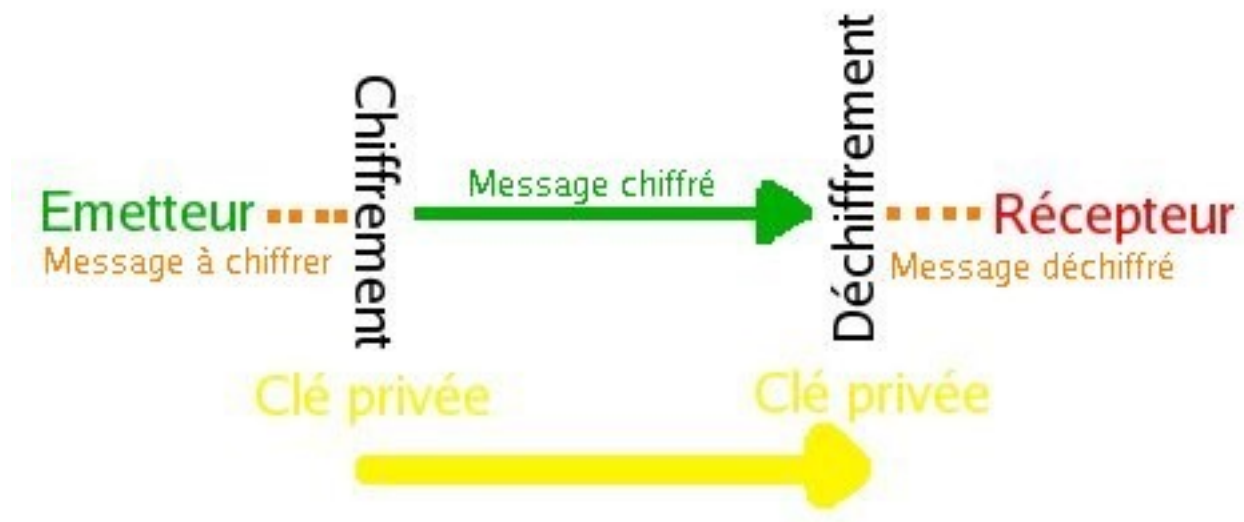


Systemes de cryptographie

Sommaire

I. Systemes à clés privées/secrètes : chiffrement symétriques.....	1
II. Systeme à clés publiques : chiffrement asymétrique (Diffie et Hellman).....	2
III. Clef de session.....	3
IV. Systeme de hachage.....	3
V. Exemples de systemes de cryptographie.....	4
a) à clés privées.....	4
b) à clés publiques.....	4
c) fonction de hachage.....	4
VI. Signature électronique.....	4
VII. Scellement de données.....	5
VIII. Certificats.....	6
a) Principe.....	6
b) Certificat de révocation.....	8
Bibliographie.....	8

I. Systemes à clés privées/secrètes : chiffrement symétriques



Ce systeme de cryptographie utilise la même clef pour crypter et décrypter les données. Pour qu'il soit inviolable, il faudrait que la clef soit au moins de la même taille que le message à crypter.

Le principal inconvénient de ce systeme est qu'il faut d'abord trouver un canal sécurisé pour transmettre la clef entre les deux personnes communicantes, ce qui n'est pas évident de nos jours. Il faudrait donner la clef sur un support comme une disquette ou un clé USB pour être sûr qu'elle ne soit pas interceptée.

Un autre problème des clés privées est qu'il faudrait une clef par canal de communication : c'est à dire que si une personne veut communiquer avec N personnes, il lui faudrait $N * (N-1) / 2$ clefs

différentes. Ce nombre de clef augmente très vite avec le nombre N.

Il existait une technique notamment utilisée pour le téléphone rouge : on génère une clé que l'on fait transporter (par exemple par valise diplomatique), on l'utilise une fois et on la détruit.

II. Système à clés publiques : chiffrement asymétrique (Diffie et Hellman)



Ce type de chiffrement est apparu relativement récemment en 1976 dans un ouvrage de Diffie et Hellman.

Dans ce type de système de chiffrement, les clefs vont toujours par paire :

- une clef publique pour le chiffrement
- une clef privée pour le déchiffrement

La démarche de mise en place est la suivante :

- l'utilisateur récepteur choisit aléatoirement sa clé privée qu'il est le seul à connaître
- à partir d'un algorithme (comme un exponentiel discret), il calcule une clé publique qu'il doit donner à toutes les personnes qui doivent lui envoyer des messages. **La clé publique peut être donnée sur un canal non sécurisé car on ne peut pas retrouver la clé privée à partir de la clé publique** (il est difficile par exemple de calculer un logarithme discret).
- Il peut publier la clé publique sur un serveur de clés (comme dans un serveur LDAP)

Lorsqu'une personne veut envoyer un message à notre utilisateur, elle a simplement à crypter le message avec la clef publique et lui envoyer.

L'utilisateur n'aura plus qu'à décrypter le message reçu avec sa clé privée.

Ce système se base sur ce que l'on appelle « les fonctions à sens unique ». Une telle fonction est très facilement calculable dans le sens clé privé --> clé publique mais est mathématiquement impossible à inverser. On ne peut donc pas retrouver facilement la clé privée à partir de la clé publique sauf si on a une trappe : la clé privée.

Il n'y a donc plus de problème d'échange de clés. Mais par contre, il faut s'assurer que la clé

publique est bien celle de la personne à qui on veut envoyer le message.

Les algorithmes de chiffrement à clés publiques sont 1000 fois plus lent que les algorithmes à clés privées.

III. Clef de session



Un autre problème des systèmes à clés publiques est qu'il sont beaucoup moins rapide en terme d'exécution que les systèmes à clés privées.

La technique des clés de session est un compromis entre les deux types de chiffrements.

Le principe est le suivant :

- on génère aléatoirement une clé d'une taille suffisante à assurer une certaine sécurité
- on crypte cette clé avec la clé publique du destinataire
- on envoie la clé cryptée au destinataire
- le destinataire décrypte la clé avec sa clé privée
- l'émetteur et le destinataire disposent alors de la même clé qu'ils sont seuls à connaître

On peut donc alors utiliser un système à clé privée avec la clé de session générée.

IV. Système de hachage



Une fonction de hachage permet d'obtenir un texte de taille fixe (digest en anglais) à partir d'un texte de longueur variable. Tout changement dans le texte variable entraîne un changement dans le digest généré. Ceci permet de savoir si le texte a été modifié. Pour cela, on recalcule le digest du texte reçu et on le compare avec le digest reçu : s'ils ne sont pas égaux, le texte a été modifié.

Autrement dit, une fonction de hachage :

- prend une donnée quelconque
- renvoie une donnée de taille fixe
- est à sens unique sans trappe
- est facile à calculer

Le digest généré représente donc en quelque sorte, l'empreinte digitale du message. Elle traite, en général, le message par blocs.

Ces fonctions servent à créer des signatures de fichiers.

V. Exemples de systèmes de cryptographie

a) à clés privées

Blowfish, DES, IDEA, RC2, RC5, RC6, RC4, Rijndael, SEAL, TripleDES

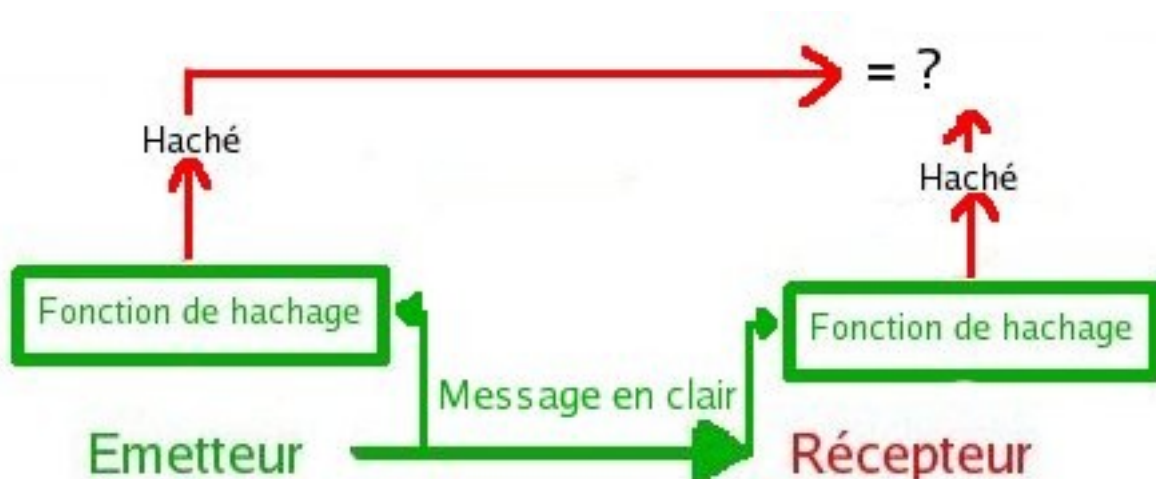
b) à clés publiques

Diffie-Hellman, DSA, PGP, RSA

c) fonction de hachage

MD2, MD4, MD5(128bits), RIPEMD-128, RIPEMD-160, SHA0(160bits), SHA1(160bits), Tiger

VI. Signature électronique

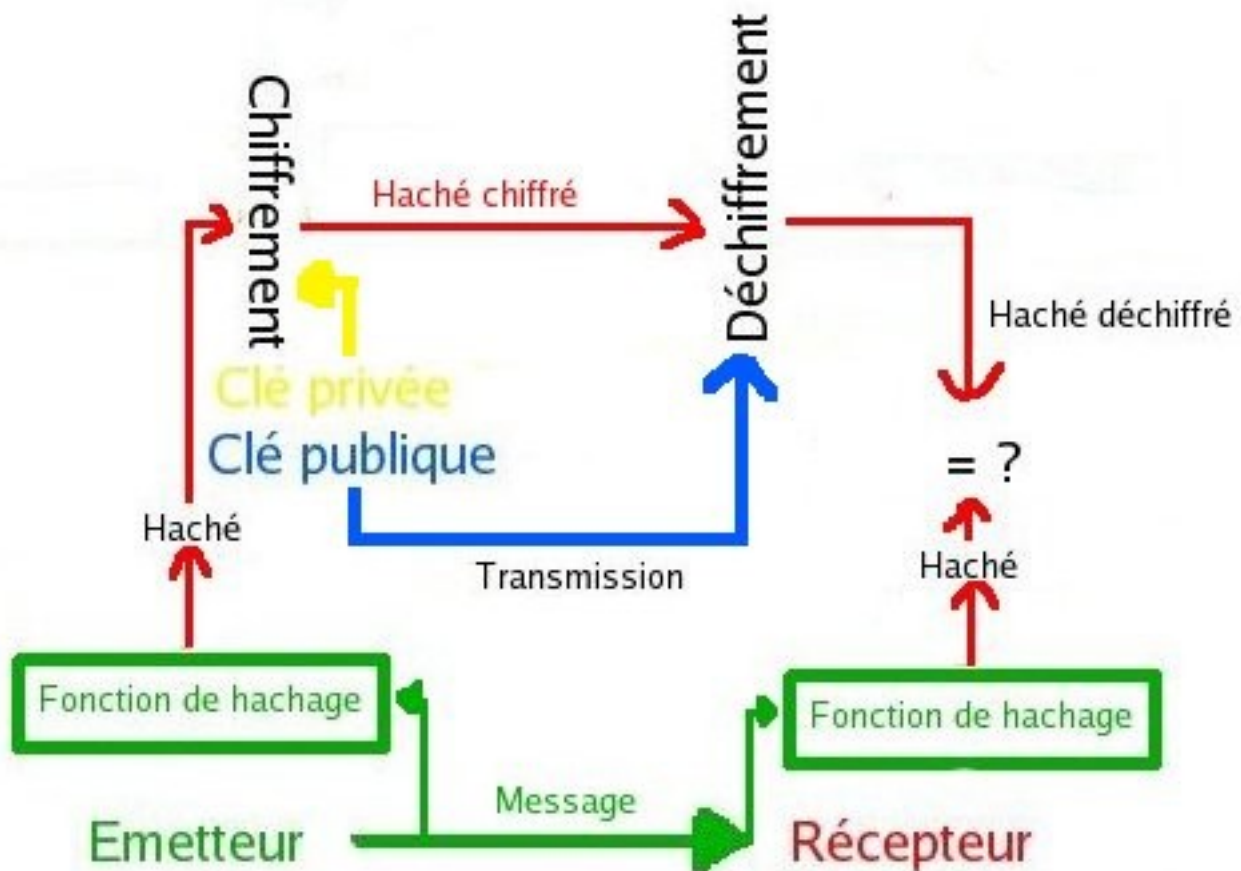


Une signature électronique permet de garantir l'authenticité de l'expéditeur et/ou l'intégrité du contenu du message. Cela permet aussi d'avoir la certitude que l'expéditeur a bien envoyé le message puis qu'il est signé.

Pour vérifier que le message est bien celui envoyé par l'expéditeur, on recalcule le digest du

message reçu, on compare avec le digest reçu : s'ils sont différents, c'est que le message ou son digest a été modifié.

VII. Scellement de données



Il demeure un problème : on peut seulement savoir si le message a été modifié mais pas être sûr que le message vient bien de la bonne personne. Pour garantir cela, il suffit à l'expéditeur de crypter (cela s'appelle *signer*) le digest du message avec sa clé privée : cela s'appelle un sceau. Le destinataire n'aura alors plus qu'à décrypter le sceau reçu avec la clé publique de l'expéditeur pour obtenir le digest et le comparer avec le digest calculé avec le message reçu.

VIII. Certificats

a) Principe



Le problème des clés publiques est qu'un pirate peut arriver à remplacer votre clé publique par la sienne, par exemple sur un annuaire. Et toutes les personnes croyant encrypter pour vous encrypteront pour le pirate. Les systèmes à clés publiques ne garantissent donc pas que la clé est bien celle de l'utilisateur à qui elle est censée appartenir.

Les certificats servent à cela : ils garantissent que la clé appartient bien à la personne qui l'a générée. Pour cela, des organismes de certification appelés CA (Certification Authority) vous fournissent un certificat (moyennant finances) garantissant cela. Elles sont en charge de délivrer des certificats, de leur donner une date de validité et de révoquer les certificats en cas de problèmes de confiance.

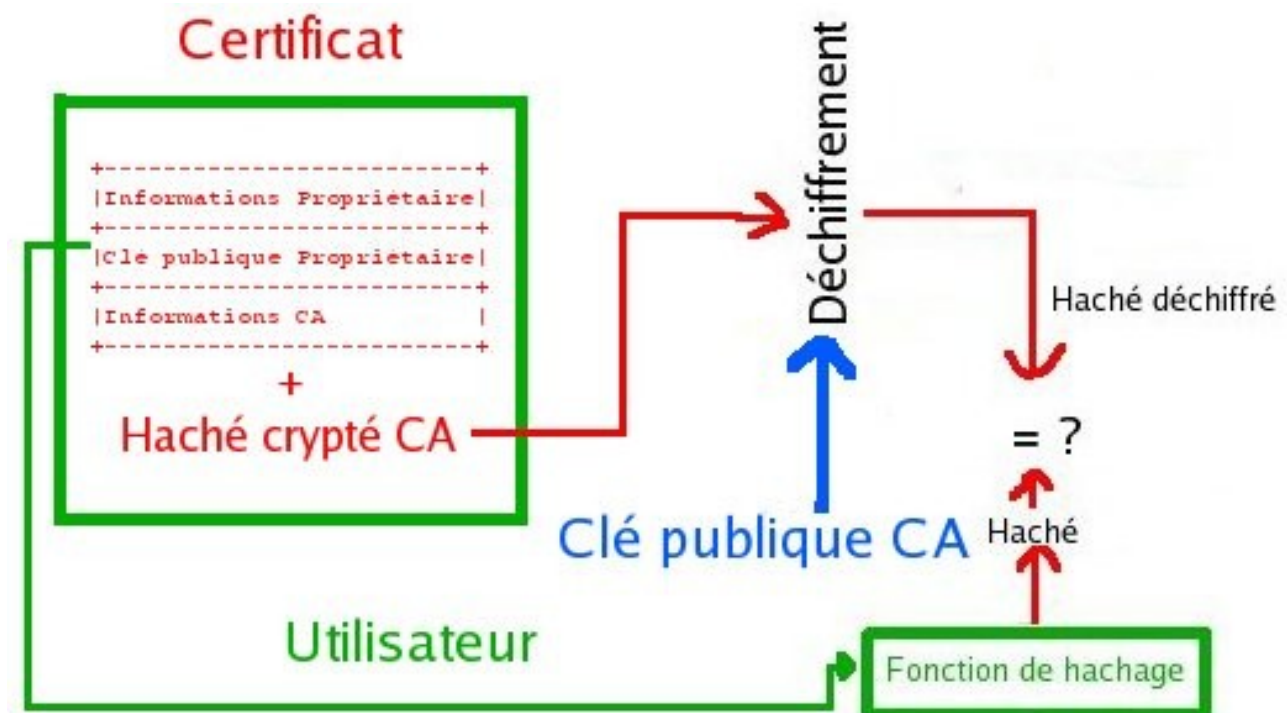
Un certificat contient (suivant la normalisation X.509):

- des informations sur le certificat :
 - la version de la norme X.509
 - le numéro de série du certificat
 - l'algorithme de cryptage utilisé pour la signature de celui-ci
 - la date de début de validité
 - la date de fin de validité
- des informations sur le demandeur/propriétaire :
 - **la clé publique du propriétaire du certificat**
 - les coordonnées du propriétaire (adresse, pays, email...)

- le nom du serveur
- des informations sur l'autorité de certification CA :
 - le nom (DN : Distinguished Name) de la CA (nom, adresse...)
 - la signature/sceau de la CA

Toutes ces informations sont signées par l'autorité de certification : elle calcule un digest du contenu du certificat puis elle crypte ce digest avec sa clé privée. Le certificat est donc scellé. La clé publique de l'autorité de certification a été au préalable très largement diffusée.

Lorsque quelqu'un communique avec cette personne, elle se procure le certificat de cette personne. Celui-ci lui permet de connaître le nom du CA qui a signé le certificat et donc d'obtenir la clé publique de ce CA.



Pour vérifier la validité du certificat, et donc être sûr de parler à la bonne personne, elle doit

- trouver le nom de l'algorithme de chiffrement utilisé pour la signature du certificat
- calculer le digest du certificat
- décrypter la signature présente dans le certificat avec l'algorithme trouvé et la clé publique de la CA
- comparer le digest calculé et le digest décrypté : s'ils sont égaux, c'est OK...

Il existe différents type de certificats :

- Les certificats signés par un organisme de certification : ils servent pour les serveurs accessibles de l'extérieur d'une organisation (site de vente en ligne) dès que l'utilisateur est un client ou un anonyme. Ils permettent d'assurer la sécurité des transactions.
- Les certificats autosignés : ils sont réservés aux tests et à l'usage en interne d'une organisation. Ils sont signés par un serveur local et ne doivent pas être présents sur des serveurs publics.

Il existe aussi plusieurs types d'utilisation des certificats :

- Les certificats clients servent à identifier un utilisateur afin de lui octroyer des droits : on peut le stocker sur tout support adéquat (poste de travail, carte à puce). Il est transmis au serveur lors de l'accès à celui-ci, en guise d'authentification par exemple. Les clés de ce type de certificat doit avoir une longueur d'au moins 512bits (et jusqu'à 1024bits).
- Les certificats serveur servent pour faire le lien entre le service proposé, généralement sous forme de page web, et le propriétaire du service (site de vente en ligne...). Ils garantissent l'identité du propriétaire du service et sécurise la transaction avec le serveur.
- Les certificats VPN qui servent à créer un tunnel crypté entre deux sites distants : chaque poste client, chaque serveur et chaque équipement réseaux ont leur propre certificat. On utilise souvent des protocoles comme PPTP, L2F, L2TP ou IPSec...

b) Certificat de révocation

Un tel certificat sert à indiquer publiquement que l'on n'utilise plus une paire de clés. Pour éviter que n'importe qui puisse générer un tel certificat, ce dernier est signé par la clef privée de la paire à révoquer. La validité d'un certificat de révocation est ainsi facilement vérifiable par tout un chacun qui possède la clé publique correspondant à la clé privée.

Bibliographie

[Cryptographie – Wikipédia](#)

[Cryptographie](#)