Cryptographie et services de sécurité

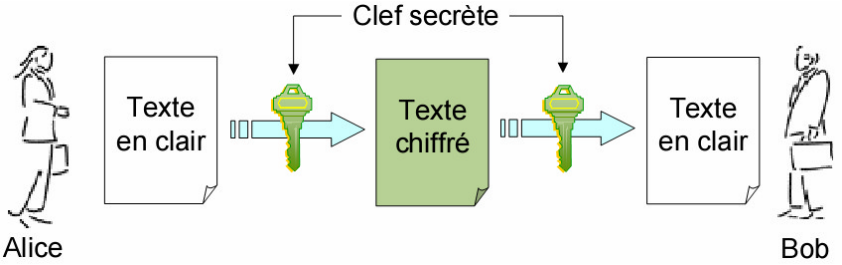
- Le but de la cryptographie traditionnelle est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle par chiffrement;
- Le but de la cryptographie moderne est de traiter plus généralement des problèmes de sécurité des communications et de fournir un certain nombre de services de sécurité :
  - Confidentialité
  - Authentification de l'origine des données
  - Intégrité
  - Non-répudiation
  - Non-rejeux
  - etc …
  - Authenticité = Authentification + Intégrité
- Les moyens mis en œuvre pour offrir ces services sont appelés mécanismes de sécurité.

Mécanismes et outils

- Les mécanismes de sécurité sont basés sur un ensemble d'outils cryptographiques :
  - Fonctions de hachage
  - Algorithmes de chiffrement
  - Générateur aléatoire
  - Protocoles, …
- Ces outils peuvent être utilisés seuls ou combinés pour réaliser des opérations de :
  - Chiffrement
  - Scellement et signature
  - Échange de clés
  - Authentification mutuelle
  - ….

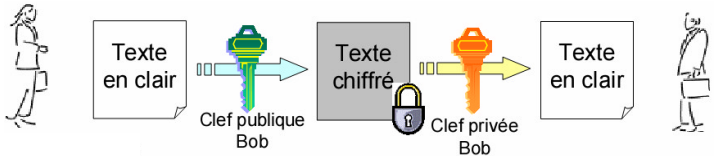
Chiffrement symétrique (2)

- **Confidentialité**

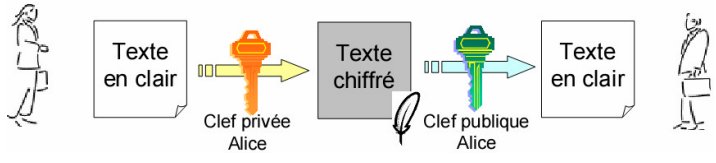


Chiffrement asymétrique (2)

- Confidentialité (Chiffrement)



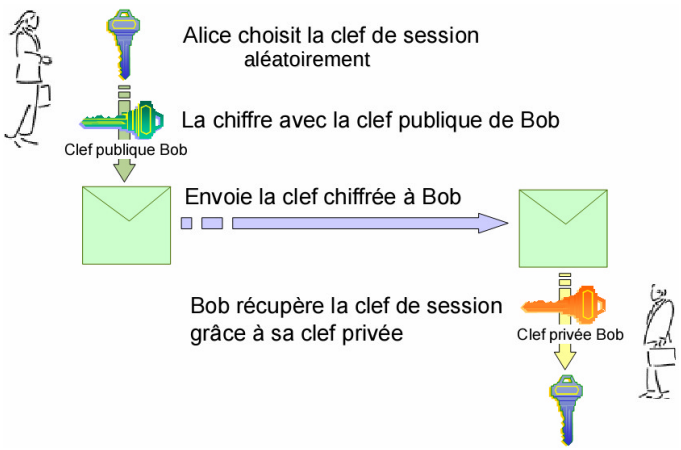
- Authentification (Signature)



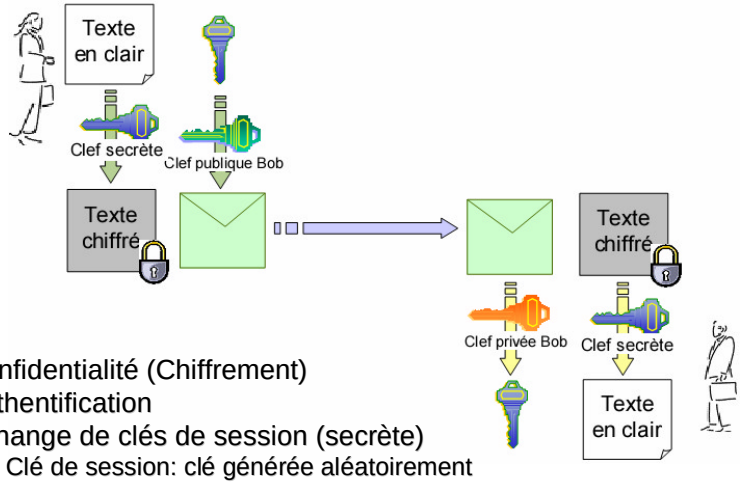
Protocoles d'échange de clés

- Tout comme les protocoles de communication, les protocoles cryptographiques sont une série d'étape prédéfinies, basées sur un langage commun (spécifications des structures de données et de messages valides), qui permet à deux entités d'accomplir des taches d'authentification mutuelle et d'échange de clés.
- Il existe 2 types de protocoles d'échange de clés:
  - Les protocoles qui supposent le partage préalable d'une information (clé publique) entre les des 2 entités (ex. RSA utilisé par HTTPS)
  - Les protocoles qui supposent aucune connaissance préalable d'informations entre les 2 entités (ex. Diffie-Hellman)

Protocole d'échange de clés: ex. RSA



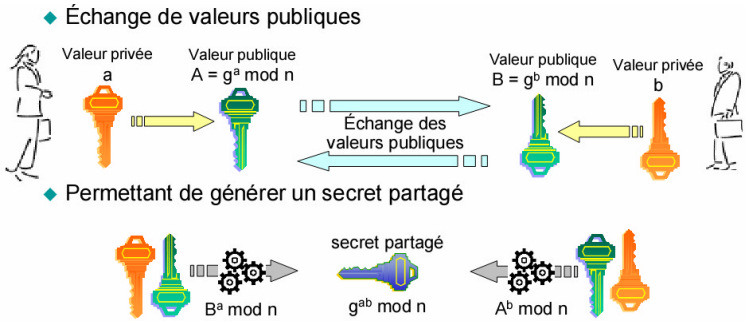
Chiffrement hybride



- Confidentialité (Chiffrement)
- Authentification
- Echange de clés de session (secrète)
  - Clé de session: clé générée aléatoirement
  - compromis entre le chiffrement symétrique et asymétrique.

Protocole d'échange de clés: ex. DH

- Qu'est ce que Diffie-Hellman (DH) ?
  - Inventé en 1976. Protocole cryptographique qui permet à deux entités de générer un secret partagé sans informations préalables l'un sur l'autre.
- Principe : basée sur la difficulté de calculer des logarithmes discrets sur un corps fini.
  - Le secret généré peut ensuite être utilisé pour dériver une ou plusieurs clés (clé de session, clé de chiffrement de clés, …)



Fonction de hachage

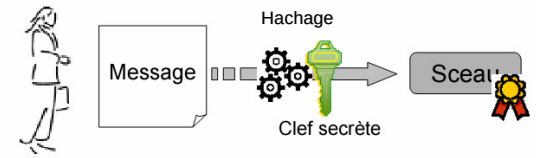
- Aussi appelée fonction de condensation
- Permet à partir d'un texte de longueur quelconque, de calculer une chaîne de taille inférieure et fixe appelé condensé ou empreinte (*message digest* ou *hash* en anglais)
- Utilisée seule, elle permet de vérifier *l'intégrité* d'un message.
- Associé à une clé privé, elle permet le calcul d'un sceau ou MAC (Message Authentification Code), pour assurer :
  - *Intégrité* des données
  - *Authentification* de la source
- Associé à un chiffrement asymétrique, elle permet le calcul de signatures, pour assurer :
  - *Intégrité* des données
  - *Authentification* de la source
  - *Non-répudiation* de la source
- Une fonction de hachage doit être :
  - à *sens unique*, c'est à dire qu'il doit être impossible étant donné une empreinte de retrouver le message original.
  - *sans collisions*, impossibilité de trouver deux messages distincts ayant la même valeur de condensé. La moindre modification du message entraîne la modification de l'empreinte.
- Exemples :
  - MD5 (Message Digest 5 - Rivest1991-RFC 1321) : calcul une empreinte de 128 bits
  - SHA-1 (Secure Hash Algorithm 1 - NIST1994) : plus sûr que MD5 - empreinte de 160 bits

Scellement (MAC)

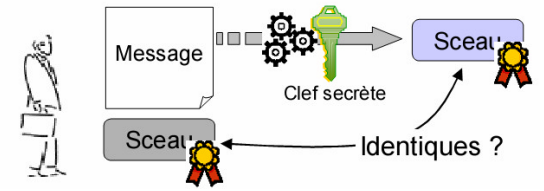
- Mécanisme qui consiste à calculer (ou sceller) une empreinte à partir d'un message et d'une clé privée pour:
  - Authentifier l'origine des données
  - Vérifier l'intégrité des données
- La scellement d'une empreinte génère:
  - un *sceau* ou
  - *code d'authentification de message (MAC)*
- Il est réalisé au moyen d'une fonction de hachage appliquée au message+clé privée:
  - Keyed-MAC (Keyed-MD-5, Keyed-SHA-1)
  - H(message, secret), H(secret, message), H(secret, message, secret)

Scellement (2)

- Scellement



- Vérification

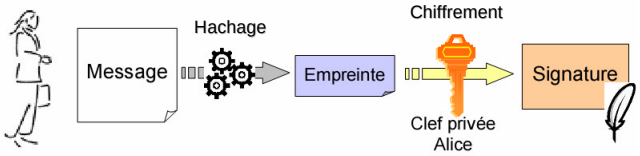


Signature numérique

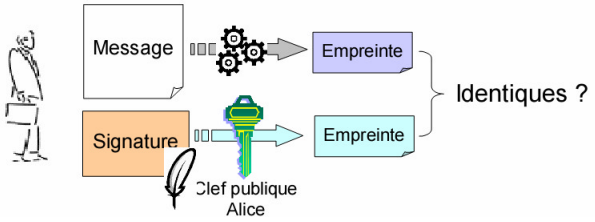
- La norme ISO 7498-2 définit la signature numérique comme des «données ajoutées à un message », ou transformation cryptographique d'un message, permettant à un destinataire de :
  - authentifier l'auteur d'un document électronique
  - garantir son intégrité
  - Protéger contre la contrefaçon (seule l'expéditeur doit être capable de générer la signature) -> non-répudiation.
- La signature électronique est basée sur l'utilisation conjointe d'une fonction de hachage et de la cryptographie asymétrique
- Depuis mars 2000, la signature numérique d'un document a en France la même valeur légale qu'une signature sur papier

Signature numérique (2)

- Signature



- Vérification



Certificat électronique

- Les certificats électroniques sont des données publiques.
  - Ex. lors de l'accès à un serveur web sécurisé, le client télécharge automatiquement le certificat.
- A chaque certificat électronique correspond une clef privée, qui est soigneusement protégée par le propriétaire du certificat, et une clé publique qui est incluse dans le certificat et qui doit être signée par une tierce organisation (l'autorité de certification).
  - Ainsi, sur Internet, le certificat permet à un client de vérifier que la clé publique et l'URL d'un site marchand appartiennent bien à leur auteur (Ex. www.laposte.fr, www.fnac.fr, ...).

Certificat électronique (2)

- C'est une carte d'identité électronique dont l'objet est principalement d'authentifier un utilisateur ou un équipement informatique (comme une passerelle d'accès ou un serveur d'application sécurisé, Ex. web marchand).
- Le certificat numérique est un bloc de données contenant, dans un format spécifié, les parties suivantes :
  - la clé publique d'une paire de clés asymétriques,
  - des informations identifiant le porteur de cette paire de clés (qui peut être une personne ou un équipement), telles que son nom, son adresse IP, son adresse de messagerie électronique, son URL, son titre, son numéro de téléphone, etc...
  - l'identité de l'entité ou de la personne qui a délivré ce certificat (autorité de certification), Ex. Verisign,
  - et enfin la signature numérique des données ci-dessus par la personne ou l'entité prenant en charge la création ou l'authentification de ce certificat et servant d'autorité de certification.

Certificat électronique (3)

- Usuellement, on distingue deux familles de certificats numériques :
  - les certificats de signature, utilisés pour signer des e-mails ou s'authentifier sur un site web, et
  - les certificat de chiffrement : les gens qui vous envoient des e-mails utilisent la partie publique de votre certificat pour chiffrer le contenu que vous serez seul à pouvoir déchiffrer
- Il existe deux façons distinctes de créer des certificats électroniques :
  - le mode décentralisé (le plus courant) qui consiste à faire créer, par l'utilisateur (ou, plus exactement par son logiciel ou carte à puce) le biclef cryptographique et de remettre la partie publique à l'AC qui va y adjoindre les informations de l'utilisateur et signer l'ensemble (information + clé publique)
  - le mode centralisé qui consiste en la création du biclef par l'AC, qui génère le certificat et le remet avec la clé privée à son utilisateur.

Certificat électronique (4)

- Les certificats électroniques respectent des standards spécifiant leur contenu de façon rigoureuse. On trouve parmi les plus connus et les plus utilisés :
  - la norme X.509 en version 1, 2, et 3, sur lequel se fondent certaines infrastructures à clés publiques.
  - OpenPGP, format standard (normalisé dans le RFC 2440) de logiciels comme GnuPG.
- Un Certificat électronique est géré tout au long de son cycle de vie (création, renouvellemnt et révocation) par l'autorité de Certification (CA) au moyen d'une infrastructure à clés publiques, ou PKI pour Public Key Infrastructure en anglais.

Autorité de certification

- Une Autorité de Certification appelée aussi AC ou CA (Certificate Authority) est chargée d'émettre et de gérer des certificats numériques.
- Elle est responsable de l'ensemble du processus de certification et de la validité des certificats émis.
- Une Autorité de Certification doit définir une Politique de certification qui va établir l'ensemble des règles de vérification, de stockage et de confidentialité des données appartenant à un certificat ainsi que la sécurité de stockage de sa propre clef privée nécessaire à la signature des certificats.
- Ex. Verisign, EnTrust.net, CyberTrust, CertPlus, …

Public Key Infrastructure

- Une PKI (Public Key Infrastructure), aussi communément appelée IGC (Infrastructure de Gestion de Clefs) ou ICP (Infrastructure à Clefs Publiques), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques, des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques.
- Une PKI permet la délivrance des certificats numériques. Ces certificats permettent d'effectuer des opérations cryptographiques, comme le chiffrement et la signature numérique.

Public Key Infrastructure (2)

- Une infrastructure à clés publiques délivre un ensemble de services pour le compte de ses utilisateurs :
  - Enregistrement des utilisateurs (ou équipement informatique),
  - Génération de certificats,
  - Renouvellement de certificats,
  - Révocation de certificats,
  - Publication des certificats,
  - Publication des listes des certificats révoqués,
  - Identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'IGC),
  - Archivage ou séquestre des certificats (option).

Typologie des solutions

Technologies de sécurité des communications

Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP
Transport layer	SSL, TLS, WTLS
Network layer	IPsec
Data Link layer	PPTP, L2TP
Physical layer	Scrambling, Hopping, Quantum Communications

MPLS

Sécurisation des échanges

- Pour sécuriser les échanges ayant lieu sur le réseau Internet, il existe plusieurs approches :
  - niveau applicatif (PGP)
  - niveau transport (SSL/TLS)
  - niveau réseau (protocole IPsec)
  - niveau physique (boîtiers chiffrant).
- Application typique : sécurisation du Web

IPsec to MPLS to VLAN Service Architecture