RFC 6234 : US Secure Hash Algorithms (SHA and SHA based HMAC and HKDF)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 mai 2011

Date de publication du RFC : Mai 2011

https://www.bortzmeyer.org/6234.html

Ce long RFC (127 pages, dont la majorité est composé de code source C) est la mise à disposition de la communauté IETF du code de FIPS 180-2 <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>, décrivant les algorithmes de cryptographie de la famille SHA-2. Il remplace le RFC 4634 [1].

Cette famille de fonctions de hachage cryptographiques normalisée par le NIST (et donc standard officiel aux États-Unis) a vocation à remplacer l'ancien SHA-1 (RFC 3174). Elle comprend SHA-224 (également décrit dans le RFC 3874), SHA-256, SHA-384 et SHA-512. Tous ont le même principe (section 1) : un document de longueur quelconque est transformé en un **condensat** cryptographique de longueur fixe (le nom de l'algorithme indique le nombre de bits du condensat), de telle manière qu'il doit extrêmement difficile de fabriquer un document ayant le même condensat qu'un document donné (ou même de fabriquer deux documents ayant le même condensat).

Notre RFC décrit également leur utilisation en HMAC (cf. RFC 2104), et en HKDF ("*HMAC-based Key Derivation Function*", cf. RFC 5869). L'essentiel du RFC est tiré directement de la norme officielle <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf> et les assertions sur la sécurité de SHA-2 viennent donc directement du NIST et pas des éditeurs du RFC.

Les sections 2 à 7 du RFC résument le fonctionnement de ces algorithmes, et la section 8 est le code source C les mettant en œuvre.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4634.txt

La licence de ce code source figure dans le fichier `sha.h`, listé en section 8.1.1. C'est une licence BSD-3 (sans la clause de publicité), qui permet tout usage, commercial ou non, ainsi que toute modification et redistribution. Elle est donc adaptée au logiciel libre.

Comme copier/coller le code source depuis le RFC en éliminant les en-têtes et pieds de page n'est pas pratique, on peut récupérer une archive « propre » en `<http://www.pothole.com/~dee3/source/sha.tar>`. Il y en a plein d'autres mises en œuvre de SHA décrites en `<http://en.wikipedia.org/wiki/SHA-2#Implementations>`.

Les changements depuis le RFC 4634 sont résumés dans l'annexe. Le principal est l'ajout de HKDF ("*HMAC-based Key Derivation Function*"). Il y a aussi pas mal d'errata `<http://www.rfc-editor.org/errata_search.php?rfc=4634&rec_status=15&presentation=table>` dans le code, détectés par le meilleur relecteur des RFC, Alfred Hoenes, et désormais réparés. La licence est nouvelle (BSD-3 désormais) et a nécessité de remplacer le code de getopt.