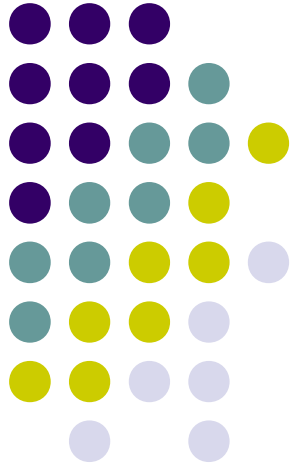
Segurança Computacional

Aula 03: Criptografia, Algoritmos e Criptoanálise

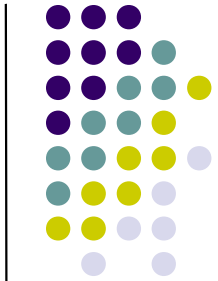
Prof.
Valério Rosset



Apresentação baseada no Livro Criptografia e Segurança de Redes: Princípios e Prática, 4a Ed. de William Stallings.

Criptografia

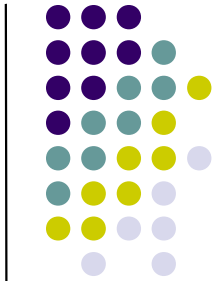
Categorias de cifra



- **Cifras de Bloco:** dividem o texto original em partes iguais chamadas de blocos. Cada bloco é cifrado separadamente, ao final juntam-se os blocos em um único texto cifrado.

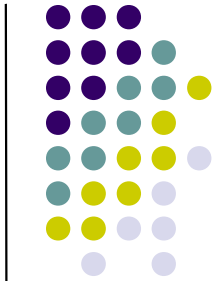
Criptografia

Categorias de cifra



- ***Cifras Sequenciais ou de fluxo***: codificam um fluxo de dados por bit ou bytes de cada vez. Sua qualidade esta ligada ao tamanho da chave que deve, quanto maior a chave maior a dificuldade de revelar a mensagem.

Criptografia
Cifras de Bloco

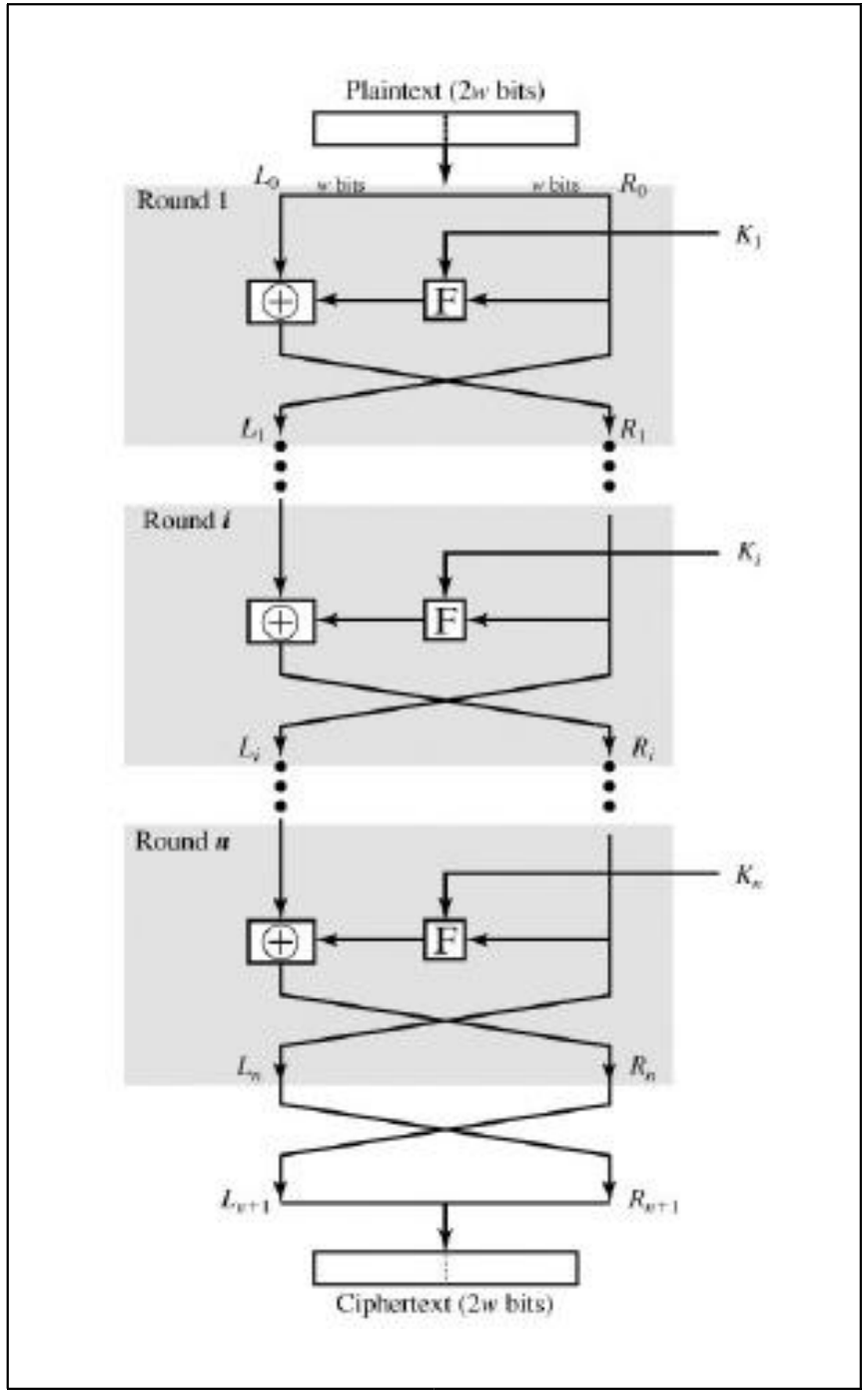


- ***Cifra de Feistel***
  - Feistel propôs uma cifra que combina substituições com permutações.
  - Esse modelo é utilizado pela maioria das cifras de bloco simétrico utilizados.

Criptografia

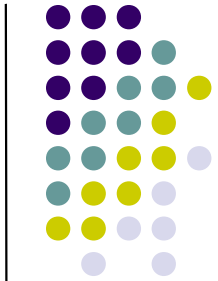
Cifras de Feistel

- Entrada de 2w bits e uma chave K
- Bloco de Texto claro é dividido em 2 metades (L_0, R_0).
- Duas metades passam por n rodadas e são combinados para formar o texto cifrado.
- A realimentação de cada rodada é feita com L e R da rodada anterior + uma chave Ki derivada da chave K.
- F é a função complexa que é aplicada a metade direita dos dados R e depois realiza um OU exclusivo com L.



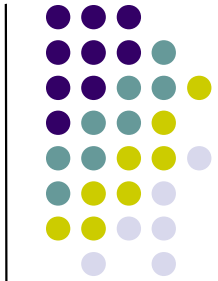
Criptografia

Cifras de Feistel



- **Parâmetros:**
  - **Tamanho do Bloco:** quanto maior mais seguro porém mais lento. 128 bits ideal
  - **Tamanho da chave:** quanto maior mais seguro porém mais lento. Também usa-se 128 bits, mas não ideal.
  - **Numero de rodadas:** esse é o fator crítico desse tipo de cifra. N=16 no DES.
  - **Função F:** quanto mais complexa geralmente poderá ser mais resistente.

Criptografia
Simple DES (S-DES)

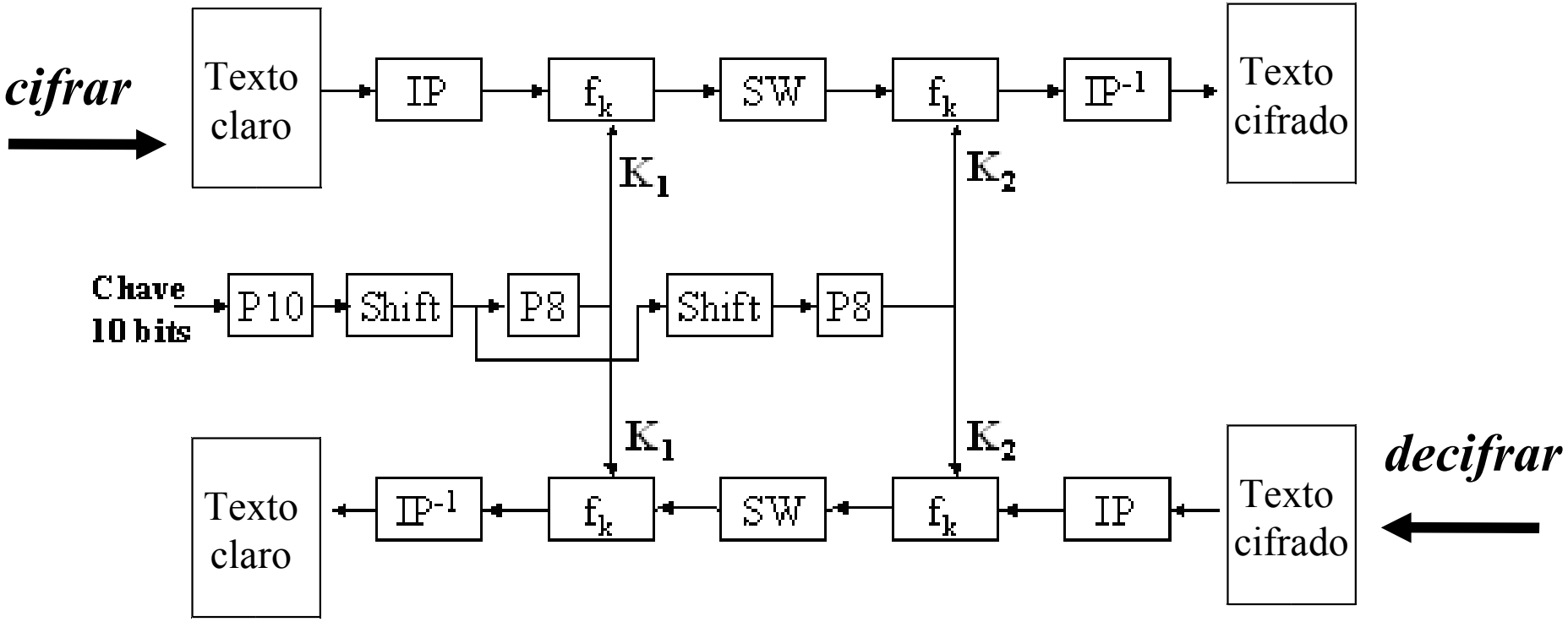


- O S-DES foi criado pelo professor Edward Shaefer da Universidade de Santa Clara com o objetivo de simplificar o ensino do funcionamento do DES.
- **O algoritmo de encriptação envolve cinco funções:**
  - permutação inicial (IP);
  - a função complexa chamada de fk, que envolve permutação e substituição dependente da chave;
  - a simples permutação de troca de duas metade dos dados (SW);
  - a função f_k novamente
  - finalmente é aplicada a função inversa da permutação inicial (IP^{-1}).

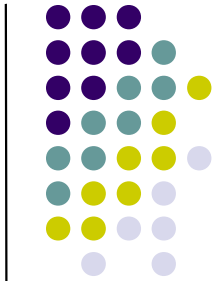
Criptografia

Simple DES (S-DES)

- **Esquema do S-DES** :
  - IP-Permutação Incial, fk – Função complexa, SW – Permutação simples



Criptografia
Simple DES (S-DES)



- **Fórmulas:**

$$\text{texto cifrado} = IP^{-1}\left(f_{k_2}\left(SW\left(f_{k_1}(IP(\text{texto claro}))\right)\right)\right)$$

$$\text{texto claro} = IP^{-1}\left(f_{k_1}\left(SW\left(f_{k_2}(IP(\text{texto cifrado}))\right)\right)\right)$$

Onde:
$$\begin{cases} K_1 = P8(Shift(P10(Key))) \\ K_2 = P8(Shift(Shift(P10(Key)))) \end{cases}$$

Criptografia

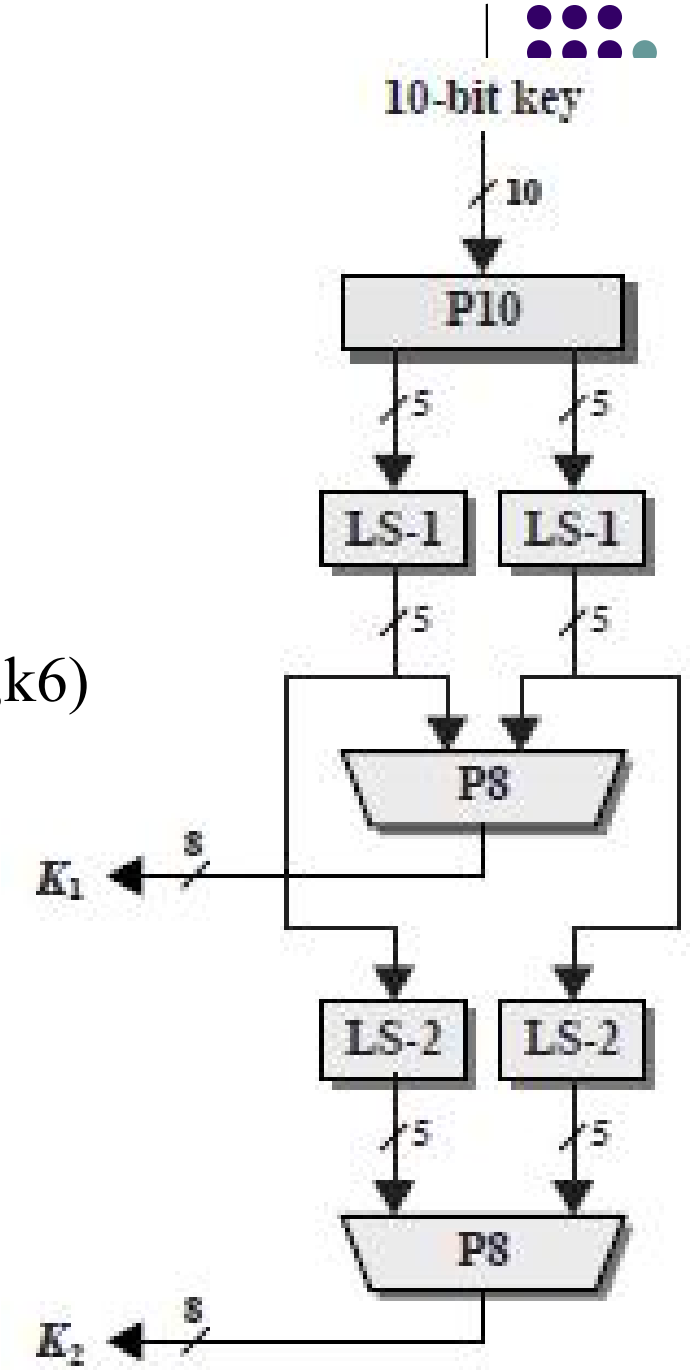
Simple DES (S-DES)

- **Geração da chave**

Chave = (k1,k2,k3,k4,k5,k6,k7,k8,k9,k10)

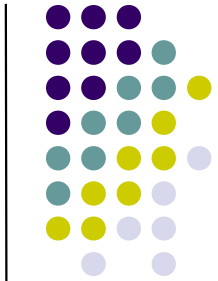
P10(Chave) = (k3,k5,k2,k7,k4,k10,k1,k9,k8,k6)

P10	P8
3 5 2 7 4 10 1 9 8 6	6 3 7 4 8 5 10 9



Criptografia

Simple DES (S-DES)

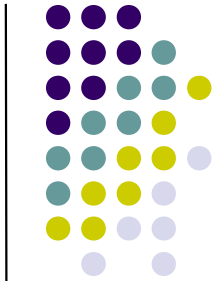


- **Exemplo de geração de chaves**

P10	P8
3 5 2 7 4 10 1 9 8 6	6 3 7 4 8 5 10 9

- **Chave K : 1010000010**
- **K1:**
  - **Permutação inicial (P10)** **1000001100**
  - **Separação** **10000 01100**
  - **Rotação a esquerda LS-1:** **00001 11000**
  - **Aplicação da tabela P8**
  - **O resultado é a sub-chave K1** **10100100**

Criptografia
Simple DES (S-DES)



- **Exemplo de geração de chaves**

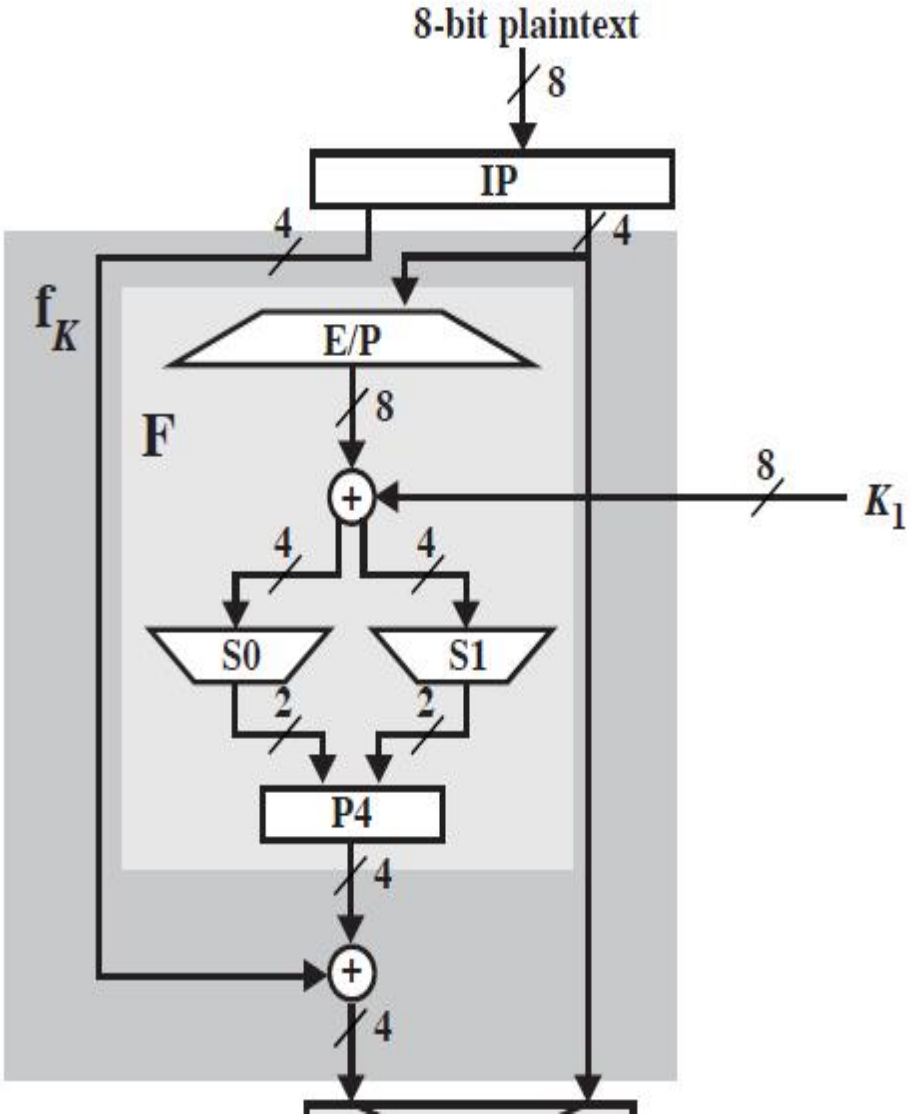
P10	P8
3 5 2 7 4 10 1 9 8 6	6 3 7 4 8 5 10 9

- **Para K2,**
- **pega-se o resultado de LS-1** **00001 11000**
- **Rotação a esquerda LS-2 duas posições** **00100 00011**
- **Aplicação da tabela P8**
- **O resultado é a sub-chave K2 é** **01000011**

Criptografia

Simple DES (S-DES)

- O componente complexo do S-DES é a função Fk,
- Combinação de funções de permutação e substituição.
- L e R são os quatro bits a esquerda e os quatro bits a direita dos 8 bits que entraram na função
- F é a função que executa as operações com os dados R e a sub-chave SKn.



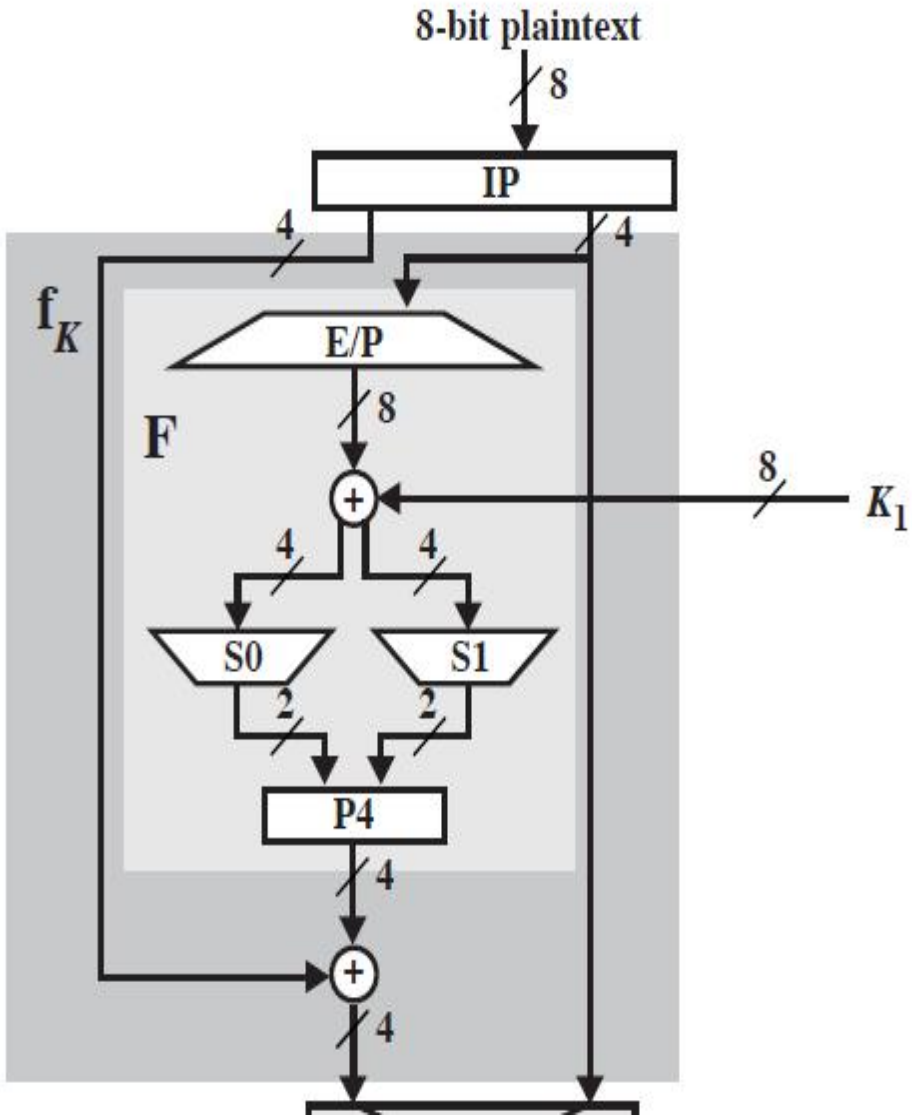
Criptografia

Simple DES (S-DES)

•A permutação inicial (IP) e final (IP^{-1}) que ocorre durante o processo de cifragem e decifragem, dos 8 bits processados, obedece a seguinte tabela:

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

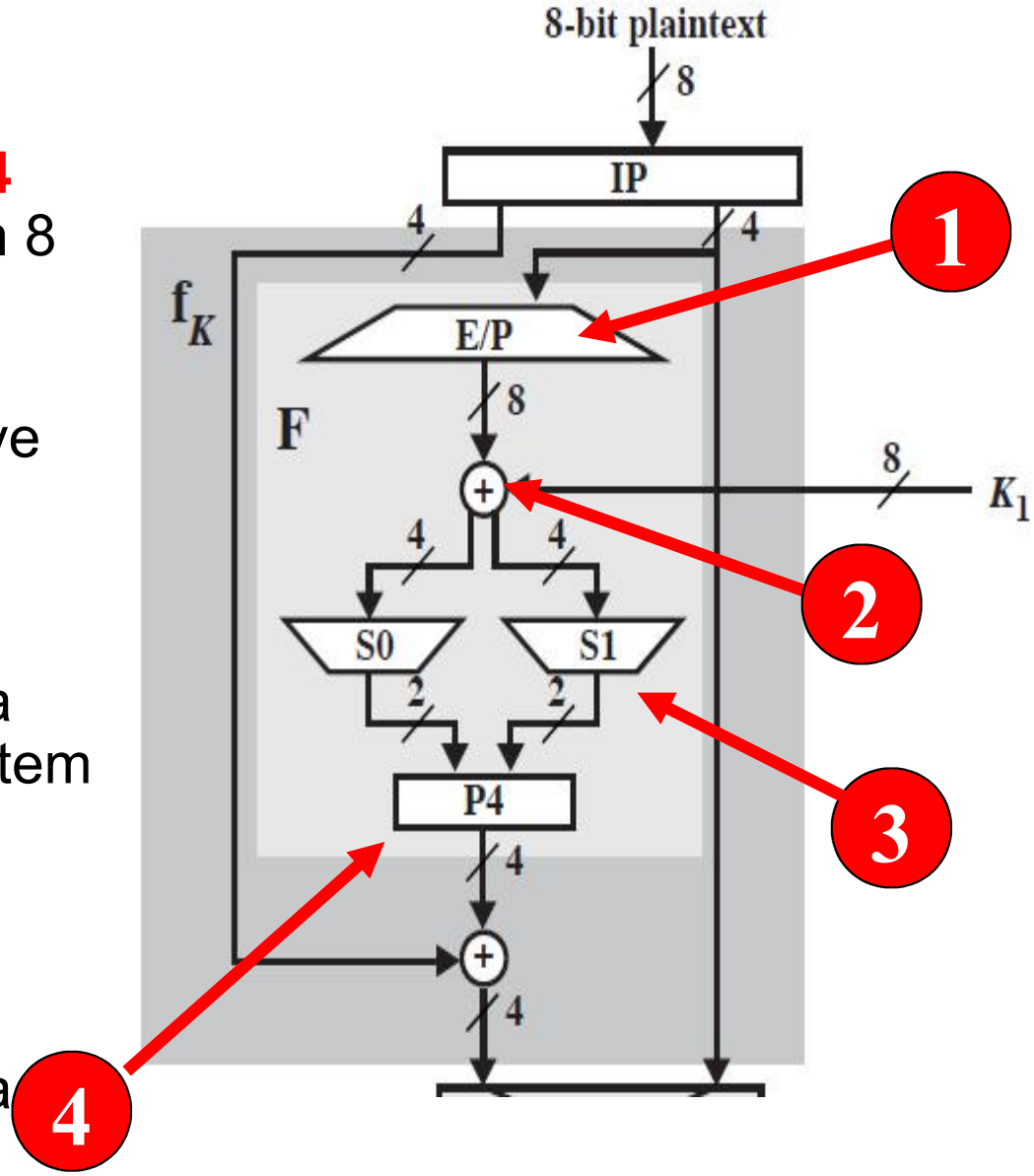


Criptografia

Simple DES (S-DES)

- **A função F(R,SK).**

1. Ocorre uma operação de ***expansão/permutação*** nos **4 bit de R**, transformando-o em 8 bits;
2. É realizada uma operação de **OU** exclusivo com a sub-chave (**K1**);
3. É então **separado em dois grupos** de **4 bits cada**, que passam por uma operação na **caixa S (S0 e S1)**. A caixa S tem uma entrada de 4 bits e uma saída de 2 bits.
4. O **produto da caixa S** é concatenado e sofre uma permutação, de acordo com a régua **P4**.



Criptografia
Simple DES (S-DES)

XOR	1	0
1	0	1
0	1	0

- **Função Fk**

E/P	P4
4 1 2 3 2 3 4 1	2 4 3 1

1) 0101

E/P = 10101010

2) XOR

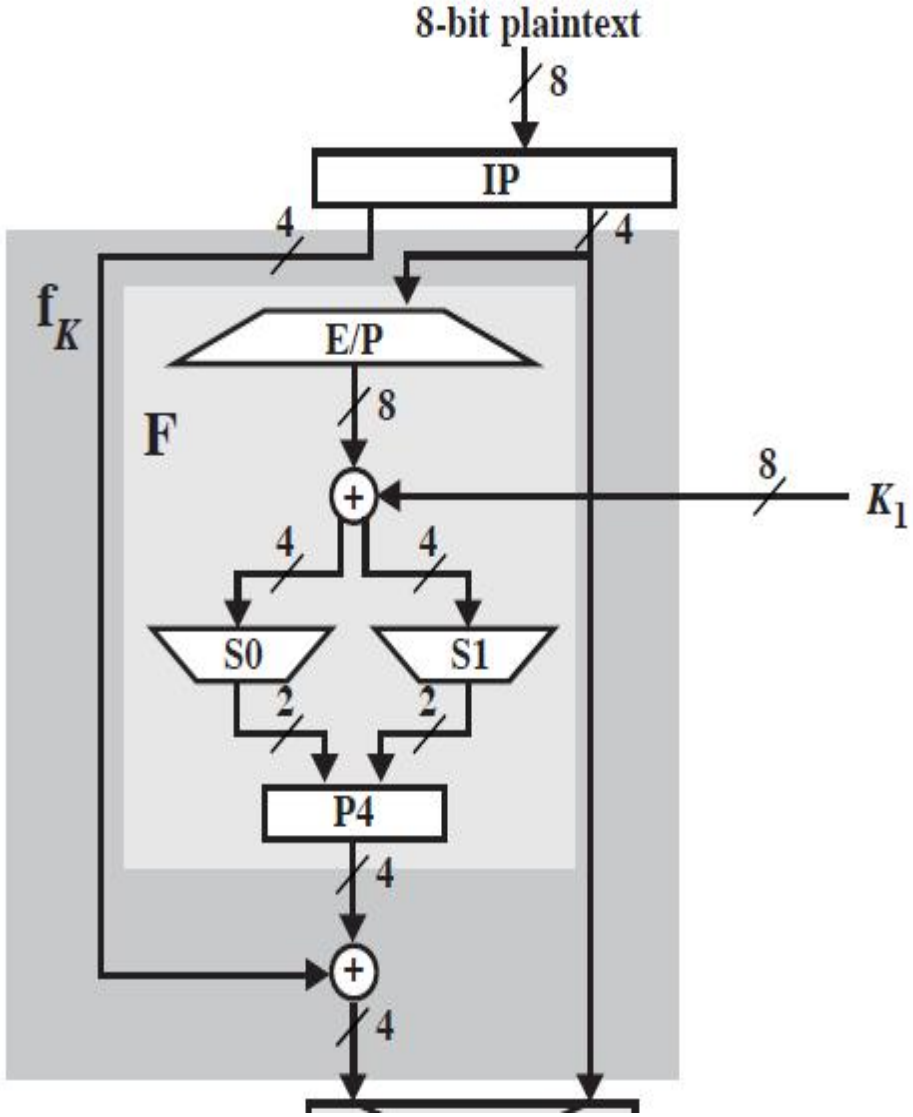
K1= 10000001

R= 00101011

3) 0010 1011

S0 =
1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S1 =
1	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3



Criptografia

Simple DES (S-DES)

XOR	1	0
1	0	1
0	1	0

E/P

4	1	2	3	2	3	4	1

P4

2	4	3	1

3) 0010 1011

00 = 0 11= 3

01= 1 01= 1

S0=00 S1=01

0001

S0 =

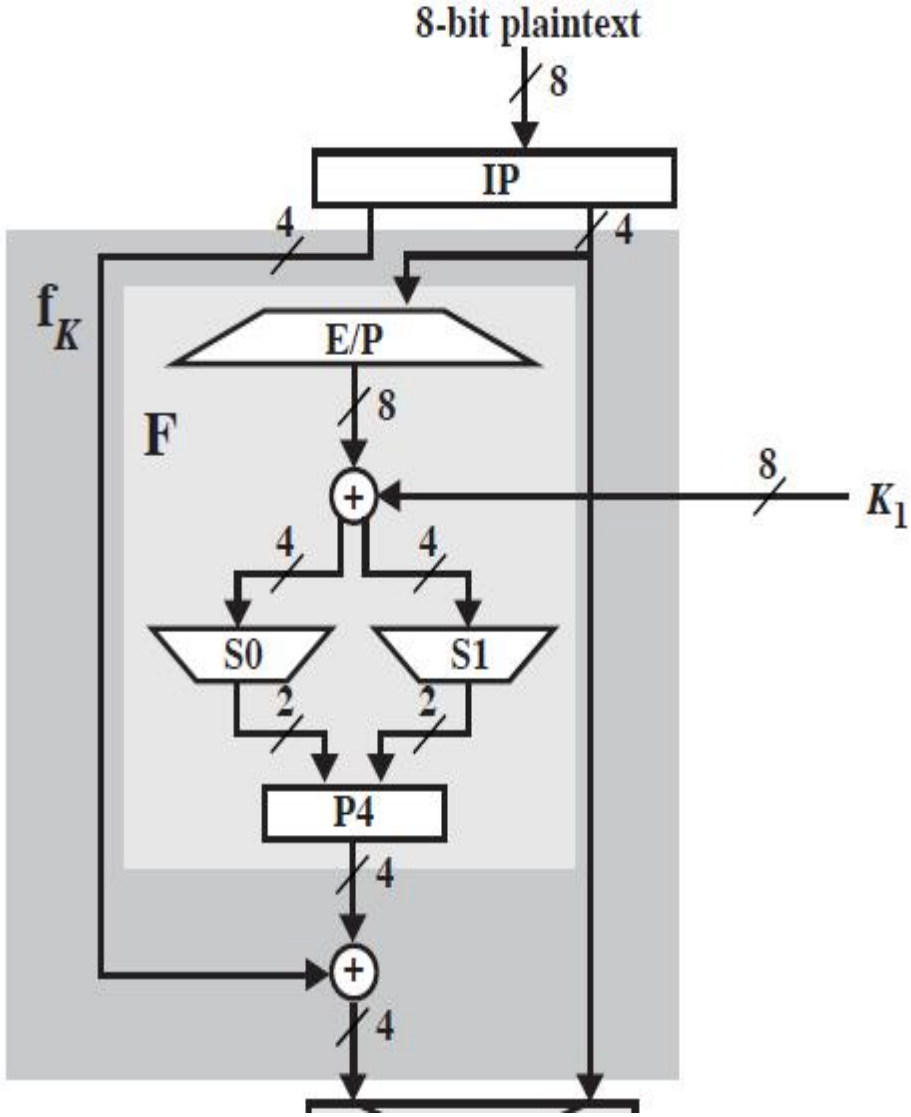
1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S1 =

1	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

4) Entra : 0001

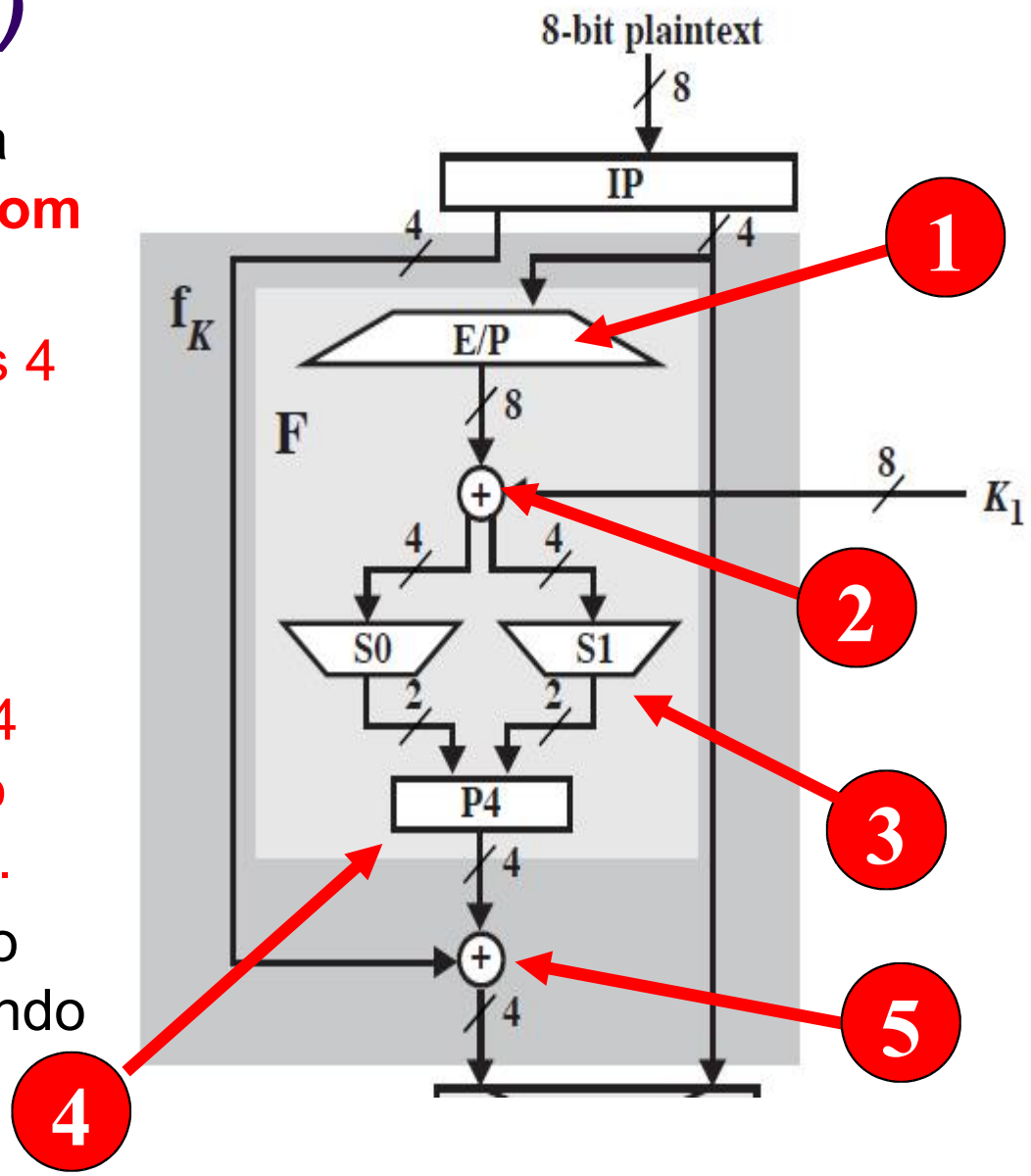
Saída(P4) = **0100**



Criptografia

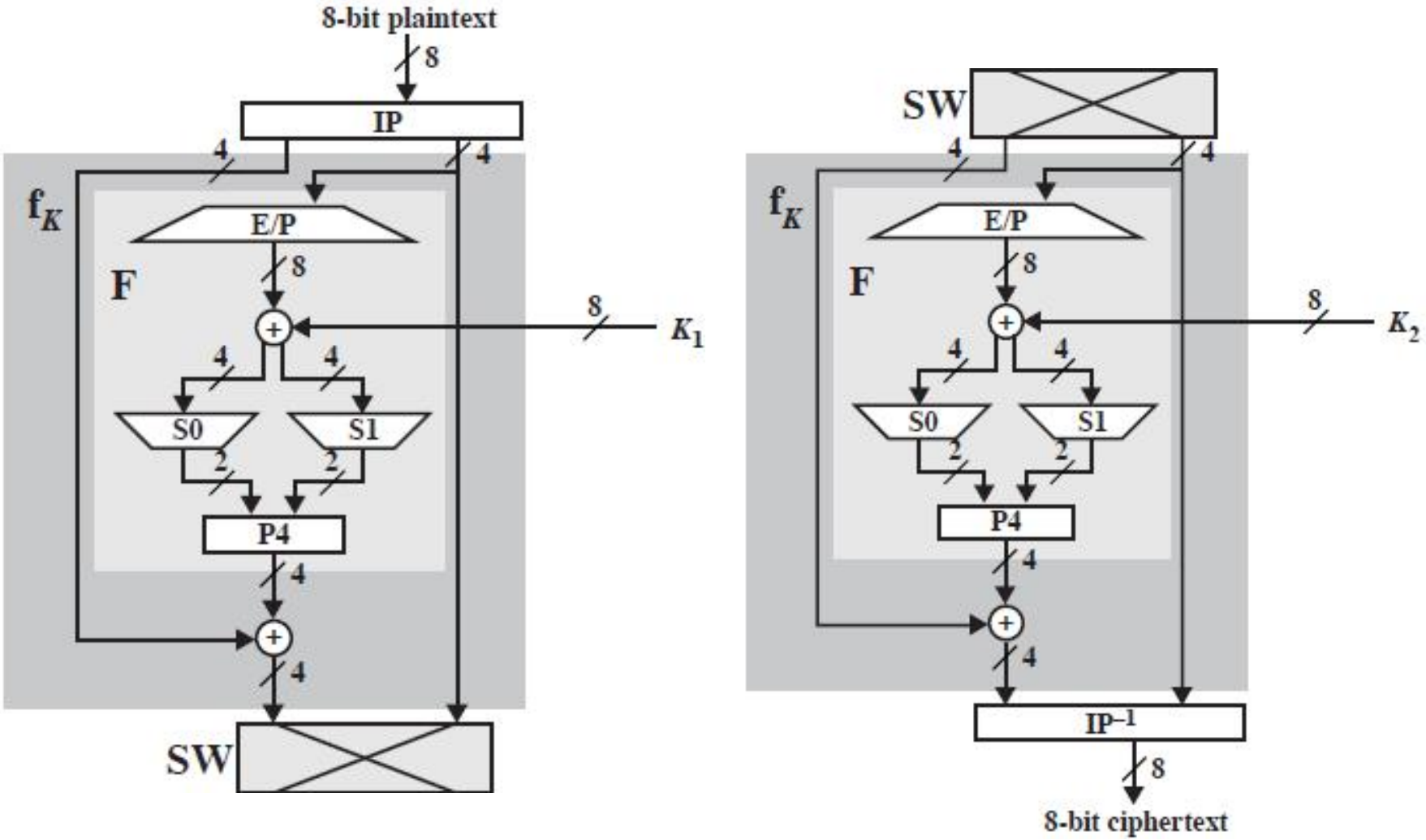
Simple DES (S-DES)

5. O **resultado de P4** sofre uma operação de **OU exclusivo com L**.
6. A função fk somente altera os 4 bits a esquerda, deixando inalterado os 4 bits da direita.
7. O próximo passo é a função Switch. A função SW executa uma **transposição**, onde os 4 bits da direita serão os quatro bits da esquerda e vice versa.
8. Estas mesmas operações são realizadas novamente, utilizando desta vez a **chave K2**.



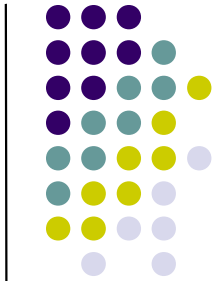
Criptografia

Simple DES (S-DES)



Criptografia

Simple DES (S-DES)



Tarefa (em duplas)

- **Implemente o algoritmo de criptografia S-DES para decifrar um texto (cifrado.seg) fornecido pelo professor. A chave K também será fornecida.**
- **A linguagem deve ser C, C++,Java ou python. Deverá rodar no laboratório e ser apresentado ao professor.**
- **Entrega: a definir**