INTITULÉ : HACKING ET SECURITE - NIVEAU 1

PRÉNOM : ARTHUR

NOM : MENDJANA

Qualification des Services Intellectuels OPQF

Fédération de la Formation Professionnelle

3 – SECURISATION DES ECHANGES

3-1 Notion de cryptographie

Définition

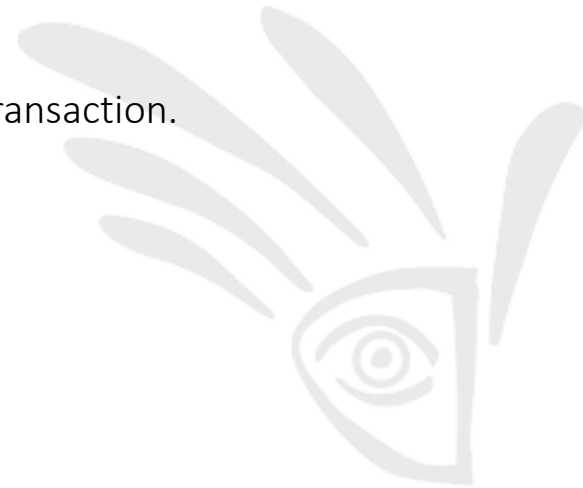
Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligible. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffrer

4 propriétés :

- La confidentialité : consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.
- L'intégrité : vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.
- L'authentification : consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants

que son partenaire est bien celui qu'il croit être un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

- La non répudiation : de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.



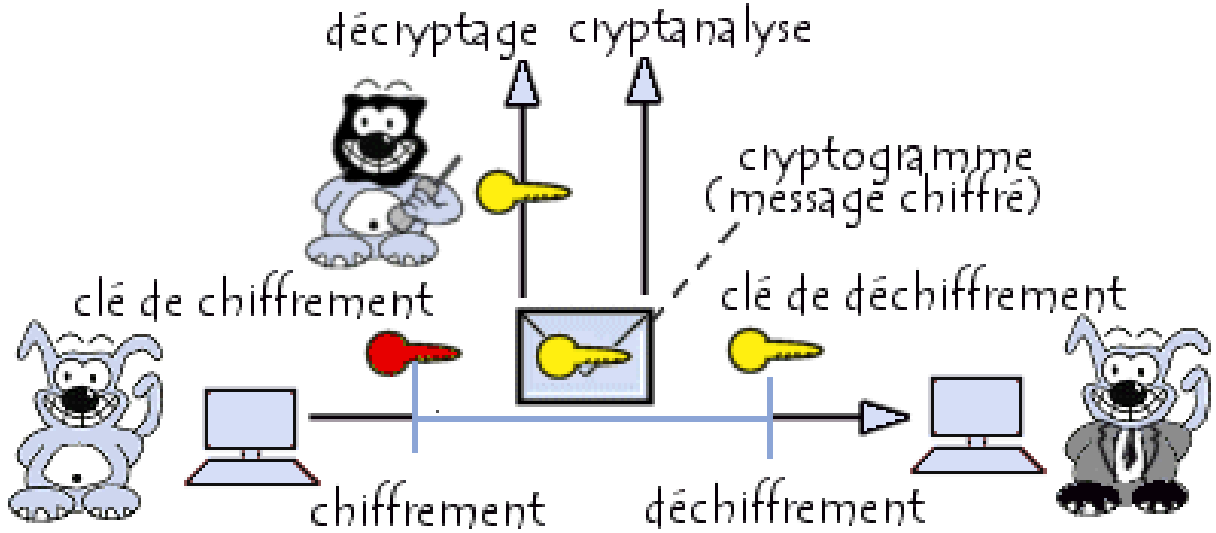
3-1 Notion de cryptographie

La cryptographie est essentiellement basée sur l'arithmétique : Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis ensuite de faire des calculs sur ces chiffres pour :

- d'une part les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification est appelé ***message chiffré*** par opposition au message initial, appelé ***message en clair*** ;
- faire en sorte que le destinataire saura les déchiffrer.

Le fait de coder un message de telle façon à le rendre secret s'appelle **chiffrement**. La méthode inverse, consistant à retrouver le message original, est appelée **déchiffrement**.

Clé = paramètre utilisé en entrée d'une opération cryptographique.

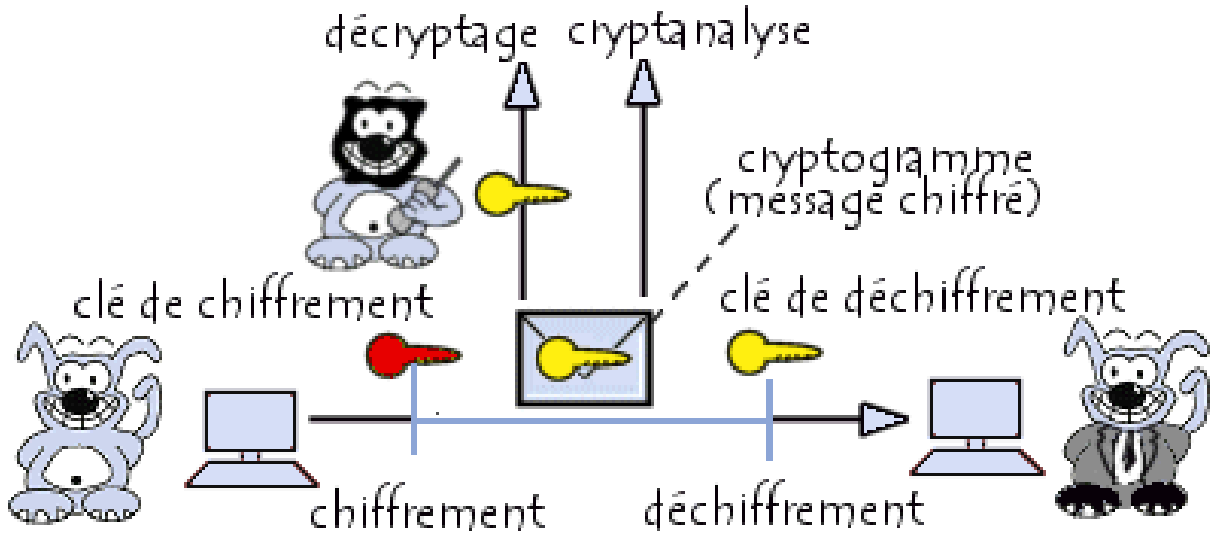


3-1 Notion de cryptographie

Le chiffrement d'informations ou du message se fait généralement à l'aide d'une ***clef de chiffrement***, le déchiffrement nécessite quant à lui une ***clef de déchiffrement***.

On distingue généralement deux types de clefs :

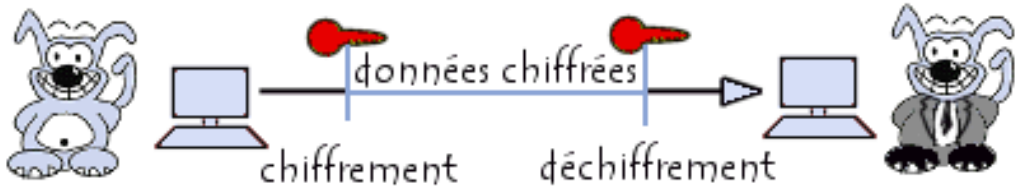
- **Les clés symétriques**: il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.
- **Les clés asymétriques**: il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement



3-1 Notion de cryptographie

❑ Chiffrement symétrique

Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clé pour le chiffrement et le déchiffrement.



Le chiffrement consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles.
le chiffrement symétrique impose d'avoir un canal sécurisé pour l'échange de la clé, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement.

Le principal inconvénient d'un cryptosystème à clefs secrètes provient de l'échange des clés. En effet, le chiffrement symétrique repose sur l'échange d'un secret (les clés). Ainsi, se pose le problème de la distribution des clés

Qu'entend-on par clé ?
On appelle clé une valeur utilisée dans un algorithme de cryptographie, afin de chiffrer une donnée.
Il s'agit en fait d'un nombre complexe dont la taille se mesure en bits. On peut imaginer que la valeur correspondant à 1024 bits est absolument gigantesque. Voir aussi bits bytes.

3-1 Notion de cryptographie

Plus la clé est grande, plus elle contribue à élever la sécurité à la solution. Toutefois, c'est la combinaison d'algorithme complexe et de clés importantes qui seront la garantie d'une solution bien sécurisée.

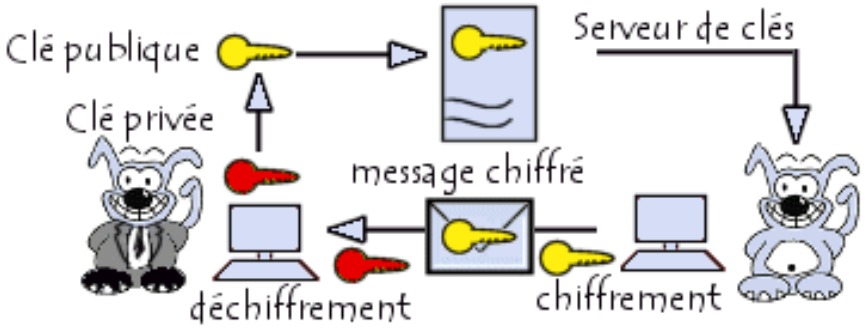
Les clés doivent être stockées de manière sécurisée et de manière à ce que seul leur propriétaire soit en mesure de les atteindre et de les utiliser.

Auguste Kerckhoffs *« La sécurité d'un système cryptographique ne doit pas reposer sur le secret de l'algorithme mais sur le secret de clé »*

❑ Le chiffrement asymétrique

Le principe de **chiffrement asymétrique** (appelé aussi **chiffrement à clés publiques**) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par *Whitfield Diffie* et *Martin Hellman*.
Dans un cryptosystème asymétrique (ou cryptosystème à clés publiques), les clés existent par paires (le terme de bi-clés est généralement employé) :

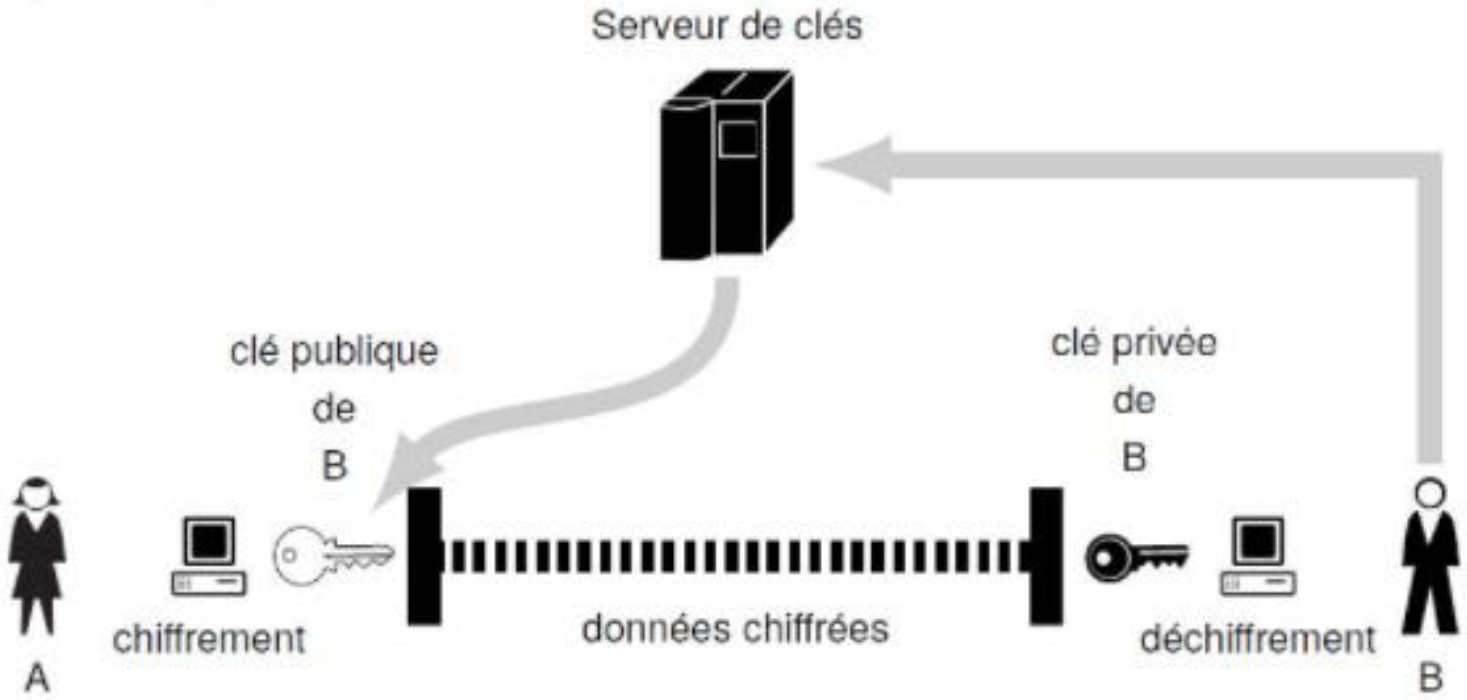
- Une clé publique pour le chiffrement ;
- Une clé secrète pour le déchiffrement.



Lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire (qu'il trouvera par exemple dans un serveur de clés tel qu'un annuaire LDAP). Ce dernier sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).

3-1 Notion de cryptographie

Principe



3-1 Notion de cryptographie

Conseils : Il est conseillé d'utiliser des clés de plus de **256bits** pour un chiffrement symétrique et de **2048bits** et plus pour un chiffrement asymétrique car la création de clés solides est le fondement du chiffrement.

Principe : Alice et **Bob** veulent communiquer dispose chacun d'une paire clé privée et publique. Pour envoyer un message à Bob Alice devrait chiffrer le message avec la clé publique de Bob et déchiffre le message avec sa clé privée.

	Chiffrement symétrique	Chiffrement asymétrique
Définition	Utilise une seule et même clé pour le chiffrement et déchiffrement	Utilise une clé publique pour le chiffrement et une clé privée pour le déchiffrement
Performance	Rapide en exécution (A cause de la longueur des clés) **2(Exposant nbre de bits) clés**	Lent en exécution en raison de la charge de calcul élevée et des algorithmes plus complexe **2(Exposant nbre de bits) clés**
Algorithme	AES, DES, 3-DES, RC4	RSA, DSA, Diffie Hellman, El Gamal
Objectif	Utilisé pour la transmission des données en masse	Souvent l'échange des clés sécrètes

3-1 Notion de cryptographie

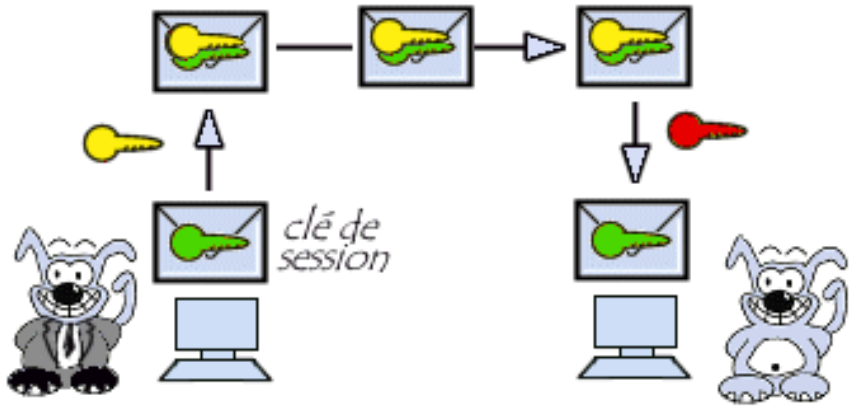
Chiffrement : Message en clair + *clé de chiffrement* + *Algorithme de chiffrement* = **Message chiffré**

Déchiffrement : Message chiffré + *clé de déchiffrement* + *Algorithme de déchiffrement* = **Message en clair**

ECHANGE DE CLES SECURISE

Notion de Clé de session :
Les algorithmes asymétriques (entrant en jeu dans les cryptosystèmes à clé publique) permettent de s'affranchir de problèmes liés à l'échange de clé via un canal sécurisé. Toutefois, ces derniers restent beaucoup moins efficaces (en terme de temps de calcul) que les algorithmes symétriques.
Le principe de la clé de session est simple : il consiste à générer aléatoirement une clé de session de taille raisonnable, et de chiffrer celle-ci à l'aide d'un algorithme de chiffrement à clef publique (plus exactement à l'aide de la clé publique du destinataire).
Le destinataire est en mesure de déchiffrer la clé de session à l'aide de sa clé privée. Ainsi, expéditeur et destinataires sont en possession d'une clé commune dont ils sont seuls connaisseurs. Il leur est alors possible de s'envoyer des documents chiffrés à l'aide d'un algorithme de chiffrement symétrique.

L'algorithme de *Diffie-Hellman* (du nom de ses inventeurs Diffie et Hellman) a été mis au point en 1976 afin de permettre l'échange de clés à travers un canal non sécurisé. Il repose sur la difficulté du calcul du logarithme discret dans un corps fini.



3-1 Notion de cryptographie

Solution Hybride

Pour remédier au problème d'échange de clé, de temps de calcul long pour le chiffrement asymétrique, et profiter des avantages du chiffrement asymétrique (la solidité des clés) et donc une sécurité plus grande, une solution a été mise en place.
C'est une combinaison du chiffrement symétrique et du chiffrement asymétrique

Expéditeur :

- Générer une clé session invisible à l'utilisateur
- Chiffrer de façon symétrique le document (message) avec la clé de session
- Chiffrer ensuite cette clé de session avec la clé publique du destinataire puis détruire la clé de session
- Envoyer le tout (clé de session chiffrée + message chiffré) au destinataire

Destinataire :

- Avec sa clé publique il va déchiffrer la clé de session
- Avec la clé de session il va déchiffrer le message

Avantages : Rapidité du chiffrement symétrique, robustesse d'un algorithme et du chiffrement asymétrique (vu la longueur)

3-2 Fonctions de hachage

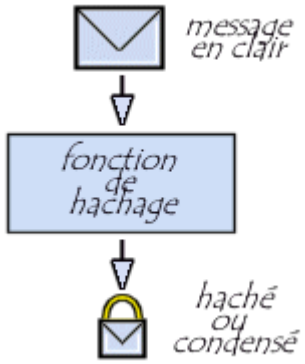
Signature électronique

Le paradigme de **signature électronique** (appelé aussi *signature numérique*) est un procédé permettant de garantir l'authenticité de l'expéditeur (fonction d'*authentification*) et de vérifier l'intégrité du message reçu.
La signature électronique assure également une fonction de non-répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message (autrement dit elle empêche l'expéditeur de nier avoir expédié le message).

Qu'est-ce qu'une fonction de hachage ?

Une **fonction de hachage** (parfois appelée *fonction de condensation*) est une fonction permettant d'obtenir un condensé (appelé aussi *haché* ou en anglais *message digest*) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense.

La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son haché).
D'autre part, il doit s'agir d'une fonction à sens unique (*one-way function*) afin qu'il soit impossible de retrouver le message original à partir du condensé. S'il existe un moyen de retrouver le message en clair à partir du haché, la fonction de hachage est dite « à brèche secrète ».



3-2 Fonctions de hachage

Ainsi, le haché représente en quelque sorte l'empreinte digitale (en anglais fingerprint) du document.

Les algorithmes de hachage les plus utilisés actuellement sont :

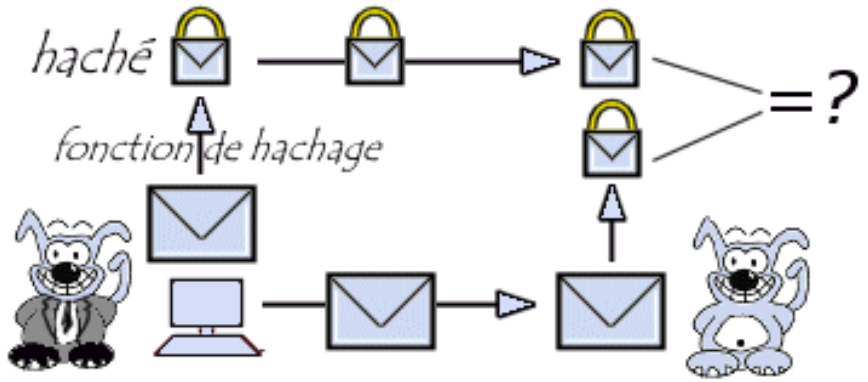
•**MD5** (*MD* signifiant *Message Digest*). Développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier)

•**SHA** (pour *Secure Hash Algorithm)*, pouvant être traduit par *Algorithme de hachage sécurisé*) crée des empreintes d'une longueur de 160 bits SHA-1 est une version améliorée de SHA datant de 1994 et produisant une empreinte de 160 bits à partir d'un message d'une longueur maximale de 2^{64} bits en le traitant par blocs de 512 bits.

Vérification d'intégrité

En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré (intentionnellement ou de manière fortuite) durant la communication.

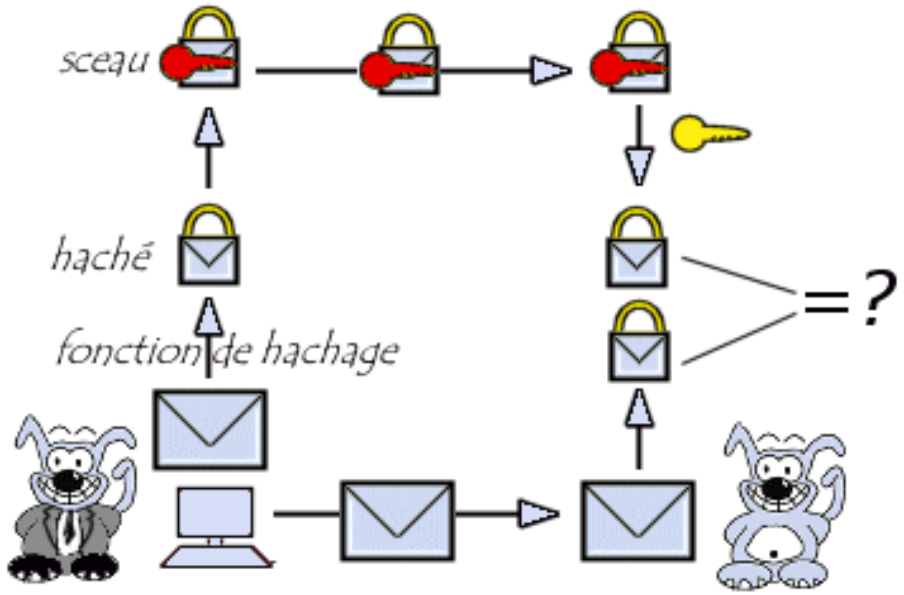
Lors de la réception du message, il suffit au destinataire de calculer le haché du message reçu et de le comparer avec le haché accompagnant le document. Si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondront pas.



3-2 Fonctions de hachage

Signature numérique ou le scellement des données

L'utilisation d'une fonction de hachage permet de vérifier que l'empreinte correspond bien au message reçu, mais rien ne prouve que le message a bien été envoyé par celui que l'on croit être l'expéditeur.
Ainsi, pour garantir l'authentification du message, il suffit à l'expéditeur de chiffrer (on dit généralement signer) le condensé à l'aide de sa clé privée (le haché signé est appelé sceau) et d'envoyer le sceau au destinataire.



A réception du message, il suffit au destinataire de déchiffrer le sceau avec la clé publique de l'expéditeur, puis de comparer le haché obtenu avec la fonction de hachage au haché reçu en pièce jointe. Ce mécanisme de création de sceau est appelé *scellement*.

3-3 Certificats

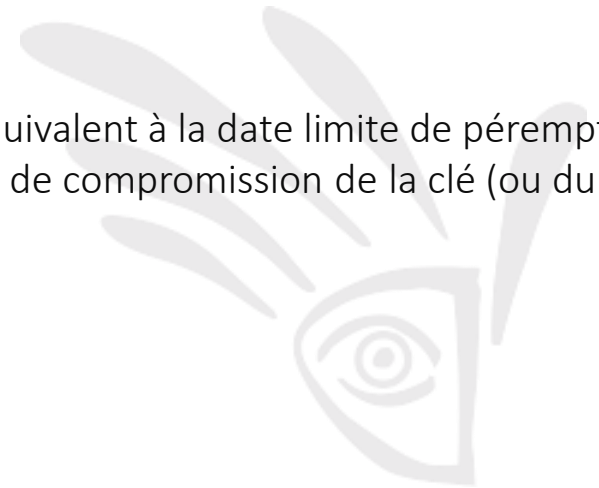
Introduction à la notion de certificat

Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique. Généralement le partage de cette clé se fait au travers d'un annuaire électronique (généralement au format LDAP) ou bien d'un site web.

Toutefois ce mode de partage a une grande lacune : rien ne garantit que la clé est bien celle de l'utilisateur a qui elle est associée.
En effet un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique.
Ainsi, le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.

Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA pour Certification Authority).

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).



3-3 Certificats

Structure d'un certificat ?

Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

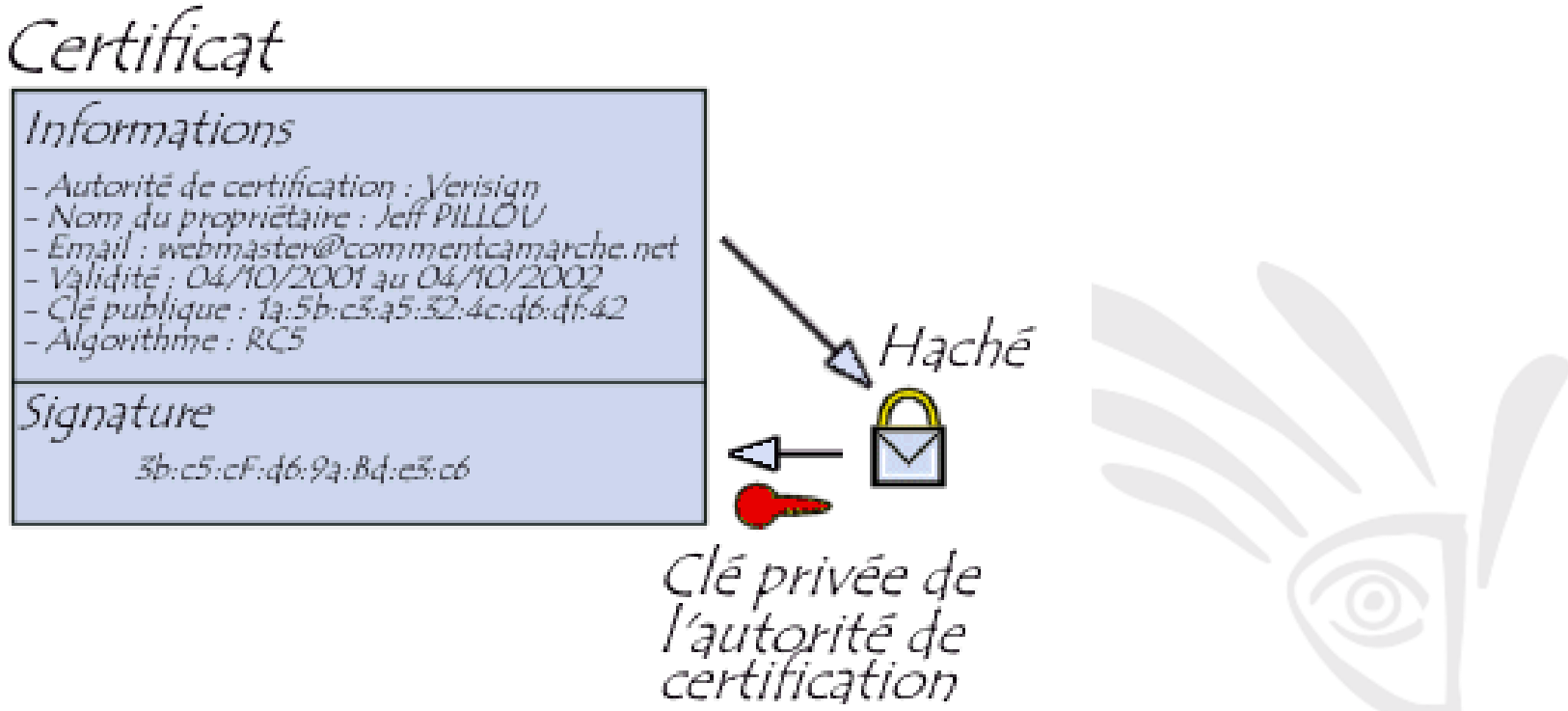
La structure des certificats est normalisée par le standard X.509 de l'UIT (plus exactement X.509v3), qui définit les informations contenues dans un certificat :

- *La version de X.509 à laquelle le certificat correspond ;*
- *Le numéro de série du certificat ;*
- *L'algorithme de chiffrement utilisé pour signer le certificat ;*
- *Le nom (DN, pour Distinguished Name) de l'autorité de certification émettrice ;*
- *La date de début de validité du certificat ;*
- *La date de fin de validité du certificat ;*
- *L'objet de l'utilisation de la clé publique ;*
- *La clé publique du propriétaire du certificat ;*
- *La signature de l'émetteur du certificat (thumbprint).*

3-3 Certificats

Structure d'un certificat ?

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par **l'autorité de certification**, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.

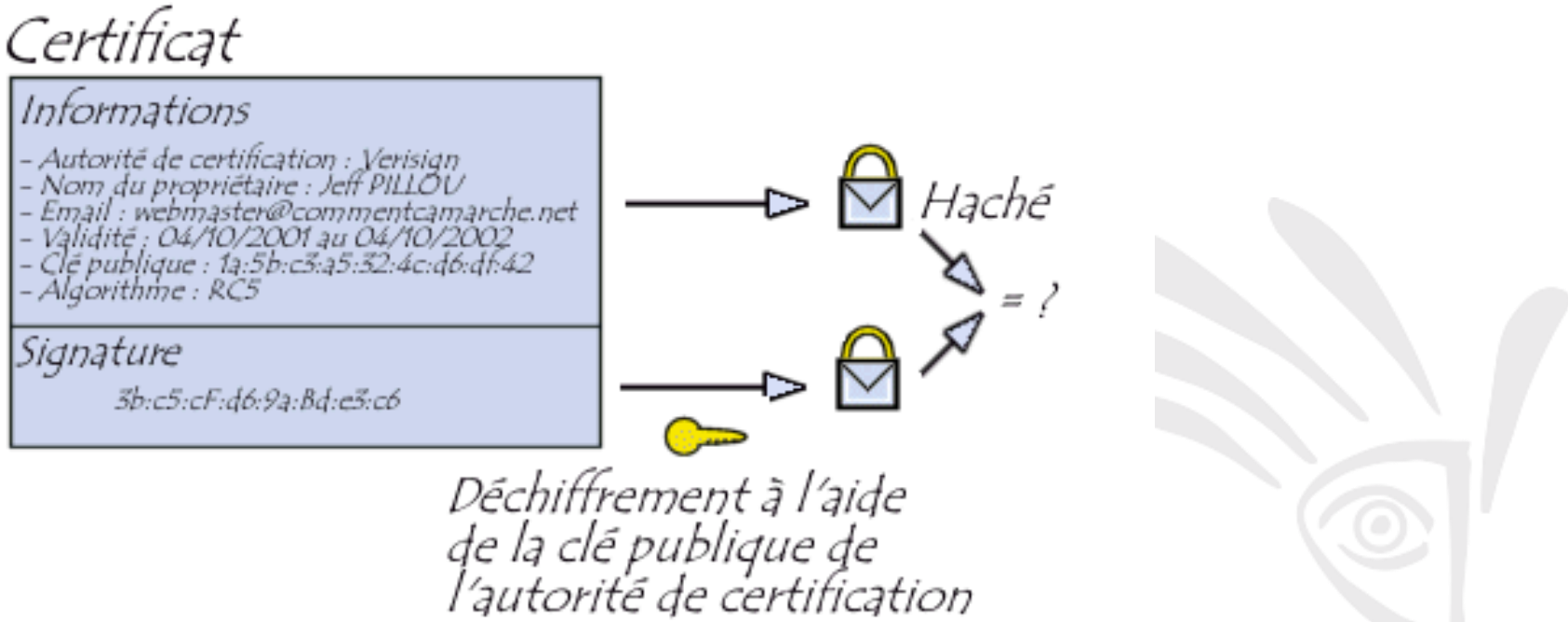


3-3 Certificats

Structure d'un certificat ?

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire.
Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification.

Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.



3-3 Certificats

Signatures de certificats

On distingue différents types de certificats selon le niveau de signature :

- Les **certificats auto-signés** sont des certificats à usage interne. Signés par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation, par exemple pour le besoin d'un intranet. Il est ainsi possible d'effectuer une authentification des utilisateurs grâce à des certificats auto-signés.

- Les **certificats signés par un organisme de certification** sont nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes, par exemple dans le cas d'un site web sécurisé accessible au grand public. Le certificateur tiers permet d'assurer à l'utilisateur que le certificat appartient bien à l'organisation à laquelle il est déclaré appartenir.

Les certificats servent principalement dans trois types de contextes :

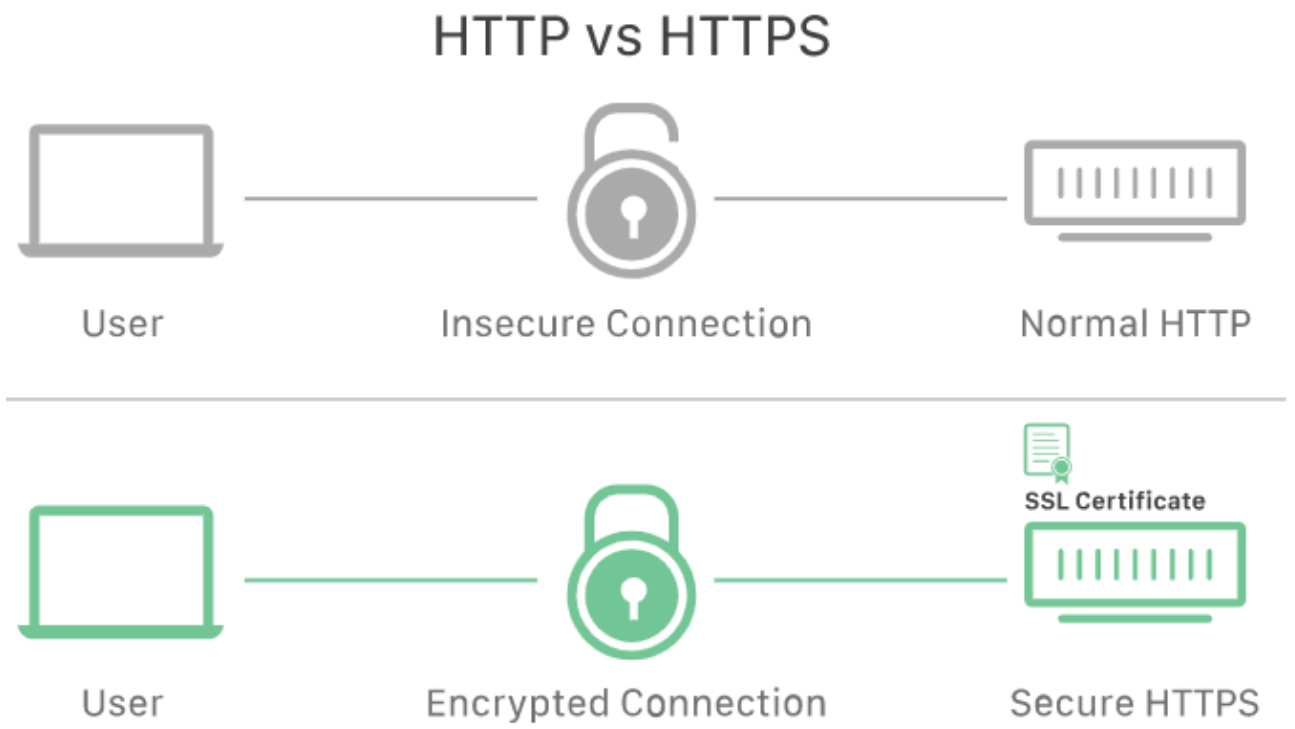
•Le **certificat client**, stocké sur le poste de travail de l'utilisateur ou embarqué dans un conteneur tel qu'une carte à puce, permet d'identifier un utilisateur et de lui associer des droits. Dans la plupart des scénarios il est transmis au serveur lors d'une connexion, qui affecte des droits en fonction de l'accréditation de l'utilisateur. Il s'agit d'une véritable carte d'identité numérique utilisant une paire de clé asymétrique d'une longueur de 512 à 1024 bits.

•Le **certificat serveur** installé sur un serveur web permet d'assurer le lien entre le service et le propriétaire du service. Dans le cas d'un site web, il permet de garantir que l'URL et en particulier le domaine de la page web appartiennent bien à telle ou telle entreprise. Par ailleurs il permet de sécuriser les transactions avec les utilisateurs grâce au protocole SSL.

•Le **certificat VPN** est un type de certificat installé dans les équipement réseaux, permettant de chiffrer les flux de communication de bout en bout entre deux points (par exemple deux sites d'une entreprise). Dans ce type de scénario, les utilisateurs possèdent un certificat client, les serveurs mettent en œuvre un certificat serveur et les équipements de communication utilisent un certificat particulier (généralement un certificat IPSec).

3-3 SSL

SSL, ou Secure Sockets Layer, est un protocole de sécurité Internet basé sur le chiffrement. Il a été développé pour la première fois par Netscape en 1995 dans le but de garantir la confidentialité, l'authentification et l'intégrité des données dans les communications Internet. Le SSL est le prédécesseur du chiffrement moderne TLS utilisé aujourd'hui.
Un site web qui met en œuvre le protocole SSL/TLS comporte un «HTTPS» dans son URL au lieu d'un « HTTP ».



3-3 SSL

Comment fonctionne le SSL/TLS ?

•Afin de garantir un degré élevé de **confidentialité**, le SSL chiffre les données transmises sur le Web. Cela signifie que quiconque tente d'intercepter ces données ne verra qu'un mélange confus de caractères quasiment impossible à déchiffrer.
•Le SSL lance un processus d'**authentification** appelé handshake entre deux dispositifs de communication pour s'assurer que les deux appareils sont vraiment ceux qu'ils prétendent être.
•Le SSL signe également numériquement les données afin d'assurer **l'intégrité des données**, en vérifiant que les données ne sont pas falsifiées avant d'atteindre leur destinataire prévu.

Le protocole SSL a connu plusieurs versions, chacune plus sûre que la précédente. En 1999, le SSL a été mis à jour pour devenir le TLS.

Pourquoi le SSL/TLS est-il important ?

À l'origine, les données sur le Web étaient transmises en texte brut que n'importe qui pouvait lire s'il interceptait le message. Par exemple, si un consommateur visitait un site web d'achat, passait une commande et saisissait son numéro de carte de crédit sur le site, ce numéro de carte de crédit voyageait sur Internet sans être caché.

Le SSL a été créé pour corriger ce problème et protéger la vie privée des utilisateurs. En chiffrant toutes les données qui circulent entre un utilisateur et un serveur web, le protocole SSL garantit que toute personne qui intercepte les données ne peut voir qu'un ensemble de caractères brouillés. Le numéro de carte de crédit du consommateur est désormais sécurisé, visible uniquement sur le site web où l'utilisateur l'a saisi.
Le SSL permet également de mettre fin à certains types de cyberattaques : il authentifie les serveurs web, ce qui est important, car les attaquants tentent souvent de créer de faux sites web pour tromper les utilisateurs et voler des données. Il empêche également les attaquants de manipuler les données en transit, à la manière du sceau de sécurité sur un emballage de médicaments.

3-3 SSL

Qu'est-ce qu'un certificat SSL ?

Le protocole SSL ne peut être mis en œuvre que par les sites web qui possèdent un certificat SSL (techniquement un « certificat TLS »). Un certificat SSL est comme une carte d'identité ou un badge qui prouve qu'une personne est bien celle qu'elle prétend être. Les certificats SSL sont stockés et affichés sur le Web par un serveur de site ou d'application.
L'une des informations les plus importantes d'un certificat SSL est la clé publique du site web.

La clé publique rend le chiffrement possible. L'appareil d'un utilisateur visualise la clé publique et l'utilise pour établir des clés de chiffrement sécurisées avec le serveur web. Entre-temps, le serveur web dispose également d'une clé privée qui est gardée secrète ; la clé privée déchiffre les données chiffrées avec la clé publique.
Les autorités de certification (AC) sont responsables de l'émission des certificats SSL.

3-3 SSL

AUTHENTIFICATION PAR CERTIFICAT