Condensés cryptographiques

Laurent Signac – CC-BY-SA – 08-06-21 1337 15a32d50757e5d803eb4

1 Condensés de messages

Il est souvent nécessaire d'obtenir, à partir d'un texte de longueur n, un texte plus court, appelé condensé de message (ou hachage ou hash), qui a les propriétés suivantes (dans le cas d'un hachage cryptographique) :

- un condensé de message doit être facile (i.e. rapide) à calculer (même si le message est très long) ;
- quel que soit le condensé, on ne peut pas l'utiliser pour retrouver le message original ;
- pour un message donné, il est impossible (comprendre hors de portée d'un calcul actuel et pour les années à venir) de trouver un autre message ayant le même condensé (alors qu'il y en a, par définition, puisque le condensé est plus court) ;
- une modification mineure dans le message modifie grandement le condensé.

Les deux méthodes les plus connues (dont nous ne détaillerons pas le fonctionnement) sont MD5 et SHA-1 qui permettent respectivement d'obtenir des condensés de 128 et 160 bits.

Bien qu'encore très utilisées, elles sont maintenant dépassées et devraient être remplacées par des versions plus modernes comme SHA-256 ou SHA-512 (famille [Sha-2]).

Le principe des condensés est utilisé dans différents contextes :

- vérification de l'intégrité d'un fichier (on peut vérifier visuellement le condensé d'un énorme fichier de plusieurs Go)
- hachage des mots de passe (pour contrer un éventuel vol de bases de données)
- signature numérique

Voici un exemple de calcul d'un condensé en ligne de commandes :

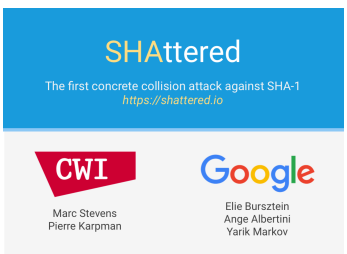
```
$ echo "Utilisez Linux!" | sha256sum
832107cfab70836be4611b1faae024cd773b3e69b77a0091ded717b72666eae1  -

$ echo "utilisez Linux!" | sha256sum
6715f0f776edf18ded91985c286af30e7ee88a7cd7ef0eea3c5846bcbe8afcb2  -
```

2 Propriétés sur les collisions

Pour une fonction de hachage h, on distingue les propriétés suivantes (par ordre croissant de difficulté) :

- Résistance aux collisions : Il est impossible d'exhiber un couple x, x_0 tel que $h(x_0) = h(x)$
- Résistance à la seconde préimage : Pour x fixé à l'avance, il est impossible de trouver x_0 tel que $h(x_0) = h(x)$
- Résistance à la première préimage : Pour y fixé à l'avance, il est impossible de trouver x tel que $h(x) = y$

Depuis 2017, SHA-1 n'est plus résistant aux collisions avec préfixe choisi (voir le site shattered.io[1]).



[1] https://shattered.io