

Politique de sécurité

Éléments de Sécurisation

Objectifs de la présentation

- Fournir une liste des éléments techniques intervenants dans la sécurisation d'un site
- Faire le point sur les éléments de sécurisation des échanges informatiques

Éléments de sécurisation

- Sécurisation des échanges
- Sécurisation des services
- Sécurisation du réseau



RFC 2196

FRC 2196: contenu

- « *Implement measures which will protect your assets in a cost-effective manner* »
- Rappels sur la politique de sécurité
- Sécurisation de l'architecture
- Sécurisation des services et procédures
- Traitement des incidents



« **Chek list** » **technique de sécurité**

Sécurisation des échanges :

Fondements

- Authentification
- Confidentialité
- Intégrité
- Non répudiation

Sécurisation des échanges :

Définitions

- **Authentification**
 - Assure l'identité d'un utilisateur
 - Garantir à chacun l'identité
- **Confidentialité**
 - Rendre l'information inintelligible à d'autres que les acteurs de la transaction
- **Intégrité**
 - Déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- **Non répudiation**
 - Garantie qu'aucun des correspondants ne pourra nier avoir effectué la transaction

Sécurisation des échanges

Principes de mise en oeuvre

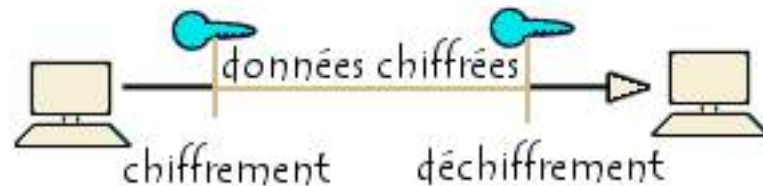
Cryptographie

- Ensemble des techniques permettant de chiffrer des messages
- Utilisation d'algorithmes mathématiques
- Utilisation de clef privé et/ou clef publique



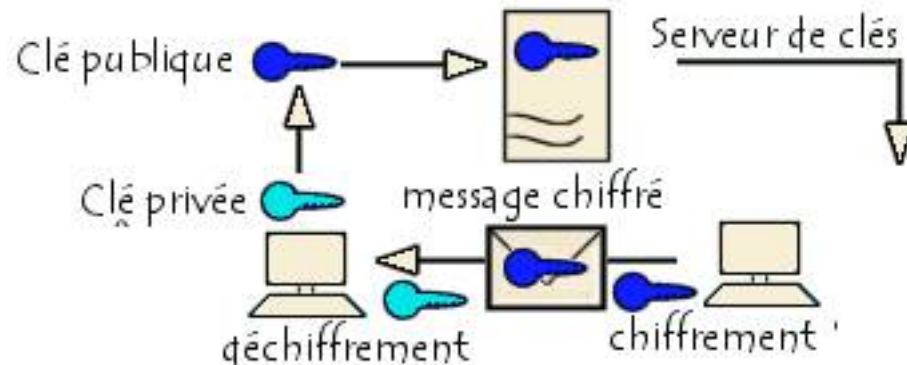
Chiffrement symétrique

- Applications d'un algorithme sur les données à partir d'une clef privée
- Le chiffrement et le déchiffrement nécessitent la même clef
- Mis au point dans les années 20
- Problème : communiquer la clef secrète



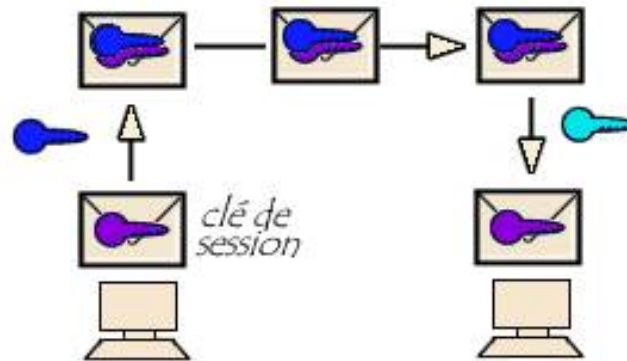
Chiffrement asymétrique

- Chiffrement à clefs publiques
- Deux clefs :
 - Une clef privée pour le déchiffrement (choisit aléatoirement)
 - Une clef publique pour le chiffrement (calculée depuis la clef privéé)
- Basé sur un fonction mathématique simple dans un sens, très complexe dans l'autre (*one-way trapdoor function*)
- Problème : être sûr que la clef est bien du destinataire !



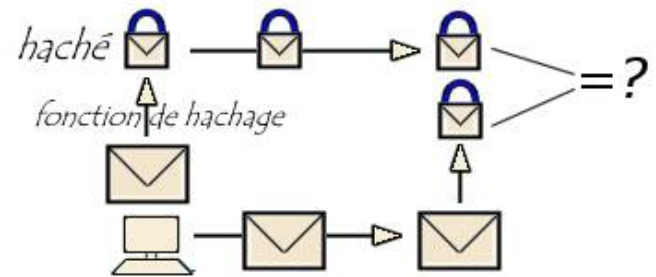
Notions de clef de session

- Problèmes du chiffrement asymétrique : gourmand en temps de calcul
- Clé de session : compromis entre symétriques et asymétriques
 - Génération aléatoire d'une clef de session
 - Chiffrement de la clef avec le chiffrement asymétrique (clef publique)
 - Établissement d'une session en chiffrement symétrique



Signature électronique

- Permet de garantir l'authenticité de l'expéditeur, de vérifier l'intégrité du message et de garantir la non répudiation
- Utilisation d'une fonction de hachage : à un texte clair est associé un et un seul texte haché (sorte d'empreinte digitale), et ne fonctionnant que dans un seul sens
- Algorithmes MD5 et SHA
- En envoyant le message + le hachage, il suffit de faire l'opération inverse à la réception pour vérifier l'intégrité du message
- Pour garantir l'authentification du message, il suffit à l'expéditeur de chiffrer le haché (alors appelé sceau) avec sa clé privée. C'est l'opération de scellement. Le destinataire déchiffre avec la clé publique de l'expéditeur.



Certificats

- Problème des clefs publiques : s'assurer que la clef est bien celle du destinataire
- Le certificat permet d'associer une clef publique à une entité afin d'en assurer la validité. Il est délivré par une autorité de certification (CA)
- Il contient :
 - Des informations sur le détenteur du certificat
 - La signature de l'autorité de certification

Création du certificat

- Le CA signe (*hache + chiffre avec sa clef privée*) le certificat
- *La clef publique du CA est diffusée*

Certificat

Informations
- Autorité de certification : Verisign
- Nom du propriétaire : Jeff PILLOU
- Email : webmaster@commentcamarche.net
- Validité : 04/10/2001 au 04/10/2002
- Clé publique : 1a:5b:c8:a5:32:4c:d6:df:42
- Algorithme : RC5

Signature
3b:c5:cF:d6:9a:8d:e3:c6



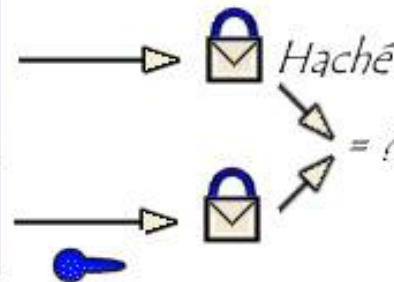
Clé privée de l'autorité de certification

Vérification du certificat

- Obtention de la clef publique
- Déchiffrement
- Vérification du hachage

Certificat

<i>Informations</i>
- Autorité de certification : Verisign - Nom du propriétaire : Jeff PILLOU - Email : webmaster@commentcamarche.net - Validité : 04/10/2001 au 04/10/2002 - Clé publique : 1a:5b:c3:a5:32:4c:d6:df:42 - Algorithme : RC5
<i>Signature</i>
3b:c5:cf:d6:9a:8d:e3:c6



*Déchiffrement à l'aide
de la clé publique de
l'autorité de certification*