

TD 2 de Cryptologie

Lundi 17 octobre 2005

1 Fonctions de hachage

Pour les fonctions de hachage ou de compression suivantes, dire si elles sont résistantes à l'inversion, aux collisions au sens fort, et aux collisions au sens faible.

1.

$$\begin{aligned} h : \{0, 1\}^{4n} &\rightarrow \{0, 1\}^n \\ x_1 || x_2 &\mapsto g(x_1 \oplus x_2), \quad |x_1| = |x_2| = 2n \end{aligned}$$

où $g : \{0, 1\}^{2n} \rightarrow \{0, 1\}^n$ est une fonction de compression résistant fortement aux collisions et \oplus désigne le ou exclusif.

2.

$$\begin{aligned} j : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ (x_1, x_2) &\mapsto x_1^2 + x_2 \end{aligned}$$

où $n = pq$ est produit de deux nombres premiers.

$$\begin{aligned} k : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ (x_1, x_2) &\mapsto x_1^2 + x_2^2 \end{aligned}$$

où $n = pq$ est produit de deux nombres premiers.

3. l définie comme j pour $n = p$ premier.

4. m définie comme k pour $n = p$ premier.

2 SHA-1 et variations

L'algorithme de hachage SHA-1 produit des hachés de 160 bits ou 20 octets. Par exemple :

SHA-1("Test SHA1") = c8d73cf5447f4db6ab75ed0bcf88f11cb3f723ed

1. Combien y-a-t-il de hachés théoriquement possibles ?
2. En prenant n messages aléatoires et en supposant que les résultats sont équirépartis dans l'espace d'arrivée, quelle est la probabilité de générer une collision avec le haché donné en exemple ?
3. En déduire l'espérance du nombre de hachés nécessaires pour obtenir une collision avec l'exemple.

Alice et Bob s'échangent souvent des fichiers via un canal non sûr. Une fois un fichier transféré, Alice et Bob se téléphonent pour confirmer le haché du fichier.

4. En supposant qu'un adversaire peut lire le fichier en cours de transmission et le remplacer par un fichier de son choix et qu'il dispose de ressources lui permettant de calculer le haché de 200Mo de données en une seconde, quelle est l'espérance du temps de calcul nécessaire à l'adversaire pour remplacer un fichier de 2Mo par un fichier de même taille? On supposera que le coût de calculer des hachés est linéaire en la taille de l'entrée.
5. Pour gagner du temps, Alice et Bob ne vérifient en général que les 2 premiers octets du haché. Que devient le travail de l'adversaire dans ce cas?