Laboratoire d'Enseignement et de Recherche sur le Traitement de l'Information Médicale

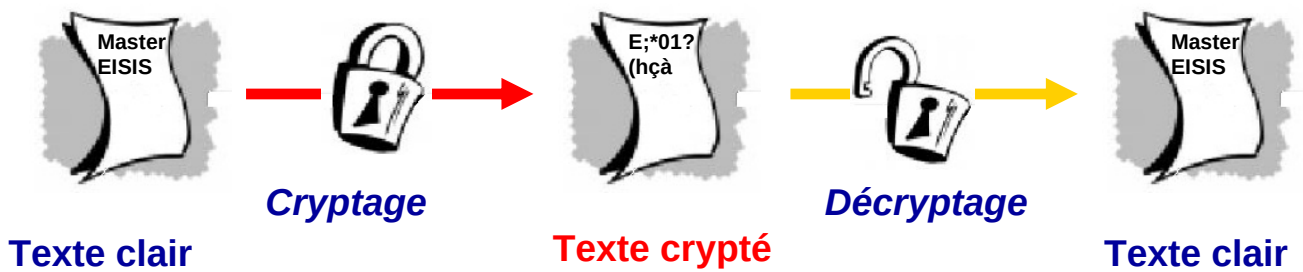
FACULTÉ DE MÉDECINE DE MARSEILLE
UNIVERSITÉ DE LA MÉDITERRANÉE AIX-MARSEILLE II

La sécurité des réseaux numériques
Cryptologie et autres techniques

Master EISIS
UE OPT7 : réseaux numériques et cryptologie

Cryptographie

- **Chiffrement (ou cryptage)**
  - procédé qui consiste à dissimuler du texte clair de façon à cacher sa substance
  - pour garantir que l'information est cachée à quiconque elle n'est pas destinée
- **Déchiffrement (ou décryptage)**
  - processus de retour du texte chiffré à son texte clair originel est appelé déchiffrement



Cryptographie, cryptanalyse, cryptologie

- **Cryptographie**
  - science qui utilise les mathématiques (algorithme) pour chiffrer et déchiffrer des données
  - Pour stocker des informations sensibles ou les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne puissent être lues par personne à l'exception du destinataire convenu
- **Cryptanalyse**
  - La cryptanalyse est la science de l'analyse et du cassage des communications sécurisées
  - cryptanalystes = attaquants
- **Cryptologie**
  - cryptographie et cryptanalyse

Force de la cryptographie

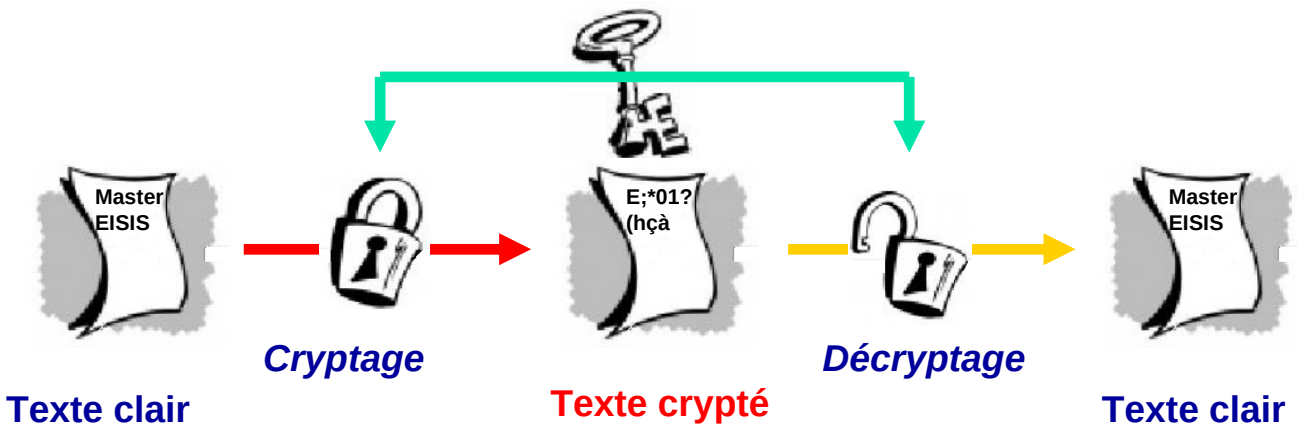
- Une cryptographie forte est un texte chiffré qui est très difficile à déchiffrer sans la possession de l'outil de déchiffrement approprié
- Personne n'a pu prouver que le plus fort chiffrement qu'on puisse se procurer aujourd'hui tiendra devant la puissance informatique de demain
- La cryptographie forte employée par PGP est la meilleure disponible aujourd'hui

Algorithme cryptographique

- **Un algorithme cryptographique, ou chiffre, est une fonction mathématique utilisée dans le processus de chiffrement et de déchiffrement**
- **Un algorithme cryptographique fonctionne en combinaison avec une clé – un mot, un nombre, ou une phrase – pour chiffrer le texte clair**
- **Le même texte clair se chiffre en un texte chiffré différent si l'on utilise des clés différentes**
- **La sécurité des données chiffrées est entièrement dépendante de deux choses :**
  - la force de l'algorithme cryptographique
  - le secret de la clé
- **Cryptosystème**
  - Un algorithme cryptographique
  - plus toutes les clés possibles
  - et tous les protocoles qui le font fonctionner

Cryptographie conventionnelle

- **Cryptographie conventionnelle (chiffrement à clé secrète ou à clé symétrique)**
  - une [seule et même] clé est utilisée à la fois pour le chiffrement et le déchiffrement
- **Exemple**
  - Le Data Encryption Standard (DES)
  - employé par le Gouvernement fédéral américain



Exemple de Cryptographie conventionnelle Le chiffre de César

- **Le chiffre de César (un chiffre à substitution)**
  - Un chiffre à substitution remplace un morceau d'information par un autre en décalant les lettres de l'alphabet
  - la clé est le nombre de caractères à décaler
- **Exemple**
  - texte clair : LERTIM
  - clé=3
  - texte crypté : OHULP
- **Chiffre à substitution=cryptographie excessivement faible au regard des normes actuelles**
- **Extension de la méthode : tables de substitution**

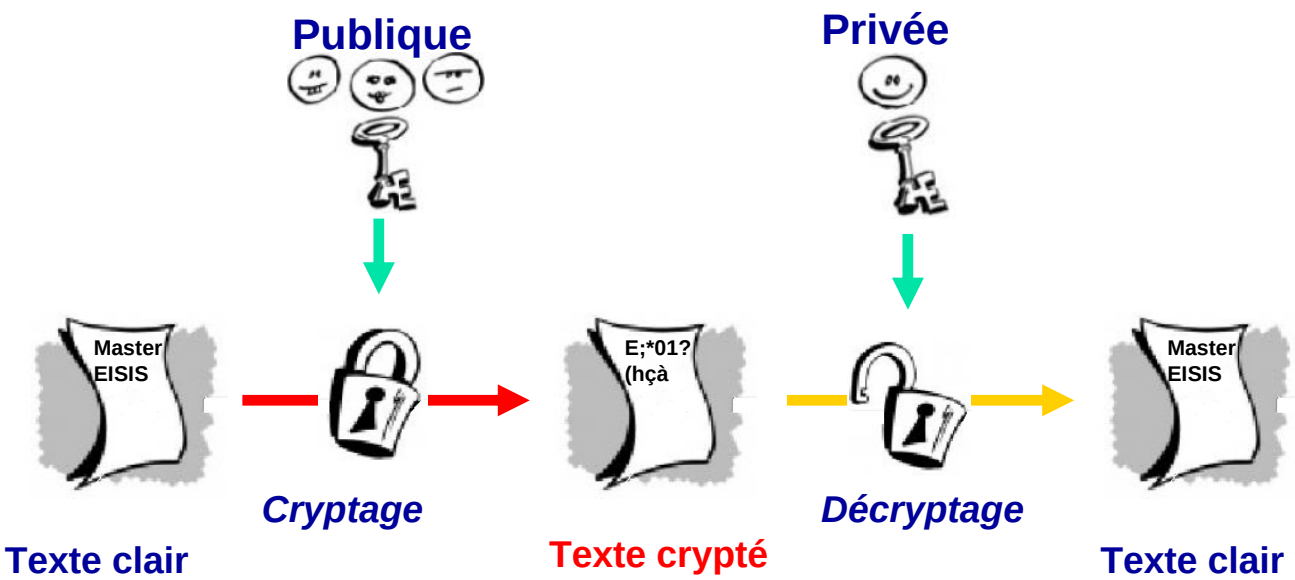
Cryptographie conventionnelle

- **Avantages**
  - chiffrement conventionnel très rapide
  - particulièrement utile pour chiffrer des données qui ne vont aller nulle part

- **Inconvénients**
  - difficulté de la distribution sécurisée de la clé
  - Pour qu'un expéditeur et un destinataire communiquent de façon sûre en utilisant un chiffrement conventionnel, ils doivent se mettre d'accord sur une clé et la garder secrète entre eux
  - Très difficile à gérer si les lieux géographiques sont différents

La cryptographie à clé publique

- **La cryptographie à clé publique**
  - Résout les problèmes de distribution de clé
  - concept inventé par Whitfield Diffie et Martin Hellman en 1975
  - repose sur un schéma asymétrique



- **Le schéma asymétrique utilise une paire de clés**
  - une clé publique qui chiffre les données (les clés publiques sont accessibles à tous)
  - et une clé privée correspondante (clé secrète) qui sera utilisée pour le déchiffrement
  - Il est mathématiquement impossible de déduire la clé privée de la clé publique

La cryptographie à clé publique

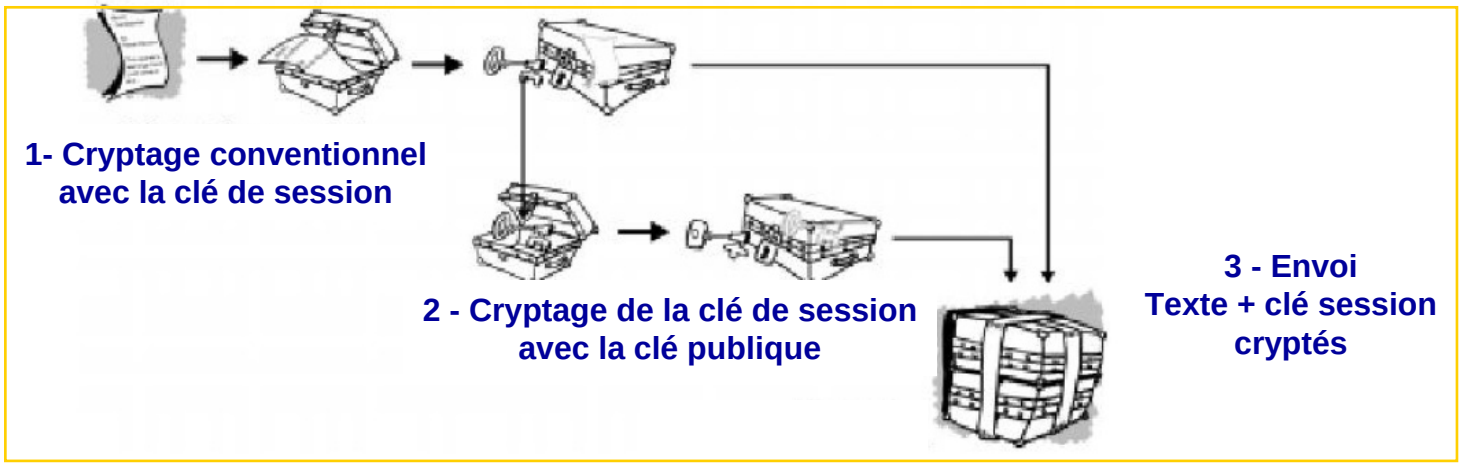
- **Modalités d'usage**
  - La clé publique est publiée, tout en gardant la clé privée secrète
  - Toute personne en possession d'une copie de votre clé publique peut ensuite chiffrer des informations
  - Quiconque a une clé publique peut chiffrer des informations mais ne peut pas les déchiffrer. Seule la personne qui a la clé privée correspondante peut déchiffrer les informations
- **Avantages**
  - permet à des gens qui n'ont pas d'accord de sécurité préalable d'échanger des messages de manière sûre
  - pas de nécessité pour l'expéditeur et le destinataire de partager des clés secrètes via un canal sûr
  - toutes les communications impliquent uniquement des clés publiques
  - aucune clé privée n'est jamais transmise ou partagée
- **Exemples**
  - Elgamal (Taher Elgamal)
  - RSA (Ron Rivest, Adi Shamir, et Leonard Aldeman),
  - Diffie-Hellman
  - DSA (David Kravitz)

PGP

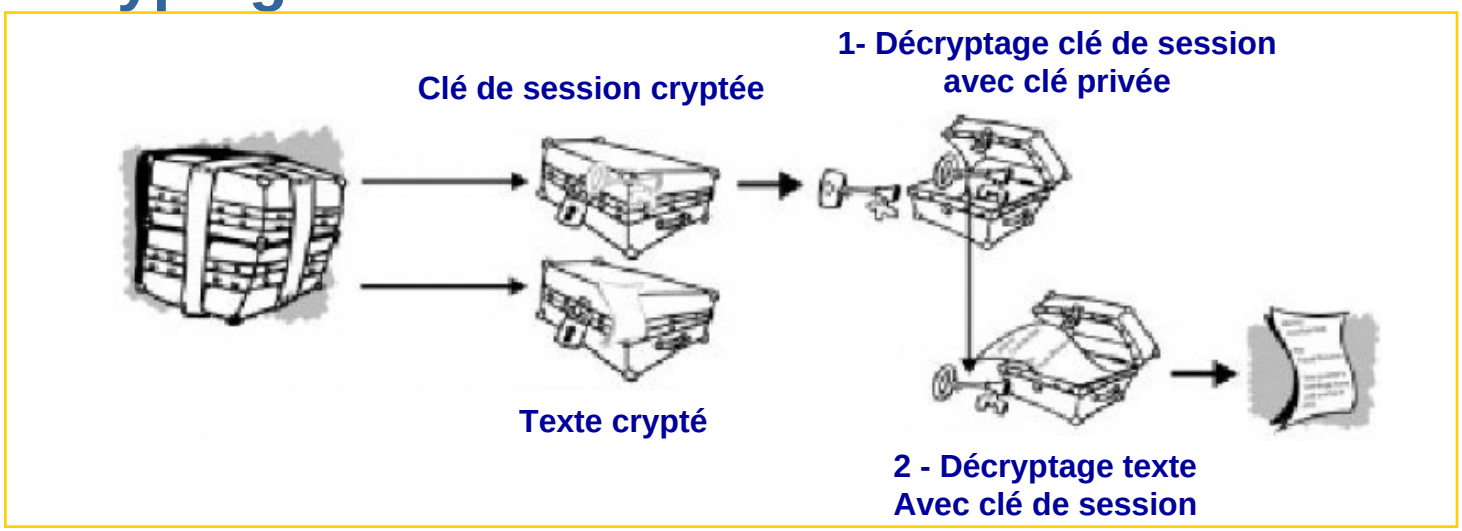
- **Cryptosystème hybride**
  - cryptographie conventionnelle avec clé de session
  - cryptographie à clé publique
- **Clé de session**
  - clé secrète qui ne sert qu'une fois
  - nombre aléatoire généré à partir de la souris et du clavier
  - fonctionne avec un algorithme de chiffrement conventionnel très sûr et rapide qui chiffre le texte clair
  - clé de session chiffrée avec la clé publique du destinataire et transmise avec le texte chiffré
- **Associe performances et sécurité**

PGP

- **Cryptage**



- **Décryptage**



Les clés

- **Plus la clé est grande, plus le chiffrement est sûr**

- **Taille d'une clé publique**
  - pas comparable avec la taille des clés secrètes employées en cryptographie conventionnelle
  - clé conventionnelle de 80 bits = sécurité équivalente à celle d'une clé publique de 1024 bits
  - clé conventionnelle de 128 bits = sécurité équivalente à celle d'une une clé publique de 3000 bits

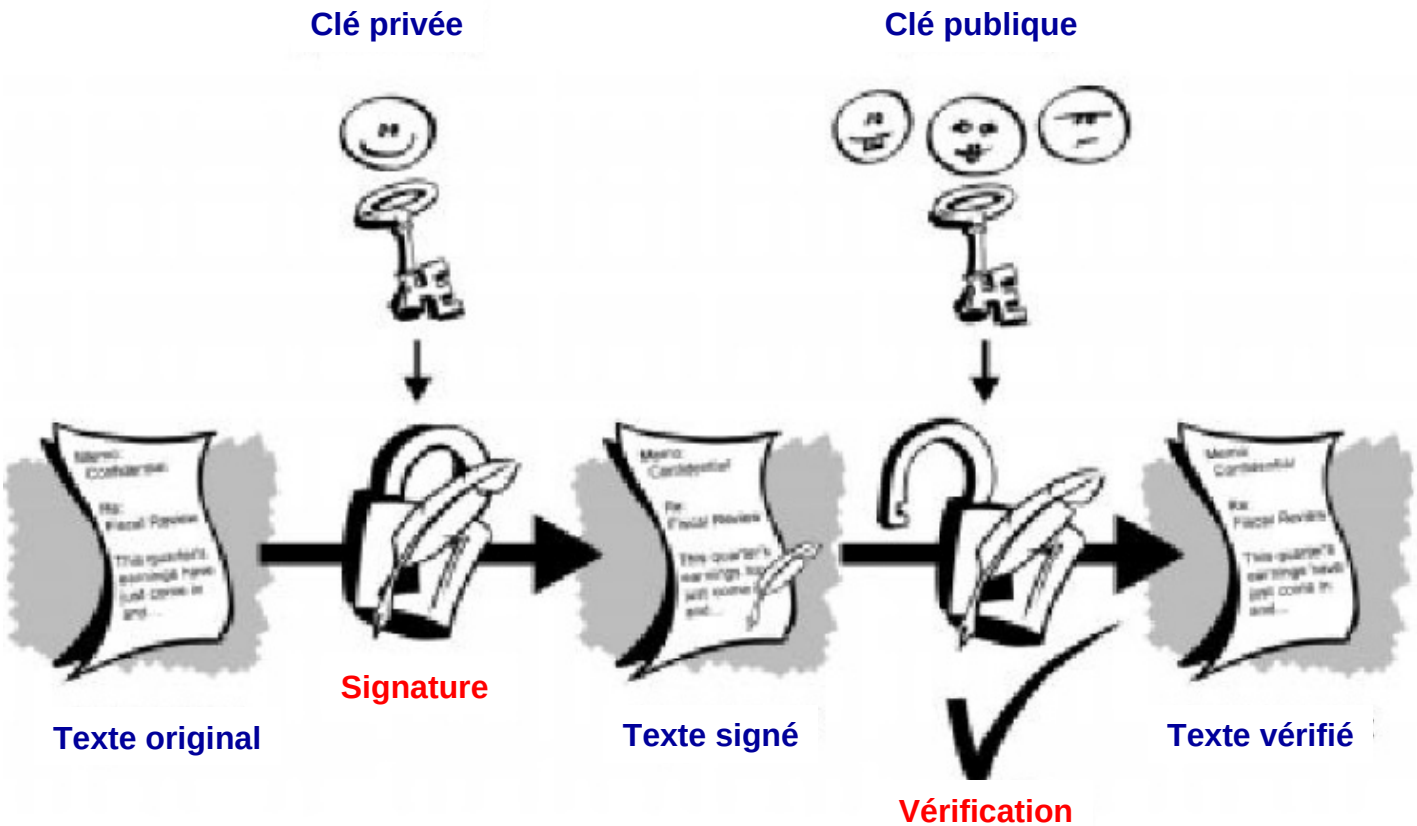
- **Très difficile de déduire la clé privée en partant de la seule clé publique**
  - mais, il est toujours possible de déduire la clé privée si l'on dispose de suffisamment de temps et de puissance de calcul
  - compromis : choisir une clé d'une taille convenable assez grande pour être sûre, mais suffisamment petite pour pouvoir être utilisée relativement rapidement

- **Les clés les plus grandes resteront cryptographiquement sûres pour une plus longue période**

Signatures numériques

- **Signatures numériques**
  - contrôler l'authenticité de l'origine de l'information
  - et de vérifier que l'information en question est intacte (intégrité)
- **Non répudiation**
  - Une signature numérique empêche l'expéditeur de contester ultérieurement qu'il a bien émis une information
- **Force de la signature numérique**
  - signature numérique supérieure à une signature manuelle
  - pratiquement impossible à contrefaire
  - atteste le contenu de l'information autant que l'identité du signataire
- **Alternative : chiffrement ou signature numérique**
  - utiliser les signatures plus le chiffrement
  - Ex : dépôt de 1000 (savoir que le dépôt a lieu ou plutôt avec qui ?)
- **Méthode de base**
  - chiffrer l'information en utilisant sa propre clé privée (et non la clé publique d'autrui)
  - Si l'information peut être déchiffrée avec ma clé publique, c'est qu'elle provient bien de moi

Signature numérique simple



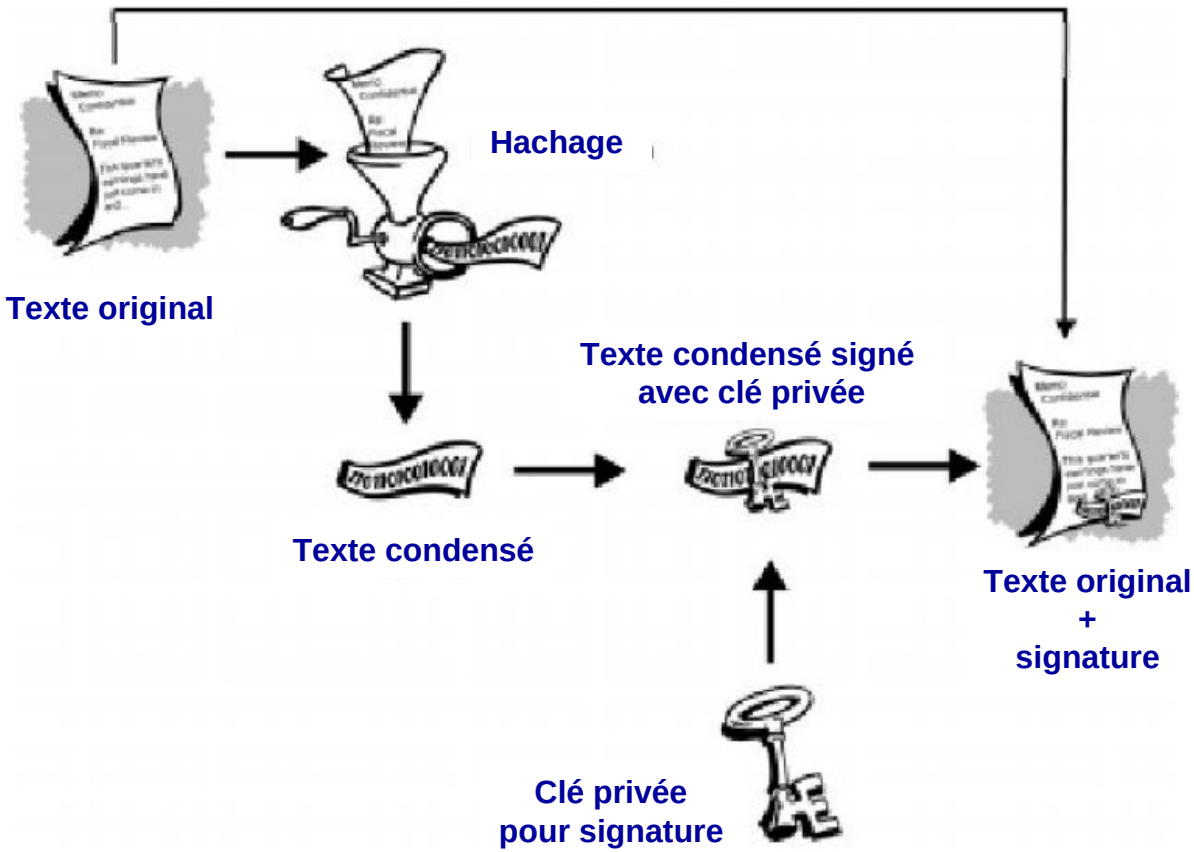
Système lent (double la quantité d'information)

Fonction de hachage

- **Fonction de hachage à sens unique**
  - texte en entrée de longueur variable
  - texte en sortie de longueur fixe et courte/message (160 bits)
  - Texte en sortie : contraction de message ou texte condensé

- **Principe**
  - Toute modification sur le texte d'origine (même un seul bit) conduit à un texte condensé totalement différent

Signature numérique avec hachage



Certificats

- **Problème de clés publiques**
  - échange de clés sur des serveurs publics
  - personne interposée
  - clé publique bidon portant le nom et l'identifiant d'utilisateur du destinataire réel des messages

- **Certificats numériques (ou signatures)**
  - permettent d'établir la réelle appartenance d'une clé publique à son propriétaire supposé

Certificats

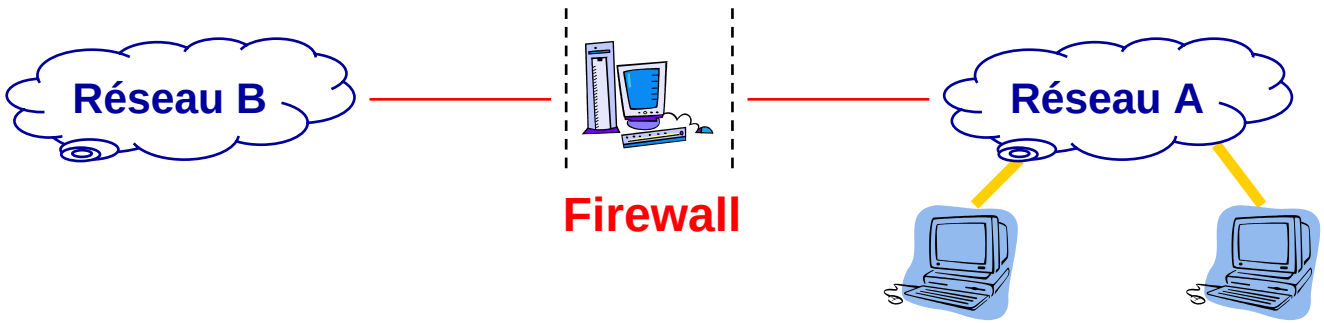
- **Un certificat numérique fonctionne comme une pièce d'identité matérielle**
- **Un certificat numérique**
  - est une information attachée à une clé publique
  - permet de vérifier que cette clé est authentique (ou valide)
- **Un certificat numérique comporte trois éléments**
  - une clé publique
  - une information de certification (identité de l'utilisateur : nom, adresse e-mail, ...)
  - une signature numérique afin de garantir que les informations de certification ont été contrôlées par un organisme accrédité (Autorités de Certification)
- **Exemple : certificat serveur web**

Autres technologies

- Firewall
- Proxy
- VPN
- WIFI et sécurité

Firewall

- **Firewall (pare-feu)**
  - gère les contrôles d'accès entre deux réseaux



  - Filtrer les paquets de données (niveaux 3 et 4 de l'OSI)
  - constitue un point unique où l'audit et la sécurité peuvent être imposés
- **Protection +/-**
  - laisser uniquement passer le courrier électronique
  - bloquer uniquement les services reconnus comme étant des services dangereux
  - configurés pour protéger contre les accès non authentifiés du réseau externe
    - empêche les vandales de se connecter sur des machines de votre réseau interne
    - autorise les utilisateurs de communiquer librement avec l'extérieur
  - Coûts financiers et en temps d'administration

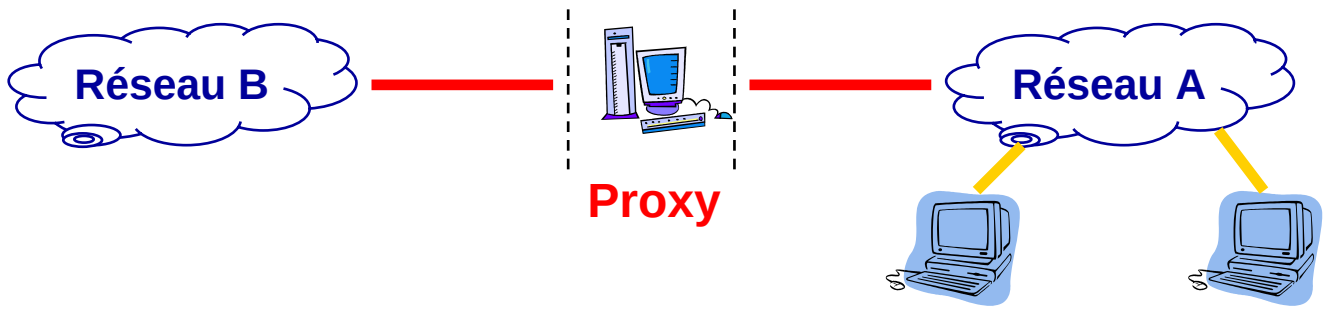
Firewall

- **Limites d'un firewall**
  - ne protège pas des attaques qui ne passent pas par lui… (Firewall + modem)
  - vérifier qui a accès aux informations +++
  - attention et conscience des utilisateurs +++ (respect de règles : ne jamais ouvrir un fichier attaché à un mail sans être sûr de sa provenance, attention aux supports mobiles comme les clés)
  - ne protège pas très bien des virus (trop de manières différentes de coder des fichiers)

- **Points à prendre en compte**
  - reflet de la politique de sécurité choisie par l'organisation
  - Identifier le degré de contrôle souhaité : Analyse des risques, puis définir ce qui doit être autorisé et interdit
  - Coûts financiers et en temps d'administration

Proxy

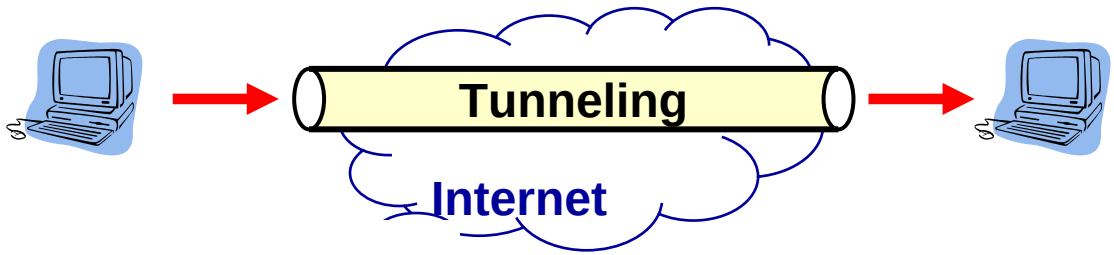
- **Serveur proxy**
  - Passerelle applicative (niveau 7 OSI)
  - Isoler une ou plusieurs machines pour les protéger



- **Proxy Internet**
  - sert de relais entre le réseau et les machines à cacher
  - adresse IP du client = adresse IP du serveur Proxy
  - gère les requêtes Internet (URL) : filtrage des requêtes
  - performances : mémoire cache

VPN

- **VPN (Virtual Private Network, réseaux privés virtuels)**
  - chemin virtuel sécurisé entre une source et une destination
  - réalisation de réseaux privés à moindre coût



- **Principe de tunnel (tunnelling)**
  - chaque extrémité est identifiée
  - les données transitent après avoir été chiffrées
- **Usages**
  - accès via Internet à l'intranet de son entreprise
  - accès sécurisés à l'intérieur d'une entreprise (sur l'intranet)

- **Principaux protocoles**
  - PPTP (Point to Point Tunnelling Protocol) de Microsoft
  - L2F (Layer Two Forwarding) de Cisco
  - L2TP (Layer Two Tunnelling Protocol) de l'IETF

Commerce électronique
Paiement en ligne

- **Le commerce électronique**
  - En plein essor
  - Des enjeux économiques très importants
- **Acteurs**
  - le commerçant
  - le consommateur, qui veut payer sans crainte et simplement
  - la banque, qui se veut garant de la bonne marche des opérations
- **Le problème du paiement sur Internet**
  - Les paiements limités par les lois du pays qui n'autorisent pas forcément le libre chiffrement des informations (c'est le cas en France)
  - Peur de donner leur numéro de carte de crédit
- **Deux possibilités existent pour le paiement en ligne.**
  - porte-monnaie électronique, géré par un organisme tiers
  - Paiement directement avec sa carte de crédit

Commerce électronique
Paiement en ligne

- **La sécurité du paiement**
  - échanges chiffrés (confidentialité)
  - Acteurs identifiés (authentification)
  - données n'ont pas été modifiées (intégrité).
  - Certification que les échanges ont bien eu lieu (non répudiation)
  - client solvable
- **Techniques**
  - SSL : Secure Socket Layers : de loin la plus utilisée,
    - chiffrement des échanges mais ne garantit pas que le marchand va vous livrer, ni que le client peut payer.
    - on sait que l'échange est sécurisé car l'adresse http:// est remplacée par https:// et un cadenas apparaît en bas du navigateur
  - SET : Secure Electronic Transaction : chiffrement des données de la carte de crédit, signature des messages et authentification des différents acteurs de l'échange.
  - C-SET : Chip Secure Electronic Transaction :
    - extension de SET avec un lecteur de carte. Ces deux systèmes sont compatibles, mais C-SET permet de contrôler d'avantage de chose de façon physique (vérification de la carte, etc…). Ce système est aussi sûr qu'un paiement par carte bancaire dans un magasin.

- **La question : Faut-il avoir peur de payer sur Internet ?**
  - se fier à une entreprise qui a pignon sur rue
  - risque de se faire voler son numéro de carte bleue n'est pas nul, mais il est improbable…

WIFI et sécurité

- **Danger des postes nomades**
  - Machine WIFI piratée = relais pour une attaque du site central
  - En pratique
    - Cryptages non activés par défaut (usagers non sensibilisés)
    - Dans un hot spot, pas de cryptage car impossible de donner la clé
- **Solutions**
  - limiter la couverture au seul besoin
  - SSID (Service Set IDentifier) SPECIFIQUE
    - identifiant de 32 caractères propre à chaque réseau (en tête)
  - Cryptage
    - WEP (128bits, clé RCA publique, sécurité moyenne)
    - WPA (clé dynamique) +++

Sécurité en santé

- **Mise en place de réseaux à grande échelle**
  - exemple : RSS (transmission feuilles de soin)
  - multiplicité d'intervenants (médecins, ministère, caisses d'assurance maladie, Ordre des médecins)
  - CNIL
- **Contraintes de sécurité**
  - enjeux financiers
  - éthique
  - secret médical
- **Choix d'une architecture à clé publique**
  - infrastructure de gestion de clés très complexe

Conclusion

- **Cryptologie et sécurité publique**
  - cryptologie libre pour la signature et l'intégrité des messages
  - Réglementation pour la confidentialité
  - Pouvoir vérifier les contenus échangés
  - Clé 40 bits vs clé 56 bits
  - Tiers de confiance et justice
- **Le combat cryptographie et cryptanalyse**