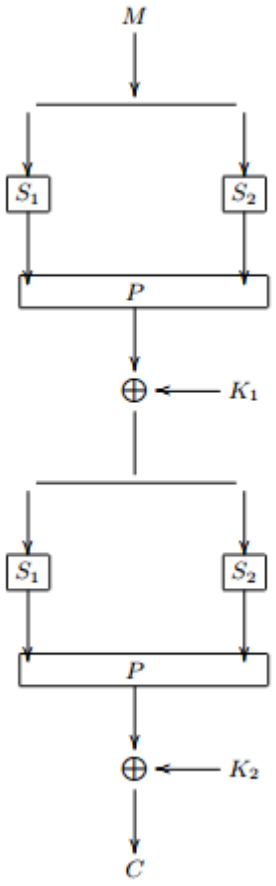
TD 3 : Chiffrement par blocs

On considère le cryptosystème donné dans la figure ci dessous:



Sachant que les boites S1 et S2 sont données par:

X	$[0,0]$	$[1,0]$	$[0,1]$	$[1,1]$
$S_1(X)$	$[1,1]$	$[1,0]$	$[0,0]$	$[0,1]$
$S_2(X)$	$[1,0]$	$[0,1]$	$[1,1]$	$[0,0]$

que les clefs de ronde se déduisent de la clef déchiffrement K = [k1; k2; k3; k4] par K1 = [k1 $\oplus$ k2; k2; k3 $\oplus$ k4; k3];K2 = [k1$\oplus$ k2 $\oplus$ k3; k2 $\oplus$ k3; k3 $\oplus$ k4; k4]

et que la permutation P est définie par $P(1) = 3; P(4) = 2; P(2) = 1; P(3) = 4$: Chiffrez le message $M = [0; 1; 1; 0]$ avec $K = [1; 1; 1; 1]$ et déchiffrez le message $C = [0; 1; 0; 1]$ chiffré avec la même clef.