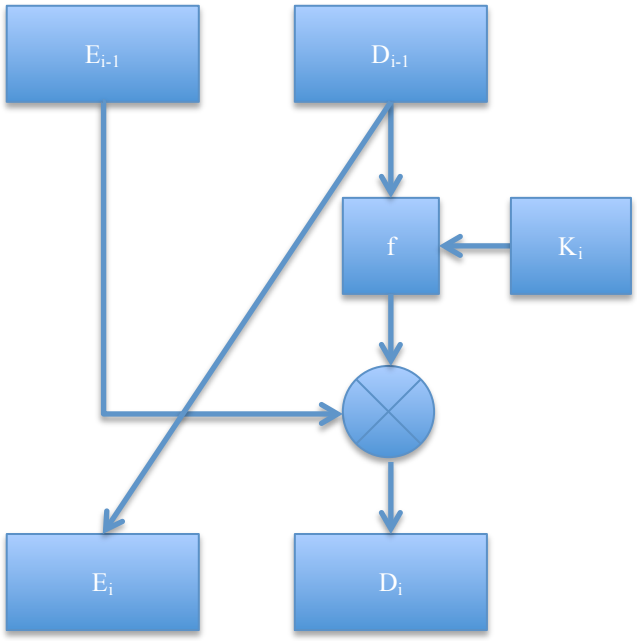
Nesta tarefa vamos implementar uma versão Super Simplificada do DES (SSDES).

Tamanho de bloco: 12 bits

Chave: chave de 9 bits

Subchaves: cada rodada do SSDES utiliza uma subchave de 8 bits derivada da chave original, simplesmente pegando os 8 primeiros bits da chave original e rotacionando os bits para a esquerda. Exemplo: se K=111000111, então K_1=11100011 e K_2=11000111 e K_3=10001111 e assim por diante.

Algoritmo: o bloco de 12 bits é dividido em dois blocos de 6 bits, $\mathbf{E_0}$ e $\mathbf{D_0}$. A *i*-ésima rodada do algoritmo transforma a entrada $\mathbf{E_{i-1}D_{i-1}}$ na saída $\mathbf{E_iD_i}$ usando a subchave $\mathbf{K_i}$, como no diagrama abaixo.



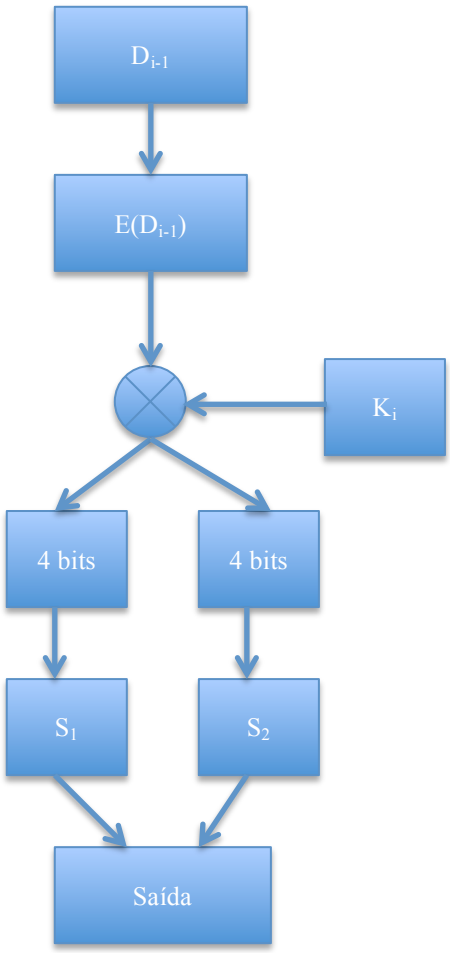
A saída da i-ésima roda é, então:

$E_i = D_{i-1}$

$D_i = E_{i-1}$ XOR $f(D_{i-1},K_i)$

Essa operação é executada por **n** rodadas e produz na saída $\mathbf{E_nD_n}$. O texto cifrado será então $\mathbf{D_nE_n}$. O processo de desencriptação é idêntico, porém as subchaves são utilizadas em ordem reversa.

Função f(D_{i-1},K_i): a função é descrita pelo diagrama abaixo.



A função de expansão $E(D_{i-1})$ recebe 6 bits e produz uma saída com 8 bits da seguinte forma:

D_{i-1}

1	2	3	4	5	6

$E(D_{i-1})$

1	2	4	3	4	3	5	6

Cada S-Box (S_1 e S_2) recebe 4 bits e produz 3 bits de saída. O primeiro bit da entrada seleciona uma linha da tabela de mapeamento e os 3 últimos bis seleciona uma coluna. As S-Boxes encontram-se abaixo:

S_1

101	010	001	110	011	100	111	000
001	100	110	010	000	111	101	011

S_2

100	000	110	101	111	001	011	010
101	011	000	111	110	010	001	100