Un nouveau standard de hachage cryptographique, pour 2012 ?

Publié le vendredi 26 janvier 2007
Voir en ligne : https://www.france-science.org/Un-nouveau-standard-de-hachage.html

Le National Institute of Standards and Technology (NIST) a lancé une compétition pour définir un nouveau standard de hachage cryptographique destiné à succéder au Secure Hash Algorithm SHA-1, défini dans le Federal Information Processing Standard 180-2. SHA-1 a été finalisé en 1994 ; depuis des failles ont été découvertes : des méthodes permettant de construire des collusions avec 2 puissance 69, puis 2 puissance 63 opérations ont été trouvées par une équipe chinoise en 2005 (au lieu de 2 puissance 80 par le paradoxe des anniversaires) et des voix se sont élevées pour demander son remplacement (voir BE 23 Cherche nouveau Hash). En mars 2006, le NIST recommandait aux agences fédérales de ne plus utiliser SHA-1 mais la famille SHA-2 (SHA-224, SHA-256, SHA-384 et SHA-512). Si des méthodes permettent une accélération de la construction de collusion, la norme ne pourrait plus être considérée comme sûre ; elle est actuellement très largement utilisée. Déjà récemment (en 1996), le NIST avait lancé une compétition pour définir une nouvelle norme de chiffrement symétrique, créant l'Advanced Encryption Standard (AES). Selon un calendrier provisoire, la date limite de soumission des algorithmes serait au troisième trimestre 2008 ; le standard serait validé au troisième trimestre 2012.

Source :

- http://www.fcw.com/article97461-01-23-07-Web&newsletter=yes
- http://www.csrc.nist.gov/pki/HashWorkshop/index.html
- http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/NIST_Policy_on_HashFunctions.htm
- BE Etats-Unis 23 - Cherche nouveau Hash
http://www.bulletins-electroniques.com/actualites/032/32298.htm

Pour en savoir plus, contacts :

-
http://www.csrc.nist.gov/pki/HashWorkshop//FederalRegister/Federal%20Register%20Notice%20for%20Requirements%20&%20Criteria%20-%20E7-927.pdf
- "Cherche nouveau Hash"
BE Etats-Unis 23, http://www.bulletins-electroniques.com/actualites/32298.htm
Code brève
ADIT : 41005

Rédacteur :

Sébastien Morbieu, deputy-stic.mst@ambafrance-us.org