Chapitre 12 : Cryptographie et sécurisation des communications

12.1 Principe et introduction

Depuis la naissance de l'écriture l'Homme a cherché à maintenir secrètes certaines communications. Dans de nombreux domaines tels que les champs politique, militaire, économique, amoureux, etc. il est nécessaire de disposer d'une forme de communication chiffrée. Dans le cas de la cryptographie, il ne s'agit pas de dissimuler un message (par exemple dans un autre texte, dans une image ou à l'encre invisible) mais de le rendre incompréhensible à ceux qui ne possèdent pas la clé de déchiffrement.
La cryptographie est utilisée depuis l'antiquité, l'une des utilisations les plus célèbres pour cette époque est le chiffre de césar, nommé en référence à Jules César qui l'utilisait pour ses communications secrètes. Mais la cryptographie est bien antérieure à cela, une des traces les plus anciennes de messages chiffrés remonte au XVe siècle avant J.C.

Définition 1
Les principes communément adoptés pour caractériser un système de chiffrement sont au nombre de trois :

1. Le système doit être mathématiquement « indéchiffrable » (reste à definir ce que l'on entend par indéchiffrable).
2. La méthode de chiffrement n'a pas à être secrète, la méthode ou l'algorithme de chiffrement peut être divulguée sans mettre en péril le chiffrement.
3. La clé de chiffrement doit pouvoir être simple à retenir et facilement communiquable, modifiable.

Noter que les chiffrements de cesar et affine vérifient ces trois conditions s'il on accepte qu'à une époque elles étaient indéchiffrables.

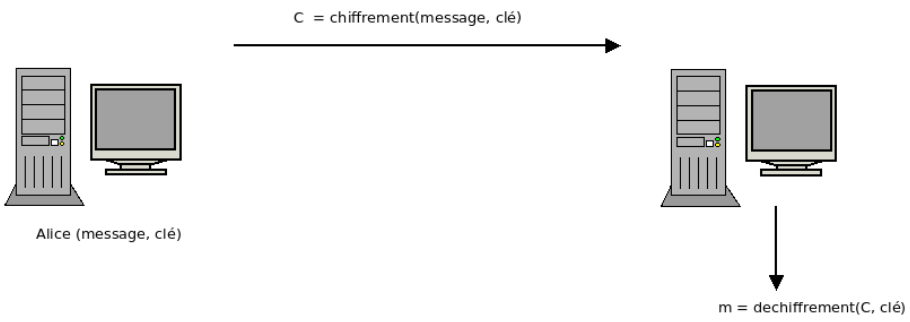
12.2 Le chiffrement symétrique

a. Principe

Tous les schémas de chiffrement utilisés jusque dans les années 1970 sont dits symétriques, ce qui signifie que la même clé est utilisée pour chiffrer et pour déchiffrer. On les appelle également schémas de chiffrement à clé secrète.
Une analogie couramment utilisée est celle du coffre-fort. L'expéditeur et le destinataire utilisent un coffre-fort partagé pour s'échanger des messages. Tous deux ont accès à la clé, aussi bien pour déposer des messages que pour en retirer.

Propriété 1
Les systèmes de chiffrement symétrique sont composés de trois algorithmes :

- un algorithme de génération de clé, qui retourne en sortie une clé secrète K partagée entre les deux utilisateurs ;
- un algorithme de chiffrement, qui prend en entrée un message m (secret) et cette clé K (secrète) et renvoie un message C (chiffré) ;
- un algorithme de déchiffrement, qui prend en entrée un message chiffré C (public) et la clé K (secrète) et renvoie le message clair m (secret).



b. Deux différents types de chiffrement symétrique

Dans un chiffrement de flux ou chiffrement y par flots (Cipher stream) en anglais, on traite des données de longueur quelconque sans les découper. Un exemple de chiffrement de flux est les chiffrement XOR (ou exclusif).

Dans un chiffrement par bloc (block stream en anglais) les données sont découpées en blocs de taille généralement fixe). Un exemple de chiffrement de bloc est l'AES (Advanced Encryption Standard).

c. Problème de la transmission des clés

Le principal inconvénient du chiffrement symétrique est la nécessité d'utiliser une clé secrète par couple d'utilisateurs. Sur un réseau de grande taille comme Internet, il est totalement illusoire de distribuer ces clés à l'avance et de les stocker. Une meilleure solution est de parvenir à créer cette clé à la volée, au début de la communication, sans supposer d'information partagée au préalable entre les deux utilisateurs.

Mais comment faire en sorte que deux personnes, qui ne se sont probablement jamais parlé, parviennent de manière sûre à construire un secret commun ?

Une solution a été proposée en 1976, avec l'invention de la cryptographie asymétrique par Diffie et Hellman, créateurs du schéma d'échange de clé qui porte à présent leur nom.

12.3 La cryptographie asymétrique

a. Échange ou distribution de clés

On distingue principalement deux cas de figure dans le problème du choix et de la transmission de la clé symétrique entre Alice et Bob :

- une première solution est qu'Alice choisisse une clé symétrique et la transmette à Bob grâce à du chiffrement asymétrique ;
- une deuxième est qu'Alice et Bob se mettent d'accord et construisent ensemble une clé.

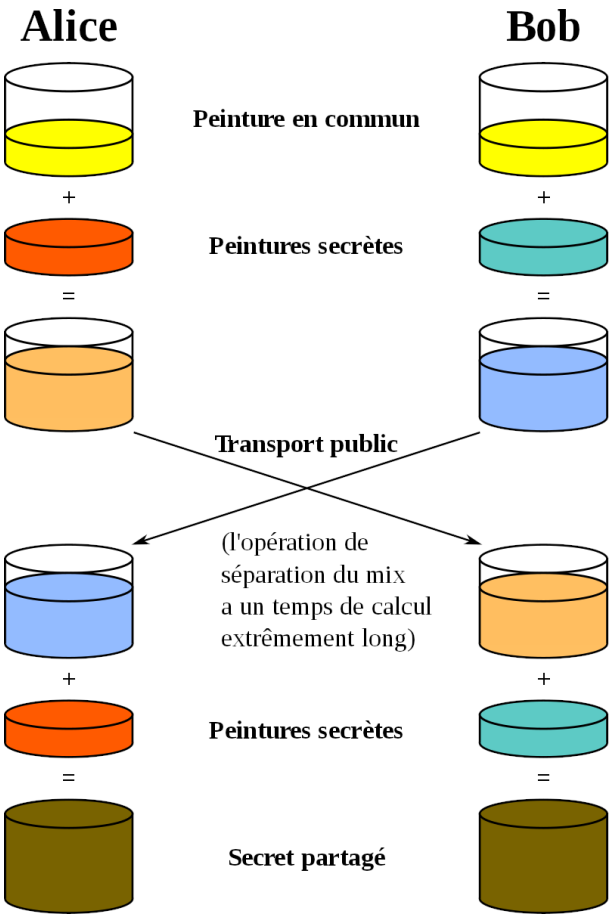
La première solution est apellée **distribution de clé** et la seconde **échange de clé**.

b. Échange de clé système à clé publique, clé privée

L'échange de Diffie-Hellman permet à Alice et Bob, sans avoir échangé au préalable, de se mettre d'accord sur une clé secrète. Cette méthode repose sur des propriétés mathématiques de l'arithmétique modulaire.

1. Alice et Bob choisissent un nombre premier p et g un entier compris entre 2 et $p-1$. Les nombres p et g sont communiqués en clair et publiquement.
2. Alice choisit un entier α qui servira d'exposant, elle calcule g^α modulo p, elle transmet en clair ce nombre à Bob. Bob pendant ce temps-là fait de même, il choisit un nombre β, calucule g^β modulo p et le transmet à Alice.
3. Alice élève à la puissance α le nombre qu'elle a reçu de Bob elle obtient $g^{\beta\times\alpha}$ modulo p, exactement la même chose que Bob qui lui aussi élève à la puissance β le nombre qu'il a reçu. Il obtient $g^{\beta\times\alpha}$ modulo p.
4. La clé secrète est $g^{\alpha\times\beta}$ modulo p.

La sécurité de cette méthode repose sur le fait qu'il est mathématiquement simple de calculer g^n mais très difficile étant donné un nombre entier M de retrouver la puissance α telle que $M = g^\alpha$ modulo p.
C'est ce que l'on appelle le problème du **logarithme discret**. Dans ce cas le choix du nombre premier initial est primordial pour que le calcul du logarithme discret dans cet ensemble soit véritablement difficile.
Une analogie très répandue pour illustrer ce principe est celle des pots de peinture. C'est A.J. Han Vinck professeur d'informatique à l'université de Duisburg-Essen qui est en est l'auteur.



c. Distribution de clé

Lors d'une distribution d'une clé symétrique une personne comme Bob veut communiquer avec Alice. Il souhaiterait lui communiquer une clé de chiffrement symétrique . Pour illustrer le principe de cette méthode on utilise l'analogie de la boîte aux lettres. Alice possède une boîte aux lettres dont elle seule posséde la clé, n'importe quel expéditeur peut lui faire parvenir un message, son adresse est publique. Cependant elle seule peut l'ouvrir et lire le message.

Chiffrement RSA

Inventé en 1978 par Rivest, Shamir et Adleman, trois chercheurs en informatique, le cryptosystème RSA est le chiffrement asymétrique le plus utilisé au monde actuellement.
Voici son principe sous forme d'un exemple numérique :

1. Alice choisit deux grands nombres premiers. On décide pour cet exemple élémentaire de prendre deux petits nombres premiers $p = 7$ et $q = 71$.
2. Alice calcule le produit $n = p \times q$. Ici $n = 497$.
3. Alice calcule $\varphi(n) = (p-1) \times (q-1)$. Ici $\varphi(n) = 432$
4. Alice choisit un nombre entier e premier avec $\varphi(n)$. Ici $e = 205$
5. Alice est là seule à pouvoir calculer d l'inverse de e modulo $\varphi(n)$. Ici $d = 373$ c'est la clé de déchiffrement.

Dans la pratique Alice publie le couple (n, e) c'est ce que l'on appelle la clé publique.

Bob pour communiquer un message M à Alice, calcule $S = M^e$ modulo n et lui envoie. Pour retrouver le message, Alice n'a qu'à calculer S^d modulo n. Dans cette méthode Alice est la seule à déchiffrer et Bob le seul à chiffrer, leurs rôles sont tout à fait différents : **asymétrique**.

d. Signature numérique

Les deux méthodes ci-dessus sont vulnérables à une attaque de type Man In the Middle. Pour éviter cela il faut imaginer un dispostif capable d'authentifier l'auteur d'un message, un dispostif de signature numérique.
Dans le chiffrement RSA, la paire de clés publiques d'ALice est connue de tous. Elle peut s'en servir pour créer un dispositif de signature car elle est la seule à connaître la clé privé.

1. Alice choisit un message m qu'elle chiffre avec sa clé privée en calculant $s = m^d$ modulo n (rappel elle est la seule à connaître d).
2. Elle envoie à Bob m et s.
3. Bob, ou n'importe qui d'autre, connaît la clé publique d'Alice, il calcule donc s^e modulo n. S'il retrouve m le message est bien d'Alice. S'il trouve un autre résultat ce n'est pas la signature d'Alice, la signature a été falsifiée.

Il reste encore un point faible à cette méthode, comment être sûr que la clé publique d'Alice est bien celle la sienne. Ce problème est bien connu, notamment pour le fonctionnement du protocole HTTPS.
La solution choisie consiste à faire confiance à des organismes certificateurs qui garantissent que la clé publique d'un serveur web est bien celle du serveur web qu'il prétend être.