

ch 3 : Intégrité des données

I) Fonctions de hachage

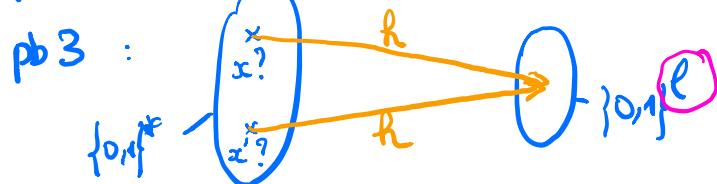
① Introduction

② Définition des fonctions de hachage

③ Complexité des attaques génériques

pb 1 → algorithme de complexité $\approx 2^l$

pb 2 → $\frac{1}{2^l}$



Algorithme : Choisir aléatoirement x_1, x_2, \dots, x_k et calculer $y_1 = h(x_1), \dots, y_k = h(x_k)$ jusqu'à trouver une relation du type

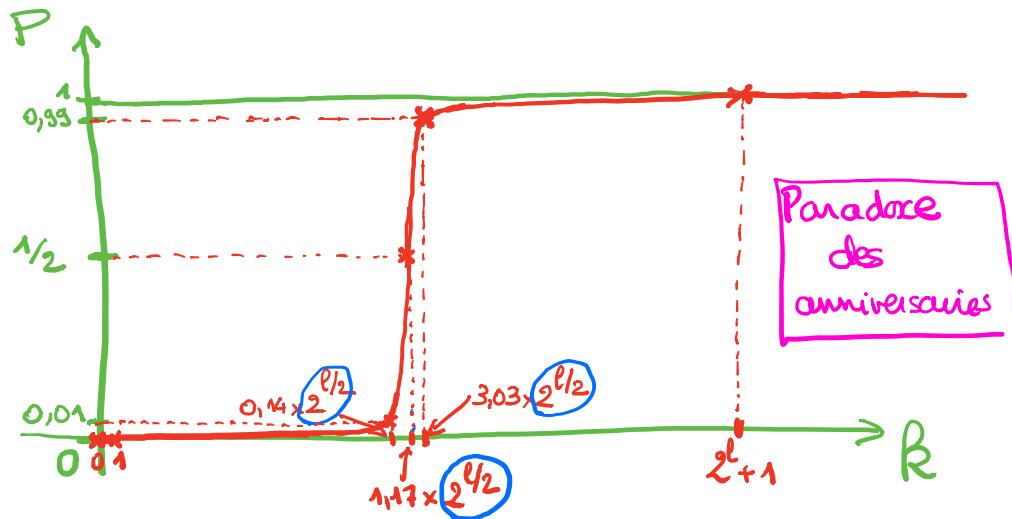
$$y_i = y_j \quad (i < j)$$

↓
collision

P = probabilité d'avoir une collision

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

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



$$P = \frac{1}{2} \Leftrightarrow k \approx 2^{\frac{k}{2}} \sqrt{2 \ln \frac{1}{1-\frac{1}{2}}} = 2^{\frac{k}{2}} \underbrace{\sqrt{2 \ln 2}}_{\approx 1.17}$$

$$P = 0.99 \Leftrightarrow k \approx 2^{\frac{k}{2}} \sqrt{2 \ln \frac{1}{1-\frac{99}{100}}} = 2^{\frac{k}{2}} \underbrace{\sqrt{2 \ln 100}}_{\approx 3.03}$$

$$P = 0.01 \Leftrightarrow k \approx 2^{\frac{k}{2}} \sqrt{2 \ln \frac{1}{1-\frac{1}{100}}} = 2^{\frac{k}{2}} \underbrace{\sqrt{2 \ln \frac{100}{99}}}_{\approx 0.14}$$

Rémarque : Au lieu de considérer une fonction de hachage $h: \{0,1\}^* \rightarrow \{0,1\}^l$
on peut considérer $f: \{\text{personnes}\} \rightarrow \{1, 2, 3, \dots, 365\}$

Probabilité que 2 personnes aient la même date anniversaire

$$\left\{ \begin{array}{l} P \approx 1 - e^{-\frac{f(k)(k-1)}{2 \times 365}} \\ k \approx \sqrt{365} \times \sqrt{2 \ln \frac{1}{1-P}} \end{array} \right.$$

nb d'éléments de l'ensemble d'année

$$P = \frac{1}{2} \Leftrightarrow k \approx \sqrt{365} \sqrt{2 \ln 2} \approx 23$$

$$h=73 \Leftrightarrow P \approx 1 - e^{-\frac{73 \times 72}{2 \times 365}} \approx 99,92\%$$

Comment trouver la collision (parmi tous les $y_i = h(x_i)$ $1 \leq i \leq k$) ?

Méthode "naïve": On prend y_1

et on cherche si cette valeur n'apparaît pas dans la liste $\xrightarrow{\text{oui}} \square$ $\xrightarrow{\text{non}}$

- On prend y_2 et on cherche $\xrightarrow{\text{liste}} \xrightarrow{\text{oui}} \square$ $\xrightarrow{\text{non}}$

$$\text{Complexité} \approx (k-1) + (k-2) + \dots + 1 = \frac{k(k-1)}{2} = O(k^2)$$

$$\text{si } k \approx 2^{l/2} \rightarrow l^2 \approx 2^l$$



- Méthode à utiliser:
- on commence par trier la liste
complexité: $O(k \ln k)$
(par exemple : quick sort)
 - une fois la liste triée, trouver la collision est en complexité: $O(k)$

\Rightarrow complexité de l'algorithme générique pour le pb3

- construction de la liste $\rightarrow O(k)$
- tri de la liste $\rightarrow O(k \ln k)$
- trouver la collision $\rightarrow O(k)$

Au total, complexité $O(k \ln k)$
avec $k \approx 2^{l/2}$

$$\rightarrow \text{complexité } O(2^{l/2} \ln 2^{l/2}) = O(2^{l/2})$$

$\frac{1}{2} \ln 2 \rightarrow \text{constante}$

Remarque: Il existe un raffinement de l'attaque qui donne $\mathcal{O}(2^{l/2})$

Consequence: Pour empêcher un attaquant de trouver des collisions, on choisit l tel que

$$2^{l/2} \geq 2^{80}$$

c'est à dire $l \geq 160$

(ou $2^{l/2} \geq 2^{128} \Leftrightarrow l \geq 256$)

Résumé

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

s'ait une "bonne" fonction de hachage

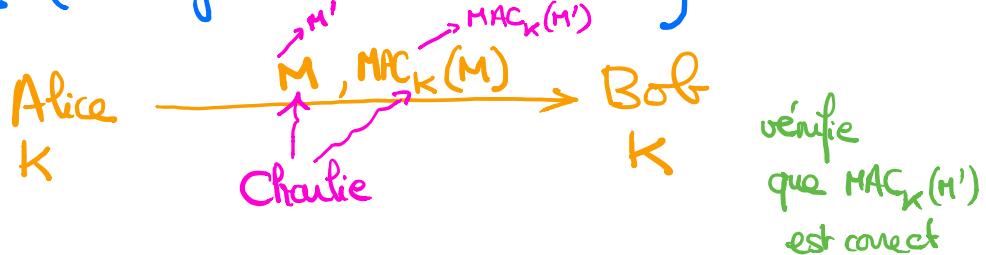
il faut que $l \geq 160$ (ou $l \geq 256$)

④ Exemples de fonctions de hachage

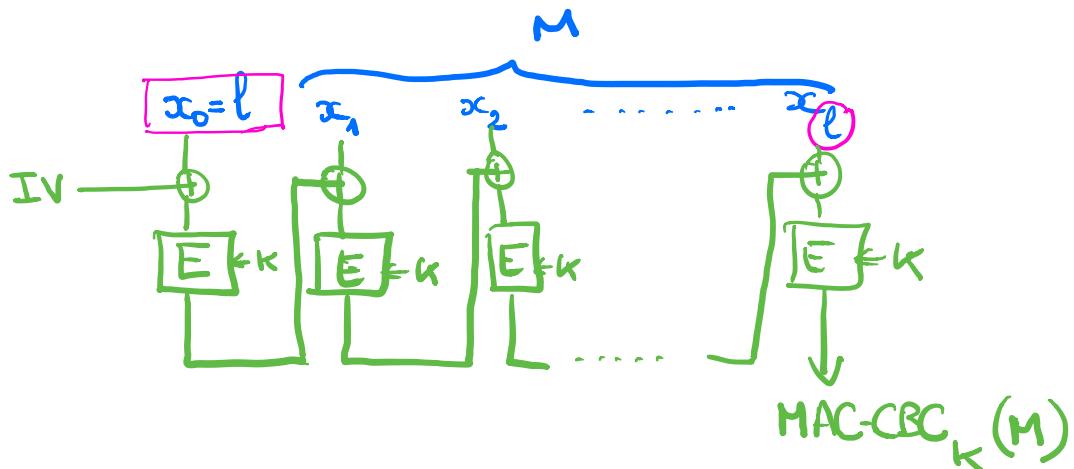
Nom	Inventeur(s)	Année	l	Complexité "anniversaire"	Meilleure attaque connue
MD4 <i>Message Digest</i>	Rivest	1990	128	2^{64}	1995: Dobbertin ↳ collisions
MD5	Rivest	1991	128	2^{64}	2005: Wang ↳ attaque en 2^{24} pour trouver des collisions
SHA-0 <i>Secure Hash Algorithm</i>	NIST (NSA)	1993	160	2^{80}	2004: Antoine Joux ↳ collisions en 2^{251}
SHA-1	NIST (NSA)	1994	160	2^{80}	2006: Wang → algo en 2^{69} pour obtenir des collisions
SHA-256 SHA-384 SHA-512 Famille SHA-2	NIST (NSA)	2002	256 384 512	2^{128} 2^{192} 2^{256}	

RECOM	SHA-3 (2008 → 2011) (KECCAK)	NIST (G.Bertoni, J.Daemen, M.Peeters, G.Van Assche)	2011	224 256 384 512	112 128 192 256

II] MAC (Message Authentication Code)



Exemple : MAC-CBC



Remarque : Ici, IV doit être fixe

S'il ne l'était pas, il faudrait qu'Alice le transmette

Alice $\xrightarrow[\underbrace{M, \text{IV}, \text{MAC-CBC}_K(M)}]{} \text{Bob}$

charlie peut - modifier x_1 , - modifier IV { sans changer le résultat du MAC

ex : MAC-CBC-AES