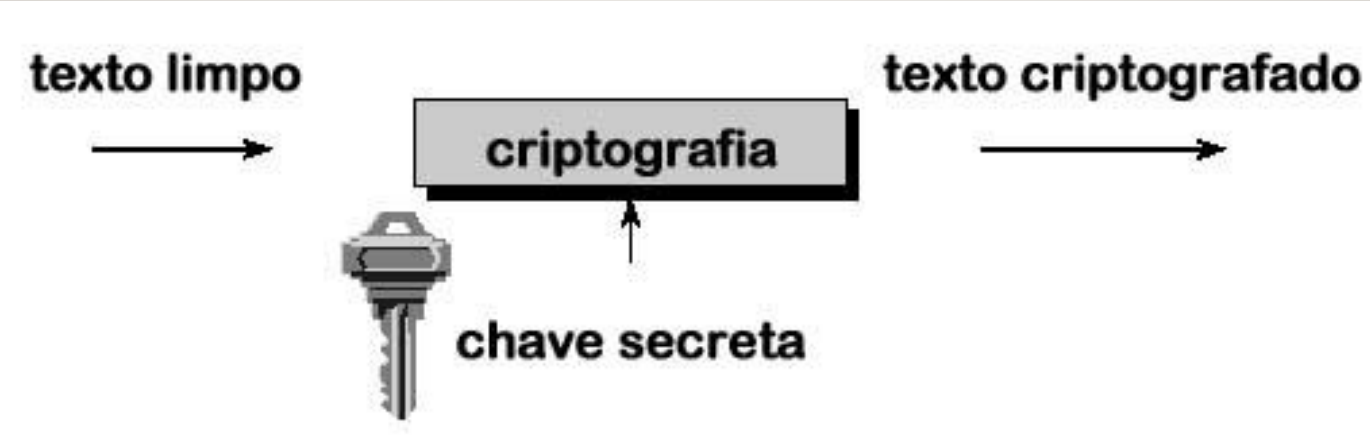
ALGORITMO DE CRIPTOGRAFIA DES

- **Princípios da criptografia;**
- **Componentes criptográficos;**
- **Criptografia de chaves privadas ou simétricas (algoritmo DES);**
- **Outros algoritmos.**

CRIPTOGRAFIA - ALGORITMOS

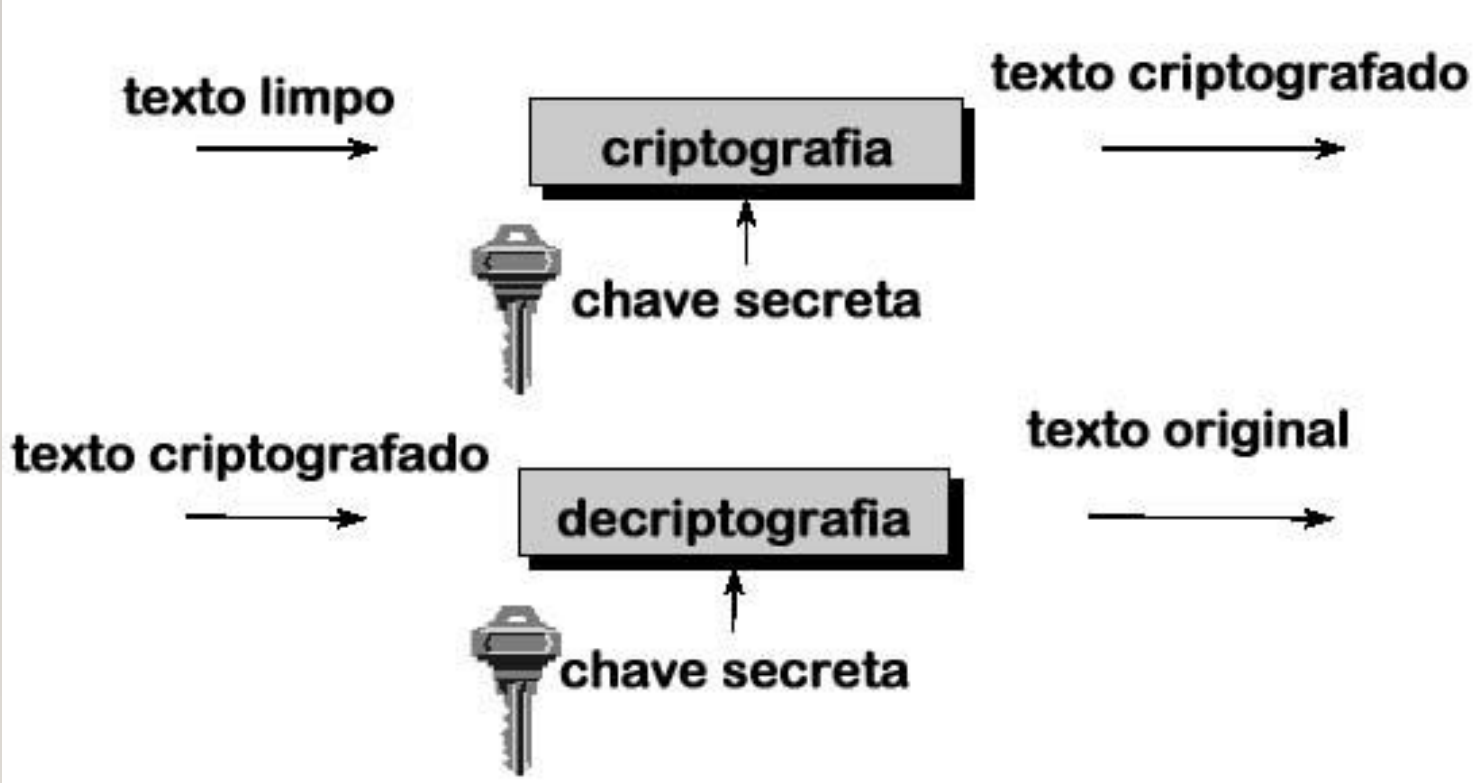
- Criptografia
  - O algoritmo de criptografia recebe uma chave secreta e o texto limpo produzindo o texto criptografado.



CRIPTOGRAFIA - ALGORITMOS

- Decriptografia
  - O algoritmo de criptografia recebe uma chave secreta (igual ou não a primeira) e o texto criptografado, produzindo o texto original.

CRIPTOGRAFIA - ALGORITMOS



CRIPTOGRAFIA SIMÉTRICA

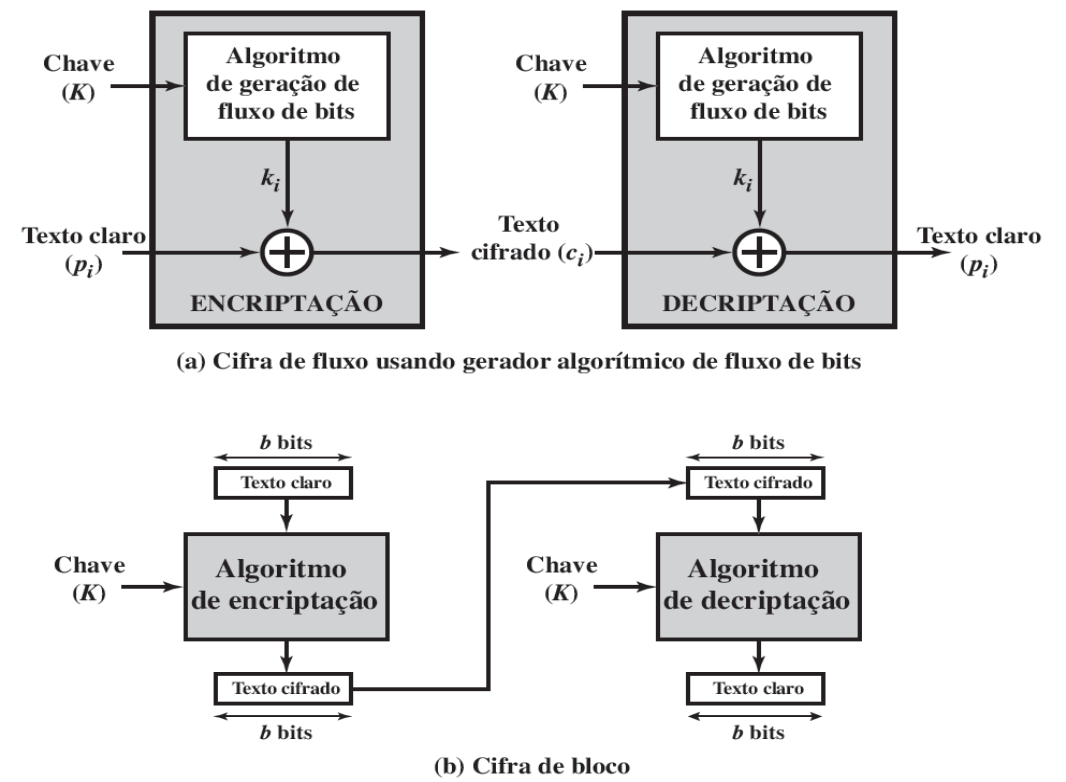
- Algoritmos de chaves simétricas utilizam somente uma chave secreta;
- Chaves simétricas possuem comprimento em geral de 56 à 256 bits;
- A chave secreta é escolhida aleatoriamente;
- Quanto maior for a aleatoriedade da chave maior será a sua segurança.

CRIPTOGRAFIA SIMÉTRICA

- Desvantagens da criptografia simétrica:
  - Todos os pontos em comunicação precisam conhecer a chave secreta;
  - Surge o problema do gerenciamento e distribuição das chaves;
- Exemplos de algoritmos:
  - DES (proteção de arquivos de usuários e senhas), 3DES (sistemas de pagamento eletrônico), AES (sistemas de arquivos criptografados, tais como NTFS, criptografia em HD);
  - RC4 (Rivest Cipher) no WEP;
  - IDEA (International Data Encryption Algorithm) no PGP.

ESTRUTURA TRADICIONAL DE CIFRA DE BLOCO

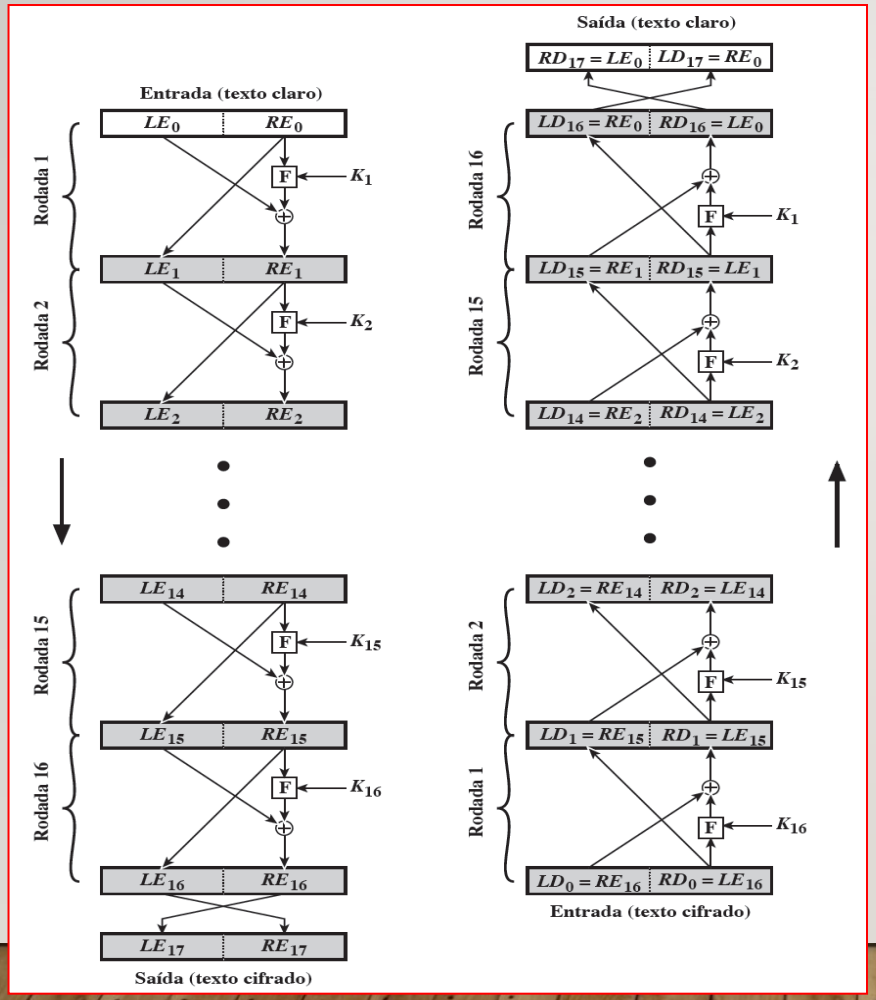
- Uma **cifra de fluxo** é aquela que encripta um fluxo de dados digital um bit ou um byte por vez.
- Uma **cifra de bloco** é aquela em que um bloco de texto claro é tratado como um todo e usado para produzir um de texto cifrado com o mesmo tamanho.



CIFRA DE FEISTEL

- É uma estrutura simétrica usada na construção de cifras de bloco, o nome é uma homenagem ao físico e criptógrafo alemão **Horst Feistel**, que foi o pioneiro na pesquisa enquanto trabalhava na IBM (EUA); esta cifra é comumente conhecida como rede de **Feistel**.
- Em particular, Feistel propôs o uso de uma cifra que alterna substituições e permutações:
  - **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



Encriptação e decriptação de Feistel (16 rodadas):

CIFRA DE FEISTEL

- A execução exata de uma rede de Feistel depende da escolha dos seguintes parâmetros e recursos de projeto:
  - **Tamanho de bloco**: tamanhos de bloco maiores significam maior segurança (mantendo as outras coisas iguais), mas velocidade de encriptação/decriptação reduzida para determinado algoritmo.
  - **Tamanho de chave**: tamanho de chave maior significa maior segurança, mas pode diminuir a velocidade de encriptação/decriptação.
  - **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**: novamente, maior complexidade geralmente significa maior resistência à criptoanálise.

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- História do DES (Data Encryption Standard)
  - Início dos anos 70: O Governo americano abre uma licitação para um padrão de criptografia para uso civil.
  - Em 15 de Maio de 1973, durante o *reinado* de Richard Nixon, o National Bureau of Standards (NBS) solicitou formalmente propostas de algoritmos criptográficos para proteger transmissões e armazenamento de dados.
  - 1977: O NSA (National Security Agency) altera a proposta da IBM (Lucifer), reduzindo o tamanho da chave de 128 bits para 56 bits e torna o algoritmo DES como padrão.

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Especificação para o padrão DES
  - Deve prover alto nível de segurança;
  - Deve ser completamente especificado;
  - Deve ser de fácil compreensão;
  - A segurança do algoritmo deve residir na chave.
  - Deve estar disponível a todos os usuários;
  - Deve ser adaptável a diversas aplicações;
  - Deve ser de uso eficiente;
  - Deve ser economicamente implementável em equipamentos eletrônicos.

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Características do DES:
  - Blocos cifrados de 64 bits;
  - Chave secreta de 56 bits (64 bits com 8 de verificação);
  - Mesma chave para cifrar/decifrar;
  - Facilmente implementável;
    - hardware ou software;
    - transposições e substituições;
  - Altamente não linear;
  - Saída é função muito complexa da entrada e da chave;
  - 56 bits resulta em 7.2x10^16 chaves;
  - Simulador:
    - http://des.online-domain-tools.com

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- 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} ns = 1,125 ano	1 hora
128	AES	$2^{128} \approx 3{,}4 \times 10^{38}$	2^{127} ns = $5{,}3 \times 10^{21}$ anos	$5{,}3 \times 10^{17}$ anos
168	Triple DES	$2^{168} \approx 3{,}7 \times 10^{50}$	2^{167} ns = $5{,}8 \times 10^{33}$ anos	$5{,}8 \times 10^{29}$ anos
192	AES	$2^{192} \approx 6{,}3 \times 10^{57}$	2^{191} ns = $9{,}8 \times 10^{40}$ anos	$9{,}8 \times 10^{36}$ anos
256	AES	$2^{256} \approx 1{,}2 \times 10^{77}$	2^{255} ns = $1{,}8 \times 10^{60}$ anos	$1{,}8 \times 10^{56}$ ano

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Considerações iniciais do DES
  - O DES trabalha com bits ou números binários (0s e 1s). Cada grupo de 4 bits corresponde a um valor hexadecimal, cuja base é 16. O binário "0001" corresponde ao número hexadecimal "1", o binário "1000" é igual ao número hexadecimal "8", "1001" é igual ao hexadecimal "9", "1010" é igual a o hexadecimal "A" e "1111" é igual ao hexadecimal "F".
  - O DES funciona encriptando grupos de 64 bits de mensagem, o que significa 16 números hexadecimais. Para realizar a encriptação, o DES utiliza "chaves" com comprimento aparente de 16 números hexadecimais, ou comprimento aparente de 64 bits. Entretanto, no algoritmo DES, cada oitavo bit da chave é ignorado, de modo que a chave acaba tendo o comprimento de 56 bits. Mas, para todos os efeitos, o DES é organizado baseando-se no número redondo de 64 bits (16 dígitos hexadecimais).

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Considerações iniciais do DES
  - Por exemplo, se tomarmos a mensagem clara hexadecimal 8787878787878787 e a encriptarmos com a chave DES hexadecimal 0E329232EA6D0D73, obteremos o texto cifrado hexadecimal 0000000000000000. Se o criptograma for decifrado com a mesma chave secreta, o resultado será o texto claro original 8787878787878787 hexadecimal.
  - Considere agora a seguinte mensagem: "Criptologia sempre NumaBoa". Esta mensagem clara possui 28 bytes (56 dígitos hexadecimais) de comprimento. Neste caso, para encriptar a mensagem, seu comprimento precisa ser ajustado com a adição de alguns bytes extras no final. Depois de decifrar a mensagem, estes bytes extras são descartados. É lógico que existem vários esquemas diferentes para adicionar bytes. Aqui nós iremos adicionar apenas zeros no final, de modo que a mensagem total seja um múltiplo de 8 bytes (ou 16 dígitos hexadecimais, ou 64 bits).

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Considerações iniciais do DES

Binário	Decimal	Hexa	Glifo
0010 0000	32	20	
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?

Binário	Decimal	Hexa	Glifo
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	[
0101 1100	92	5C	\
0101 1101	93	5D	]
0101 1110	94	5E	^
0101 1111	95	5F	_

Binário	Decimal	Hexa	Glifo
0110 0000	96	60	`
0110 0001	97	61	a
0110 0010	98	62	b
0110 0011	99	63	c
0110 0100	100	64	d
0110 0101	101	65	e
0110 0110	102	66	f
0110 0111	103	67	g
0110 1000	104	68	h
0110 1001	105	69	i
0110 1010	106	6A	j
0110 1011	107	6B	k
0110 1100	108	6C	l
0110 1101	109	6D	m
0110 1110	110	6E	n
0110 1111	111	6F	o
0111 0000	112	70	p
0111 0001	113	71	q
0111 0010	114	72	r
0111 0011	115	73	s
0111 0100	116	74	t
0111 0101	117	75	u
0111 0110	118	76	v
0111 0111	119	77	w
0111 1000	120	78	x
0111 1001	121	79	y
0111 1010	122	7A	z
0111 1011	123	7B	{
0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

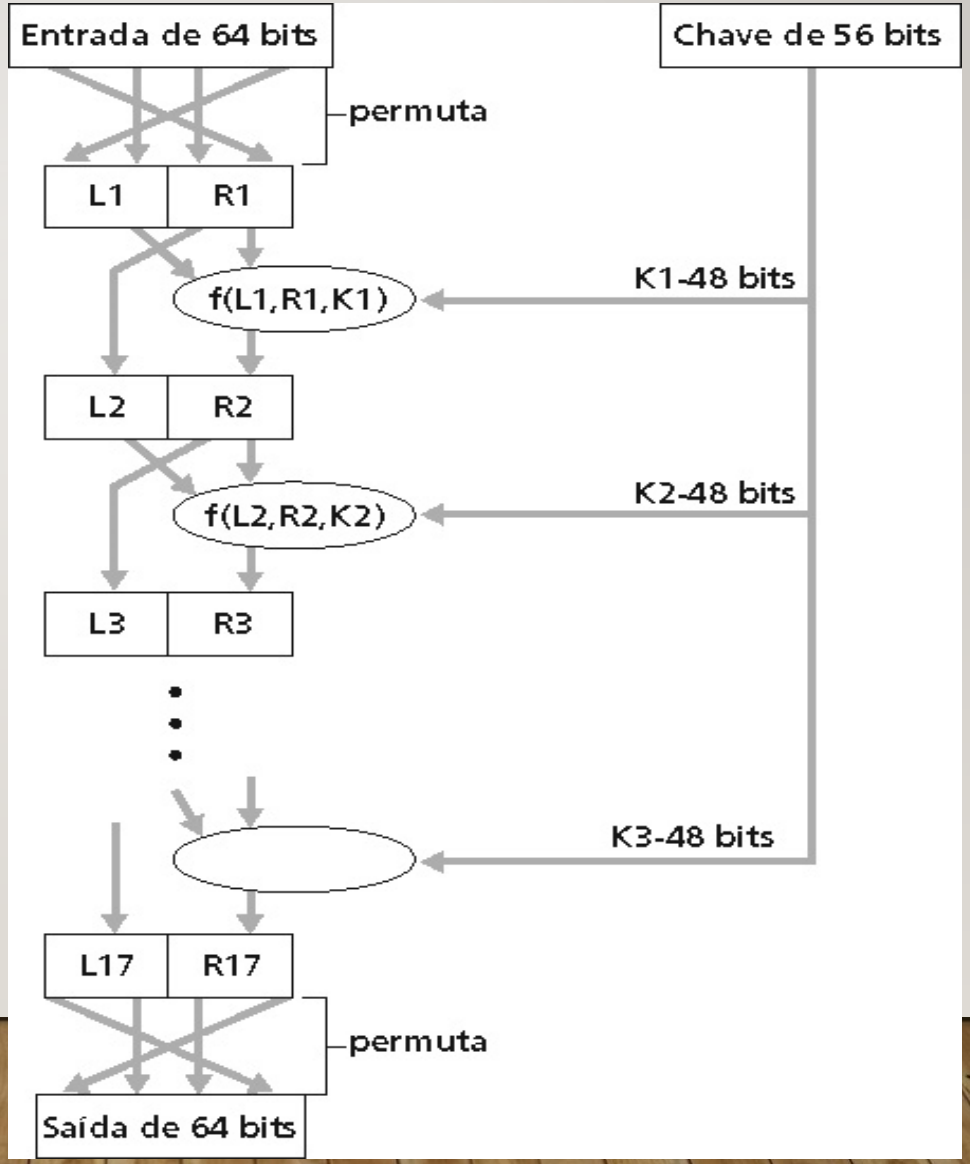
DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Texto claro "Criptologia sempre NumaBoa" é, em hexadecimal.
- Cifrando a mensagem clara em blocos de 64 bits (16 dígitos hexadecimais), usando a chave DES "0E329232EA6D0D73", obtem-se o seguinte texto cifrado:
- ```
  a1 bf 4c 8c 1f 44 6a 4c ca 4d e4 28 6e de 99 50
  f5 59 66 2b b5 09 d9 3c 45 e6 0a b2 5c 67 e5 85
  ```
  ```

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

Operação do DES

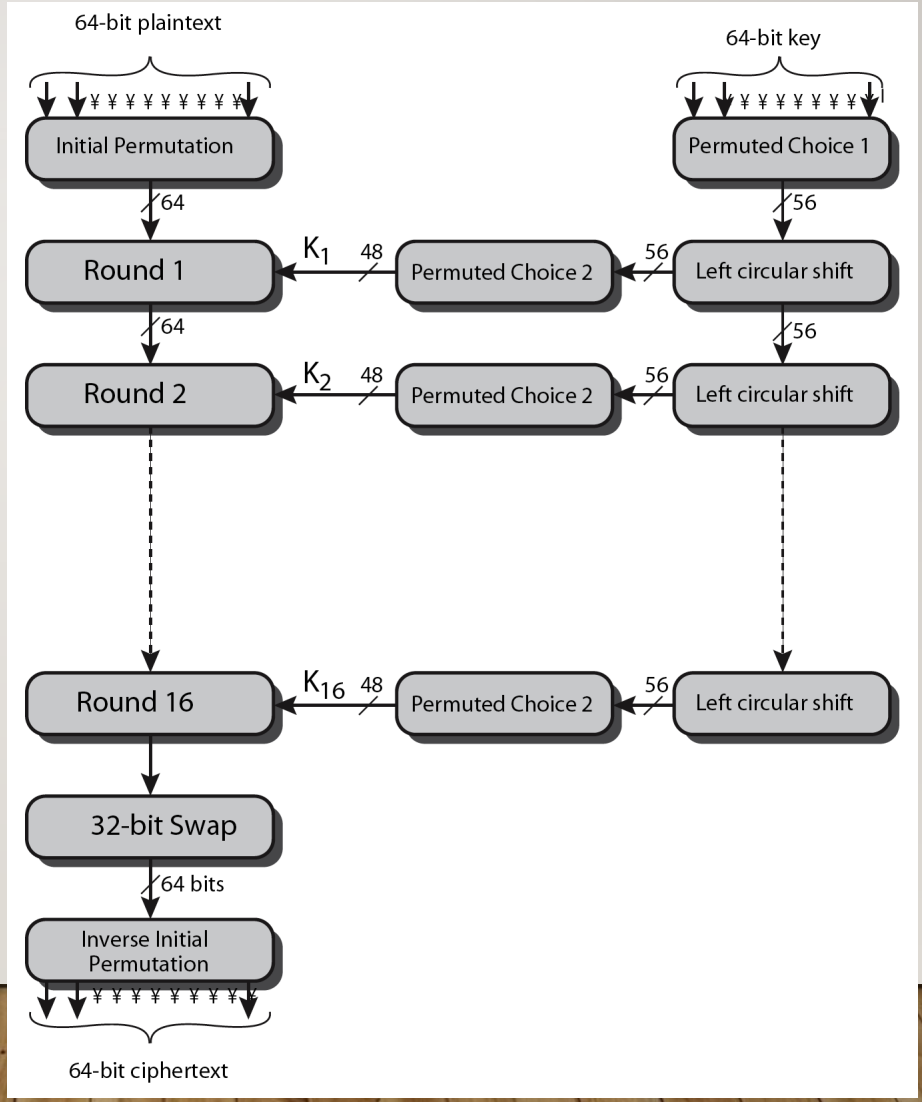
- permutação inicial
- 16 rodadas idênticas de função de substituição, cada uma usando uma diferente chave de 48 bits
- permutação final



DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

Operação do DES

- permutação inicial
- 16 rodadas idênticas de função de substituição, cada uma usando uma diferente chave de 48 bits
- permutação final



DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Exemplo: Seja M o texto claro da mensagem M = 0123456789ABCDEF, onde M está no formato hexadecimal (base 16). Reescrevendo M em formato binário obtemos o bloco de texto de 64 bits:

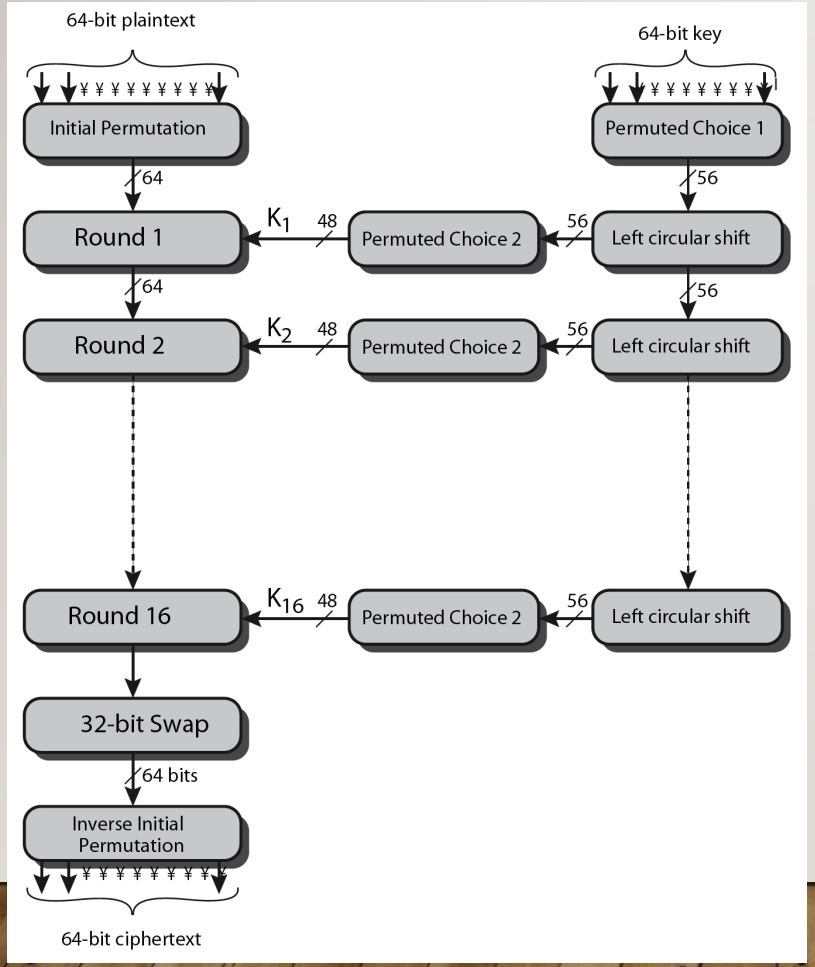
```
M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111
L = 0000 0001 0010 0011 0100 0101 0110 0111
R = 1000 1001 1010 1011 1100 1101 1110 1111
```

- Exemplo: seja K a chave hexadecimal K = 133457799BBCDFF1. Isto nos dá a chave binária (substituindo 1 = 0001, 3 = 0011, etc, agrupados em oito bits):

```
K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001
```

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Transformação na chave



(a) Input Key

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

(b) Permuted Choice One (PC-1)

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

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(d) Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

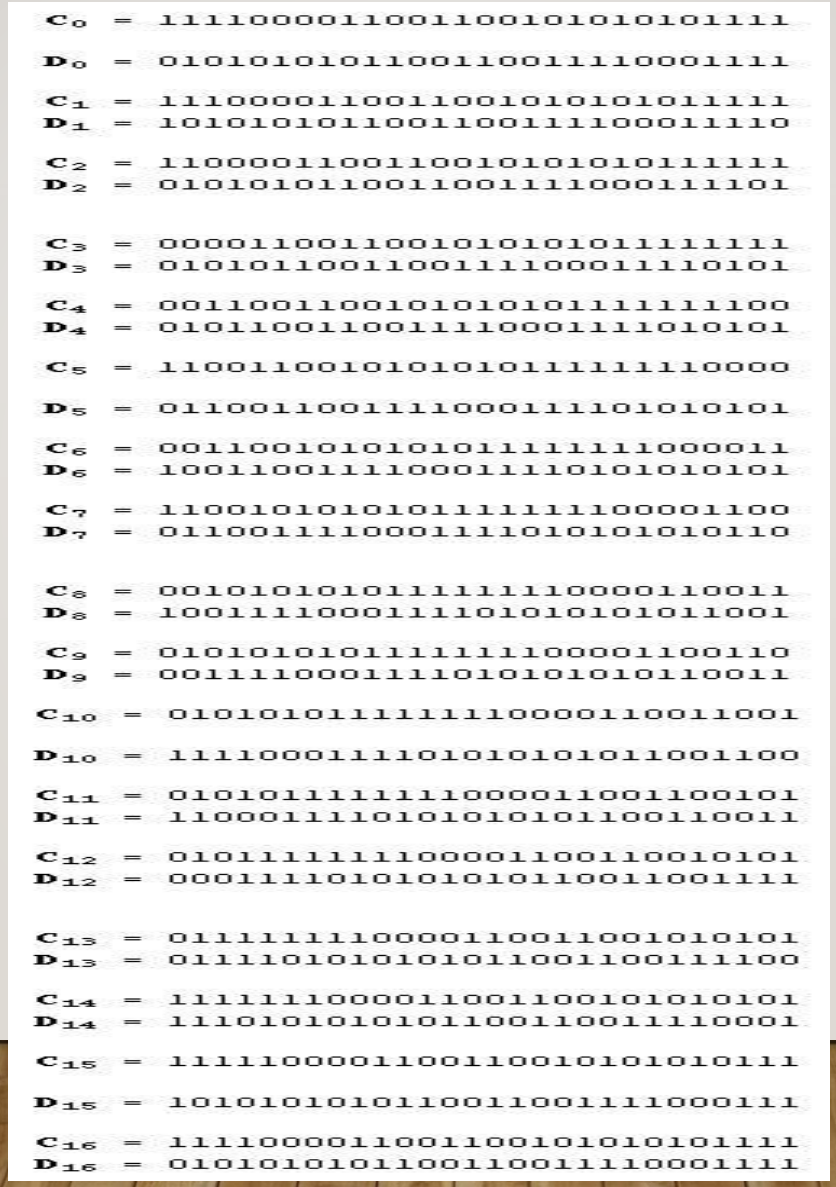
- A partir da chave de 56 bits, criar 16 subchaves de 48 bits

PC-1

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

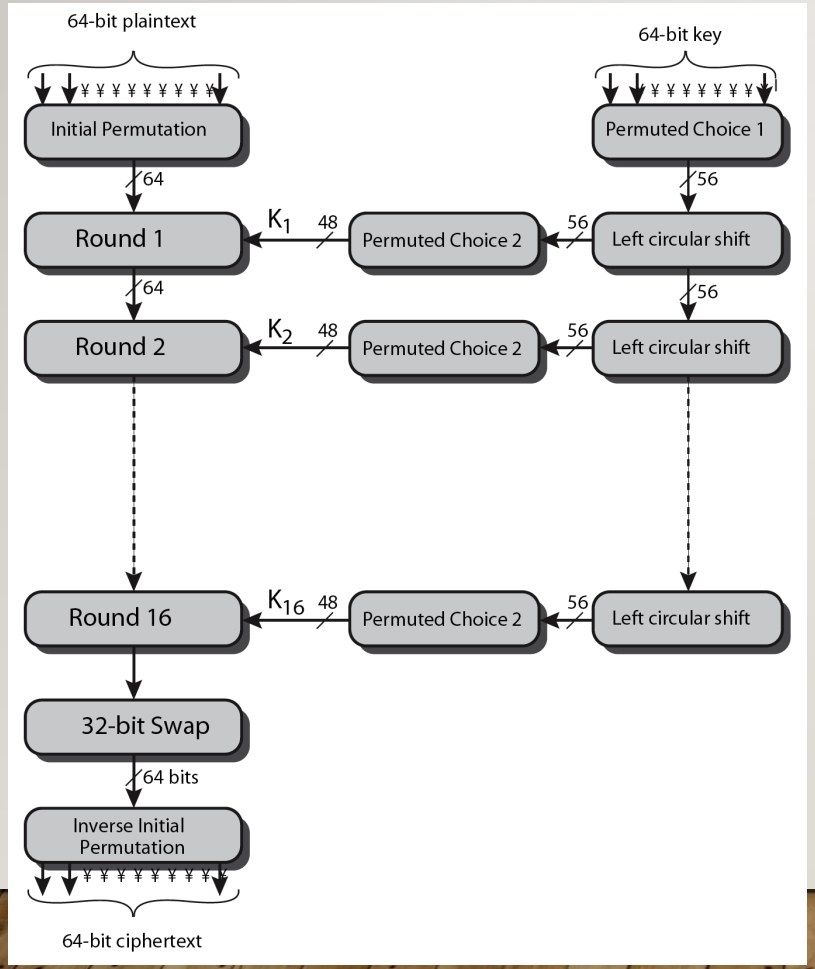
- **Exemplo**: Da chave original de 64 bits
  - **K** = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001
  - Obtem-se a permutação de 56 bits
  - **K+** = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111
  - A seguir, dividimos esta chave em duas metades, esquerda C0 e direita D0, onde cada metade tem 28 bits.
- **Exemplo**: Da chave permutada **K+** obtem-se
  - **C0** = 1111000 0110011 0010101 0101111
  - **D0** = 0101010 1011001 1001111 0001111

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA



DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Transformação na chave



(a) Input Key

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

(b) Permuted Choice One (PC-1)

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

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(d) Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- São montadas as chaves **Kn**, para 1<=**n**<=16, aplicando a tabela de permutação em cada um dos pares concatenados **CnDn**. Cada par possui 56 bits, porém **PC-2** usa apenas 48 deles.

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

- Portanto, o primeiro bit de **Kn** é o 14º bit de **CnDn**, o segundo bit o 17º, e assim sucessivamente, terminando com o 48º bit de **Kn** sendo o 32º de **CnDn**.
- **Exemplo**: Para a primeira chave tem-se:
  - **C1D1** = 1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110
  - a qual, após aplicar a permutação **PC-2** transforma-se em
  - **K1** = 000110 110000 001011 101111 111111 000111 000001 110010

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Para outras chaves tem-se:

K_2 = 011110 011010 111011 011001 110110 111100 100111 100101
K_3 = 010101 011111 110010 001010 010000 101100 111110 011001
K_4 = 011100 101010 110111 010110 110110 110011 010100 011101
K_5 = 011111 001110 110000 000111 111010 110101 001110 101000

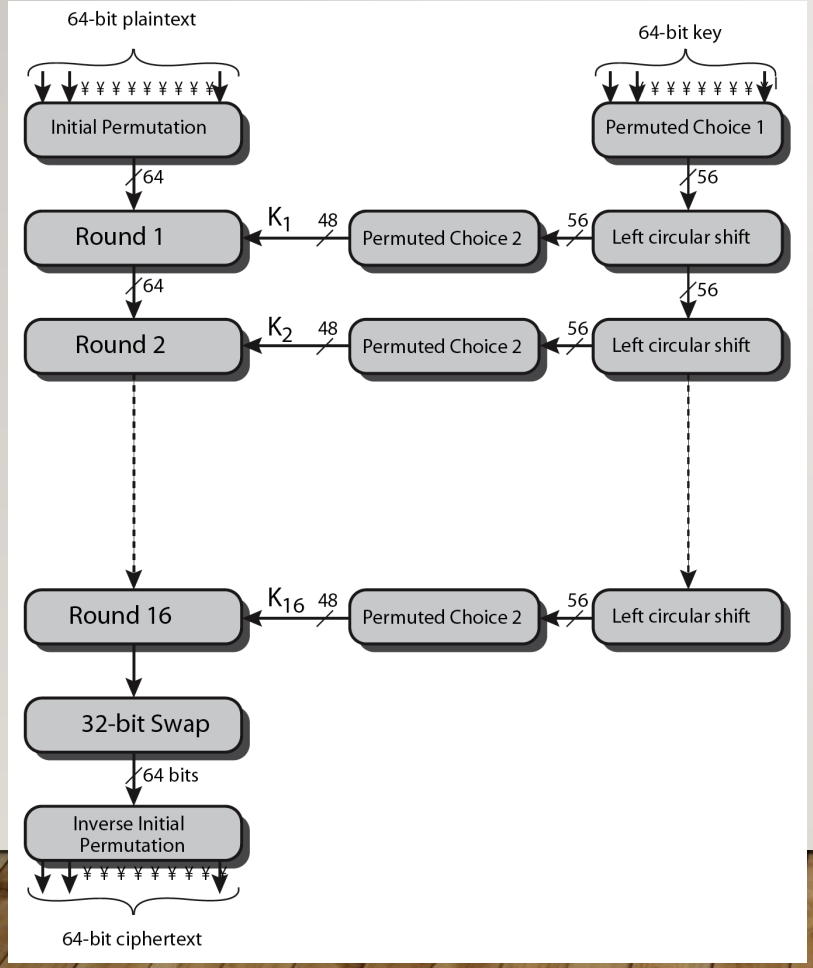
K_6 = 011000 111010 010100 111110 010100 000111 101100 101111
K_7 = 111011 001000 010010 110111 111101 100001 100010 111100
K_8 = 111101 111000 101000 111010 110000 010011 101111 111011
K_9 = 111000 001101 101111 101011 111011 011110 011110 000001
K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111

K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110
K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001
K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001
K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010
K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010

K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Codificar cada bloco de 64 bits de dados (mensagem)
- Tabelas de permuta



(a) Initial Permutation (IP)

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

(b) Inverse Initial Permutation (IP^1)

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

(c) Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Permutação inicial (IP)

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

- Antes
  - **M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111**
- Depois
  - **IP = 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010**

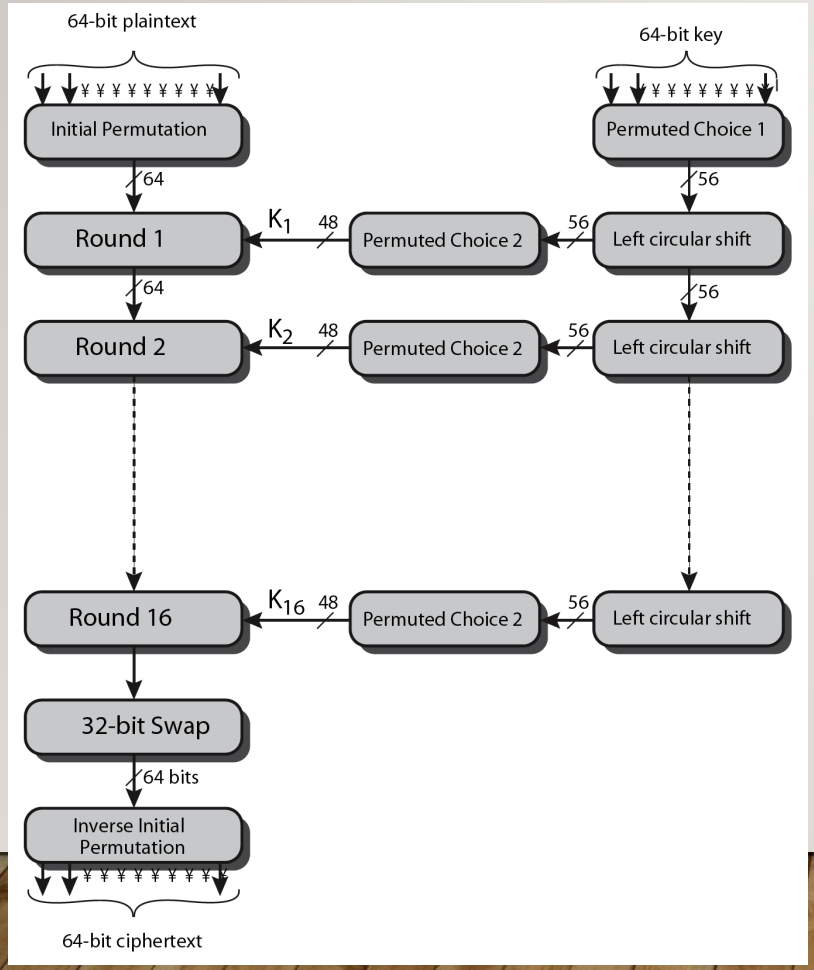
DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Obtem-se **L0** e **R0** de **IP**

L_0 = 1100 1100 0000 0000 1100 1100 1111 1111
R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Codificar cada bloco de 64 bits de dados (mensagem)
- Tabelas de permuta



(a) Initial Permutation (IP)

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

(b) Inverse Initial Permutation (IP^1)

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

(c) Expansion Permutation (E)

	32	1	2	3	4	5
	4	5	6	7	8	9
	8	9	10	11	12	13
	12	13	14	15	16	17
	16	17	18	19	20	21
	20	21	22	23	24	25
	24	25	26	27	28	29
	28	29	30	31	32	1

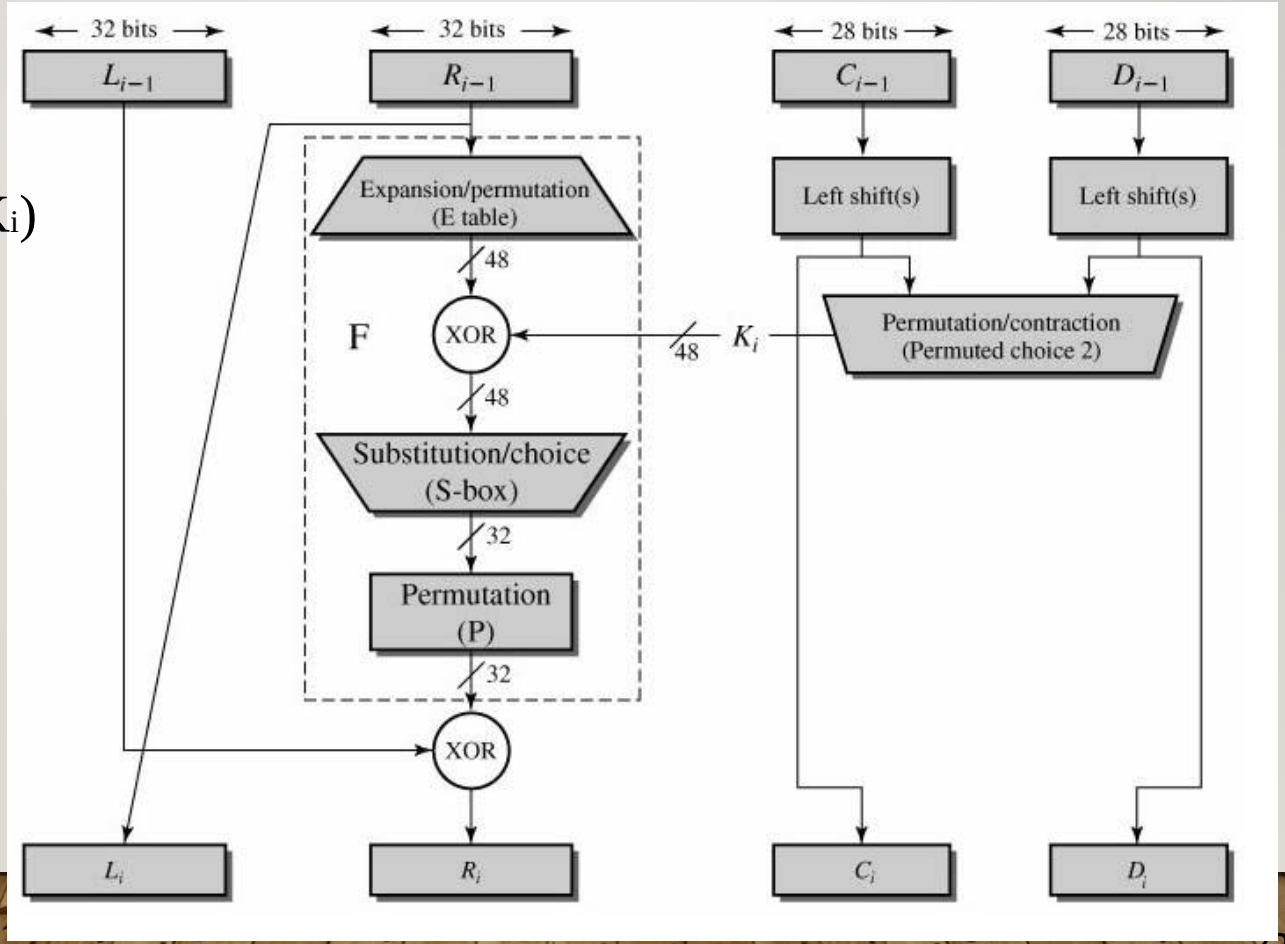
(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Esquema de uma iteração do DES

- $L_i = R_{i-1}$
- $R_i = L_{i-1}$ xor $F(R_{i-1}, K_i)$



DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Para i=1:

$$K_1 = 000110\ 110000\ 001011\ 101111\ 111111\ 000111\ 000001\ 110010$$

$$L_1 = R_0 = 1111\ 0000\ 1010\ 1010\ 1111\ 0000\ 1010\ 1010$$

$$R_1 = L_0 + f(R_0, K_1)$$

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Tabela de expansão (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- A entrada R possui 32 bits. Essa entrada é primeiro expandida em 48 bits usando permutação mais uma duplicação de 16 bits dos R bits.

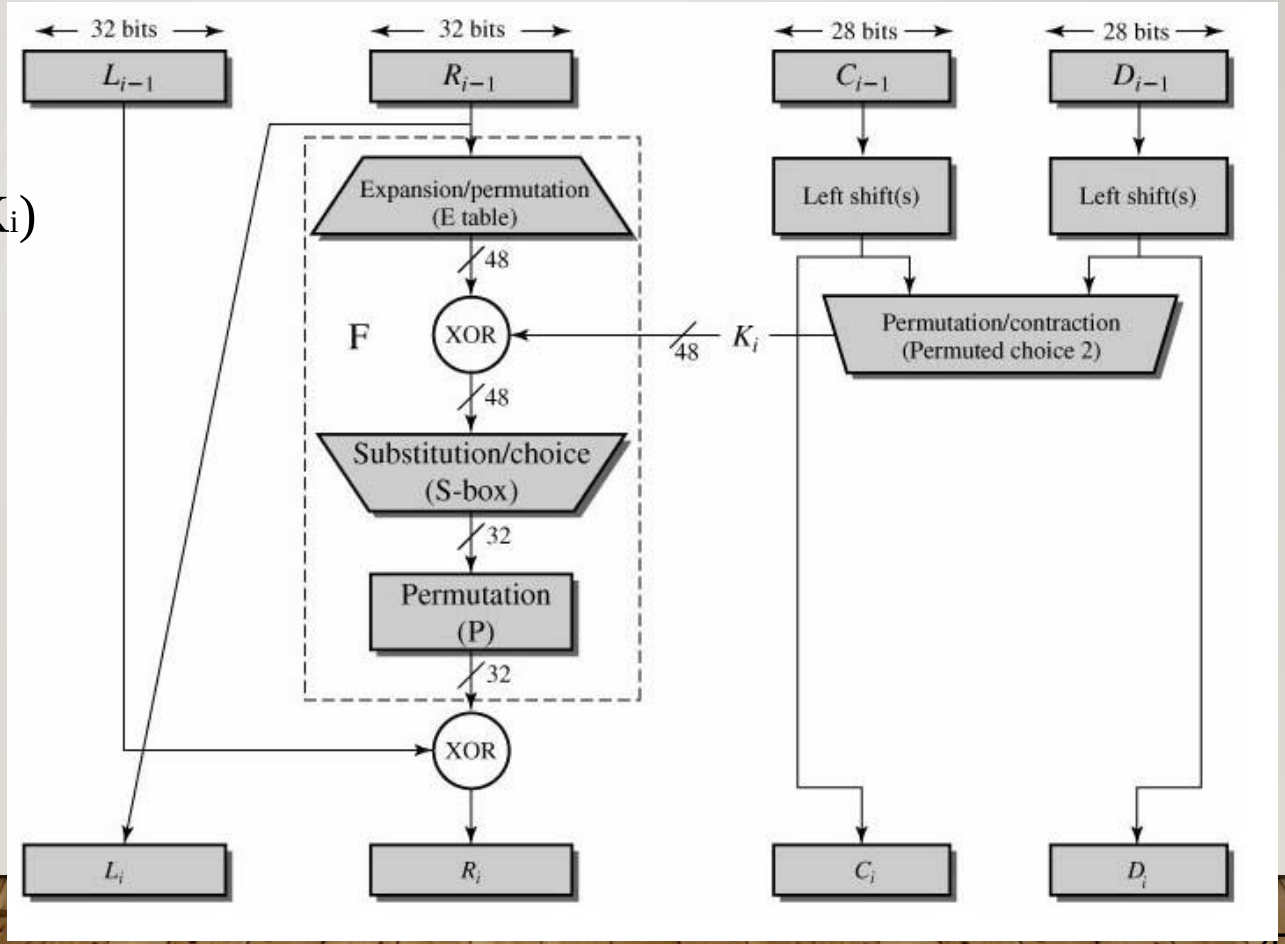
R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Esquema de uma iteração do DES

- $L_i = R_{i-1}$
- $R_i = L_{i-1}$ xor $F(R_{i-1}, K_i)$



DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

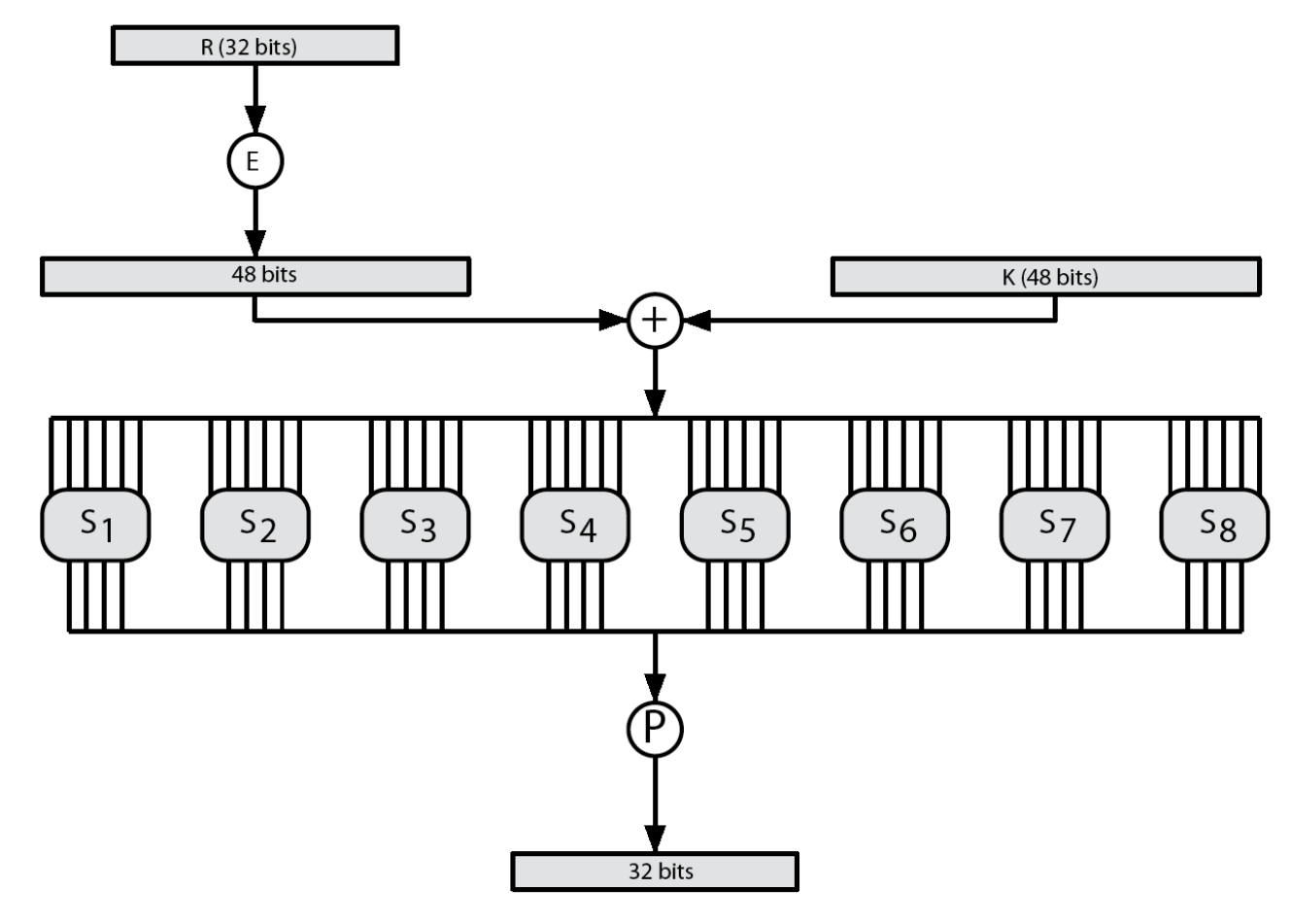
- Cálculo de F(R,K)
  - A seguir, no cálculo de **f**, é feito um XOR na saída **E**(**Rn-1**) com a chave **Kn**. O motivo de se utilizar o XOR lógico é porque este é reversível. Se A xor B = C, então A xor C = B e B xor C = A. A reversibilidade é importante para reverter o processo quando quiser decifrar a mensagem cifrada.

$$K_n + E(R_{n-1})$$

$$\begin{aligned} K_1 &= 000110\ 110000\ 001011\ 101111\ 111111\ 000111\ 000001\ 110010 \\ E(R_0) &= 011110\ 100001\ 010101\ 010101\ 011110\ 100001\ 010101\ 010101 \\ K_1 + E(R_0) &= 011000\ 010001\ 011110\ 111010\ 100001\ 100110\ 010100\ 100111 \end{aligned}$$

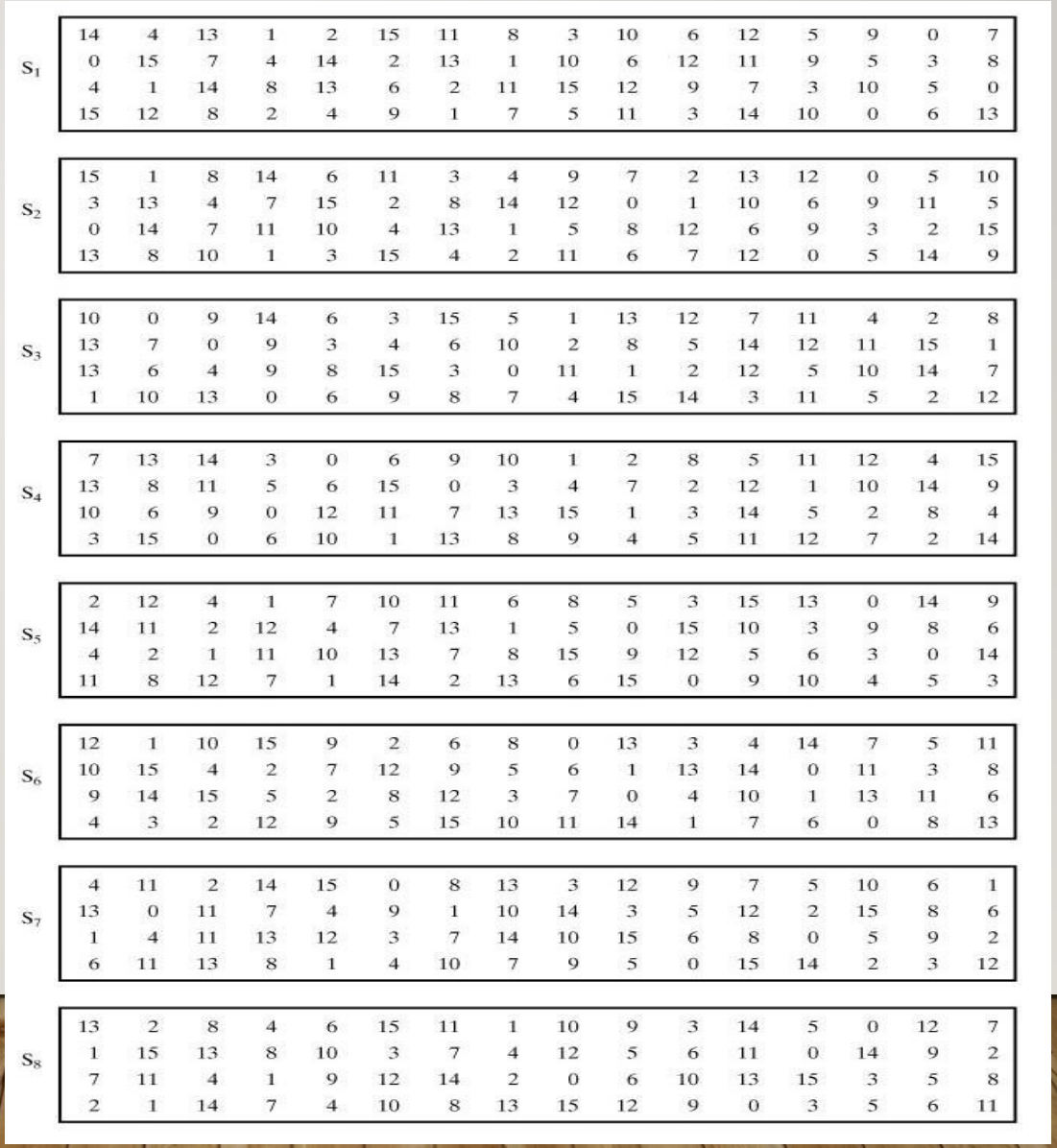
DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Cálculo de F(R,K)



DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- S-boxes
  - Supondo que o primero grupo (S1) seja composto dos seguintes bits (110010) na entrada.
  - A linha é (1,0)=2 - terceira linha e a coluna é (1001)=9 – décima coluna.
  - A saída do grupo (S1) será 12 (1100).



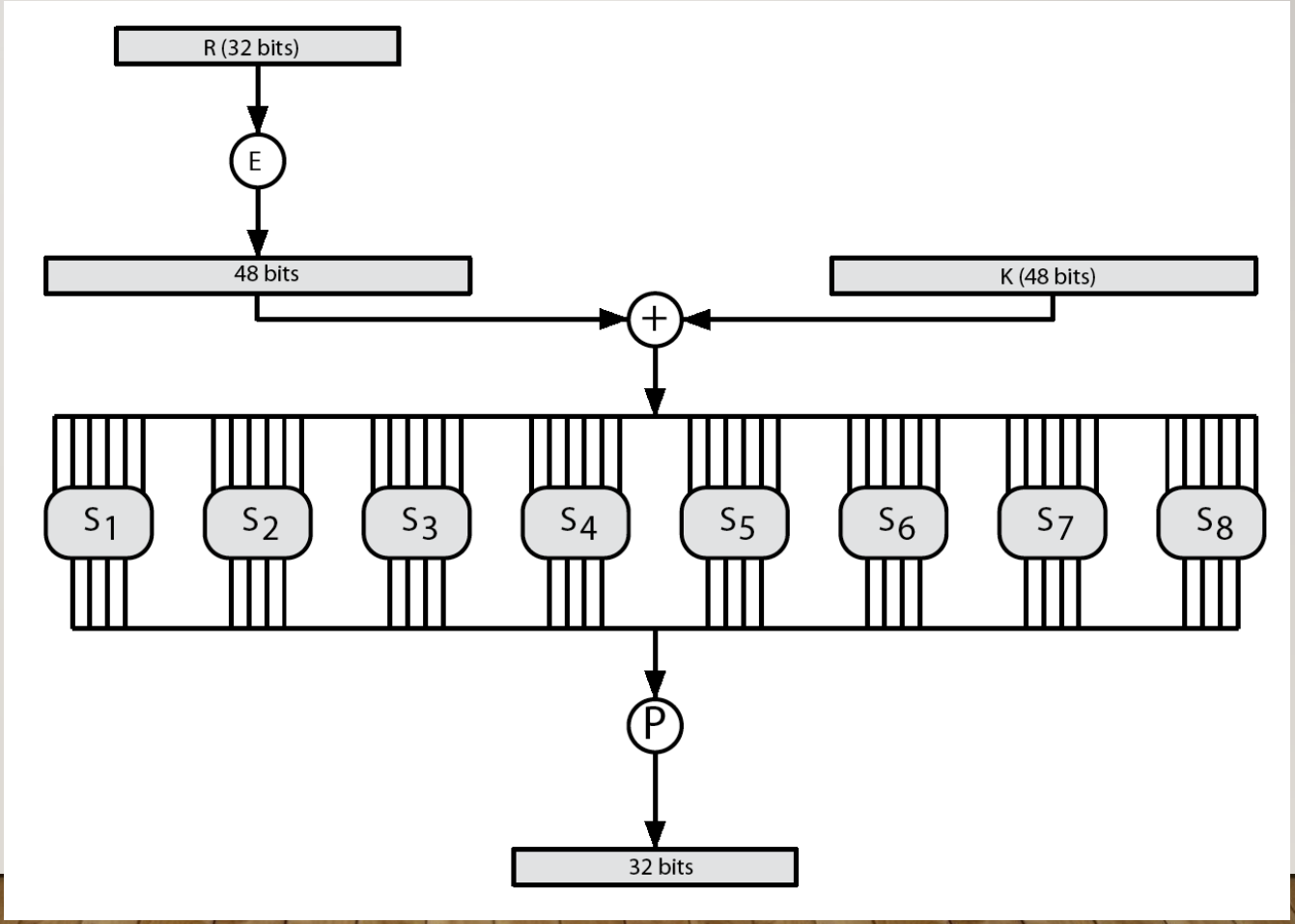
S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- **Exemplo**: Para a primeira rodada, obtem-se como saída das oito caixas **S**:
  - **K1** + **E**(**R0**) = 011000 010001 011110 111010 100001 100110 010100 100111
  - **S1**(**B1**)**S2**(**B2**)**S3**(**B3**)**S4**(**B4**)**S5**(**B5**)**S6**(**B6**)**S7**(**B7**)**S8**(**B8**) = 0101 1100 1000 0010 1011 0101 1001 0111

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Permutação (P)



DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Permutação (P)

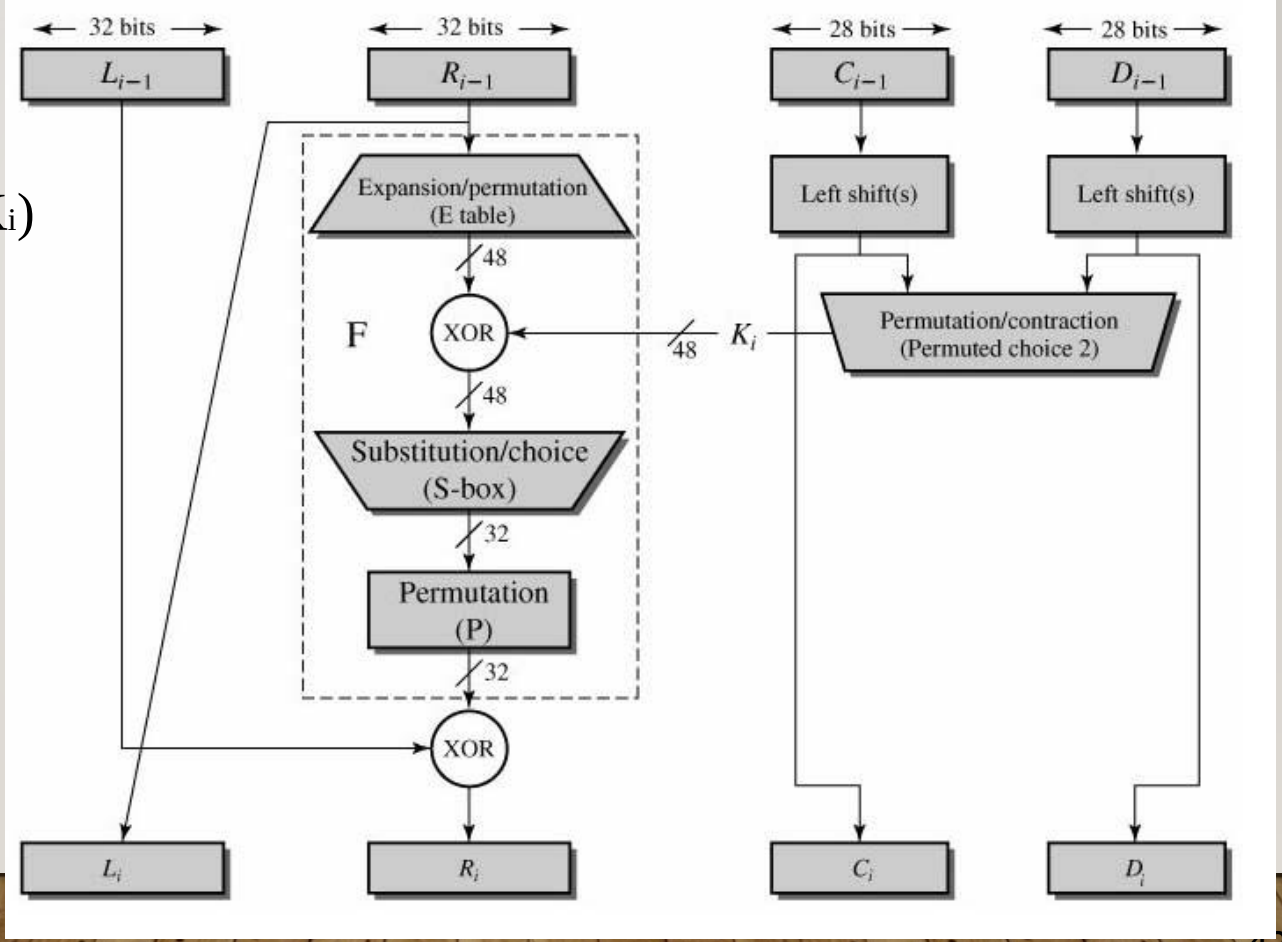
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

- **Exemplo**: Da saída das oito caixas **S**
  - **S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)** = 0101 1100 1000 0010 1011 0101 1001 0111
  - Obtem-se
  - P = 0010 0011 0100 1010 1010 1001 1011 1011

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Esquema de uma iteração do DES

- $L_i = R_{i-1}$
- $R_i = L_{i-1}$ xor $F(R_{i-1}, K_i)$



DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

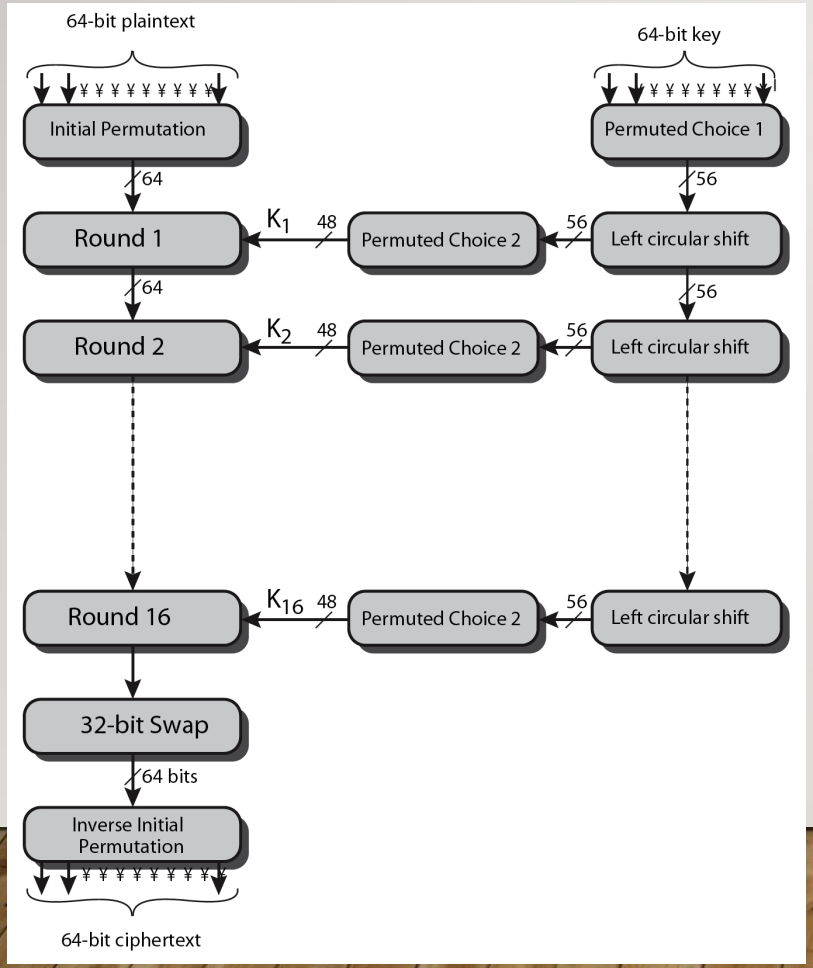
- Agora já se tem todos os elementos necessários para calcular R1, ou seja, **R1** = **L0** + **f(R0** ,**K1**)

$$
\begin{aligned}
L_0 &= 1100\ 1100\ 0000\ 0000\ 1100\ 1100\ 1111\ 1111 \\
f(R_0, K_1) &+ 0010\ 0011\ 0100\ 1010\ 1010\ 1001\ 1011\ 1011 \\
R_1 &= 1110\ 1111\ 0100\ 1010\ 0110\ 0101\ 0100\ 0100
\end{aligned}
$$

- Na próxima rodada obtem-se **L2** = **R1**, que é o sub-bloco que foi calculado, e depois calcular **R2** = **L1** + **f(R1**, **K2**) e assim sucessivamente por 16 rodadas. No final da décima sexta rodada tem-se os sub-blocos **L16** e **R16**. Invertendo então a ordem dos dois sub-blocos num bloco de 64 bits, ou seja, **R16L16**, e aplica-se permutação final **IP-1.**

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Codificar cada bloco de 64 bits de dados (mensagem)
- Tabelas de permuta



(a) Initial Permutation (IP)

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

(b) Inverse Initial Permutation (IP^1)

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

(c) Expansion Permutation (E)

32	1	2	3	4	5	
4	5	6	7	8	9	
8	9	10	11	12	13	
12	13	14	15	16	17	
16	17	18	19	20	21	
20	21	22	23	24	25	
24	25	26	27	28	29	
28	29	30	31	32	1	

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Permutação final

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

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

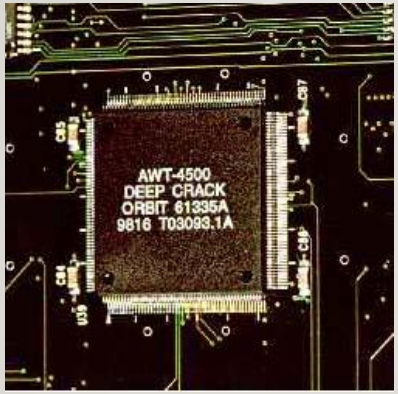
- **Exemplo**: Se processarmos todos os 16 blocos usando o método definido previamente, obteremos, na 16ª rodada
  - **L16** = 0100 0011 0100 0010 0011 0010 0011 0100
  - **R16** = 0000 1010 0100 1100 1101 1001 1001 0101
- Invertendo a ordem destes dois blocos e aplicando a permutação final em
  - **R16L16** = 00001010 01001100 11011001 10010101 01000011 01000010 00110010 00110100
  - **IP-1** = 10000101 11101000 00010011 01010100 00001111 00001010 10110100 00000101
  - formato hexadecimal, é 85E813540F0AB405.
  - Portanto, a forma cifrada de **M = 0123456789ABCDEF** é **C = 85E813540F0AB405**.
- Decifrar é simplesmente o inverso de cifrar, seguindo os mesmos passos acima descritos porém invertendo a ordem das sub-chaves aplicadas.

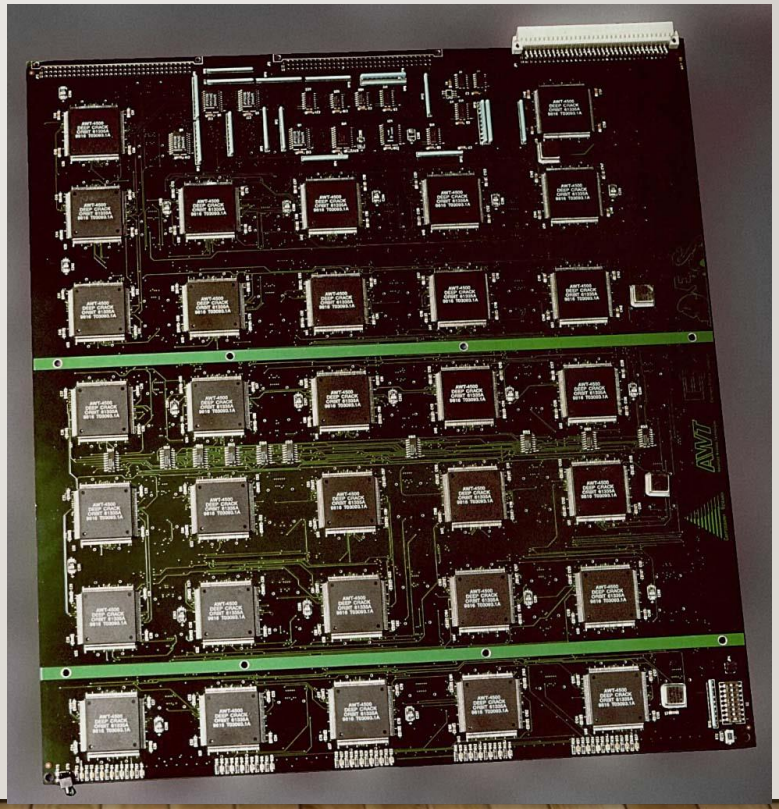
DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Desconfiança do padrão DES?
  - O DES foi adotado oficialmente como padrão de encriptação nos EUA em julho de 1977;
  - A segurança do algoritmo foi questionada por muitos especialistas;
  - Sempre houve muita especulação sobre:
    - Comprimento da chave (56 bits);
    - Chaves fracas (chave inicial é modificada para se obter a sub-chave para cada rodada do algoritmo, certas chaves iniciais são **chaves fracas)**, 64 chaves fracas são insignificantes quando comparadas com o conjunto de mais de 72 quatrilhões de chaves possíveis (2^56), mas se uma chave for escolhida ao acaso, é mínima a possibilidade de pegar justamente uma das fracas
    - O número de iterações (16 iterações);
    - A estrutura das caixas S (S-boxes) - as caixas S, com todas aquelas constantes sem uma razão aparente para a disposição usada, eram particularmente misteriosas, alguns especialistas temiam que a NSA (National Security Agency) tivesse colocado um "alçapão" (trapdoor) no algoritmo para que a agência tivesse um meio fácil de decifrar mensagens.

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Deep Crack: 27 placas, cada uma com 64 chips, e é capaz de testar 90 bilhões de chaves por segundo.





DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Propostas para maior segurança
  - Triple-DES é apenas o DES efetuado três vezes com duas chaves usadas numa determinada ordem.
  - O triple-DES também pode ser feito usando-se três chaves diferentes, ao invés de apenas duas.
  - O espaço das chaves pode ser de 2^{112} ou de 2^{168}.
  - Usar o AES com 128, 192, 256 bits de chave

DES – CRIPTOGRAFIA COM CHAVE SIMÉTRICA

- Em outubro de 2000, o NIST anunciou que o bloco AES / Rijndael
  - A cifra foi escolhida como substituta do DES.
  - A especificação original do Advanced Encryption Standard (AES) exigia o processamento de blocos de 128 bits, mas o Rijndael excedeu essa especificação, permitindo uso de um tamanho de bloco igual a qualquer um dos três comprimentos de chave. O número de rodadas de criptografia depende do tamanho da chave escolhida:
    - Chaves de 128 bits exigem 10 rodadas de criptografia.
    - Chaves de 192 bits exigem 12 rodadas de criptografia.
    - Chaves de 256 bits requerem 14 rodadas de criptografia.

BIBLIOGRAFIA

- **Bibliografia:**

  - STALLINGS, W. Criptografia e Segurança de Redes - Princípios e Práticas - 6ed., Pearson, 2015.
  - DES Simulator. Disponível em: <http://des.online-domain-tools.com>. Acesso em: 09.08.2024.
  - AES Rijndael Cipher explained as a Flash animation. <https://www.youtube.com/watch?reload=9&v=gP4PqVGudtg>. Acesso em: 09.08.2024.
  - Notas de aula.