Depuis quelques années un certain nombre de fonctions de hachage ont été cassées. Soit qu'on ait trouvé en pratique des collisions, c'est-à-dire des messages distincts ayant la même empreinte, soit que la sécurité de la fonction ait été diminuée de manière notable par rapport à sa sécurité attendue. Rappelons qu'une fonction de hachage qui fournit une empreinte de 2n bits (2n=160, 224, 256, 384,512) ne devrait pas succomber à une attaque où le nombre d'essais serait bien moindre que 2^n, c'est-à-dire à une attaque qui serait bien meilleure que l'attaque des anniversaires sur cette fonction. L'une d'entre elles, SHA1, dont l'empreinte est de 160 bits a vu sa sécurité réduite à 2^{63} essais au lieu des 2^{80} attendus. Bien que SHA2, qui regroupe SHA224, SHA256, SHA384,SHA512, soit indemne, le NIST qui propose ces fonctions dans son standard de fonctions de hachage, a ouvert un appel d'offre international, ainsi qu'il avait fait pour AES, pour un futur standard SHA3 qu'il espère mettre en place en 2012. On pourra suivre les évolutions de ce concours sur cette page du site du NIST . On peut aussi visiter
le site wikipedia sur ce sujet
.