cette attaque marche théoriquement par le résultat du paradoxe des anniversaires, appliqué ici,

Soit t messages $(x_1, \dots, x_t)$ doit produire Oscar tels que $h(x_i) = h(x_j)$. $\bar{m}$ x_i message de taille n:

$$\mathbb{P}(\text{pas collision}) = \prod_{i=1}^{t-1} \left(1 - \frac{i}{2^n}\right)$$

Or $\lambda = 1 - \mathbb{P}(\text{pas collision})$

$$\simeq 1 - e^{t(t-1)/2^{n+1}}$$

$t \gg 1 \Rightarrow$ $$\boxed{t \simeq 2^{(n+1)/2} \cdot \left(\ln\left(\frac{1}{1-\lambda}\right)\right)^{1/2}} \quad (1).$$

Par ex: $n = 80$ bits.

$t \simeq 2^{80/2}$ bits. ☒

Exercice. Montrer en détail (1).

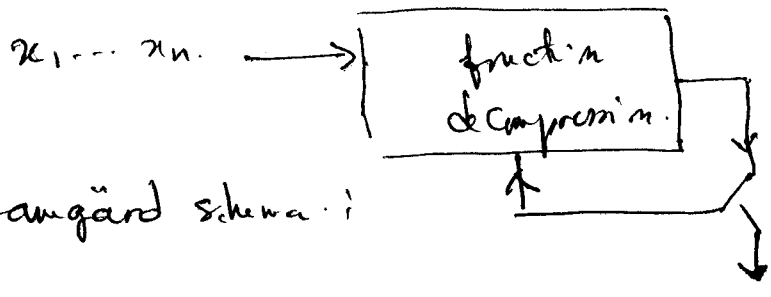
§ 4.2.2. Construction de fonctions de hachage.

Deux manières:

(A) Fonctions Dédiées: fonctions spécifiques pour le hachage.

(B) Fonctions Basé sur le B-cryptage: DES, AES,

Comme suit: x = message = $x_1 \cdots x_n$ divisé en bloc.



Merkle-Damgård schema: