Lycée Voltaire

Sécurité des communications

N.S.I

Table des matières

Sécurité des communications

1 Vocabulaire

Coder(encoder)/decoder/chiffrer/déchiffrer/Décrypter/Cryptanalyse

Coder :

Décoder :

Chiffrer :

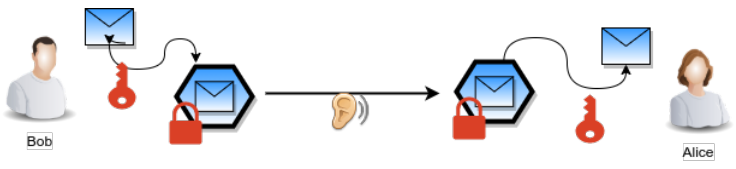
Déchiffrer :

Décrypter :

Pour résumer :
— Chiffrer un message consiste à ...
— Déchiffrer un message consiste à ...
— Décrypter un message consiste à ...
Le terme "crypter" est à proscrire : lien

2 Chiffrement symétrique

Il y a de nombreux chiffrements symétriques. Nous avons vu un exemple avec l'utilisation du .....
Quelque soit le chiffrement symétrique, le principe est toujours le même :



Avantages :

1. Très efficace. Chiffrement/déchiffrement en temps réel.(vidéos chiffrée en temps réel)
2. Si la clef est bien choisie, le décryptage est très difficile.

Inconvénients :

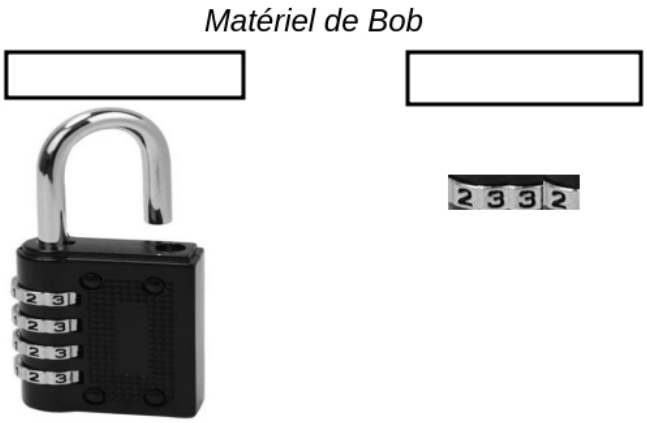
1. (Le plus grand défaut) ...

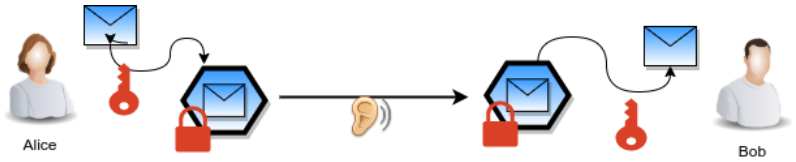
2. Si la clef est trop courte (ou naïve), on peut décrypter (par ..... par exemple).
3. Si Bob veut communiquer avec 100 personnes, il lui faut ..... clefs. Si ces 100 personnes veulent communiquer entre elles, il faut ..... clefs.

3 Chiffrement asymétrique (où chiffrement à clef publique)

Principe général : (Utilisation de cadenas)

1. Alice demande à Bob un cadenas ouvert. .....
2. Alice reçoit le cadenas de Bob, elle met son message dans une boite qu'elle ferme avec le cadenas.
3. Bob reçoit la boite qu'il peut ouvrir grâce à SON CODE (qu'il est le seul à connaître). .....





A retenir :

— Connaissant la clef publique de Bob K_{Bob}^{pub}, il est ..... de deviner la clef privée de Bob K_{Bob}^{priv}

— Connaissant le message m crypté avec K_{Bob}^{pub} noté $K_{Bob}^{pub}(m)$, il est ..... de trouver m

— Connaissant le message m crypté avec K_{Bob}^{priv} noté $K_{Bob}^{priv}(m)$, il est ..... de trouver m

Certains chiffrements asymétriques comme R.S.A sont ..... c'est à dire :

$$K_{Bob}^{pub}(K_{Bob}^{priv}(m)) = K_{Bob}^{priv}(K_{Bob}^{pub}(m)) = m$$

Cette réversibilité sera utilisée comme moyen d'authentification. (Voir paragraphe 5)

Avantages :

1. Contrairement au chiffrement symétrique. Alice et Bob n'ont pas à se mettre d'accord sur la clef.
2. Chaque personne possède son jeu de clefs.
3. Il est actuellement impossible de décrypter un message sans connaître la clef privée.

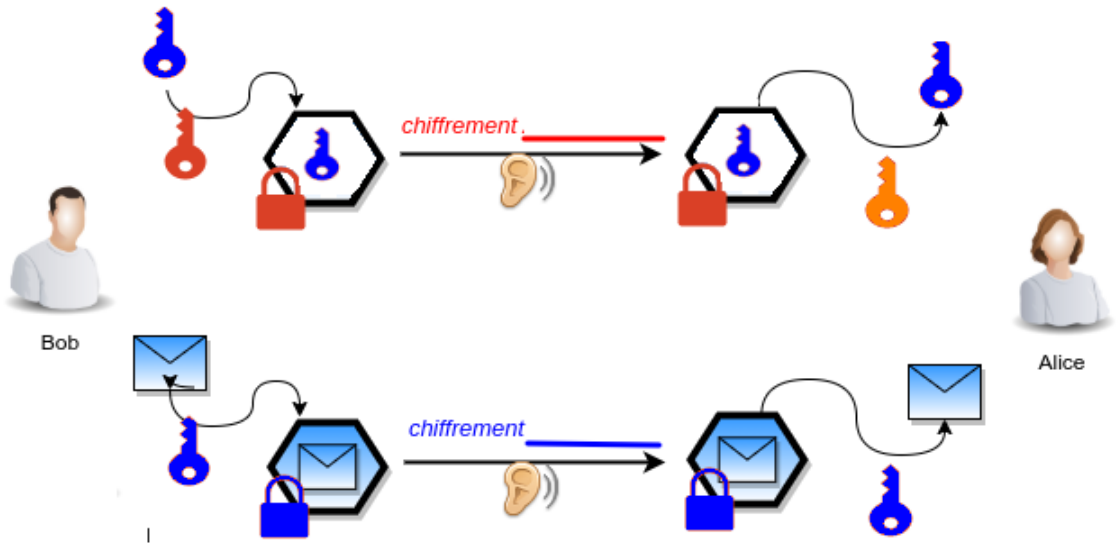
Inconvénients :

1. Le chiffrement et le déchiffrement nécessitent des calculs coûteux. Il est donc impossible de l'utiliser pour des flux de communication, visioconférence). Environ ..... fois plus long qu'avec un chiffrement symétrique.
2. Le message codé est environ ..... fois plus grand que le message lui-même !

4 Utilisation des deux chiffrements

1. Grace à la clef publique d'Alice, Bob va lui envoyer une clef (clef partagée) chiffrée avec un chiffrement.....
2. Alice va déchiffrer cette clef avec .....
3. Grace à cette clef, ils vont pouvoir communiquer avec un chiffrement .....

Compléter le schéma illustrant le principe ci-dessus :



5 Authentification

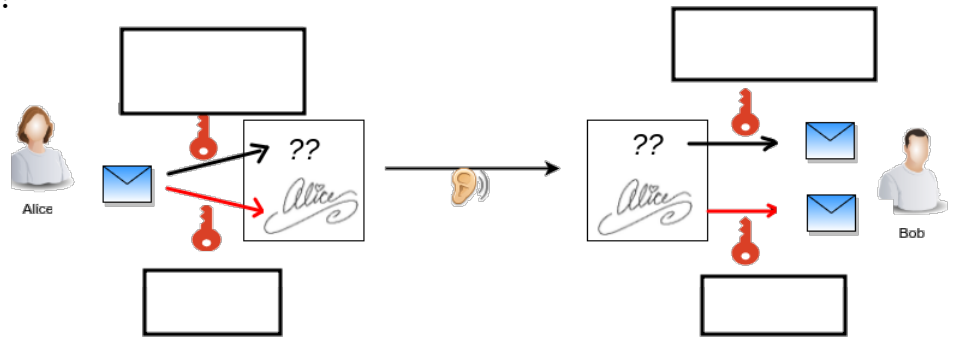
Problème : Bob correspond avec Alice et souhaite être sûr que les messages qu'il reçoit ont bien été écrits par Alice.

Il s'agit d'un problème de signature, on souhaite donc pouvoir garantir :
— l'authentification un document : provient-il bien du bon auteur ?
— qu'une modification ultérieure du document doit invalider la signature.

Solution : Nous allons utiliser caractère réversible de certains systèmes de chiffrement asymétrique (comme RSA) pour mettre en œuvre une signature.

$$K_{Bob}^{pub}(K_{Bob}^{priv}(m)) = K_{Bob}^{priv}(K_{Bob}^{pub}(m)) = m$$

Première idée :



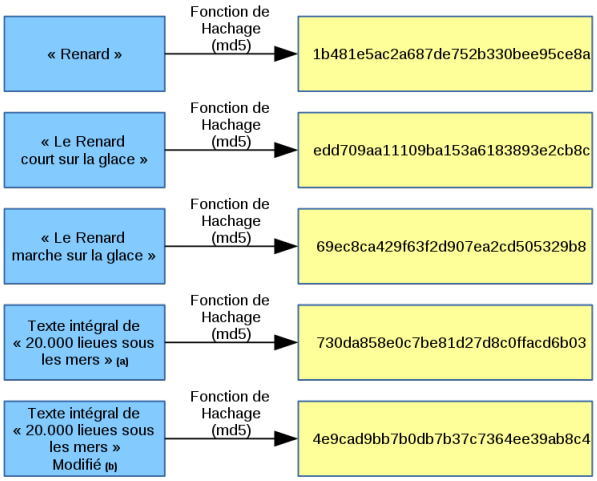
Si le contenu des deux enveloppes est identiques cela signifie que c'est bien Alice qui a rédigée le message et que celui ci n'a pas été modifié lors du transport.

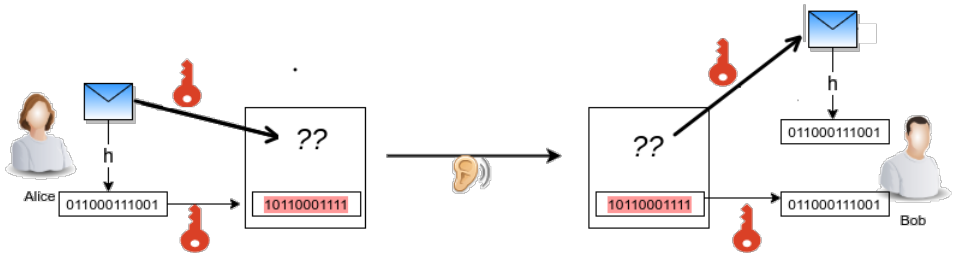
Deux inconvénients :

1. produire et vérifier la signature est long et coûteux ;
2. la signature est aussi grosse que le document.

Deuxième idée :

On utilise une fonction de hachage h qui permet d'obtenir un condensé d'un message. En principe, cette fonction doit être :
— difficilement réversible ;
— injective : Si $h(m) = h(m')$ alors $m = m'$





Bilan :

L'authentification d'un document permet de garantir au destinataire que l'expéditeur du document est bien l'auteur de ce document et que ce document n'a pas été modifié par un tiers.

MAIS le destinataire est-il sûr que l'expéditeur est bien la "bonne" personne ?

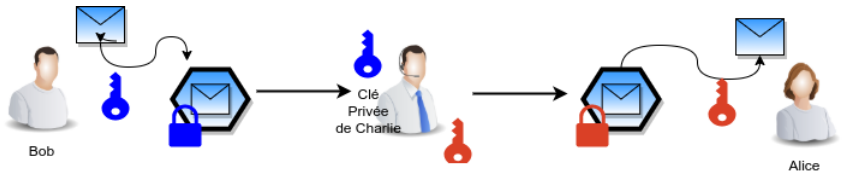
6 Les certificats électroniques

Attaque de l'homme du milieu

— Imaginons qu' Alice souhaite communiquer à Bob sa clé publique.
— L'attaquant Charlie parvient, par un moyen ou un autre, à intercepter les communications entre Alice et Bob.
— Il intercepte la diffusion de la clé publique ;
— Il envoie à Bob sa propre clé publique en se faisant passer pour Alice ;

Attaque :

— L'usurpation fonctionne alors dans les deux sens :
— lorsque Alice signe un message, il le signe avec sa propre clé privée
— lorsque Bob envoie un message chiffré à Alice, il utilise la clé de Charlie.



Les certificats

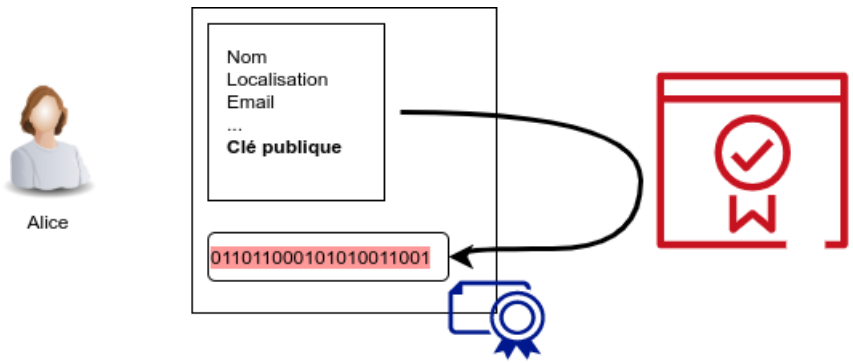
Les certificats électroniques sont une réponse à ce problème de diffusion non sécurisée de la clé publique.
Il y a deux modèles :
— modèle hiérarchique : basé sur des autorités de certification
— modèle réseau : pgp, mail

Autorité de certification

Un certificat met en jeu une autre entité : l'autorité de certification.
Il s'agit d'organismes dûments enregistrés et certifiés auprès des autorités publiques.
Les systèmes d'exploitation et navigateurs web incluent nativement les listes des clés publiques de ces autorités de certification.
Un certificat électronique est un ensemble de données contenant :
— des informations d ?identification (nom, email, ?)
— une clé publique
— une signature des données précédentes obtenue avec la clé privée d'une autorité de certification.

Création du certificat

Lorsque Alice veut diffuser sa clé publique, elle effectue une demande auprès d'une autorité de certification. Celle ci reçoit la clé publique et l'identité d'Alice.
Après avoir vérifié la clé publique et l'identité d'Alice par des moyens conventionnels, elle crée un certificat contenant les données et la signature calculée avec sa clé privée.



Bob souhaite communiquer avec Alice. Celle-ci lui envoie son certificat.
Bob peut alors vérifier l'intégrité du certificat en utilisant la clé publique de l'autorité de certification.
S'il authentifie le certificat, alors il peut utiliser la clé publique qu'il contient pour échanger avec Alice.

Utilisation du certificat

Bob souhaite communiquer avec Alice. Celle-ci lui envoie son certificat.
Bob peut alors vérifier l'intégrité du certificat en utilisant la clé publique de l'autorité de certification.
S'il authentifie le certificat, alors il peut utiliser la clé publique qu'il contient pour échanger avec Alice.