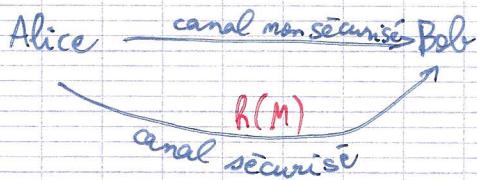


I. Fonctions de hachage

Alice $M, h(M)$ \rightarrow Bob

Si M et $h(M)$ sont changés par M' et $h(M')$ \rightarrow problème



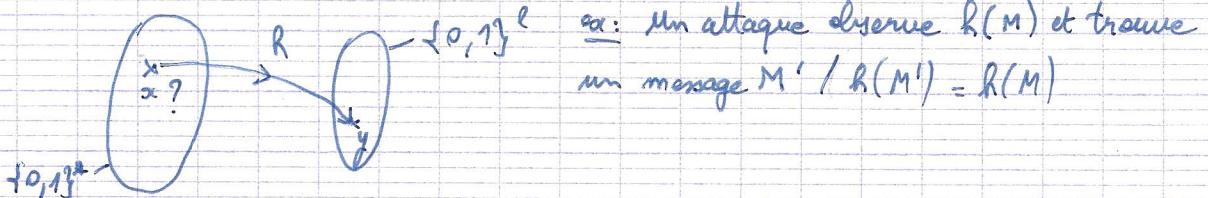
Contraintes :

- $h(M)$ est "petit"
- il doit être difficile de construire 2 messages M et M' ayant la même image par h .

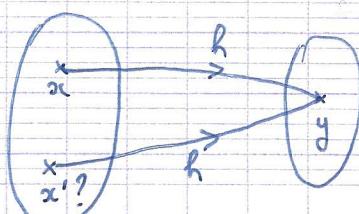
Définition: $h: \{0,1\}^* \rightarrow \{0,1\}^l$ (l est un entier fixe)

est appelée fonction de hachage si elle vérifie les 3 propriétés suivantes :

- h est à sens unique (one way). étant donné $y \in \{0,1\}^l$ il est calculatoirement difficile de trouver $x \in \{0,1\}^*$ / $h(x) = y$.



- h est à collisions faibles difficiles (second pre image résistant). étant donné $x \in \{0,1\}^*$ et $y = h(x)$, il est calculatoirement difficile de trouver $x' \in \{0,1\}^*$ tel que $\begin{cases} x' \neq x \\ h(x') = y \end{cases}$



- h est à collisions fortes difficiles (collision résistant) : il est calculatoirement difficile de trouver $x \in \{0,1\}^*$ et $x' \in \{0,1\}^*$ tels que $\begin{cases} x \neq x' \\ h(x) = h(x') \end{cases}$

P1 (on ne fixe pas à l'avance y)

P1 résolution

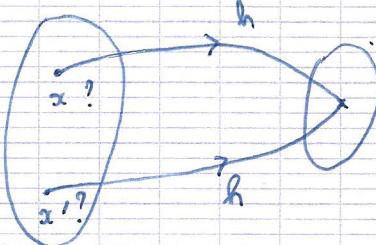
\uparrow
P1

P2 résolution

\uparrow
P2

P3 résolution

\downarrow
P3



ex: Alice prétend avoir envoyé x alors qu'elle a envoyé x'

P3 plus simple que P2 et P1

P3 est la plus cruciale

- Attaque de résolution P1 : Algo 1:

Générer $x \in \{0,1\}^*$ aléatoire jusqu'à ce que $h(x) = y$
probabilité de succès (pour chaque tirage de x) = $\frac{1}{2^l}$
complexité $O(2^l)$ avec $l > 80$

- Attaque de résolution P2 : Algo 2:

Générer $x' \in \{0,1\}^*$ aléatoire et $\neq x$ jusqu'à ce que $h(x') = y$
probabilité de succès = $\frac{1}{2^l}$ avec $l > 80$

- Attaque de résolution P3 : Algo 3:

Générer des messages x_1, x_2, \dots, x_m et calculer $y_1 = h(x_1), \dots, y_m = h(x_m)$ jusqu'à trouver une égalité du type $y_i = y_j$ (avec $i \neq j$)

P = probabilité que x_1, \dots, x_m donnent une collision

$1 - P$ = probabilité que x_1, \dots, x_m ne donnent pas de collision.

p_1 = probabilité que le tirage de x_1 ne donnent pas de collision $p_1 = \frac{1}{2^{l-1}}$

$p_2 = \frac{1}{2^l}$

$p_3 = \frac{1}{2^l}$

\vdots

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

$$p_m = 1 - \frac{m-1}{2^l}$$

$$\Rightarrow 1 - P = p_1 \times p_2 \times p_3 \times \dots \times p_m$$

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

$$\ln(1 - P) = \ln 1 + \ln\left(1 - \frac{1}{2^e}\right) + \ln\left(1 - \frac{2}{2^e}\right) + \dots + \ln\left(1 - \frac{m-1}{2^e}\right)$$



on $\ln(1-m) \approx -m$

$$\text{D'autre part } \ln(1-P) = \frac{-1}{2^e} - \frac{2}{2^e} - \dots - \frac{m-1}{2^e} = \frac{-1}{2^e} [1+2+\dots+(m-1)] \\ = \frac{-1}{2^e} \times \frac{m(m-1)}{2}$$

$$\text{D'autre part } \ln(1-P) \approx \frac{-m(m-1)}{2^e \cdot 2} \Rightarrow m(m-1) = 2 \times 2^e \ln\left(\frac{1}{1-P}\right)$$

$$-\ln(a) = \ln\left(\frac{1}{a}\right)$$

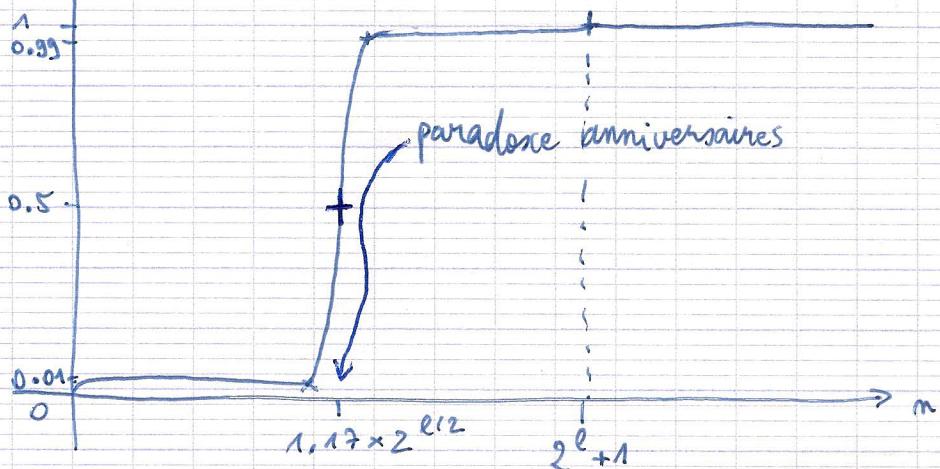
$$1 - P = \exp\left(-\frac{m(m-1)}{2^e \cdot 2}\right)$$

$$\Rightarrow m^2 = 2 \times 2^e \ln\left(\frac{1}{1-P}\right)$$

$$P = 1 - \exp\left(-\frac{m(m-1)}{2^e \cdot 2}\right)$$

$$\text{D'autre part } m = 2^{e/2} \sqrt{2 \ln\left(\frac{1}{1-P}\right)}$$

collision P



$$P = \frac{1}{2} \text{ quand } m = 2^{e/2} \sqrt{2 \ln 2} \approx 1.17 \times 2^{e/2}$$

$$P = 0.99 \text{ quand } m = 2^{e/2} \sqrt{2 \ln 100} \approx 3 \times 2^{e/2}$$

$$P = 0.01 \text{ quand } m = 2^{e/2} \sqrt{2 \ln \frac{100}{99}}$$

complexité de l'algo 3 $\rightarrow O(2^{e/2}) \rightarrow$ on doit prendre $e \geq 160$

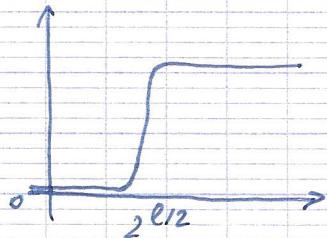
$$2^{e/2} \rightarrow 80 \text{ donc } e \geq 160$$

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

$$n \approx 2^{l/2} \sqrt{2 \ln \frac{1}{1-p}}$$

$$h: \{0,1\}^* \rightarrow \{0,1\}^l$$

$$h: \{\text{personnes}\} \rightarrow \{\text{dates d'anniversaire}\}$$



Pour le paradoxe des anniversaires : 365 jrs

$$P \approx 1 - \exp\left(-\frac{m(m-1)}{2 \times 365}\right)$$

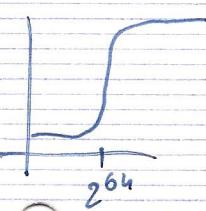
$$m \approx \sqrt{365} \sqrt{2 \ln \frac{1}{1-p}}$$

$$\text{ex: } P \approx 50\% \rightarrow m \approx 1.17 \times \sqrt{365} \approx 23$$

Secure

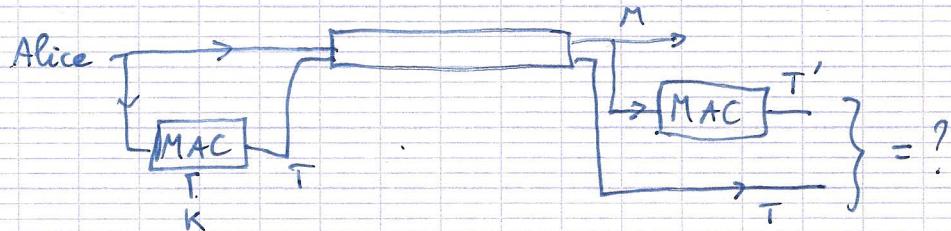
Hash
Algorithm

On prend $l \geq 160 \Rightarrow$ la complexité pour un attaquant de trouver une collision est $\geq 2^{80}$.



Nom	l	Attaque anniversaires	Meilleure attaque connue
MD4 (Rivest, 1990)	128	2^{64}	collision (Dobbertin, 1995)
MD5 (Rivest, 1991)	128	2^{64}	collision (Wang, 2005) 2^{24}
SHA-0 (NIST, 1993)	160	2^{80}	collision (Joux, 2004) 2^{51}
SHA-1 (NIST, 1994)	160	2^{80}	collision (Wang, 2006) 2^{66}
SHA-256	256	2^{128}	
SHA-384	384	2^{192}	
SHA-512	512	2^{256}	
KECCAK SHA-3 (NIST, 2012)	224	2^{112}	
	256	2^{128}	
Bertoni, Peeters, Van Assche	384	2^{112}	
ASSche	512	2^{256}	

II. MAC (Message Authentication Code)

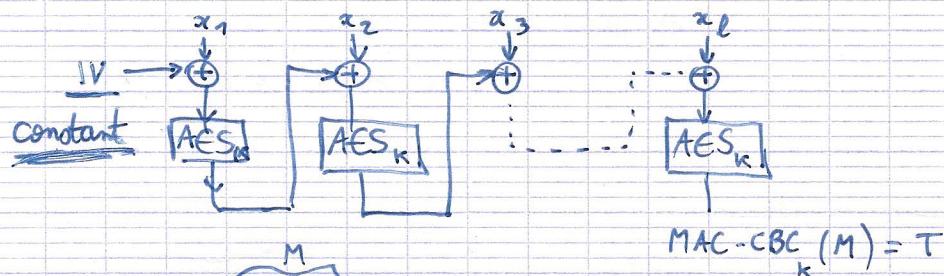


Propriété sonorisée :

Il doit être calculatoirement difficile pour un attaquant de construire un couple (M, T) tel que $\text{MAC}_K(M) = T$
(non déjà connu)

Example: MAC-CBC

$$M = x_1 \parallel x_2 \parallel \dots \parallel x_\ell$$



Alice $\xrightarrow{\text{IV}, x_1, x_2, x_3, T} \text{Bob}$

Charlie

avec x_1' tel que $V \oplus x_1 = V' \oplus x_1'$
 $\Leftrightarrow x_1' = x_1 \oplus V \oplus V'$

IV m'a pas d'intérêt pour du MAC

