Signature et authentification

Chiffrer un message m consiste mathématiquement à lui appliquer une fonction f appelée clé de chiffrement afin de former un message crypté $m' = f(m)$. Cette fonction f ne doit jamais prendre deux fois la même valeur de sorte de pouvoir introduire sa fonction réciproque que l'on notera g (ou f^{-1}) définie de sorte que

$$y = f(x) \Leftrightarrow g(y) = x$$

Cette fonction appelée clé de déchiffrement car elle permet de décrypter le message m' par le calcul

$$g(m') = g(f(m)) = m$$

Pour certains cryptosystèmes, connaître f suffit pour déterminer aisément g, c'est le cas des chiffrements par substitution et permutation. En revanche, il existe des cryptosystèmes pour lesquels la connaissance de la clé de chiffrement ne permet pas techniquement de déterminer la clé de déchiffrement. C'est le cas du cryptosystème RSA (voir article). Pour ce système, le concepteur du code détermine à la fois f et g, mais une personne étrangère à la conception du code ne peut déduire une fonction de l'autre : cela la conduirait à des calculs infaisables en pratique. Cette dissymétrie entre les deux clés f et g permet au créateur du code de diffuser l'une d'elle, par exemple, par le biais d'un annuaire. Cette clé est alors appelée clé publique tandis de l'autre est appelée clé privée.
A l'aide d'une clé publique quiconque peu chiffrer un message que seul le concepteur du code saura déchiffrer. A l'inverse, à l'aide de sa clé privée, seul le concepteur du code saura chiffrer un message voulu que quiconque pourra déchiffrer. C'est ce dernier principe que nous allons illustrer dans les protocoles qui vont suivre. Nous convenons d'appeler Alice la conceptrice du code, f sa clé privée et g sa clé publique. Nous nommerons Bob le quidam souhaitant communiquer avec Alice.

Signature électronique

Alice veut transmettre un message à Bob mais ce dernier veut s'assurer qu'Alice en est la véritable expéditrice et que le message n'a pas été corrompu par un élément intermédiaire. De plus, Bob souhaite qu'Alice ne puisse pas nier avoir envoyé ce message. Alice va alors accompagner son message d'une signature électronique. Celle-ci est réalisée en deux temps :

- Alice forme un résumé $r = h(m)$ de son message par le biais d'une fonction de hachage comme par exemple le MD5 (voir encadré).
- Alice crypte alors le résumé par le biais de sa clé secrète pour former $s = f(M)$ qui constituera la signature du message transmis par Alice.

A la réception du message m accompagné de sa signature s, Bob calcule le résumé r du message m ainsi que $g(s)$ à l'aide de la clé de chiffrement publique d'Alice. Il lui suffit alors de vérifier si $g(s) = r$ pour s'assurer qu'Alice est la véritable expéditrice du message. Par ce mécanisme, un intermédiaire mal intentionné ne peut se substituer à Alice et l'intégrité du message est assurée.
Notons que cette signature est ici plus sûre qu'une signature papier puisqu'elle est fonction du document signé.

La fonction de hachage MD5

Une fonction de hachage forme le résumé d'un texte en remplissant les deux objectifs suivants :

- la moindre modification du message initial entraîne une modification majeure du résumé,
- il n'est pas possible de former un message dont le résumé soit égal à une expression donnée.

Le résumé MD5 d'un texte est obtenu en commençant par compléter ce texte avant de le sectionné en blocs de 512 bits. Un procédé itératif modifie une valeur initiale de 128 bits convenue en fonction de chacun des blocs du texte par application de fonctions complexes (et notamment de valeurs prises par la fonction sinus). La valeur finale obtenue est le résumé cherché.
Par exemple, « Cette fille est polie » est résumé en « ce0d33c5d48f75451be35877112732b8 » alors que « Cette fille est jolie » est résumé en « 55d1f1b640797594c86e771cf55aa07d ».

Authentification par challenge.

Bob veut transmettre des informations à Alice mais il veut préalablement être certain de communiquer avec celle-ci et non un usurpateur : il souhaite l'authentifier. Pour cela il va lui lancer un challenge : il choisit arbitrairement un message m et demande à Alice de chiffrer ce message. Etant en possession de g, Alice peut former $m' = f(m)$ et lui transmet m'. A réception, Bob vérifie si $m = g(m')$ et si tel est le cas Bob est assuré qu'Alice est en possession de la clé privée f, en effet un usurpateur ne connaissant par g ne peut chiffrer un message aléatoire, il est automatiquement démasqué.
Ce principe d'authentification se retrouve lors d'échanges électroniques où les interlocuteurs ont besoin de s'identifier mutuellement avant d'échanger des informations sensibles.

Un tiers de confiance : une autorité de certification

Bob souhaite échanger des données sensibles avec Alice qu'il rencontre pour la première fois ; c'est le cas par exemple d'un client arrivant sur un site de commerce en ligne. Alice communique à Bob sa clé publique et Bob pourra chiffrer ses informations avec celle-ci avant de les transmettre à Alice qui sera la seule à pouvoir les décrypter. Mais pour Bob se pose le problème suivant, Alice ne serait-elle pas un truand avide d'informations sensibles ? Autrement dit, Bob peut-il faire confiance à cette inconnue qu'est Alice ?
Pour résoudre ce problème, Alice et Bob vont faire appel à un tiers de confiance : une autorité de certification. L'une des plus connue est Verisign mais pour notre explication celle-ci sera appelée Charlene. Alice produit auprès de Charlene différentes informations personnelles ainsi que sa clé de chiffrement publique. Charlene forme alors un certificat regroupant ces informations, un numéro de série, une période de validité ainsi qu'une signature numérique qu'elle aura réalisée à l'aide de sa propre clé privée.
Lors d'une transaction avec Alice, Bob reçoit ce certificat. Il prend connaissance de la clé publique d'Alice et peut vérifier la validité du certificat à l'aide de la clé publique de Charlene. En faisant confiance à Charlene, Bob peut faire confiance à Alice.

Ces différents protocoles sont les bases qui permettent les échanges d'informations sécurisées sur tout type de réseaux. Bien sûr ces protocoles sont invisibles de l'utilisateur, ce sont les logiciels exploités, comme par exemple le navigateur internet et les différents serveurs qui les mettent en place.
L'apport de la cryptographie à clé publique y est ici fondamental car c'est le principe suivant qui est ici pleinement exploité :

« un seul peut chiffrer, quiconque peut déchiffrer »