# Le chiffrement

## I) Chiffrement asymétrique :

Le chiffrement asymétrique repose sur l'utilisation d'une clé publique et d'une clé privée. L'algorithme utilisé est le RSA.

La clé publique sert au chiffrement alors que la clé privée sert au déchiffrement.

La cryptographie asymétrique est utilisée avec les certificats numériques. Le certificat (présent sur le poste client) contient la clé publique alors que la clé privée est stockée sur le serveur.

### 1.1) Fonctionnement du chiffrement asymétrique :

Un ami doit vous faire parvenir un secret par la poste qui ne doit être lu qu'uniquement par vous.

Afin d'être l'unique lecteur du message, envoyer à votre ami un cadenas sans sa clé en position ouverte.

Votre ami glisse son secret dans une boite qu'il ferme à l'aide du cadenas, puis l'envoie par la poste. Le facteur ne peut pas ouvrir cette boite car vous êtes le seul à posséder la clé.

Lors de la réception de la boite, vous n'avez qu'à ouvrir le cadenas à l'aide de votre clé afin de connaître le secret de votre ami.

Les algorithmes à clé publique (ou chiffrement asymétrique) sont beaucoup plus lents que les algorithmes symétriques.

### 1.2) Mécanisme d'authentification :

Si la clé publique est partagée avec plusieurs personnes, il est impossible de certifier l'identité de l'émetteur sauf en utilisant un mécanisme d'authentification par chiffrement asymétrique.

Si l'on chiffre un message en utilisant la clé publique, alors on peut déchiffrer le message en utilisant la clé privée ; l'inverse est aussi possible : si l'on chiffre en utilisant la clé privée alors on peut déchiffrer en utilisant la clé publique.

Objectif : Bob souhaite envoyer des données chiffrées à Alice en lui garantissant qu'il en est l'expéditeur.

Bob et Alice créent une paire de clés asymétriques. Ils conservent la clé privée et s'échangent la clé publique.

Bob effectue un condensat de son message "en clair" . Il chiffre le condensat avec sa clé privée puis avec la clé publique d'Alice.

Bob envoie le message chiffré accompagné du condensat chiffré à Alice.

Alice déchiffre le message avec sa propre clé privée. À ce stade le message est lisible mais elle ne peut pas être sûr que Bob en est l'expéditeur. Maintenant elle déchiffre le condensant avec la clé publique de Bob.

Alice utilise la même fonction de hachage sur le texte en clair et compare avec le condensat déchiffré de Bob.

Si les deux condensats correspondent, alors Alice peut avoir la certitude que Bob est l'expéditeur. Dans le cas contraire, on peut présager qu'une personne malveillante a tentée d'envoyer un message à Alice en se faisant passer pour Bob.

## II) Chiffrement symétrique :

Le chiffrement symétrique repose sur l'utilisation de clé privée. Cette clé sert à la fois au chiffrement et au déchiffrement.

L'algorithme DES a été abandonnée un peu avant 2001 car il ne chiffrait que sur 56 bits.
Son remplaçant l'AES permet de chiffrer sur 128 bits.