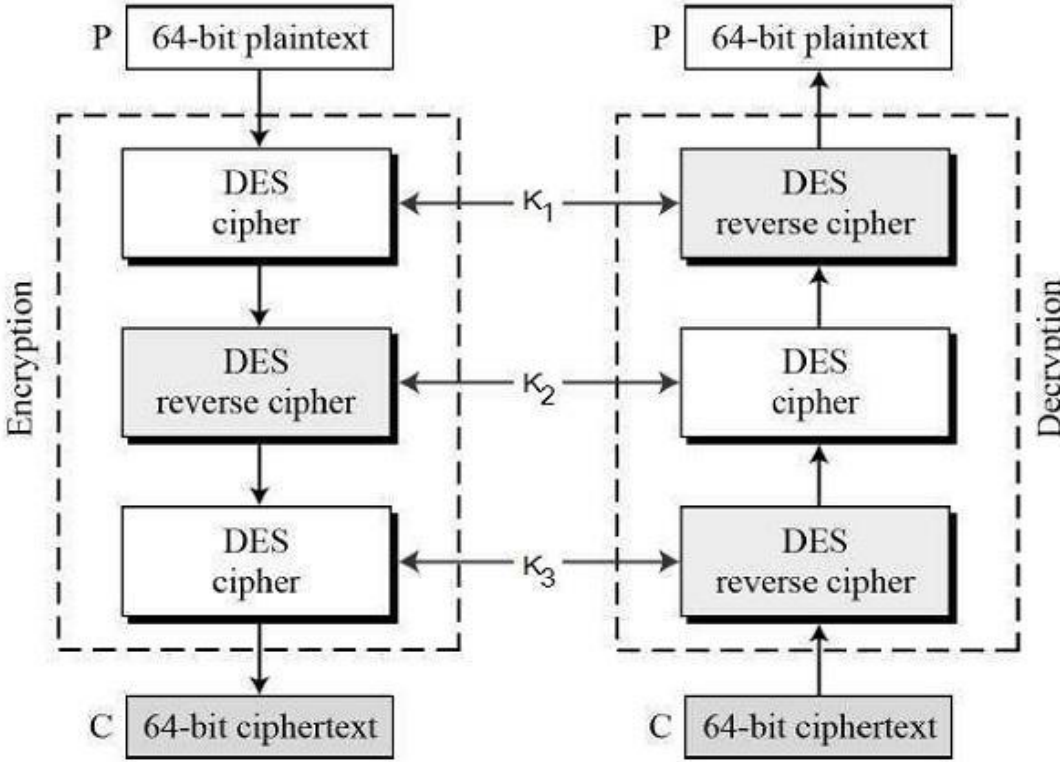
TDES

PUC Minas

TDES

No TDES, ao invés de usarmos uma chave de 64 bits (dos quais apenas 56 são necessários) como no DES, **usamos três chaves de 64 bits**, combinadas em uma longa sequência de 192 bits.

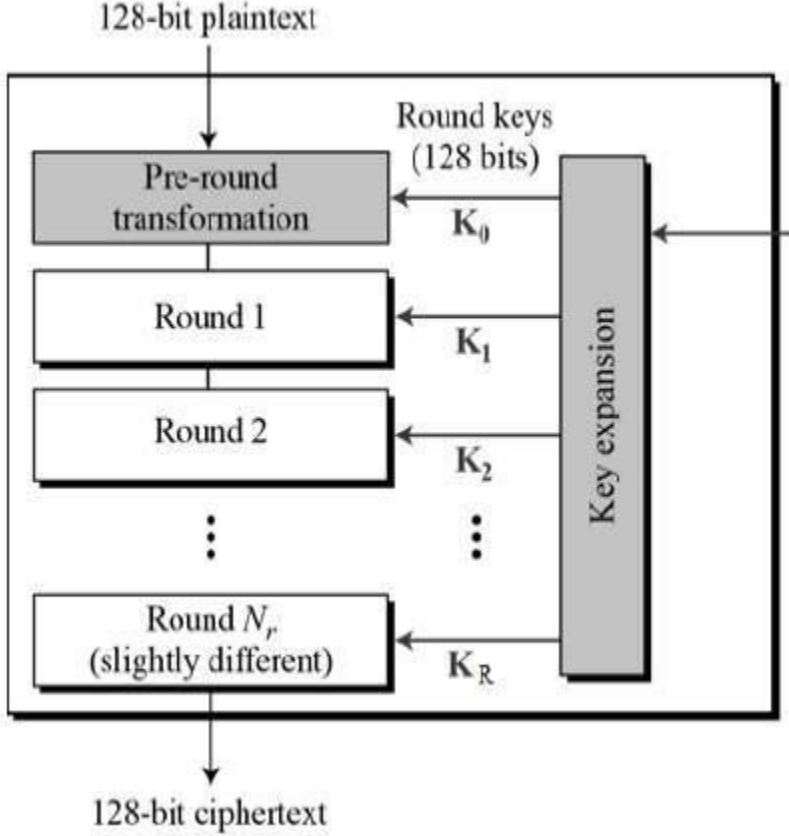
Assim, efetivamente, o sistema usa uma chave de 192 bits dos quais 1 a cada 8 bits é apenas de paridade e os outros 168 bits são usados na cifragem.



AES

PUC Minas

Advanced Encryption Standard (AES)



Cipher key
(128, 192, or 256 bits)

R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Roteiro

- Introdução
  - Cifra de César
  - Cifra de substituição
  - Cifra de Vigenére
  - Cifras de transposição
  - Cifras das colunas
- Criptografia Simétrica
  - Cifras de Fluxo - One Time Pad
  - Cifras de Bloco
    - DES
    - 3DES ou TDES
    - AES
- **Criptografia assimétrica**
  - **RSA**
  - **Assinatura Digital**
  - **Certificado Digital**

Criptografia assimétrica
ou
Criptografia de Chave Pública

PUC Minas

Criptografia assimétrica

- Chaves diferentes são usadas na cifragem e na decifragem.
- Uma dessas chaves é tornada pública e a outra é mantida secreta (privada).
  - $C = E(K_{pub}, M)$
  - $M = D(K_{priv}, C)$

- Em alguns algoritmos, as chaves são intercambiáveis.
  - $C = E(K_{priv}, M)$
  - $M = D(K_{pub}, C)$

Criptografia assimétrica

$C = E(K_{pub}, M)$ $M = D(K_{priv}, C)$

Cada um tem o seu par de chaves

$M = D(K_{priv}, C)$ $C = E(K_{pub}, M)$

Algoritmo RSA

PUC Minas

Algoritmo RSA

Rivest – Shamir – Adelman

- Escolha dois números primos extensos, p e q (maiores de 10100)
- Calcule $n = p * q$ e $z = (p - 1) * (q - 1)$
- Escolha um número relativamente primo a z e chame-o de d
- Escolha e de forma que $(e * d)\ mod\ z = 1$
- Para cifrar, calcule $C = P^e\ mod\ n$
- Para decifrar, calcule $P = C^d\ mod\ n$
- A chave pública será composta por e e n
- A chave privada será composta por d e n`

Algoritmo RSA

Rivest – Shamir – Adelman

$p = 3$
$q = 11$
$n = p \cdot q = 33$
$z = (p - 1)(q - 1) = 20$
$d = 7$, primo em relação a z
$e = 3$, pois $(e \cdot d) mod\ z = 1$

Cifragem

Texto
A
T
A
Q
U
E

Algoritmo RSA

Rivest – Shamir – Adelman

- Escolha dois números primos extensos, p e q (maiores de 10100)
- Calcule $n = p * q$ e $z = (p - 1) * (q - 1)$
- Escolha um número relativamente primo a z e chame-o de d
- Escolha e de forma que $(e * d)\ mod\ z = 1$
- Para cifrar, calcule $C = P^e\ mod\ n$
- Para decifrar, calcule $P = C^d\ mod\ n$
- A chave pública será composta por e e n
- A chave privada será composta por d e n`

$p = 3$
$q = 11$
$n = p \cdot q = 33$
$z = (p - 1)(q - 1) = 20$
$d = 7$, primo em relação a z
$e = 3$, pois $(e \cdot d) mod\ z = 1$

Cifragem

Texto	P	P^3	$C = P^3 mod(33)$
A	1	1	1
T	20	8.000	14
A	1	1	1
Q	17	4.913	29
U	21	9.261	21
E	5	125	26

Decifragem

C	C^7	$P = C^7 mod(33)$	Texto
1	1	1	A
14	105.413.504	20	T
1	1	1	A
29	17.249.876.309	17	Q
21	1.801.088.541	21	U
26	8.031.810.176	5	E

RSA

https://desenv.netproject.com.br/svn_sys/hayala.curto//tmp/rsa.html

Assinaturas Digitais

PUC Minas

Assinatura Digital

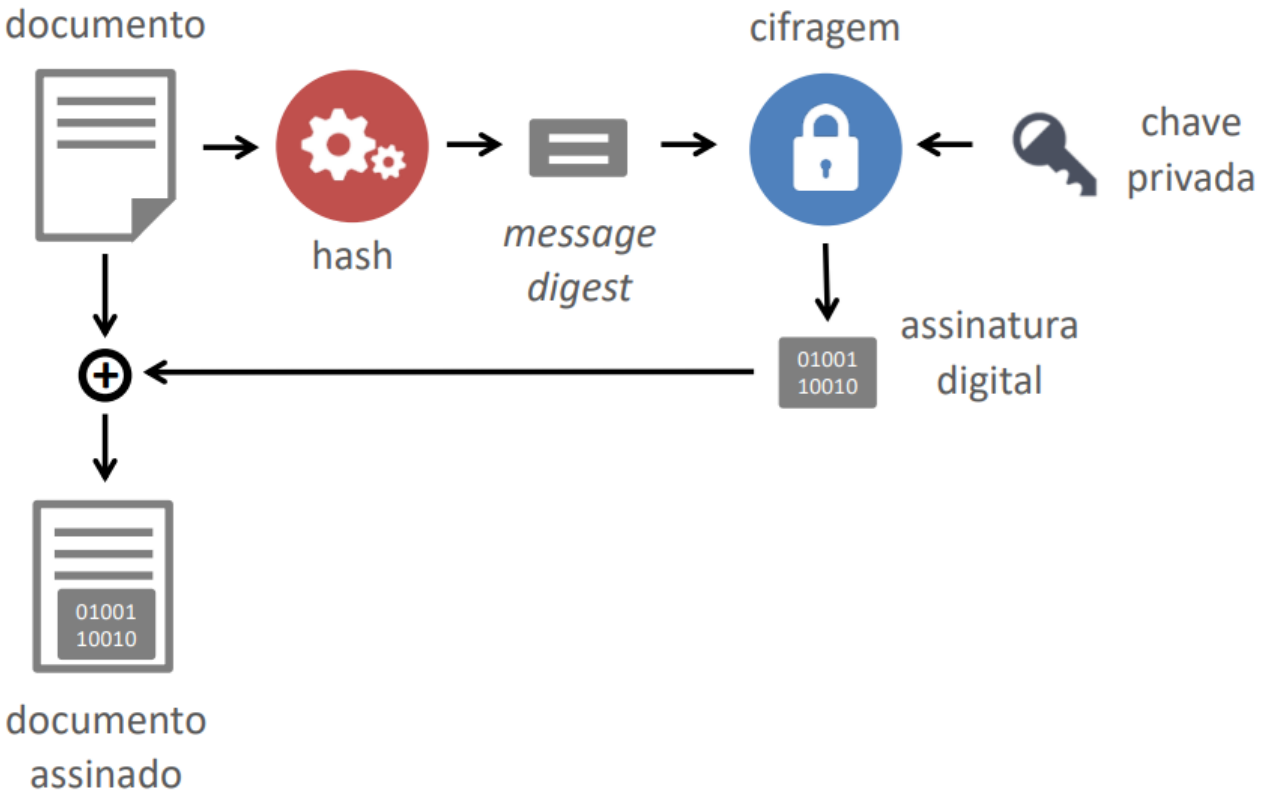
Uma assinatura é uma autorização de transação.

- Se necessário, uma entidade pode autenticar a assinatura.
- O documento (transação) não pode ser alterado
- A assinatura é parte do documento e não pode ser separada dele.

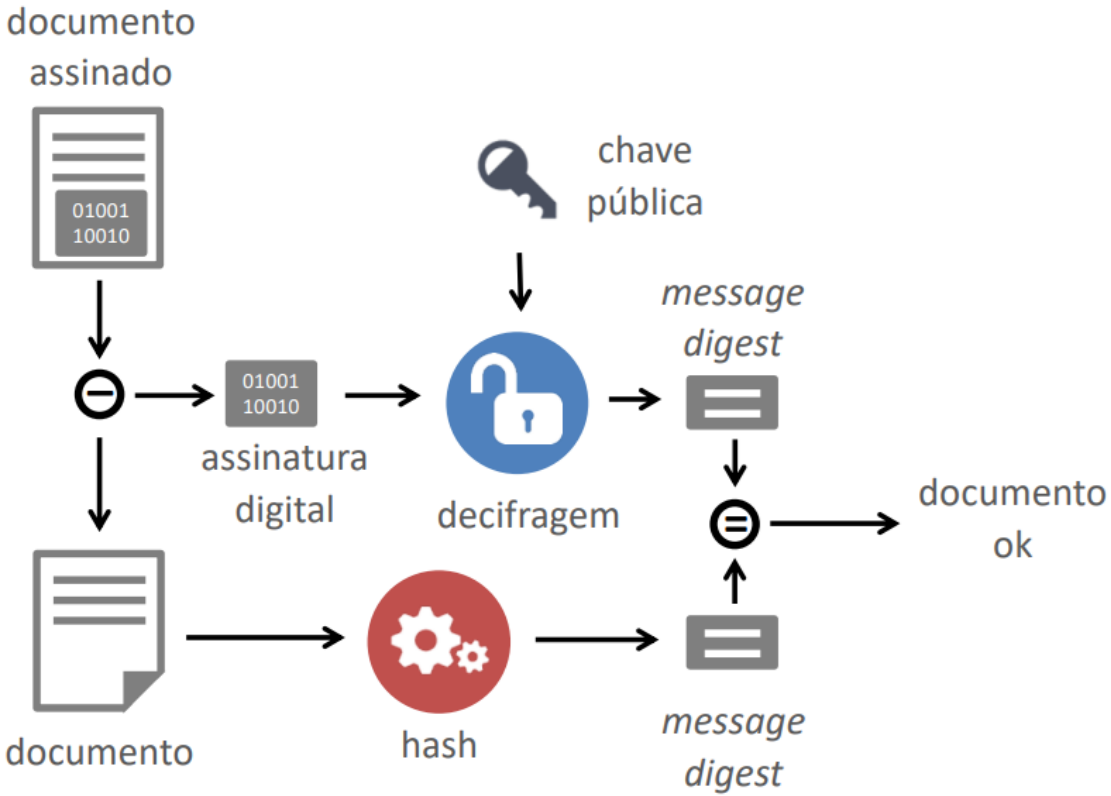
Assinatura Digital

- Uma assinatura digital é:
  - Não fraudável: é impossível alguém produzir a assinatura de outro.
  - Autenticável: é possível verificar se a pessoa assinou o documento.
  - Não repudiável: não é possível negar ter produzido a assinatura.
  - Inviolável: após geração, o documento não pode ser alterado.
  - Não reusável: a assinatura não pode ser usada em outro documento.

Assinatura


documento
hash
message digest
cifragem
chave privada
01001 10010
assinatura digital
01001 10010
documento assinado

Autenticação



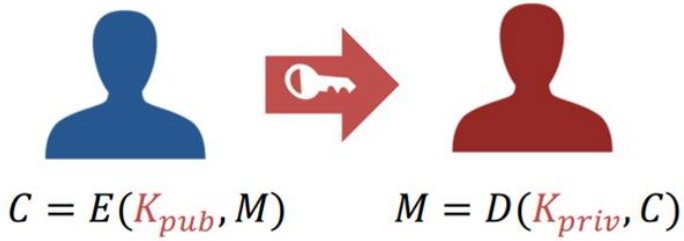
Certificado Digital

PUC Minas

Certificado Digital

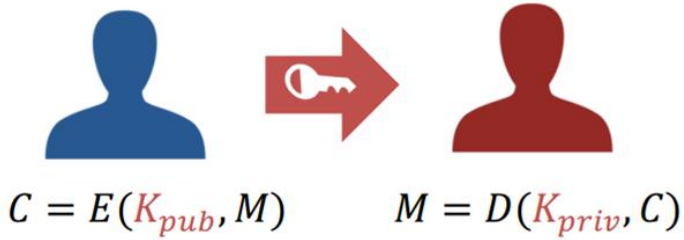
Um certificado digital é um documento eletrônico usado para provar a propriedade de uma chave pública.

O certificado contém informações sobre essa chave, o seu proprietário e sobre a entidade que emitiu o próprio certificado.



Certificado Digital

Esse documento pode ser usado de diversas formas, mas ele também precisa ser instalado no site da empresa, para que possa ser acessado pelos usuários que **navegam por esse site** (usando o protocolo HTTPS).



Certificado Digital

Alguns exemplos de entidades certificadoras são:

- Caixa Econômica Federal
- Receita Federal
- Prodemge.

Existem vários tipos de certificados digitais: para pessoas físicas, para pessoas jurídicas, em cartões, só como software, por 1 ano, por 3 anos, e assim em diante. Cada um tem um preço diferente.

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Solicita conexão via SSL/TSL

Cliente

Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}

Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}

$E(K_{pub} , K_{sessão})$

Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}

$E(K_{pub} , K_{sessão})$

$E(K_{sessão} , "ok")$

Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}

$E(K_{pub} , K_{sessão})$

$E(K_{sessão} , "ok")$

$E(K_{sessão} , mensagens)$

Servidor