Université Abou Bakr Belkaid
Faculté des sciences
Département d'Informatique

Sécurité Informatique

Chapitre 2: Mécanismes de Défense

Présenté par Mme Labraoui N.

Master 1 Réseaux et systèmes distribués

2019-2020

Introduction

Evénements marquants

- Attaques des sites CNN, Yahoo, Amazon, e*trade
- Virus "I LOVE YOU"
- Vol de 55000 numéros de cartes bancaires par un Russe
- Vol de fichiers médicaux (5000 patients)
- Faux communiqué de presse fait perdre 40% aux actions d'une société

Introduction

Exemple : www.doj.gov
(Department Of Justice)

Introduction

Conséquences

- ⇨ perte de temps, donc d'argent (sites en-ligne)
- ⇨ perte de réputation (chantage financier)
- ⇨ mise hors service des serveurs (DoS)
- ⇨ corruption possible du système / perte de données
- ⇨ vols de numéros de cartes bancaires : sans commentaire
- ⇨ vol d'informations personnelles : le site peut être poursuivi
- ⇨ publications d'infos intox : conséquences graves
- ⇨ et les centrales nucléaires … !

Introduction

Evolution des types d'intrusion

1988 :
- attaques sur mots de passe
- exploitation manuelle de vulnérabilités

Aujourd'hui :
- attaques sur mots de passe
- exploitation de vulnérabilités sous forme automatique
- trous dans les protocoles
- examen des sources
- attaques http, ftp, mail
- installation de sniffers
- falsification d'adresse IP
- refus de service
- scanning à grande échelle
- attaques distribuées

Mécanismes de défense

- **Chiffrement :** algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.
- **Signature numérique:** données ajoutées pour vérifier l'intégrité ou l'origine des données.
- **Notarisation :** utilisation d'un tiers de confiance pour assurer certains services de sécurité.
- **Contrôle d'accès :** vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.

Mécanismes de défense

- **Contrôle du routage :** sécurisation des chemins (liens et équipements d'interconnexion).
- **Contrôle d'accès aux communications :** le moyen de communication n'est utilisé que par des acteurs autorisés. Par VPN ou tunnels.
- **Certification :** preuve d'un fait, d'un droit accordé.
- **Distribution de clefs :** distribution sécurisée des clefs entre les entités concernées.

- Les outils cryptographiques de sécurité
- Les protocole de sécurité SSL, IPSec
- Architecture de sécurité informatiques (dispositifs de sécurité): pare feu, IDS , les pots de miel

La cryptographie

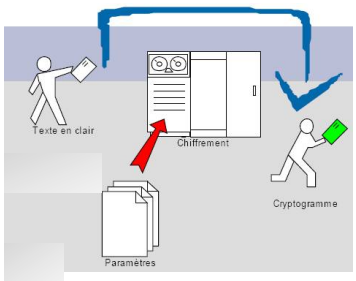
- Depuis l'Egypte ancienne, l'homme a voulu pouvoir échanger des informations de façon **confidentiel.**
- Il existe de nombreux domaines où ce besoin est vital :
  - **militaire** (sur un champ de bataille ou bien pour protéger l'accés à l'arme atomique) ;
  - **commercial** (protection de secrets industriels) ;
  - **bancaire** (protection des informations liées à une transaction financière);
  - de la **vie privée** (protection des relations entre les personnes) ;
  - diplomatique (le fameux « téléphone rouge » entre Etats-Unis et Union soviétique) ;
- ...

La cryptographie

L e chiffrement

$$M \xrightarrow{E_k} C$$

- **Texte (message) M en clair : Une information dans sa forme de base**.
- **Texte (message) C :** chiffré, crypté, codé, brouillé, ou cryptogramme : **l'information transformée de façon à ce que son sens soit caché**
- L'opération de transformation Ek est appelée :le chiffrement, le cryptage, l'encryptage, le codage, le brouillage



La cryptographie

L e chiffrement

- **Un chiffre concerne plutôt une** technique de cryptage portant sur des éléments de taille fixe (caractères alphabétiques par exemple).
- **Un code désigne plutôt un** cryptage portant sur des éléments de taille variable (mots ou phrases)
- La possibilité de crypter repose sur la connaissance de:

  la clé (algorithme E, secret k)
- l'ensemble des paramètres permettant la réalisation des opérations de cryptage ou de chiffrement.

La cryptographie

L e déchiffrement

$$C \xrightarrow{\quad D_{k'} \quad} M$$

- **Déchiffrer un message chiffré C est** l'opération qui permet de restituer un texte en clair M à partir d'une clé de déchiffrement Dk' que l'on possède.
- **Décrypter ou casser un code c'est** parvenir au texte en clair sans posséder au départ les règles ou documents nécessaires au chiffrement.
- L'art de définir des codes est **la cryptographie (cryptographe).**
- L'art de casser des codes est appelé **cryptanalyse ou cryptologie** (cryptanalyste, cryptologue ou casseur de codes)
- **Un cryptosystème est l'ensemble des** deux méthodes de chiffrement et de déchiffrement utilisable en sécurité.

Les deux familles d'algorithmes de chiffrement

Cryptographie moderne

- Ce type de chiffrement repose sur l'utilisation :
  - d'un algorithme **public, connu de tous;**
  - d'une **clé.**
- Il correspond à la cryptographie moderne, par rapport aux codes par substitution et transposition.
- Auparavant, les algorithmes étaient **simples mais utilisaient des clés longues.** Exemple : un XOR entre le message à transmettre et une clé de même taille suffit à le rendre indéchiffrable…technique du masque jetable
- Maintenant, le but est d'utiliser des algorithmes **sophistiqués et complexes associés à des clés courtes.**
- Il existe deux familles d'algorithmes :
  1. La cryptographie symétrique
  2. La cryptographie asymétrique

Chiffrement à clé symétrique

- **Principe**
- Le cryptage à clé symétrique (ou secrète)
- La **même clé doit être employée pour chiffrer ou déchiffrer le message;**

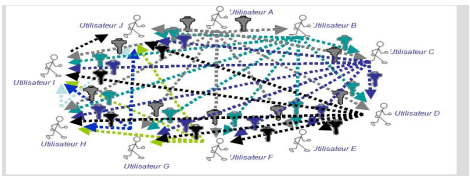
- Le chiffrement consiste alors à effectuer une opération entre la clé privée et les données à chiffrer.
- Le déchiffrement se fait à l'aide de cette **même clé secrète.**

Chiffrement à clé symétrique

- **Remarques**
- La qualité d'un crypto système symétrique se mesure par rapport :
  - à des propriétés statistiques des textes chiffrés ;
  - à la résistance aux classes **d'attaques connues.**
- **En pratique :** ***tant qu'un crypto système symétrique n'a pas été cassé, il est bon, après il est mauvais !***

Les limites de la cryptographie Symétrique

- **La multiplication des clés**
- Pour établir un canal de communication entre deux individus :
  - Il faut qu'il soit chiffré avec une **clé partagée entre les deux individus ;**
  - Il est ainsi confidentiel pour ceux qui ne possède pas la clé de chiffrement.



- Pour que deux canaux de communications soient indépendants l'un de l'autre, c-à-d. qu'une personne accède à l'un mais pas à l'autre, il faut que ces deux canaux utilisent des clés différentes.
- *Il est possible qu'un des interlocuteurs connaissent plusieurs clés utilisés dans différents canaux le reliant à des utilisateurs différents.*
- Exemple : l'utilisateur D possède une clé pour chaque lien (avec J, I, H, G, F et E).
- **Problème :** **comment échanger toutes ces clés ?**

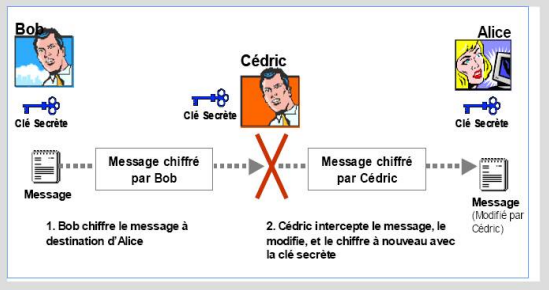
Les limites de la cryptographie Symétrique

- Le principal inconvénient d'un cryptosystème à clefs secrètes provient de **l'échange des clés.**
- Le chiffrement symétrique repose sur **l'échange d'un secret** (les clés).
- Pour être totalement sûr : les chiffrements à clés secrètes doivent utiliser des clés d'une longueur au moins égale à celle du message à chiffrer (*One Time Pad ou « Masque Jetable »)*
- **En pratique :** les clés ont une taille donnée, **suffisante.**

- Lors d'échange entre **plusieurs intervenants :** une clé est partagée que par 2 interlocuteurs, donc pour N interlocuteurs il faut N*(N-1)/2 clés.

Les limites de la cryptographie Symétrique

- **Pas d'intégrité et d'identification de l'auteur**
- Si Alice, Bob et Cédric partage le même lien de communication alors ils partagent la même clé de chiffrement symétrique.



- Chacun peut intercepter et modifer les messages qui s'échangent.

Cryptage à clé symétrique

- Ce cryptage repose sur la définition d'une formule mathématique de la forme :

  Donnée chiffrées = Fonction (données, clé)

- Avec une fonction inverse de la forme :

  Données = Fonction_inverse (données_chiffrées, clé)

- Dans cette méthode de chiffrement, on distingue deux types d'algorithmes :
  - l'algorithme **par bloc** qui prend une longueur spécifiée de données comme entrée, et produit une longueur différente de données chiffrées (exemple : DES, AES…)
  - l'algorithme en **flux continu** qui chiffre les données un bit à la fois (exemple : IDEA, CAST, RC4, SKIPjack…).

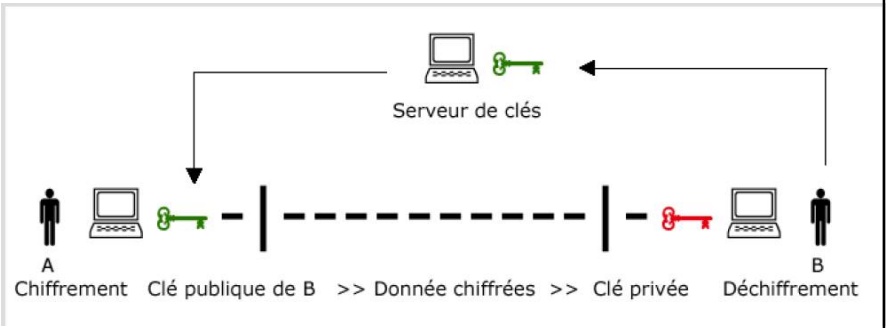
Cryptage à clé symétrique

- La plupart des codes utilisés
  - sont **relativements rapides ;**
  - peuvent s'appliquer à un **fort débit de donnée à transmettre.**
- *Il existe des processeurs spécialement conçu pour réaliser le chiffrement et le déchiffrement.*
- Principaux algorithmes utilisés :
  - **DES**, *Data Encryption System IBM 1977 ;*
  - **IDEA**, *International Data Encryption Algorithm Lai et Massey 1990 ;*
  - **Blowfish**, Schneir 1994.

- **Problème d'assurer la sécurité des clés.**
- Problème de la **distribution des clés,** qui doit se faire par un canal qui doit être sûr.

Chiffrement à clé asymétrique

- **Principe**
- Il utilise :
  - une **clé publique connue de tous ;**
  - une **clé privée connue seulement du destinataire du cryptogramme.**
- Ces chiffrements a « clé publique» ont été découvert par James Ellis (Angleterre) en 1969 et par Whitfield Diffie (Etats unis) en 1975.
- *L'idée de la conception de tels algorithmes revient à Diffie et Hellman en 1976.*



Chiffrement à clé asymétrique

- **Construction des clés**

  Les utilisateurs (A et B) choisissent une **clé aléatoire** dont ils sont seuls connaisseurs (il s'agit de la clé privée).

  A partir de cette clé, ils **déduisent** chacun automatiquement par un algorithme **la clé publique.**

  Les utilisateurs **s'échangent** cette clé publique au travers d'un canal **non sécurisé.**

- **Chiffrement d'un message**

  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 ou bien en signature d'un courrier électronique).

  Le destinataire sera en mesure de **déchiffrer** le message à l'aide de sa clé privée **(qu'il est seul à connaître).**

Chiffrement à clé asymétrique

- **Rapports entre les clés**

  La recherche de la clé privée à partir de la clé publique revient à résoudre un **problème mathématique notoirement très compliqué,** c-à-d. demandant un grand nombre d'opérations et beaucoup de mémoire pour effectuer les calculs -> infaisable !

- *Par exemple dans RSA, l'algorithme le plus utilisé actuellement, la déduction de la clé privée à partir de la clé publique revient à résoudre un problème de factorisation de grand nombre que lequel travaille les mathématiciens depuis plus de 2000 ans !*

- Le choix des clés doit être fait de la manière la plus **imprédictible possible :** éviter les mots du dictionnaire, nombres **pseudo-aléatoires** à germe de génération difficile à deviner, etc.

Cryptage à clé asymétrique

- Il repose sur la connaissance d'une fonction mathématique **unidirectionnelle** **("*one-way function*"),** munie d'une **porte arrière** **("*one-way trapdoor function*").**

- *Une fonction* ***unidirectionnelle est une fonction y = f(x) telle que, si l'on connaît la valeur y,*** il est *pratiquement impossible de calculer la valeur x (c'est-à-dire d'inverser la fonction f).*

- *On dit que cette fonction est* ***munie d'une porte arrière*** s'il existe une fonction x = g(y, z) telle que, si *l'on connaît z, il est facile de calculer x à partir de y. Z est appelée trappe.*

Chiffrement à clé asymétrique:

une métaphore avec des cadenas et des valises

- **Des clé et des cadenas**
- Alice :
  - crée une **clé aléatoire (la clé privée) ;**
  - puis fabrique un grand **nombre de cadenas (clé publique) qu'elle met à disposition dans un casier** accessible par tous (le casier joue le rôle de canal non sécurisé).
- Bob :
  - prend un **cadenas (ouvert) ;**
  - ferme une **valisette contenant le document qu'il souhaite envoyer ;**
  - envoie la valisette à Alice, propriétaire de la clé publique (le cadenas). *Cette dernière pourra ouvrir la valisette avec sa clé privée*

Cryptage à clé asymétrique

- **Les contraintes pour un tel algorithme**
- Il faut trouver un **couple de fonctions f** (fonction unidirectionnelle) et **g** (fonction de porte arrière) :

  C'est un problème mathématique difficile !
- Au départ, le système à clé publique n'a d'abord été qu'une idée dont la faisabilité restait à démontrer.
- **Des algorithmes ont été proposés par des mathématiciens**
- Un des premiers algorithmes proposé repose sur la **factorisation du produit de deux grands nombres entiers.**
- Cette factorisation demanderait un temps de calcul de plusieurs millions d'années.

  Le problème est résolu !
- Cet algorithme a été proposé par Rivest, Shamir et Adleman en 1977, ce qui a donné naissance à RSA.

Cryptage à clé asymétrique

- RSA: L'idée générale est la suivante :
- la **clé publique c** est le produit de **deux grands nombres entiers;**
- la clé **privée z** est l'un de ces **deux nombres entiers;**
- g comporte la factorisation de c.
- *Seul Bob, qui connaît z, peut factoriser c et donc déchiffrer le message chiffré.*
- **La force du chiffrement** dépend de **la longueur de la clé utilisée.**
- Ce protocole a l'avantage d'utiliser des clés de longueur variable de 40 à 2048 bits ;
- Il faut actuellement utiliser une clé au minimum de 512 bits (Six laboratoires ont dû unir leurs moyens pour casser en août 1999 une clé à 512 bits)

L'authentification

- **L'authentification est suivie par l'autorisation**
- L'autorisation définit les ressources, services et informations que la personne identifiée peut utiliser, consulter ou mettre à jour, exemple : son courrier électronique, des fichiers sur un serveur FTP...
- **L'approche traditionnelle**
- Combinaison d'une identification et d'un mot de passe (code secret personnel).
- Le mot de passe doit posséder certaines caractéristiques : non trivial, difficile à deviner, régulièrement modifié, secret...
- Des outils logiciel ou hardware de génération de mots de passe existent, mais les mots de passe générés sont difficiles à retenir !
- **L'approche évoluée, la notion de challenge/réponse**

L'authentification

- **L'approche évoluée, la notion de challenge/réponse**
- Alice envoie à Bob un **message aléatoire (challenge)**
- Chiffement à **clé secrète :**
  - Alice et Bob partage une même clé secrète ;
  - Bob renvoie à Alice le message **chiffré à l'aide de la clé secrète (réponse) ;**
  - Alice peut **déchiffrer le message chiffré avec la clé secrète...C'est Bob !**
- Chiffrement à **clé publique :**
  - Bob renvoie à Alice le message chiffré à l'aide de sa clé privée (réponse) ;
  - exploitation de la propriété chiffrement(déchiffrement(M)) = déchiffrement(chiffrement(M)) ;
  - Alice peut déchiffrer ce message chiffré à l'aide de la clé publique de Bob... c'est donc Bob !
- **Problème :** cette méthode permet de faire des attaques sur la clé privée de Bob en soumettant des messages aléatoires bien choisi.
- **Solution :** calculer un **«résumé»** du message aléatoire initial, un "digest", et l'utiliser à la place du message aléatoire lors du chiffrement.
- L'obtention de ce «résumé» se fait à l'aide **d'une fonction de hachage**.

Fonction de hachage

- Une fonction de hachage est une fonction permettant d'obtenir un résumé d'un texte, c-à-d. une suite de caractères assez courte représentant le texte qu'il résume.
- La fonction de hachage doit :
  - être telle qu'elle **associe un et un seul résumé à un texte en clair (cela signifie que la moindre** modification du document entraine la modification de son résumé), c-à-d. « **sans collision ».**
  - être une **fonction à sens unique (*one-way function*) *afin qu'il soit impossible de retrouver le message*** original à partir du résumé.

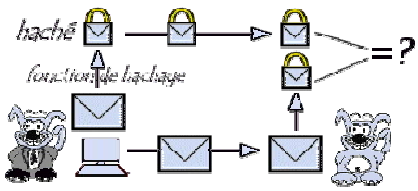
    y = F(x), mais il est impossible de retrouver x à partir de y !

Fonction de hachage

- **Propriétés**
- une fonction de hachage "H" transforme une entrée de données d'une dimension variable "m" et donne comme résultat une sortie de données inférieure et fixe "h" (h= H(m)).
  - l'entrée peut être de dimension variable ;
  - la sortie doit être de dimension fixe ;
  - H(m) doit être relativement facile à calculer ;
  - H(m) doit être une fonction à sens unique ;
  - H(m) doit être « sans collision ».

Utilisation de la Fonction de hachage

- **Assurer Authentification et 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.
- pour la construction du **MAC**, Message Authentication Code, ou code d'authentification de message, il permet de joindre l'empreinte du message chiffré avec une **clé secrète** ce qui permet d'assurer l'intégrité et la provenance du message en même temps.



Principaux algorithmes des fonction de hachage

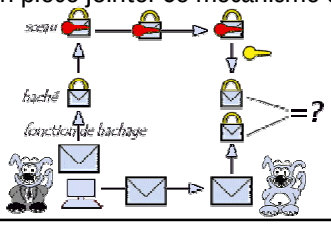
- **MD2, MD4 et MD5** (MD signifiant Message Digest), développé par Ron Rivest (société RSA Security), créant une empreinte digitale de 128 bits pour MD5.
- Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du résumé du document permettant de vérifier l'intégrité de ce dernier
- **SHA** (pour Secure Hash Algorithm, pouvant être traduit par Algorithme de hachage sécurisé), développé par le NIST en 1995.
- il crée des empreintes d'une longueur de 160 bits. (SHA0 et SHA1)
- **RACE** Integrity Primitives Evaluation Message Digest, développé par Hans Dobbertin, Antoon Bosselaers et Bart Preneel ;
- **RIPEMD**-128 et RIPEMD-160, créé entre 88 et 92 ;
- **Tiger,** développé par Ross Anderson et Eli Biham, plus rapide que MD5 (132Mb/s contre 37Mb/s sur une même machine, optimisé pour processeur 64bit).

Signature électronique

3. Le scellement ou sceau ou signature électronique

- 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*.



Signature électronique (fonctionnement)

1. L'expéditeur calcule **l'empreinte** de son **texte en clair** à l'aide d'une fonction de hachage ;
2. L'expéditeur chiffre **l'empreinte** avec sa **clé privée** ;

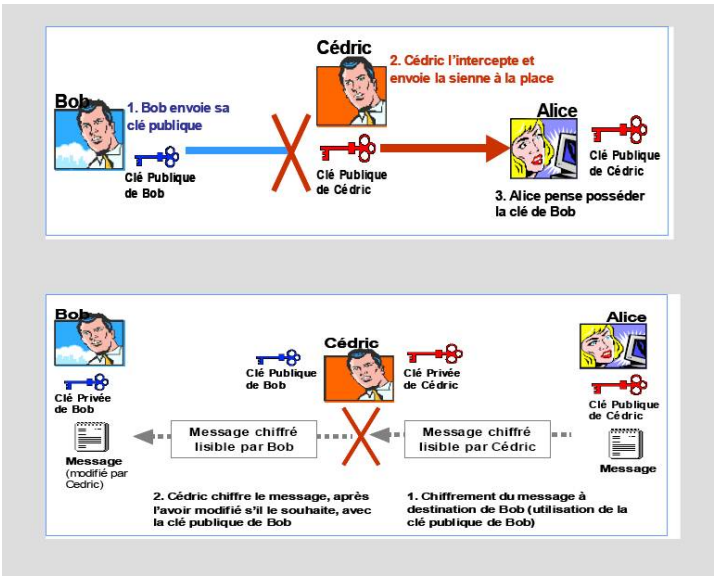
Le chiffrement du document est optionnel si la confidentialité n'est pas nécessaire.

3. L'expéditeur chiffre le **texte en clair** et **l'empreinte chiffrée** à l'aide de la clé publique du destinataire.
4. L'expéditeur envoie le **document** chiffré au destinataire ;
5. Le destinataire déchiffre le **document** avec sa clé privée ;
6. Le destinataire déchiffre **l'empreinte** avec la **clé publique** de l'expéditeur (authentification) ;
7. Le destinataire calcule **l'empreinte** du **texte clair** à l'aide de la même fonction de hachage que l'expéditeur ;
8. Le destinataire compare les deux empreintes.

Deux empreintes identiques impliquent que le texte en clair n'a pas été modifié (intégrité).

Le standard américain est le **DSS** (Digital Signature Standard), qui spécifie trois algorithmes : le **DSA** (Digital Signature Algorithm), **RSA** et **ECDSA** (Elliptic Curves Digital Signature Algorithm).

L'attaque « Man in the middle »



SOLUTION AU PROBLEME DU MAN IN THE MIDDLE

- **IL FAUT CERTIFIER L'IDENTITE DU PORTEUR DE CETTE CLE**

La signature électronique et la notion de certificat

- **Le problème de la diffusion des clés publiques**
- Le problème est de s'assurer que la clé que l'on récupére provient bien de la personne concernée : rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée.
- Un pirate peut **remplacer la clé publique présente dans un annuaire par sa clé publique (man in the middle)**
- **Notion de certificat**
- Un **certificat** permet **d'associer** une **clé publique** à **une entité (**une personne, une machine, ...) afin d'en assurer la **validité.**
- ***Le certificat est la carte d'identité de la clé publique****, délivré par un organisme appelé* ***autorité de certification.***
- Ces certificats sont émis et signé par une tierce partie, **l'autorité de certification ou CA (Certificate** Authority).

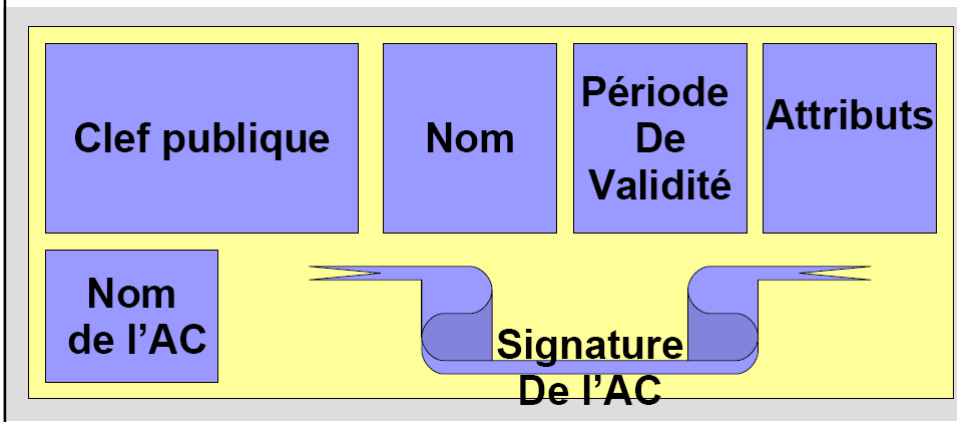
La signature électronique et la notion de certificat

L'autorité de certification est chargée de

- **délivrer les certificats ;**
- d'assigner une **date de validité** aux certificats (équivalent à la date limite de péremption des produits alimentaires) ;
- **révoquer** éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

Certificat X509

- Le certificat établit un lien fort entre le nom (DN) de son titulaire et sa clé publique



Le certificat x509

- Il est construit suivant une norme reconnue internationalement pour faciliter l'interopérabilité.

Un certificat est un petit fichier séparé en **deux parties :**

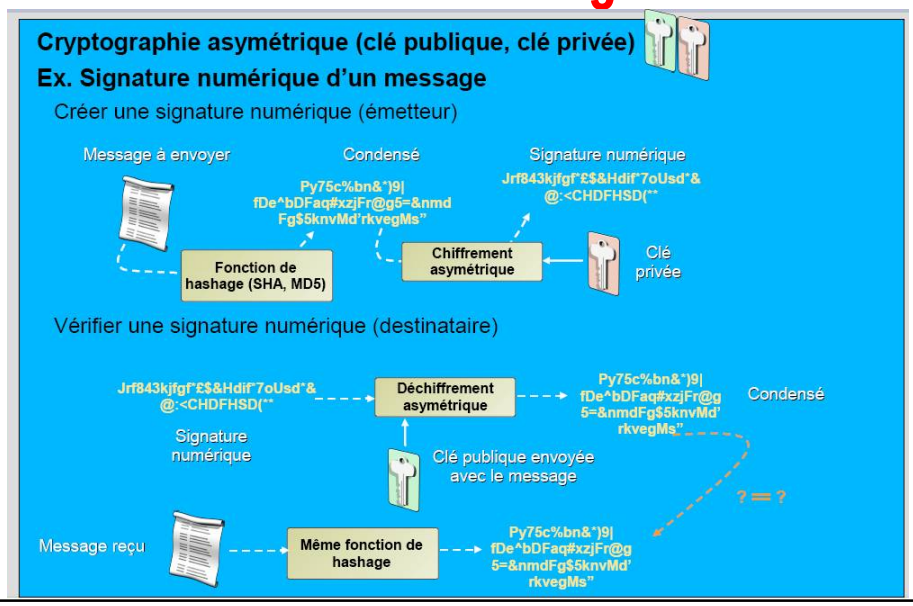
- une contenant les informations suivantes (norme ISO X509) :
  - le nom de l'autorité de certification
  - le nom du propriétaire du certificat
  - la date de validité du certificat très important, mais pas facile à gérer…
  - l'algorithme de chiffrement utilisé
  - la clé publique du propriétaire
- une autre contenant la **signature de l'autorité de certification**

- La confiance s'établit en faisant confiance à une **autorité supérieure : VeriSign, GTE, CommerceNet…**

Le certificat x509

- **La construction du certificat**
- L'ensemble des informations (le nom de l'autorité de certification, du propriétaire du certificat…) est **signé** par l'autorité de certification, à l'aide **d'un sceau :**
  - une fonction de hachage crée une **empreinte de ces informations,**
  - ce résumé est chiffré à l'aide de la **clé** privée de l'autorité de certification, la clé publique ayant été préalablement largement diffusée *ou elle même signée par une autorité de niveau supérieur.*
- *Grâce à ce sceau, il est possible de s'assurer de la qualité du certificat.*
- Cette méthode repose sur la **confiance** dans une structure dont on dispose de la clé publique.

Certificats numériques : vérification de la signature



Certificats numériques

Certificats X509 v3
Équivalent d'une pièce d'identité pour un utilisateur ou une machine

La signature numérique garantie l'intégrité des données (idem pour une CRL)

De plus en plus intégrés avec les services et applications

Ouverture de session par carte à puce, messagerie sécurisée, applications de signature électronique, VPN, WiFi, etc.

Certificats numériques

- **Notion de tiers de confiance**
- Cela consiste à adhérer auprès d'un organisme que l'on appelle autorité de certification.
- Cet organisme délivre des certificats.
- Cet organisme intègre sa clé publique par exemple au niveau :
  - du **navigateur** de la machine dans le cas de la sécurisation d'une transaction web;
  - du **système d'exploitation** pour la vérification des mises à jour ou l'installation de logiciel
- **Notion d'Infrastructure de Gestion de Clef (IGC ou PKI Public Key Infrastructure)**
- Une Infrastructure de Gestion de Clef est un système assurant la gestion de certificats électroniques au sein d'une communauté d'utilisateurs.
- Une IGC est composée
  - d'au moins une **autorité de certification,**
  - d'au moins une **autorité d'enregistrement chargée :** de vérifier les données d'identification des utilisateurs de certificat électronique, et de contrôler les droits liés à l'utilisation des certificats électroniques conformément à la politique de certification.

Certificats numériques

- Une PKI fournit :
  - les fonctions de **stockage de certificats d'un serveur de certificats,**
  - des fonctions de **gestion de certificats** (émission, révocation, stockage, récupération et fiabilité des certificats).
- **Vérification d'un certificat**
  - vérifier que le certificat n'a pas expiré, que sa date de validité est correcte ;
  - authentifier l'empreinte (provenance de l'AC) et l'intégrité (pas de modification du certificat) ;
  - consulter la liste de révocation de l'AC pour savoir s'il n'a pas été révoqué.

Applications

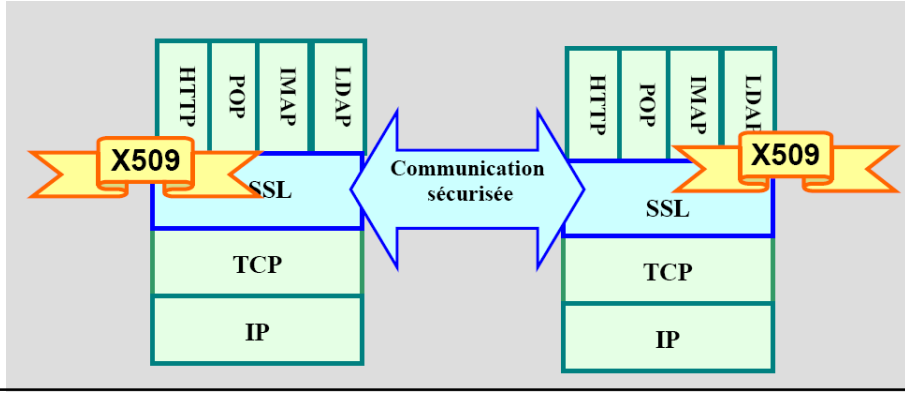
- Applications de confiance (applet JAVA, pilote Windows XP, ...)
- Sécurisation des processus « web services » en particulier les serveurs d'authentification (SSO)
- Signature
- E-commerce
- E-Vote
- **Les Usages**
- Messagerie S/MIME : signature (certificat de l'émetteur) et/ou chiffrement (certificat du destinataire)
- SSL ou TLS : en particulier HTTPS pour chiffrer les sessions du client et authentifier le serveur.
- — VPN et IPsec

Secure Socket Layer
SSL

- un protocole de sécurisation des échanges, développé par Netscape.
- Il a été conçu pour assurer la sécurité des transactions sur Internet (notamment entre un client et un serveur), et il est intégré depuis 1994 dans les navigateurs.
- Il existe plusieurs versions: la version 2.0 développée par Netscape; la version 3.0 qui est actuellement la plus répandue, et la version 3.1 baptisée TLS (transport Layer Security)
- SSL fonctionne de manière indépendante par rapport aux applications qui l'utilisent; il est obligatoirement au dessus de la couche TCP et certains le considèrent comme un protocole de niveau 5 (couche session).

Secure Socket Layer
SSL

- L'utilisation de SSL permet :
- D'établir un canal de communication chiffré ;
- D'authentifier l'un ou l'autre des interlocuteurs, voire les deux, à l'aide de certificat (au format x509).



.

Secure Socket Layer
SSL

SSL permet d'assurer les services de sécurité suivants:

1. confidentialité : elle est obtenue par l'utilisation d'algorithmes à chiffrement symétrique de blocs comme DES, FORTEZZA, IDEA, 3DES ou RC2, ou par des algorithmes à chiffrement symétrique de flots comme RC4
2. intégrité : l'intégrité des données est assurée par l'utilisation de MACs (Message Authentication Code) basés sur les fonctions de hachage MD5 (16 octets) ou SHA-1 (20 octets).

- authentification : SSL permet l'authentification des 2 entités (authentification client facultative) basé sur des certificats X.509, et l'authentification des données grâce aux MACs.
- Un serveur web sécurisé par SSL possède une URL se termine par s

Principe de fonctionnement de SSL

- Le navigateur se connecte à un serveur sécurisé, une clé de cryptage unique est alors mise en place tout au long de la transaction entre le serveur et le navigateur.
- Le navigateur envoie des données cryptées à destination du serveur, qui sera seul à même de déchiffrer les informations reçues, grâce à la mise en place d'une clé d'échange unique entre eux.
- Le serveur envoie un avis de bonne réception de l'information.
- Une nouvelle transaction cryptée peut débuter, en reprenant le même processus.
- C'est donc une solution logicielle qui chiffre le numéro de carte bancaire lorsqu'il transite sur le réseau depuis le poste du client. Il est ensuite décrypté sur le serveur du marchand. Cette étape est suivie d'une opération de **télépaiement** par carte bancaire traditionnelle (**ce n''est pas gratuit**).

TLS

- TLS : Transport Layer Security
- On parle souvent de SSL/TLS = protocole de sécurisation des échanges sur Internet
- Actuellement TLS est utilisé à la place de SSL

Architecture de sécurité informatiques

- La sécurité est intégrée à l'infrastructure dès le départ. Les mesures de sécurité portent notamment sur :
  - Une séparation entre le réseau des Jeux et l'Intranet,
  - Une segmentation du réseau olympique en domaines de sécurité,
  - Des processus stricts de gestion de la configuration (mécanismes de sécurité tels que logiciels anti-virus et sécurité de port),
  - Un positionnement stratégique de Systèmes de Détection des Intrusions (IDS).

Architecture de sécurité informatiques

- Pare-feu
- DMZ
- IDS
- Log
- VPN

Architecture de sécurité informatiques