

Cours crypto

Fonctions de hachage

Laurent Fousse

November 10, 2008

Outline

1 Fonctions de hachage

Définition des fonctions de hachage

Definition (Fonction de hachage (unkeyed))

Une fonction de hachage h est une fonction

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

Propriétés des fonctions de hachage

Definition (Preimage resistance)

Étant donné une sortie y , il est difficile de trouver x tel que

$$h(x) = y$$

Definition (2nd preimage resistance)

Étant donné une entrée x , il est difficile de trouver x' tel que

$$h(x') = h(x)$$

Properties of hash functions

Definition (Collision resistance)

Il est difficile de trouver x et x' tel que

$$h(x) = h(x')$$

Properties of hash functions

Terminologie:

- *pre-image resistant* \equiv *à sens unique*
- *2nd pre-image resistant* \equiv *faible résistance aux collisions*
- *collision resistant* \equiv *résistance forte aux collisions*

Utilité des fonctions de hachage

Idée: calculer une version condensée y d'un message m . Le condensé/résumé devrait être spécifique à ce message.

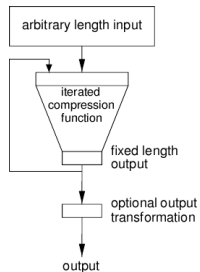
- Utiliser y au lieu de m de façon sûre.
- «*As-tu reçu m correctement? Voici y pour vérifier.*»
(partage de fichier)
- «*As-tu déchiffré c correctement?*»
- «*Je signe y pour prouver que j'ai écrit m .*»

Fonction de compression

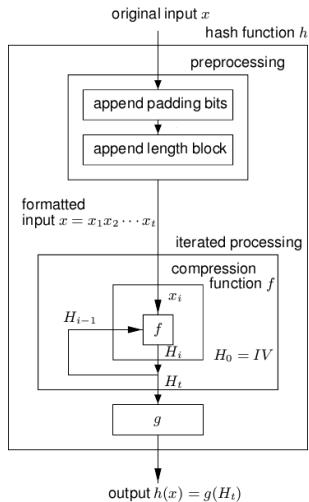
Definition (Fonction de compression)

Une fonction $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$ où $n < m$ est appelée une fonction de compression.

Construction des fonctions de hachage



Construction des fonctions de hachage



Construction des fonctions de hachage (Merkle-Damgård)

- 1 Couper le message x à hacher en blocks de taille $r = m - n$:

$$x = x_1 x_2 \dots x_t$$

- 2 Padder x_t avec des zéros si nécessaire.
- 3 Définir x_{t+1} comme la taille en bit de x .
- 4 Itération sur les blocks:

$$H_0 = 0^n$$

$$H_i = f(H_{i-1} || x_i)$$

$$h(x) = H_{t+1}$$

Construction des fonctions de hachage

Theorem

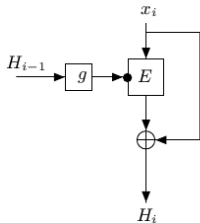
Si la fonction de compression f est résistante aux collisions, alors la fonction de hachage obtenue est résistante aux collisions.

Fonction de hachage avec clef

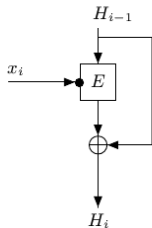
- Une fonction de hachage sans clef est aussi appelée *modification detection code* (MDC). On peut s'en servir pour s'assurer de l'intégrité d'un message.
- Une fonction de hachage avec clef est aussi appelée *message authentication code* (MAC). Elle a un paramètre additionnel (la clef) qui permet de vérifier l'intégrité et la provenance du message en même temps.

Fonctions de hachage basées sur des chiffrements par blocs

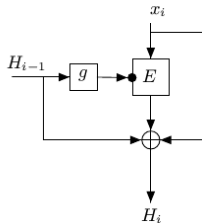
Matyas-Meyer-Oseas



Davies-Meyer



Miyaguchi-Preneel



Fonctions de hachage basées sur des chiffrements par blocs

