Initiation à la cryptographie

Travaux Dirigés de cryptographie n°3

—TELECOM Nancy 2A Formation par Apprentissage—

1 Fonctions de hachage

▸ **Exercice 1.** Hachage super rapide

Discuter des mérites des fonctions de hachage suivantes, et de leur éventuelle sécurité par rapport aux propriétés désirées.

— Schéma 1 : découper le message en blocs de 128 bits, calculer le XOR de tous les blocs, et en faire le haché.
— Schéma 2 : idem, mais le haché est le résultat de l'application de `sha3` au résultat du schéma précédent.
— Schéma 3 : découper le message en blocs de 64 bits nommés $(m_1, m_2, \ldots, m_k)$. Soit p_i le plus petit nombre premier tel que $p_i \geq m_i$. Le haché est le produit des p_i.

▸ **Exercice 2.** Archivage

La société X propose un service de sauvegarde et d'archivage longue durée très onéreux, pour des données de très grand volume (imaginons des centaines de téraoctets).

L'entreprise Y, cliente de la société X, lui soumet des volumes de données qu'elle (l'entreprise Y) continue à détenir. On va supposer que ces données sont constituées de très nombreux fichiers d'un gigaoctet (donc des centaines de milliers de tels fichiers).

L'entreprise Y souhaite s'assurer que son argent n'a pas été dépensé pour rien : si jamais la société X est remplie d'escrocs, l'éventualité d'un procès gagné par Y contre X pour motif d'escroquerie ne consolerait que mollement la société Y, qui veut surtout avoir l'assurance que ses données sont bien sauvegardées, et ne seront pas perdues en cas de panne matérielle dans les locaux de Y.

L'entreprise Y demande donc à X d'effectuer des simulations de restauration de données [1]. Le commercial de la société X leur propose le mode alternatif décrit dans le paragraphe suivant.

≪ Les tests de restauration seraient trop compliqués à mettre en place, étant donné les volumes en question. Nous vous recommandons plutôt, chaque jour, de nous demander la valeur de hachage par la fonction `SHA1` d'un fichier de votre choix parmi la centaine de milliers de fichiers soumis. Nous répondrons, vous prouvant ainsi que nous disposons bien des données. ≫

1. Où est l'arnaque ? Faudrait-il choisir une autre fonction de hachage ?

Le commercial concède que le mécanisme qu'il propose ne prouve pas grand-chose. Il propose une version améliorée. Chaque jour, Y doit demander à X la valeur de hachage par la fonction `SHA1` d'un fichier quelconque (choisi par Y) parmi la centaine de milliers de fichiers soumis, *auquel est ajoutée, à la fin, une séquence d'un kilooctet choisie par* Y. Si F_i est le i-ème fichier, la preuve que doit fournir X est donc :

$$\mathtt{SHA1}(F_i \| \sigma),$$

où σ est un bloc aléatoire choisi par Y.

2. Est-ce mieux ? Expliquer.

1. Dans un cas pareil, il faut *toujours* faire de telles simulations !

2 RSA

▸ **Exercice 3.** À la main !

Considérons le système RSA construit à partir des entier $p = 19$ et $q = 23$. Vous avez le droit à la calculatrice : ce n'est pas un exercice de calcul !

1. Calculer N et $\varphi(N)$.
2. Calculer l'exposant de déchiffrement d associé à $e = 5$ et l'exposant de déchiffrement d associé à $e = 9$.
3. Calculer le chiffré associé au message $m = 42$ quand $e = 5$.