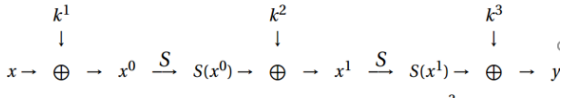
TD 4 : Cryptanalyse différentielle

- **Exercice 1: (Cryptanalyse différentielle)**

On considère le cryptosystème suivant:



Où les x représentent les trois bits. La S-Box est une substitution sur F_2^3. Trouvez la condition pour la sécurité parfaite/imparfaite avec les probabilités.

- **Exercice 2: (Chiffrement par bloc et fonction de compression)**

Soit E : $\{0,1\}^n\{0,1\}^n \to \{0,1\}^n$ un système de chiffrement par blocs qui utilise des clés de bits pour chiffrer des messages de n bits. Montrer que les trois fonctions de compression F_1, F_2 et F_3 ne sont pas résistantes à la pré-image.

- f_1: $\{0,1\}^n\{0,1\}^l$: $f_1(h,m) = E_m(h)$
- f_2: $\{0,1\}^n\{0,1\}^l$: $f_2(h,m) = E_h(m) \oplus h(avec \;\; l = n)$
- f_3: $\{0,1\}^n\{0,1\}^l$: $f_3(h,m) = E_m(h) \oplus m(avec \;\; l = n)$

par bloc.png