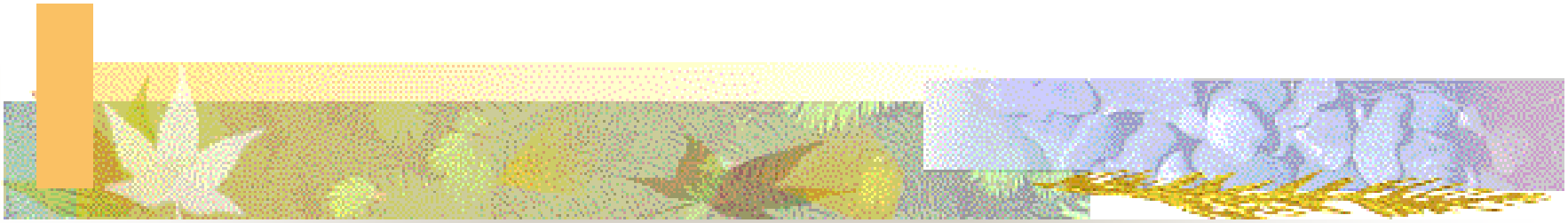
# Introdução a Criptografia



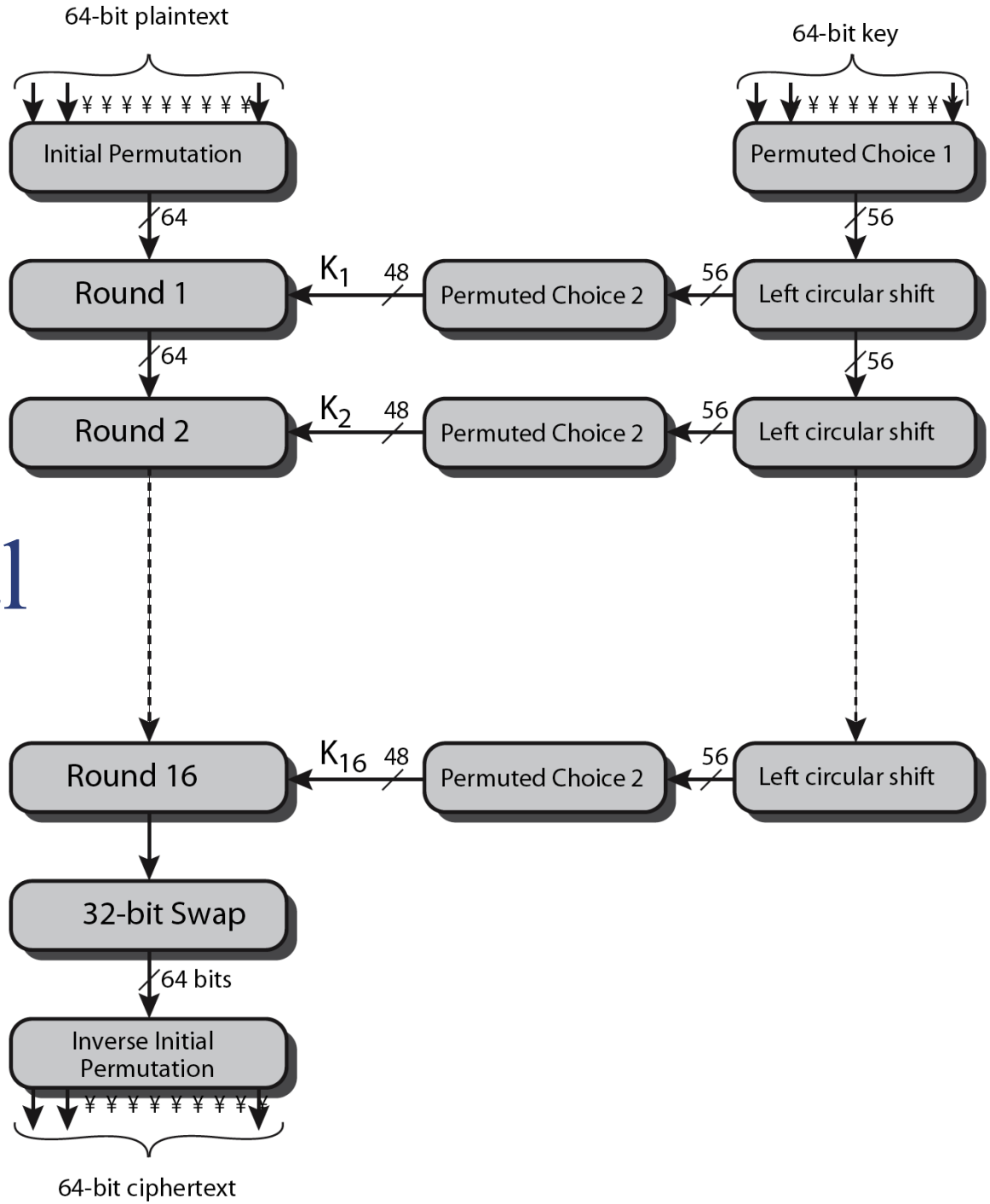
Profa. Yeda

Aula 03 – Criptografia Simétrica – DES

(**Cap. 3**)

# DES

# Visão Geral



# Permutação Inicial (IP)

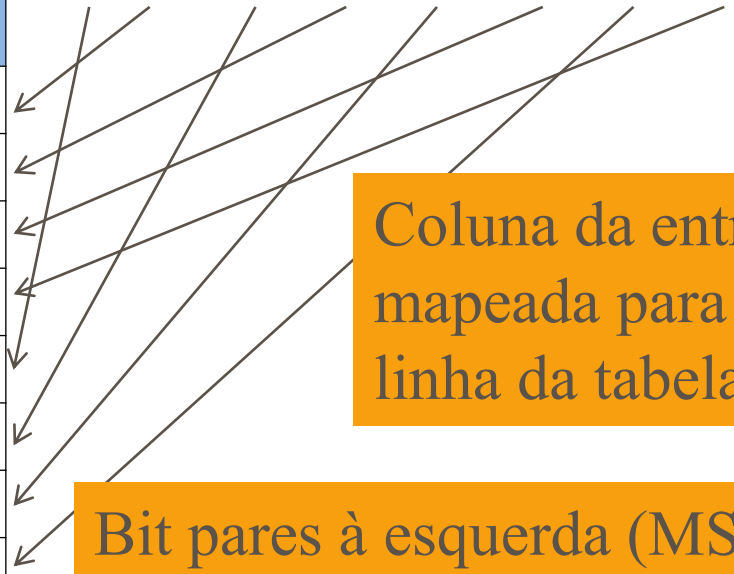
- Primeiro passo da computação de dados
  - reordena os bits de entrada de dados
    - bits pares para a metade esquerda
    - bits impares para a metade direita
  - Estrutura regular de fácil implementação em hardware
- Exemplo:

  IP(67 5A 69 67 5E 5A 6B 5A) = FF B2 19 4D 00 4D F6 FB

# Permutação Inicial (IP)

| Tabela Ordem de Entrada | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **0** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **8** | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| **16** | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| **24** | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| **32** | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| **40** | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| **48** | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| **56** | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |

| Tabela Permutação Inicial (IP) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **0** | 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| **8** | 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| **16** | 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| **24** | 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| **32** | 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| **40** | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| **48** | 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| **56** | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |



Coluna da entrada mapeada para linha da tabela IP

Bit pares à esquerda (MSB)
Bits impares à direita (LSB)

# Permutação Inicial (IP)

| Tabela Ordem de Entrada | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **0** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **8** | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| **16** | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| **24** | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| **32** | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| **40** | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| **48** | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| **56** | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |

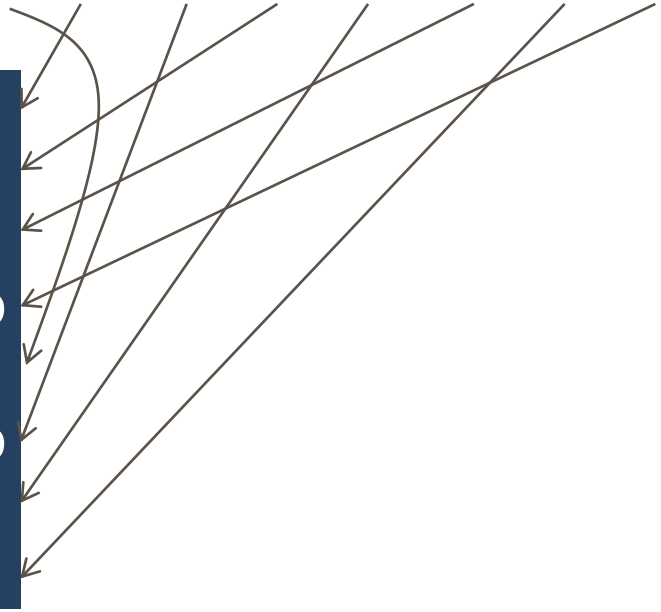
| Entrada bits: 67 5A 69 67 5E 5A 6B 5A | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | |
| **0** | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 67 |
| **8** | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 5A |
| **16** | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 69 |
| **24** | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 67 |
| **32** | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 5E |
| **40** | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 5A |
| **48** | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 6B |
| **56** | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 5A |

IP(67 5A 69 67 5E 5A 6B 5A)

# Permutação Inicial (IP)

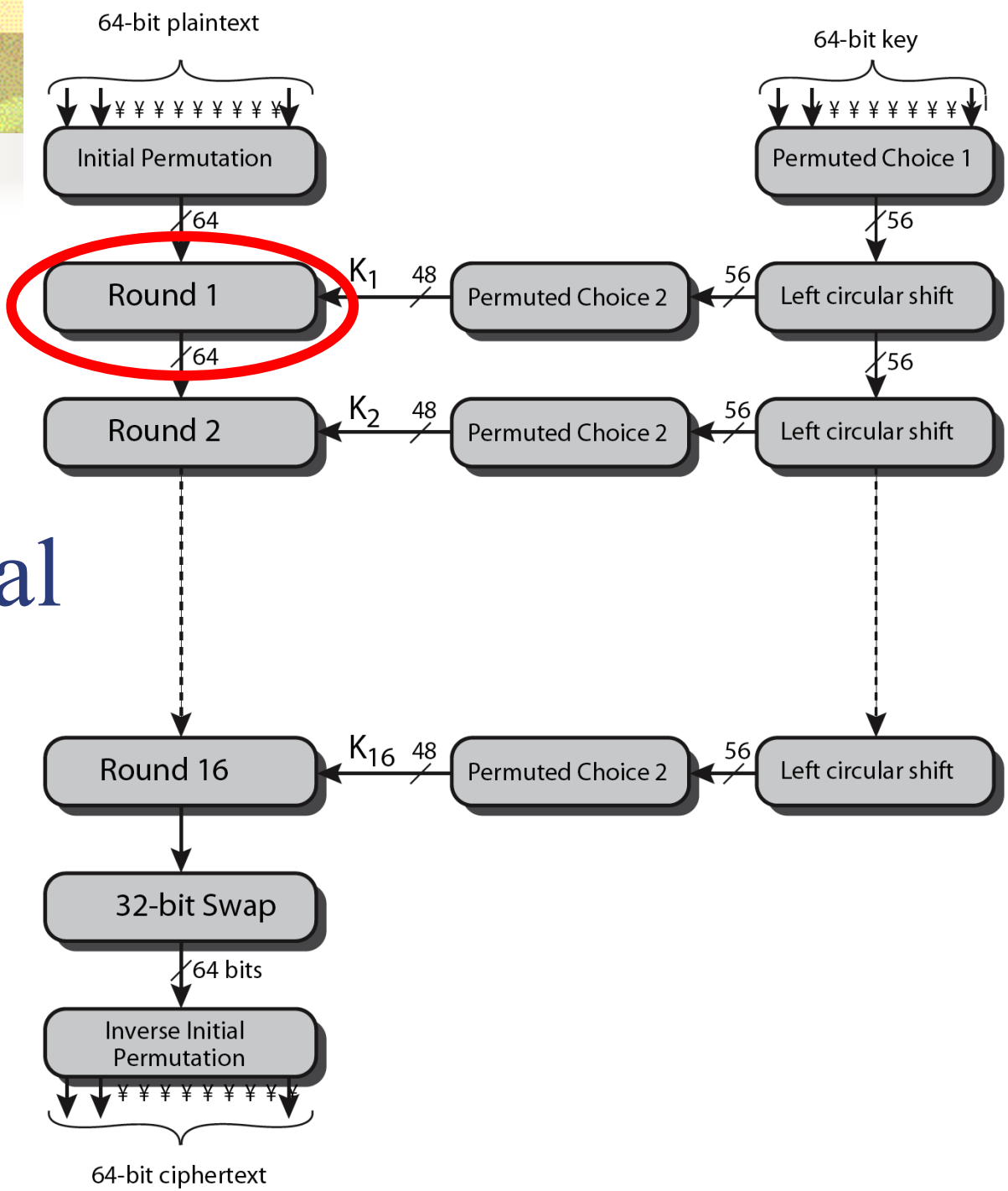
| Entrada bits: 67 5A 69 67 5E 5A 6B 5A | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **0** | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| **8** | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| **16** | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| **24** | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| **32** | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| **40** | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| **48** | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| **56** | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |

| Saida de bits IP: FF B2 19 4D 00 4D F6 FB | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | |
| **0** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | FF |
| **8** | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | B2 |
| **16** | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 19 |
| **24** | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 4D |
| **32** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 00 |
| **40** | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 4D |
| **48** | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | F6 |
| **56** | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | FB |



# DES

# Visão Geral



# Estrutura das etapas do DES

- use duas metades de 32-bit (L & R)
- como para qualquer cifra de Feistel (i-ésima etapa):
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- F toma 32-bit da metade R e 48-bit de subchave:
  - expande R para 48-bits usando permutação E
  - adiciona à subchave usando XOR
  - passa através das 8 S-boxes para obter 32-bit resultantes
  - finalmente permuta 32-bits com permutação P

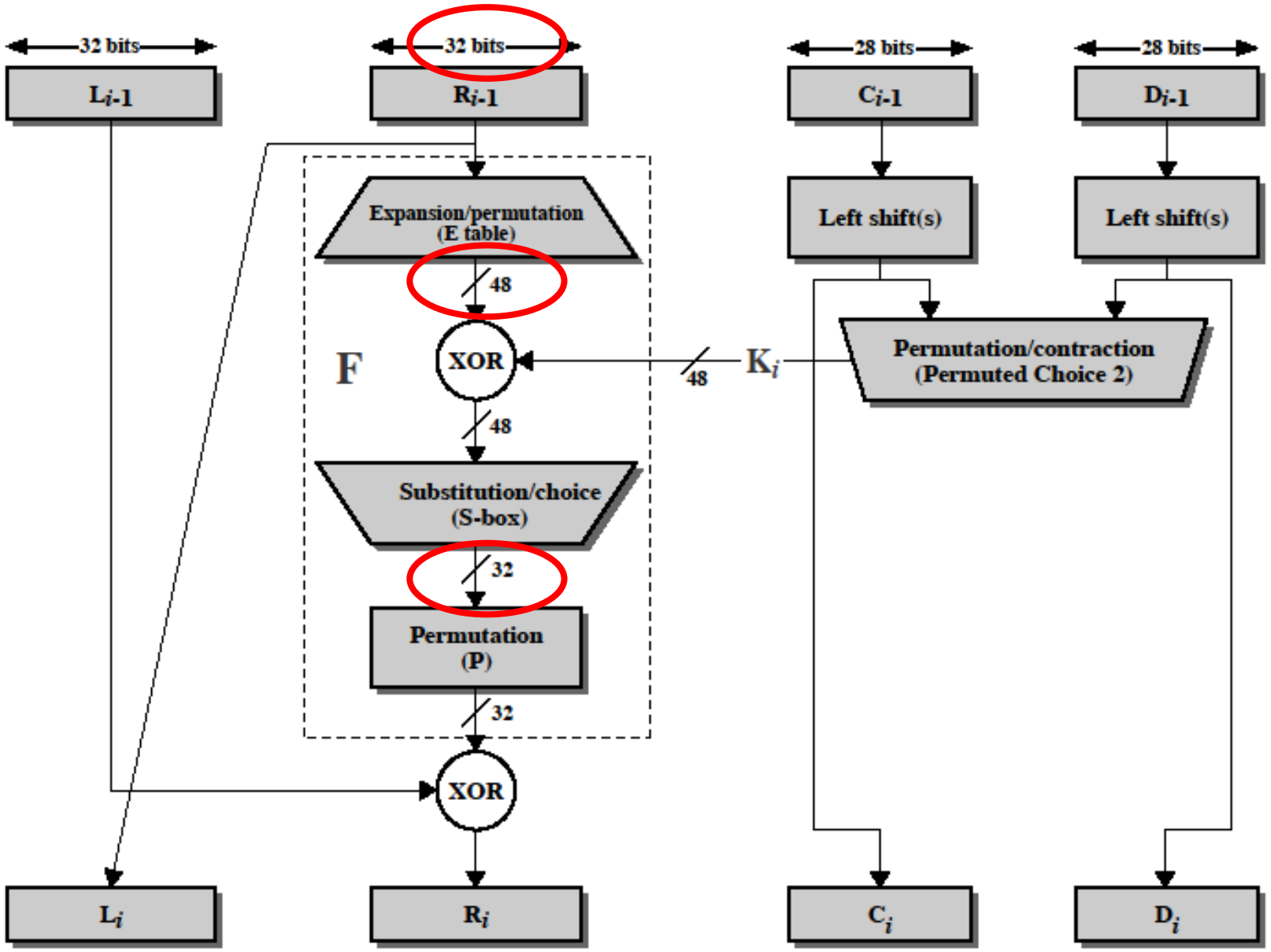
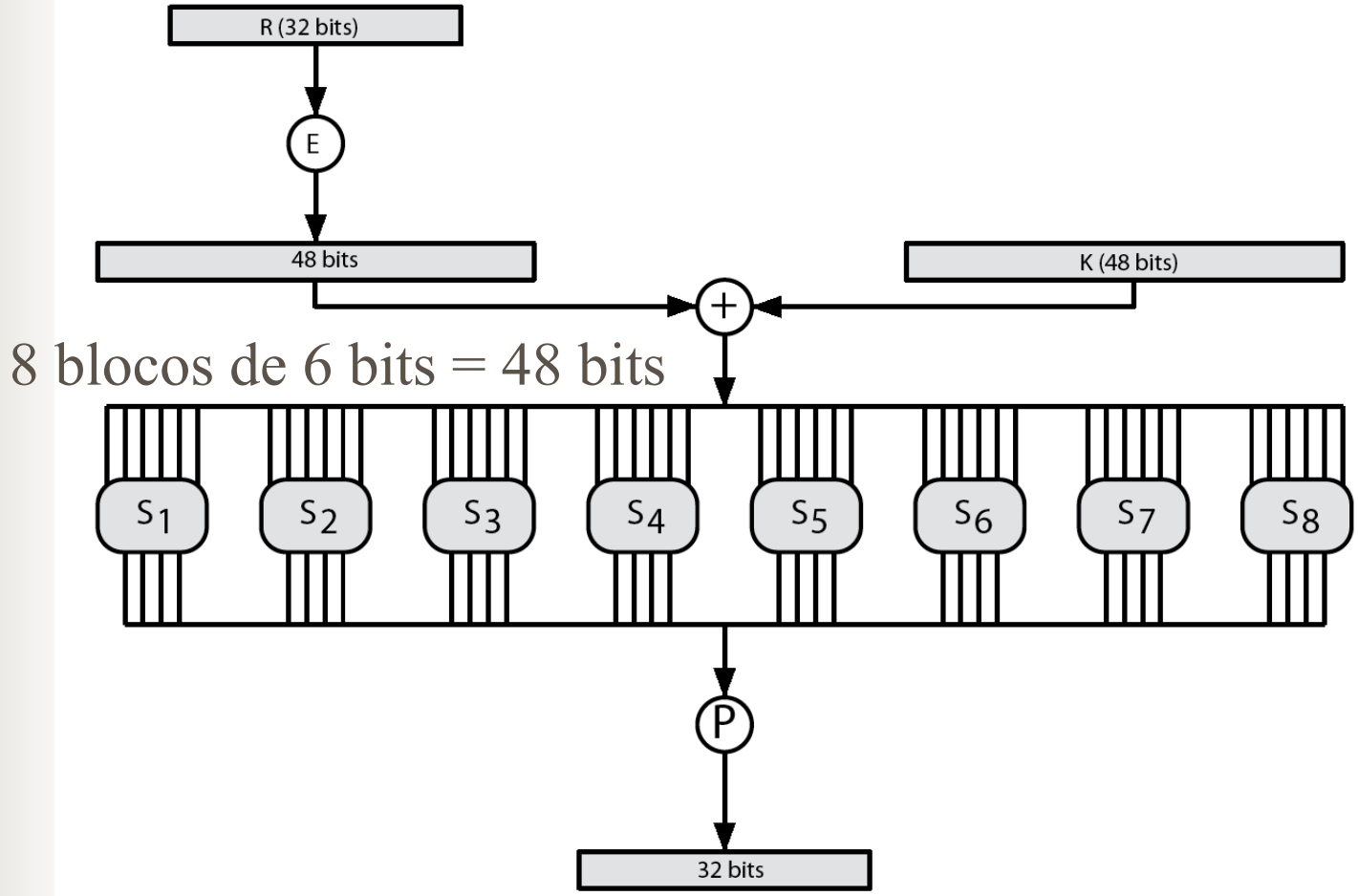



**Figure 3.5 Single Round of DES Algorithm**

# Função F das Etapas DES



# Tabela de Permutação/Expansão E

| Permutação de Expanção (E) | | | | | | |
|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** |
| **0** | 32 | 1 | 2 | 3 | 4 | 5 |
| **6** | 4 | 5 | 6 | 7 | 8 | 9 |
| **12** | 8 | 9 | 10 | 11 | 12 | 13 |
| **18** | 12 | 13 | 14 | 15 | 16 | 17 |
| **24** | 16 | 17 | 18 | 19 | 20 | 21 |
| **30** | 20 | 21 | 22 | 23 | 24 | 25 |
| **36** | 24 | 25 | 26 | 27 | 28 | 29 |
| **42** | 28 | 29 | 30 | 31 | 32 | 1 |

shift

Os 48 bits de E são somados com XOR à chave de etapa Ki, Então divididos em 8 blocos e 6 bits, os quais são utilizados como entrada das S-boxes

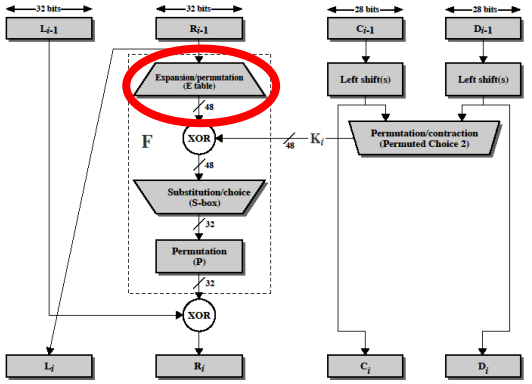
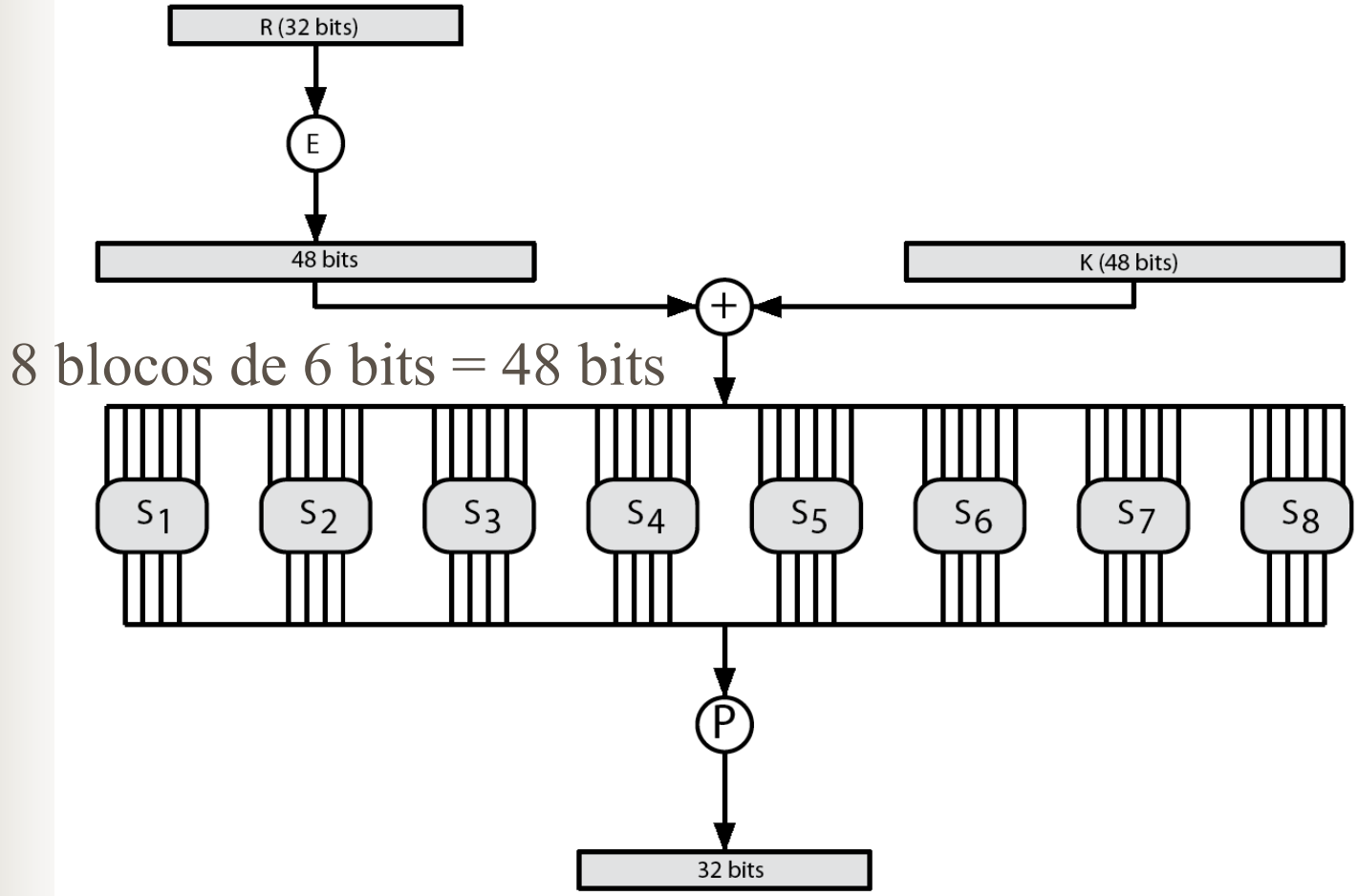


Figure 3.5 Single Round of DES Algorithm

# Substituição: S-Boxes

- possui 8 S-boxes que mapeia 6 para 4 bits
- Os bits de entrada da S-box selecionam uma linha e uma coluna da tabela, como segue.
  - bits mais externos 1 e 6 (bits) selecionam uma linha de 4.
  - bits mais internos 2 a 5 (bits) selecionam uma coluna de 16
  - a saída da S-Box é o valor do elemento da S-box
  - o resultado são 8 blocos de 4 bits, ou seja, 32 bits
- a seleção da linha depende do dado e da chave
- exemplo: S(18 09 12 3D 11 17 38 39) = 5F D2 5E 03

# Função F das Etapas DES



| S1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 1 | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 2 | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 3 | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

| S2 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 1 | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 2 | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 3 | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

| S3 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 1 | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 2 | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 3 | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

| S4 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 1 | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 2 | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

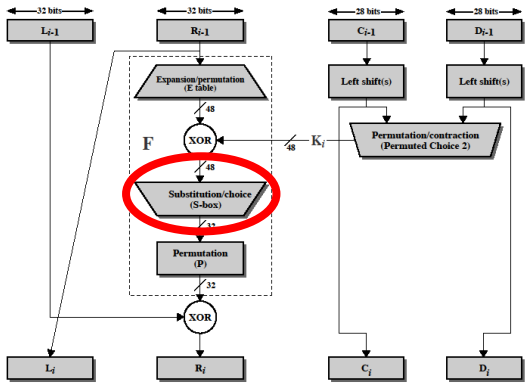



Figure 3.5 Single Round of DES Algorithm

| S5 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 1 | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 2 | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 3 | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

| S6 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 1 | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 2 | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 3 | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

| S7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 1 | 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 2 | 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 3 | 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

| S8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 2 | 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 3 | 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

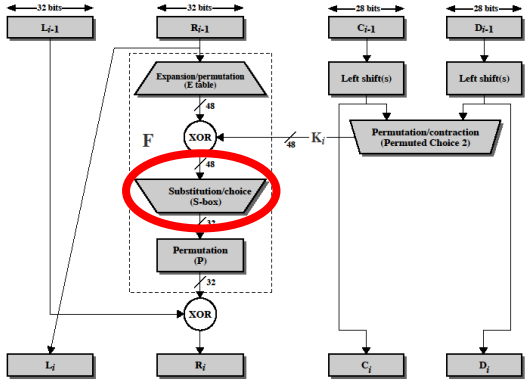



Figure 3.5 Single Round of DES Algorithm

# Substituição: S-Boxes

| S1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 1 | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 2 | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 3 | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

| S2 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 1 | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 2 | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 3 | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

S(18 09 12 3D 11 17 38 39) = 5F D2 5E 03

18 = 011000 (6 bits)
Linha = 00 = 0
Coluna = 1100 = 12
$S_1(18)=5$

09 = 001001 (6 bits)
Linha = 01 = 1
Coluna = 0100 = 4
$S_2(09)=15$

# Tabela de Permutação P

| Função de Permutação (P) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **0** | 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| **8** | 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| **16** | 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| **24** | 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

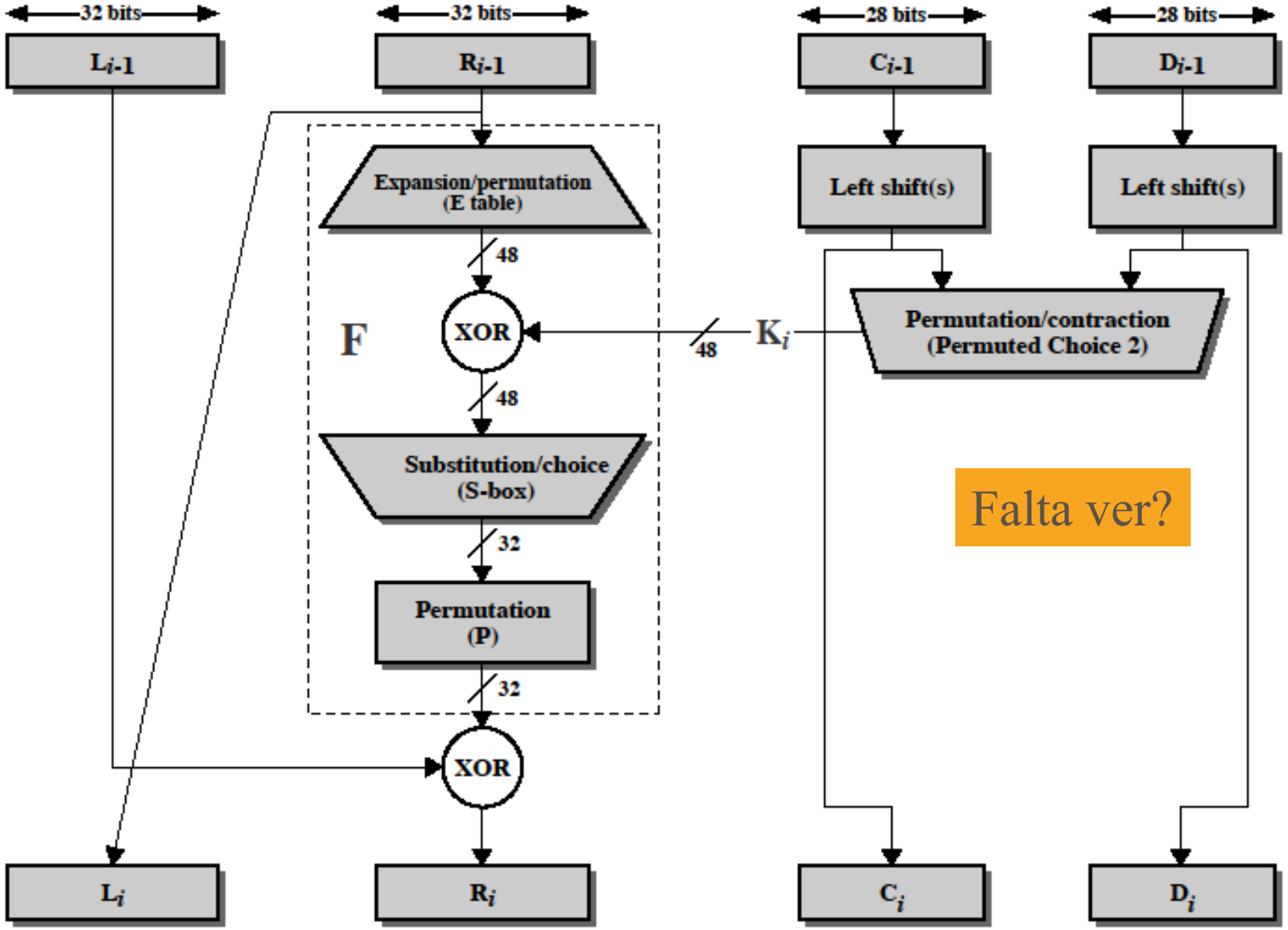


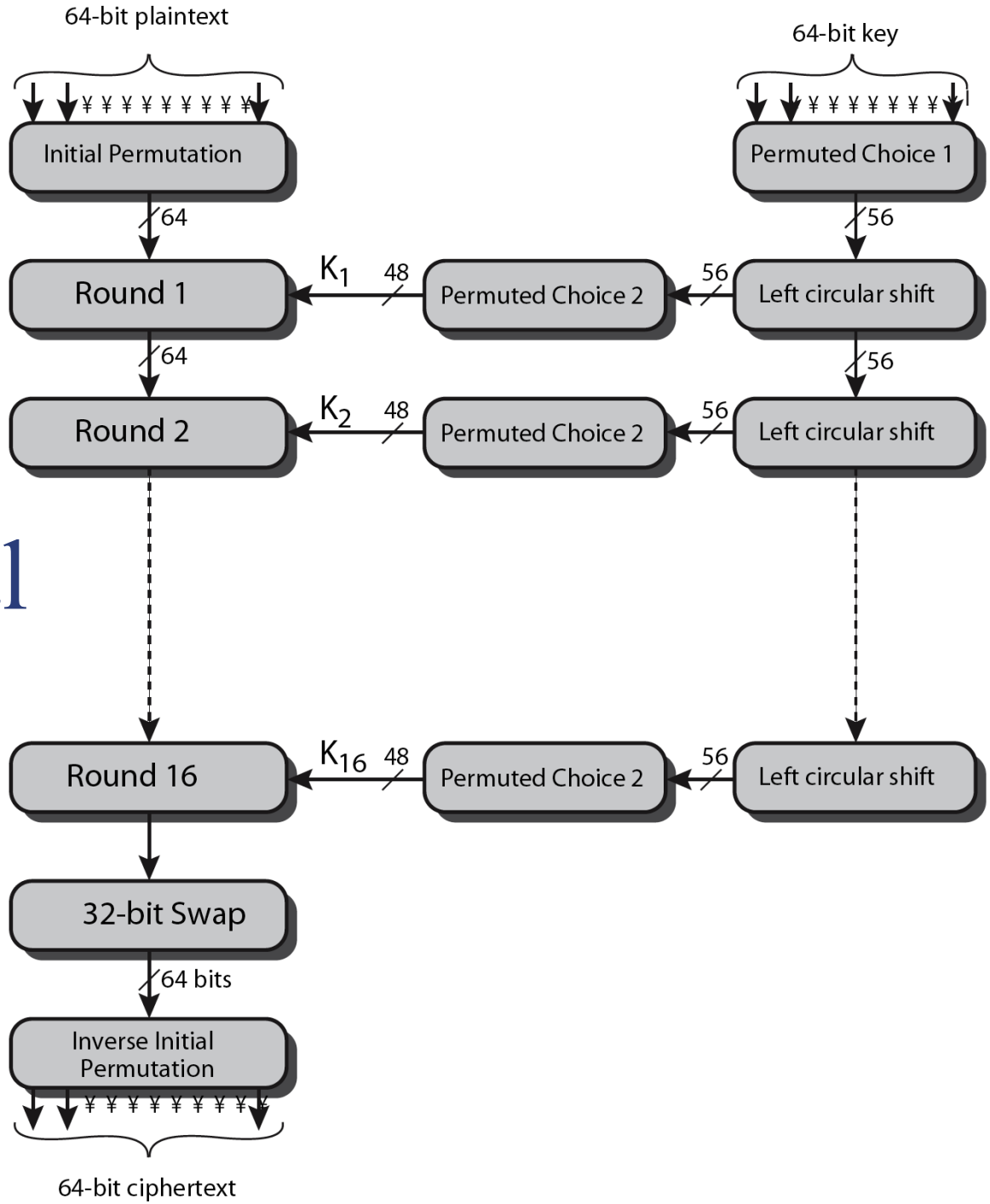

**Figure 3.5 Single Round of DES Algorithm**

# Escalonamento de Chaves DES

- Forma as subchaves usadas em cada etapa
  - permutação inicial de chave (PC-1)
    - seleciona 56-bits e divide em duas metades de 28-bits
  - são 16 etapas consistindo de:
    - rotacionar cada metade separadamente 1 ou 2 posições, dependendo da etapa;
    - selecionar 24-bits de cada metade e permutá-los com PC-2 para uso na função de etapa F

# DES

# Visão Geral



# Escalonamento de Chaves DES

| Escolha Permutada UM (PC-1) | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **0** | 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| **7** | 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| **14** | 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| **21** | 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| **28** | 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| **35** | 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| **42** | 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| **49** | 21 | 13 | 5 | 28 | 20 | 12 | 4 |

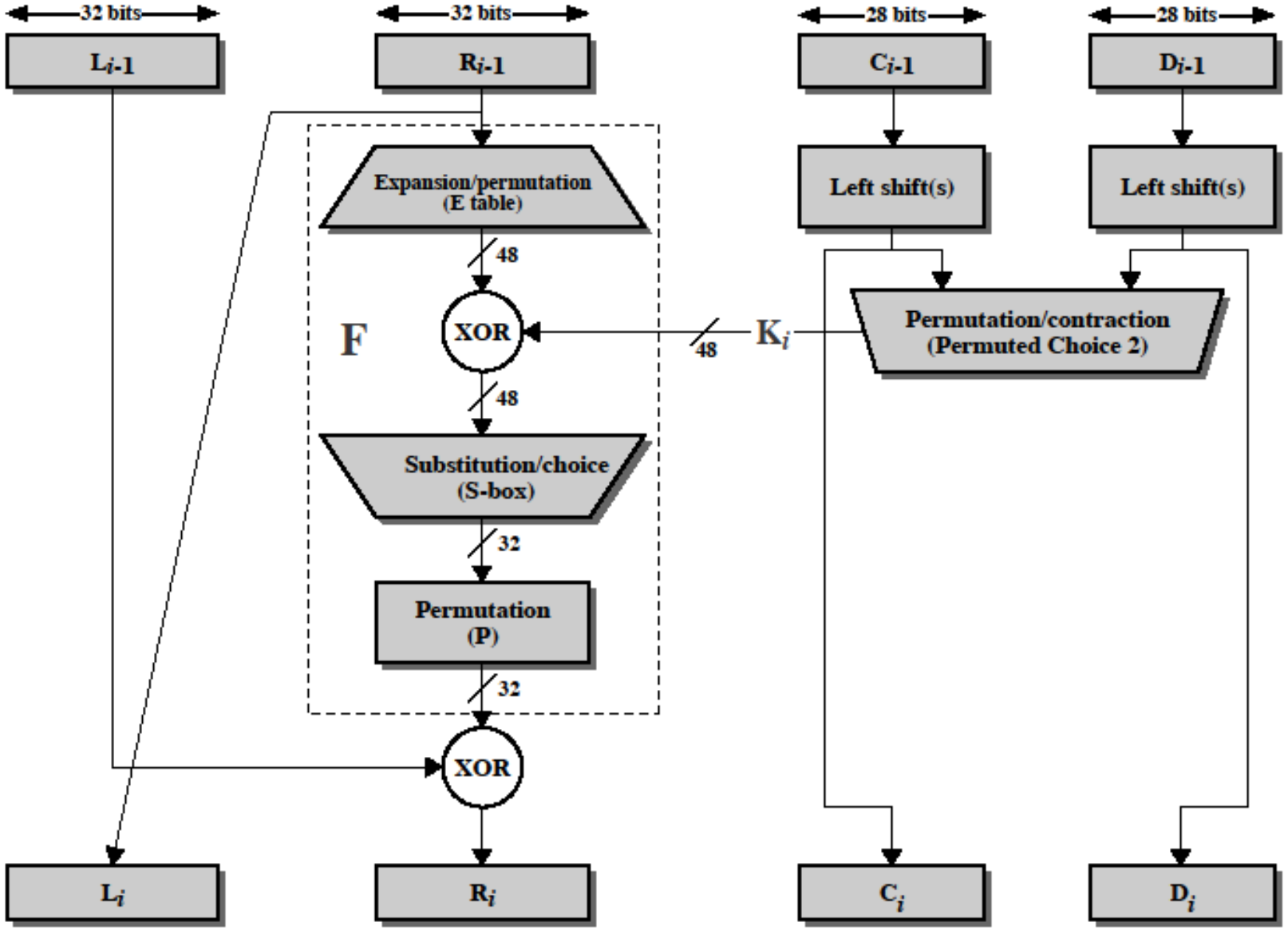



**Figure 3.5 Single Round of DES Algorithm**

# Escalonamento de Chaves DES

| Etapa | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Rotações | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

| Escolha Permutada DOIS (PC-2) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **0** | 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 |
| **8** | 15 | 6 | 21 | 10 | 23 | 19 | 12 | 4 |
| **16** | 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| **24** | 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| **32** | 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| **40** | 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

# Decifragem DES

- Decriptografia deve inverter os passos
- com o projeto de Feistel, basta fazer os passo da criptografia novamente usando as subchaves na ordem inversa ($SK_{16}$ … $SK_1$)

# Efeito Avalanche

- Propriedade desejável da chave do algoritmo
- Uma mudança de um bit na entrada ou chave resulta em mudança em aproximadamente metade dos bits de saída
- DES possui forte avalanche

Software Ilustrativo

# Força do DES – Tamanho da chave

- 56-bit de chave tem $2^{56} = 7.2 \times 10^{16}$ valores
- ataque de força bruta é difícil
- recentes avanços tem mostrado que é possível:
  - em 1997, na Internet, em alguns meses,
  - em 1998 sobre HW dedicado (EFF) em poucos dias,
  - em 1999 combinação acima em 22H
- Ainda pode ser utilizado para reconhecer texto claro,
- mas atualmente deve ser considerado outras alternativas ao DES, tais como 3DES e AES.

# Força do DES – Ataque Analítico

- Atualmente há diversos ataques analíticos ao DES
- Utilizam alguma estrutura interna do cifrador
  - coletando informações sobre criptografias,
  - pode eventualmente recuperar algum/todos bits da chave
  - se necessário, busca exaustivamente os demais bits
- Geralmente são ataques estatísticos
- Inclui:
  - Criptoanálise diferential
  - Criptoanálise linear
  - Ataques relacionados a chave