(4.2) Question de sécurité encore

- (1) $Dec_{k_i}(x_1) \stackrel{?}{=} y_1$ où (x_1, y_1) paire clair/chiffré.

  $i = 1, \ldots, 2^{56} - 1$.

Trouver k_i.

il se peut que égalité dans (1), mais k_i est une fausse clé.

Théorème Soit un B-cryptage dont la taille de clé est x, de taille de cryptage n et soit $(x_1, y_1), \ldots, (x_t, y_t)$ paire clair/chiffré. La moyenne de fausse clés réalisant (1) est 2^{x-tn}.

- On augmente la sécurité soit en cryptant + sieurs fois! ou la technique 'key whitening' (KW):

- Déf (KW):

  cryptage : $y = e_{k,k_1,k_2}(x) = e_k(x \oplus k_1) \oplus k_2$

  décryptage : $x = e^{-1}_{k,k_1,k_2}(y) = e^{-1}_k(y + k_2) \oplus k_1$.