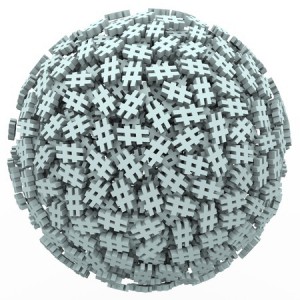
**Qu’est-ce qu’un „hash“ ? (fa8bc2ba308356be3aac4a98535aacc393cb90e5)**

In [Info Sécurité](http://blog.emsisoft.com/fr/category/security-knowledge-fr/) by [Monika](http://blog.emsisoft.com/fr/author/monika/) on May 5, 2014 | Français, [English](http://blog.emsisoft.com/2014/05/05/what-is-a-hash/), [Deutsch](http://blog.emsisoft.com/de/2014/05/05/was-ist-ein-hash/)

[](http://blog.emsisoft.com/wp-content/uploads/2014/05/19744849_s.jpg)

La [vulnérabilité „Heartbleed“](http://blog.emsisoft.com/?p=6191) a attiré l’attention de tous sur le concept de la cryptographie ainsi que tout un tas de mots-clé annexes. Par conséquent, les utilisateurs d’ordinateur lambda se voient faire face à déchiffrer tout seuls une conversation souvent aussi cryptique que son contenu. Le „hash cryptographique“ est un des ces termes les plus fondamentaux et récurrents.

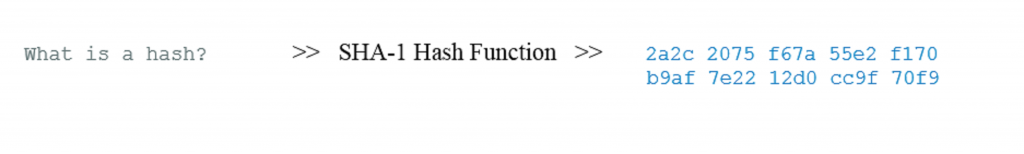
**Les hashs – une introduction**

Un hash cryptographique est une série de chiffres et lettres générée par une fonction de hash cryptographique. Une fonction de hash cryptographique n’est rien d’autre qu’un algorithme ou une série d’opérations mathématiques effectuées par un ordinateur. Pour que vous commenciez à mieux comprendre, regardons le titre intimidant de cet article :

Qu’est-ce qu’un „hash“ ? (fa8bc2ba308356be3aac4a98535aacc393cb90e5)

En français, le titre de cet article est Qu’est-ce qu’un hash ? Dans la langue cryptographique hash SHA-1, ceci se traduit par fa8bc2ba308356be3aac4a98535aacc393cb90e5.

Il est vrai que ceci a l’air compliqué, mais en réalité, il ne s’agit que d’une relation input-output. Afin d’effectuer la traduction, l’entrée Qu’est-ce qu’un hash ? est transférée à un logiciel qui y applique la fonction de hash SHA-1 cryptographique et puis donne le hash comme output.

[](http://blog.emsisoft.com/wp-content/uploads/2014/04/hash_table_3.1.png)

Veuillez noter la division du hash en 10 morceaux, dont chacun est de 4 caractères, ce qui donne une totalité de 40 caractères. Bien que le format soit différent, le hash est toujours identique. Ce format sert à donner une meilleure lisibilité et aide les analystes à déchiffrer un hash lorsque c’est nécessaire. En voici quelques autres exemples :

[](http://blog.emsisoft.com/wp-content/uploads/2014/04/hash_table_1.1.png)

Veuillez noter que, quoique le nombre de caractères de chaque entrée soit différent, le hash SHA-1 qui en résulte est toujours de 40 caractères. Ceci rend les hashs difficiles à craquer. Par exemple, vous pourriez hasher votre lettre favorite „E“ ou le contenu complet de votre livre favori, „Da Vinci Code“, et dans les deux cas, le hash qui en résulte serait toujours de 40 caractères. Ceci rend le hashing un outil cryptographique puissant.

Ce qui est encore plus intéressant, c’est l’effet dit „l’effet avalanche“ qu’il est possible de démontrer en s’appuyant sur une faute d’orthographe commune du nom de notre entreprise :

[](http://blog.emsisoft.com/wp-content/uploads/2014/04/hash_table_2.1.png)

Veuillez noter la différence minuscule en ce qui concerne la saisie – on a omis le premier S d’Emsisoft –, qui, suite à l’effet avalanche, donne quand même un résultat tout à fait différent, une capacité très désirable d’une fonction de hash cryptographique. Juste une lettre donne un hash entièrement différent, ce qui rend le déchiffrage manuel assez difficile.

Autrement dit, une lettre fait toute une différence !

**À quoi servent les hashs ?**

Les hashs sont une partie fondamentale de la cryptographie vu qu’il permettent d’associer un ensemble de données de n’importe quelle taille à une signature aléatoire. Dans l’exemple que vous voyez en haut, nous avons démontré la fonction de hash SHA-1 cryptographique, mais en réalité, il y a un bon nombre de fonctions de hash sur lesquelles on peut s’appuyer. À part SHA-1, les experts en matière de sécurité informatique emploient également SHA-2 et MD5. Les différentes fonctions sont capables de donner différents degrés de complexité et s’utilisent donc dans différents scénarios, en fonction du niveau de sécurité requis.

**Le hashing de mots de passe**

Pour l’utilisateur d’ordinateur lambda, le plus souvent, il se verra face aux hashs par les mots de passe. Lorsque vous créez un mot de passe et le partagez avec un prestataire de service, celui-ci l’archivera sous forme de hash au lieu de la forme en texte clair, pour que, lorsque leur serveur est piraté, l’agresseur n’ait que des hashs chiffrés en butin. Le problème de Heartbleed (ce qui a également mené à le considérer une crise majeure) était qu’il a permis aux agresseurs de s’emparer de mots de passe en texte clair dans la mémoire vive d’un serveur au lieu de mots de passe sauvegardés sous forme chiffrée dans les archives du serveur.

D’ailleurs, le chiffrement de mots de passe n’est pas facile à manier. [Des mots de passe utilisés d’habitude](http://blog.emsisoft.com/fr/2014/01/21/emsisoft-vous-presente-les-pires-mots-de-passe-de-2013/) tels que „123456” ou „password” sont toujours et encore susceptibles d’une attaque dite attaque par dictionnaire. Cela est dû au fait qu’un agresseur peut simplement saisir ces mots de passe communs dans une fonction de hash, trouver le hash, créer un dictionnaire de hashs communs de mots de passe et puis „consulter“ les hashs de mots de passe chiffrés volés.

Des pirates déterminés peuvent également se servir de “rainbow tables” (tableaux arc-en-ciel) pour déchiffrer des mots de passe hashés – s’ils arrivent à s’en emparer. Heureusement, il est possible de contourner cette méthode en se servant d’un hash “salé”. Un hash salé reprend le hash du mot de passe d’origine et y ajoute un petit extra, tel qu’un chiffre aléatoire ou une ID d’utilisateur (c’est-à-dire, “une prise de sel”). Le hash salé est encore une fois hashé, ce qui fournit une couche de sécurité supplémentaire qu’il est presque impossible de contourner.

**Le hashing de malwares**

Chez Emsisoft, les hashs cryptographiques servent le plus souvent à identifier des malwares. Lorsque la communauté se dédiant à l’analyse de malware trouve une nouvelle menace, on y associe un hash cryptographique servant de signature. Le [scanneur anti-malware à deux moteurs](http://blog.emsisoft.com/fr/2012/11/08/tec121108fr/) d’Emsisoft comprend plus de 12.000.000 de ces signatures, dont il se sert pour protéger votre ordinateur. En principe, ceci ressemble à la base d’empreintes digitales de la police. Lorsque vous analysez votre ordinateur pour trouver des malwares à l’aide d’Emsisoft Anti-Malware, le logiciel compare les signatures de tous vos fichiers à celles de malwares connus dans sa base de données – une base de données mise à jour toutes les 15 minutes. Lorsque le logiciel en trouve deux qui correspondent, il sait que votre ordinateur est infecté et vous fait savoir qu’il vaudrait mieux supprimer ce fichier malicieux.

Il y a quand même un tout petit problème lors de l’analyse. Suite à l’effet avalanche, le créateur d’un malware peut changer la signature de hash de son malware assez facilement. Tout ce qu’il faut, c’est une petite modification du code du malware. Cela veut dire que des tonnes de nouvelles signatures de malwares sont générées chaque jour et que même la base de signatures de malwares la mieux entretenue par les analystes les plus vigilants ne peut pas y faire jeu égal. Ce petit défaut est bel et bien la raison pour laquelle Emsisoft Anti-Malware s’appuie sur la [technologie d’analyse de comportement](http://blog.emsisoft.com/fr/2012/10/16/tec121016fr/), une innovation permettant de reconnaître un fichier lorsqu’il essaie d’exécuter un processus malicieux. Dans ce sens, l’analyse de comportement sert de protection de secours pour le cas peu probable où la nouvelle menace n’est pas encore été enregistrée dans la base de données.

**Autres applications pour les hashs**

Autre que dans la sécurité, la nature de signature des hashs cryptographiques permet de les utiliser pour sécuriser des contenus numériques. On s’en sert souvent pour protéger les droits d’auteur de médias numériques, et ceci souvent par les prestataires de services de partage de fichiers en vue d’empêcher que leurs utilisateurs ne partagent des contenus protégés illégalement. C’est un outil puissant, étant donné qu’il permet aux prestataires de services de surveiller ce que leurs utilisateurs sauvegardent sans même violer leur vie privée. De manière très identique à ce que nous faisons pour vous protéger des malwares, les prestataires de services de partage de fichiers créent simplement des bases de données de hashs associés aux fichiers protégés. Lorsqu’ils se rendent compte qu’un utilisateur essaie de transférer un fichier ayant un de ces hashs, ils sont à même d’intervenir et empêcher que cet utilisateur ne partage des contenus protégés illégalement.

Les hashs peuvent également servir pour vérifier „’l’intégrité de messages“ à l’aide d’une „somme de contrôle“. Lorsque deux partis désirent partager un fichier, ils peuvent s’appuyer sur des signatures de hashs cryptographiques pour vérifier que le fichier n’a pas été manipulé par un tiers pendant la transmission. Cela fonctionne parce qu’un fichier qui n’a pas été manipulé devrait donner le même hash lors de l’envoi que lors de la réception. Si la comparaison révèle que les hashs sont différents, ceux qui partagent le fichier sauront que quelqu’un d’autre a „tripoté“ leur paquet !

**Qu’est-ce qui se passe lorsqu’on hashe un hash ?**

L’aspect le plus merveilleux et en même temps effrayant de la cryptographie est qu’elle est basée sur des principes très simples telle que les hashs, mais toujours et encore donne une complexité énorme. Ceci fait la cryptographie un outil puissant et en même temps dangereux. D’une part, la cryptographie permet eux experts en matière de sécurité informatique de protéger tout allant des données bancaires d’un utilisateur privé aux documents secrets des autorités militaires comprenant des informations relatives aux armes les plus puissantes du monde. D’autre part, la cryptographie permet également aux auteurs de malwares de créer des formes avancés de malwares telles que [Cryptolocker](http://blog.emsisoft.com/?p=1615) – une menace qu’il reste encore à contourner.

Peu importe comment vous l’abordez, la cryptographie est un sujet complexe – et la vulnérabilité critique „Heartbleed“ découverte au début du mois d’avril a en fait été une conséquence de cette complexité. La toile continuera à évoluer, et sans aucun doute, il y aura de nouvelles technologies et de nouveaux termes cryptographiques qui apparaissent, mais cela ne veut pas dire que les utilisateurs lambda ne peuvent pas participer à la conversation et en comprendre les éléments de base. Bien au contraire, tous ceux qui se servent d’Internet tous les jours et ne comprennent pas bien comment cela fonctionne forment la majorité, et l’enseignement de cette majorité en matière de sécurité représente un élément fondamental pour une toile globale entièrement sûre.

Android

Firewall UTM

Attaques

Toip

PKI