Cifras de Blocos
DES – *Data Encryption Standard*

Prof. Dr. Avelino Francisco Zorzo
Faculdade de Informática - PUCRS

Importância histórica do DES

- Antes 1970s, cripto era uma ciência *proibida*
  - Quase não existiam artigos científicos.
  - National Security Agency tinha conhecimento considerável sobre cripto, mas eles não adminitiam a existência.
  - Todavia, transações financeiras devem ser protegidas.
  - Um padrão de criptografia era necessário.

Importância histórica do DES

- Em 1972, *National Bureau of Standards* (NBS) iniciou o desenvolvimento de uma cifra padrão
  - Deve prover um alto grau de segurança.
  - Deve ser completamente especificada e fácil de entender.
  - A segurança deve estar na chave e não no algoritmo.
  - Deve estar disponível para todos usuários.
  - Deve ser adaptável para todas aplicações.
  - Deve ser economincamente implementável em equipamentos.
  - Deve ser eficiente para uso.
  - Deve ser capaz de ser validável.
  - Deve ser exportável.

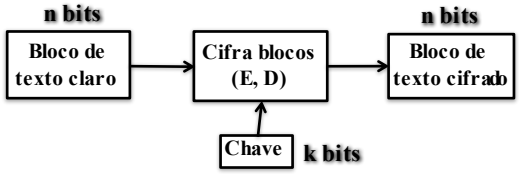
Importância histórica do DES

- Em 1974, NBS fez uma segunda chamada
  - IBM submeteu Lucifer
- NBS solicitou à NSA ajuda na avaliação
  - NSA reduziu a chave de 128 para 56 bits
  - Isto ocasionou diversas críticas
- 1976, o Lucifer foi adotada como padrão.
- Depois 1976
  - Pequisa pública em cripto não parou mais.

Data Encryption Standard

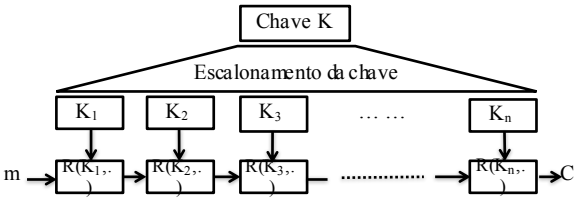
- 1970s: Horst Feistel projetou Lucifer - IBM
- 1973: NBS solicitou cifras de blocos
  - IBM submeteu um variação da (chave de 128 bits e tamanho de bloco de 128 bits)
- 1977: NBS adotou DES como padrão
  - Reduziu a chave para 56 bits e tamanho de bloco para 64 bits
- 1997: DES quebrada por pesquisa exaustiva
  - Chave de 56 bits é muito pequena
- 2000: NIST adotou AES para trocar DES

Cifra de blocos: resumo



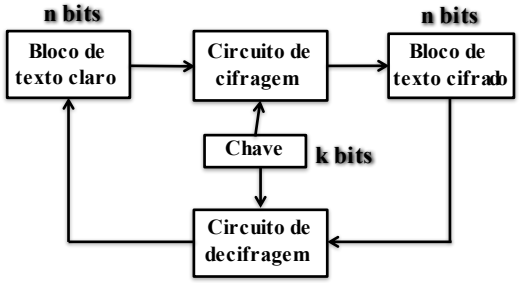
- Exemplos:
  - DES: n=64 bits k=56 bits
  - 3DES: n=64 bits k=168 bits
  - AES: n=128 bits k=128, 192, 256 bits

Construção iterativa



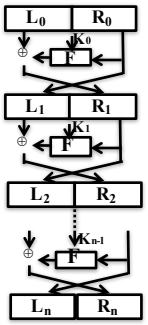
- R(K,.) é chamada função da rodada
- DES 16 rodadas, 3DES 48 rodadas, AES-128 10 rodadas

Um desafio em eficiência



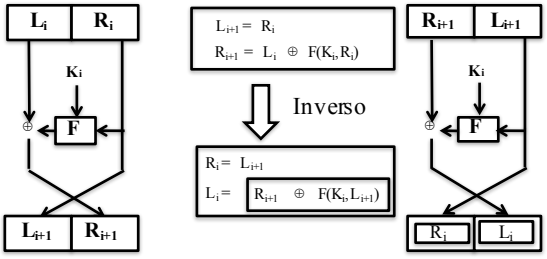
Podemos usar o mesmo circuito para cifrar/decifrar?

Rede de Feistel

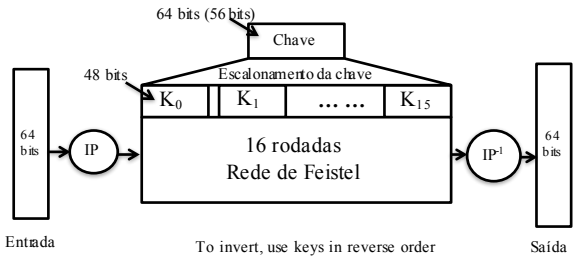



```
For i = 0, 1, … n-1
   Li+1 = Ri
   Ri+1 = Li ⊕F(Ki, Ri)
End
```


Projeto reversível



DES: Rede de Feistel de 16 rodadas



To invert, use keys in reverse order

Tabelas de Permutação

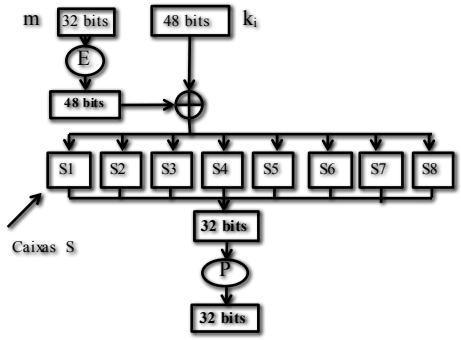
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP

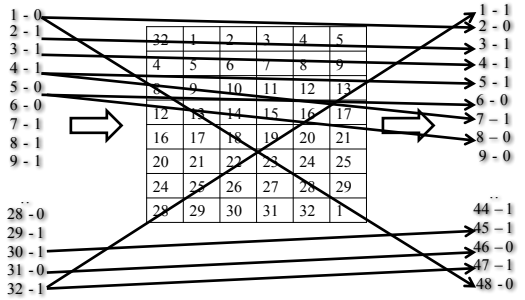
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	43	10	50	18	58	26
33	1	41	9	49	17	57	25

IP^{-1}

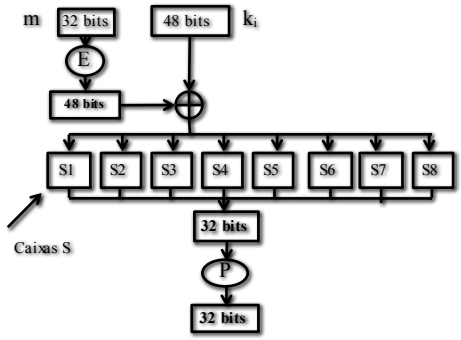
Função F: F(k_i,m)



Expansão (E)



Função F: F(k_i,m)



Caixas S

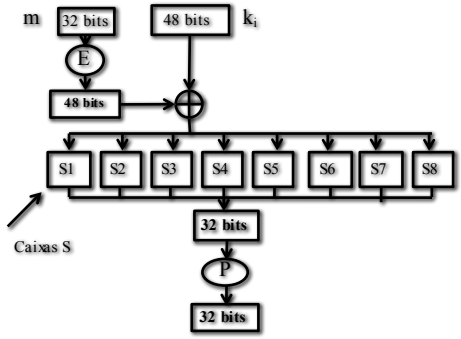
- S_i: $\{0,1\}^6 \rightarrow \{0,1\}^4$

S_1	4 bit do meio na entrada															
2 bits de fora	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

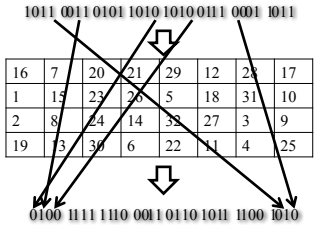
Por exemplo:

- Entrada= 101110 — 10: linha 2; 0111: coluna 7
- Saída= **1011** — Valor: 11

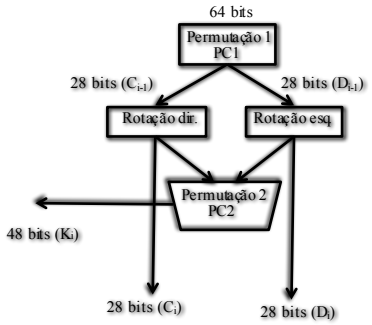
Função F: F(k_i,m)



Permutação (P)



Escalonamento da chave



Chave: permutação 1 (PC1)

- Todo oitavo bit é descartado
  - 8º, 16º, …

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

Chave: permutação 2 (PC2)

- 28 bits da esquerda e 28 bits da direita

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

Rotação

- Número de bits para rotacionar é diferente em cada rodada

Round	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
N. Bits	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Escolha das caixas S e permutações

- Caixas S permutações P deve ser uma escolha cuidadosa
- Escolha aleatório pode resultar em uma cifra insegura
- Diversas regras para escolha de S e P
  - Nenhum bit de saída pode ser uma função linear dos bits de entrada
  - Caixas S são um mapeamento 4 para 1.

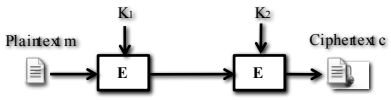
… …

Ataque de força bruta no DES

- Deasafio DES proposto pela RSA
  - Dado um texto plano e o texto criptografaeo encontre a chave
- 1997:
  - Usando a Internet levou 96 dias
- 1998
  - Máuina para DES (EFF), 56 horas
  - Custo: US$250K
  - Prêmio: US$10K
- 1999
  - Combinação entre busca na Internet e máquina DES 22 **horas**
- Conclusão: chavede 56 bits é muito muito fraca

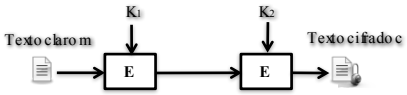
↗
1 sec

DES Duplo



- Usa duas chaves e criptografa duas vezes
  - 112 bits
  - E(k_1,E(k_2,m))
- Isto é seguro?

Quebrando criptografia do 2DES



Encontro no meio do caminho: conhecendo alguns pares

K_1 (56 bit)	$E(K_1, m_1)$
00….000	… …
00…001	… …
… …	… …
11…111	… …

$D(K_2, c_1)$	K_2 (56 bit)
… …	00….000
… …	00…001
… …	… …
… …	11…111

3DES