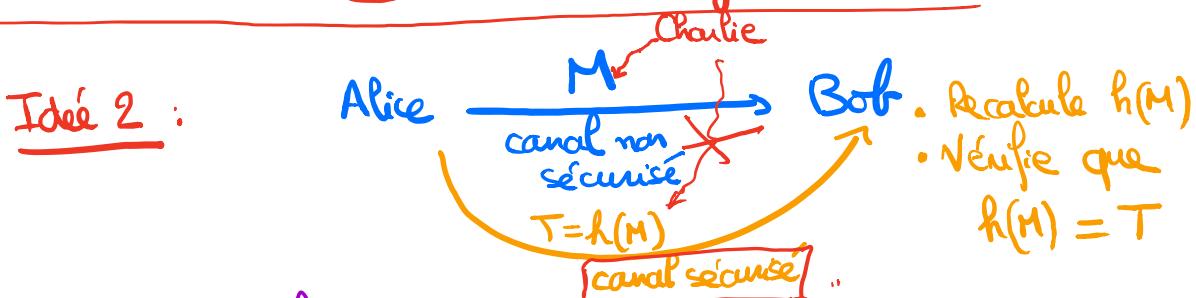
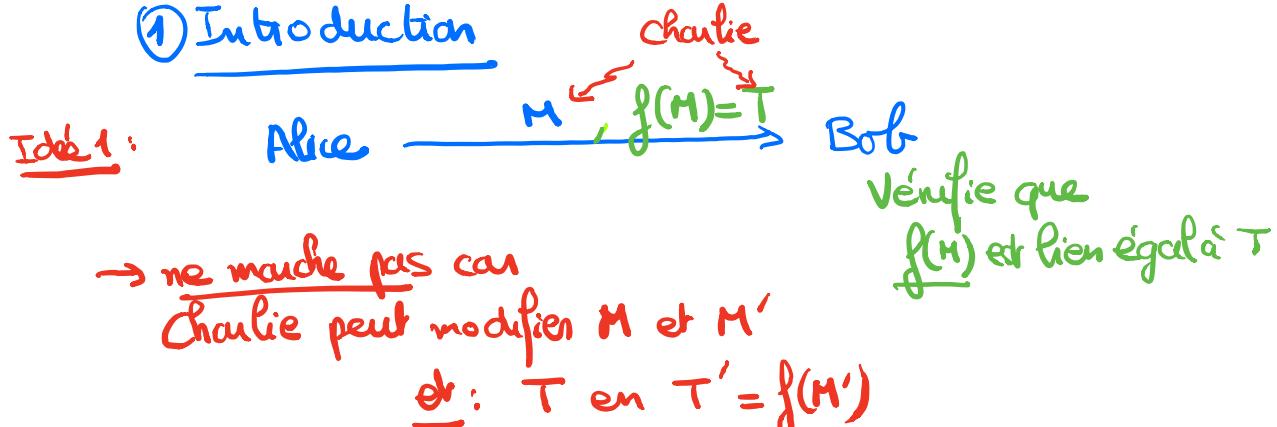


## ch 3 : Intégrité des données

### I] Fonctions de hachage

#### ① Introduction



ex:  $\begin{cases} \text{canal non sécurisé} = \text{mail} \\ \text{canal sécurisé} = \text{SMS, voix, ...} \end{cases}$

ex:  $M$  = contenu du disque dur

En pratique, les fonctions  $h$  qui vont convenir pour cet objectif (garantir l'intégrité) vont être les fonctions de hachage

#### ② Définition des fonctions de hachage

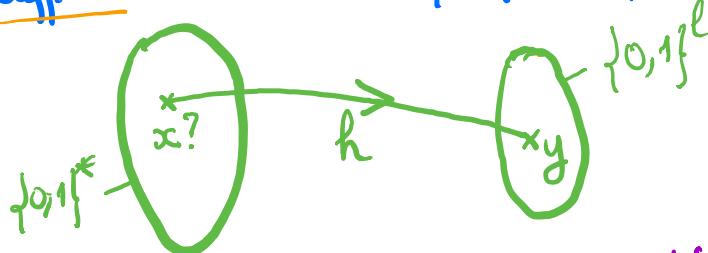
$$h: \underbrace{\{0,1\}^*}_{\text{message de taille quelconque}} \longrightarrow \underbrace{\{0,1\}^l}_{\text{valeur de } l \text{ bits}} \text{ avec } l \text{ fixé}$$

$$\{0,1\}^* = \bigcup_{n \geq 0} \{0,1\}^n$$

messages de  $n$  bits  
(il y en a :  $2^n$ )

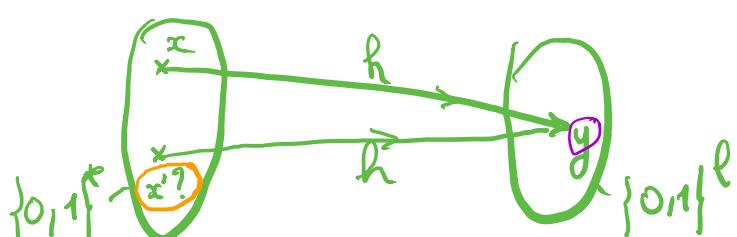
Définition: Une fonction  $h: \{0,1\}^* \rightarrow \{0,1\}^l$  ( $l$  fixé) est appelée fonction de hachage si elle vérifie les 3 propriétés suivantes:

P1)  $h$  est à sens unique (one-way): si  $y \in \{0,1\}^l$ , il est calculatoirement difficile de trouver  $x \in \{0,1\}^*$  tel que  $h(x) = y$



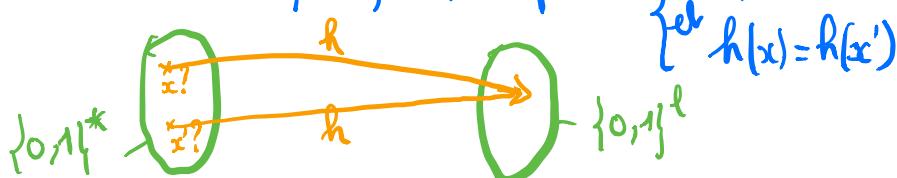
P2)  $h$  est à collisions faibles difficiles (second-preimage resistant):

Si  $x \in \{0,1\}^*$  et  $y = h(x)$ , alors il est calculatoirement difficile de trouver  $x' \in \{0,1\}^*$  tel que  $\begin{cases} x' \neq x \\ h(x') = y \end{cases}$

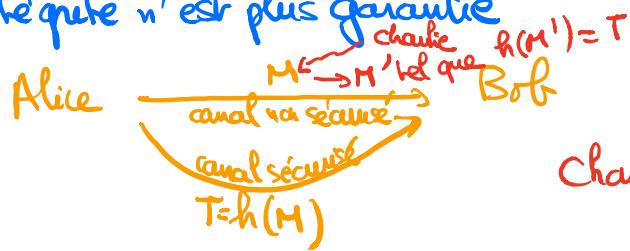


P3)  $h$  est à collisions fates difficiles (collision-resistant):

Il est calculatoirement difficile de trouver  $x \in \{0,1\}^*$  et  $x' \in \{0,1\}^*$  tels que  $\begin{cases} x \neq x' \\ h(x) = h(x') \end{cases}$



Remarque: Si P1) n'était pas réalisée (i.e.  $h$  n'est pas à sens unique)  
l'intégrité n'est plus garantie



Charlie obtient  
 $T = h(M)$

- Trouve un message  $M'$  tel que  $h(M') = T$

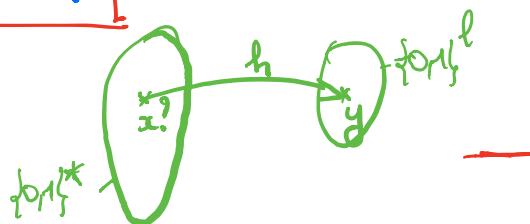
• Idem si P2) n'était pas réalisée

par exemple Alice pourrait construire deux messages  $M$  et  $M'$  ( $\neq M$ ) tels que  $h(M) = h(M')$

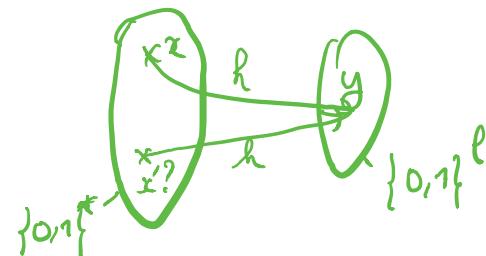
puis envoyer  $M$  à Bob, et peut-être ensuite avoir envoyé  $M'$

Remarque:  $P3 \Rightarrow P2 \Rightarrow P1$

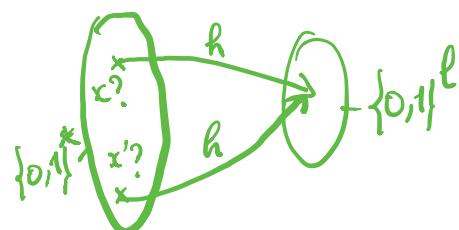
Savoir résoudre le pb de P1



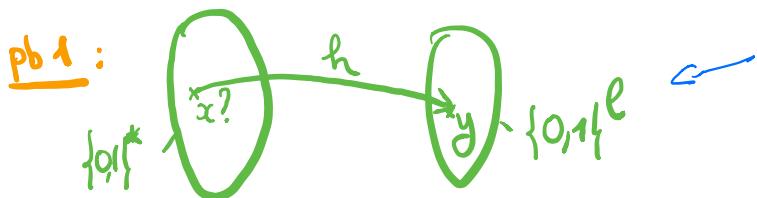
Savoir résoudre le pb de P2



Savoir résoudre le pb de P3



## Complexité des 3 problèmes sous-jacents



Algorithme générique pour trouver  $x$  tel que  $h(x) = y$

[ On tire aléatoirement des messages  $x \in \{0,1\}^*$   
jusqu'à ce que  $\boxed{h(x) = y}$  ]

Analyse de la complexité : probabilité de succès pour un tirage de  $x$

$$P = \frac{1}{2^l}$$

Remarque :  $\therefore$  avec proba  $\frac{1}{6}$

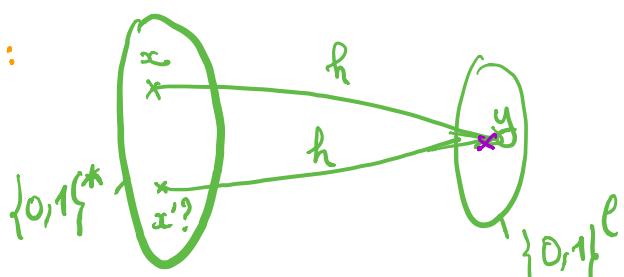
$\rightarrow \simeq 6$  tirages en moyenne pour tomber sur  $\therefore$

$\Rightarrow$  l'algorithme a une complexité de  $\boxed{O(2^l)}$   
en moyenne

$\rightarrow$  pour que ce pb soit calculablement difficile (i.e que la P1 soit vraie), il suffit de prendre  $\underline{l \geq 80}$

(si on considère que  $2^{80}$  est inatteignable pour un attaquant)

pb 2 :



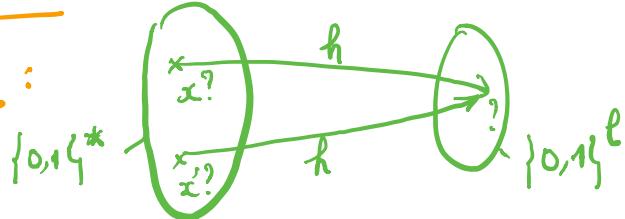
Algorithme générique : on tire  $x'$  aléatoirement (tel que  $x' \neq x$ )  
jusqu'à obtenir  $\boxed{h(x') = y}$

$$\text{prob de succès} = \frac{1}{2^l}$$

$\Rightarrow$  complexité  $\boxed{\mathcal{O}(2^l)}$  en moyenne

→ pour que  $P_2$  soit nulle (i.e. le pb2 est calculatoirement difficile), il suffit de prendre  $l \geq 80$

pb3 :



Algorithm générique

On tire aléatoirement des messages  
 $x_1, x_2, x_3, \dots, x_k \in \{0,1\}^k$   
et on calcule leurs images  
 $y_1 = h(x_1), y_2 = h(x_2), \dots, y_k = h(x_k)$   
jusqu'à ce qu'il apparaisse une relation  
du type  $\boxed{y_i = y_j}$  (avec  $i \neq j$ )

collision

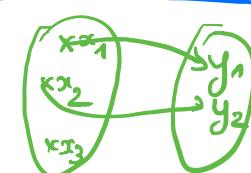
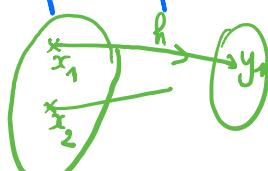
$P$  = probabilité de succès (en fonction de  $l$  et de  $k$ )

- $P_1$  = probabilité que le 1<sup>er</sup> tirage ne provoque pas de collision  
 $= 1$
- $P_2$  = probabilité que le 2<sup>ème</sup> tirage ne provoque pas plus de collision

$$P_2 = \frac{2^l - 1}{2^l} = 1 - \frac{1}{2^l}$$

$$P_3 = \frac{3^{\text{ème}}}{P_2}$$

$$P_3 = \frac{2^l - 2}{2^l} = 1 - \frac{2}{2^l}$$



$$\bullet P_B = \frac{\text{femmes}}{2^l} = \frac{2^l - (k-1)}{2^l} = 1 - \frac{k-1}{2^l}$$

Probabilité que les  $k$  tirages ne provoquent pas de collision

$$1-P = P_1 \times P_2 \times P_3 \times \dots \times P_k$$

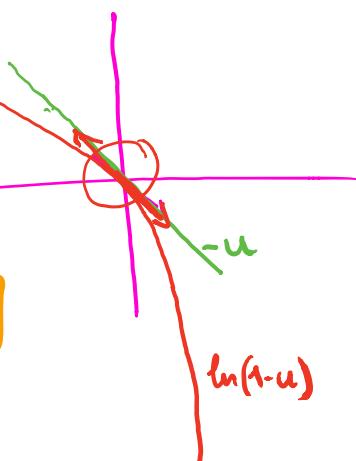
$$1-P = 1 \times \left(1 - \frac{1}{2^l}\right) \times \left(1 - \frac{2}{2^l}\right) \times \dots \times \left(1 - \frac{k-1}{2^l}\right)$$

Simplifions cette formule

$$\ln(1-P) = \sum_{u=0}^k \ln\left(1 - \frac{u}{2^l}\right) + \ln\left(1 - \frac{2}{2^l}\right) + \dots + \ln\left(1 - \frac{k-1}{2^l}\right)$$

$$\boxed{\ln(1-u) \approx -u} \quad (u \text{ petit})$$

$$\begin{aligned} \Rightarrow \ln(1-P) &\approx -\frac{1}{2^l} - \frac{2}{2^l} - \dots - \frac{k-1}{2^l} \\ &\approx -\frac{1}{2^l} \underbrace{\left[1+2+3+\dots+(k-1)\right]}_{=\frac{k(k-1)}{2}} \end{aligned}$$



$$\ln(1-P) \approx -\frac{k(k-1)}{2 \times 2^l} \quad \leftarrow$$

$$\Rightarrow 1-P \approx e^{-\frac{k(k-1)}{2 \times 2^l}}$$

$$\boxed{P \approx 1 - e^{-\frac{k(k-1)}{2 \times 2^l}}} \quad (1)$$

si  $k \rightarrow +\infty$   
P  $\rightarrow 1$   
si  $l \rightarrow +\infty$   
P  $\rightarrow 0$

$$\underline{k(l-1)} \simeq -2 \times 2^l \ln(1-P)$$

$$k^2 \simeq 2 \times 2^l \ln \frac{1}{1-P}$$

$$\Rightarrow k \simeq 2^{l/2} \sqrt{2 \ln \frac{1}{1-P}} \quad (2)$$