CHIFFREMENT : SYNTHÈSE DE COURS

1) Les 3 exigences d'une communication sûre

- **Confidentialité :** Le pirate ne peut pas lire vos messages.
- **Intégrité :** Le pirate ne peut pas modifier vos messages.
- **Authentification :** Le pirate ne peut pas se faire passer pour votre interlocuteur

2) Chiffrement symétrique

> ***Définition :***
> On parle de **chiffrement symétrique** quand la même clé permet à la fois de chiffrer et de déchiffrer un message.

Remarques :

- En informatique, ce ne sont pas des « lettres » que l'on chiffre mais des nombres. Pour chiffrer un texte, il faut bien sur commencer par le transformer en une suite de nombres.
- Les algorithmes utilisent souvent le XOR qui a comme propriété intéressante : $(a \oplus b) \oplus b = a$
  (= Si on rechiffre un message chiffré avec la même clé, on retombe sur le message initial).
- Un simple chiffrement avec un XOR est impossible à casser si la clé est vraiment aléatoire, aussi longue que le message et à usage unique.
- Le chiffrement symétrique le plus connu actuellement est le **chiffrement AES**. Ce chiffrement est beaucoup plus compliqué qu'un simple XOR mais reste très difficile à casser, même si la clé est beaucoup plus courte que le message.
- Les méthodes modernes de chiffrement symétrique sont très sûres et consomment peu de ressources mais supposent que les deux personnes qui communiquent aient pu au préalable s'échanger une ou plusieurs clés secrètes.

3) Chiffrement asymétrique

> ***Définition :***
> On parle de **chiffrement asymétrique** quand il y a deux clés différentes : une **clé publique** pour chiffrer et une **clé privée** pour déchiffrer :
> - Le destinataire du message envoie sa clé publique à l'émetteur.
> - L'émetteur chiffre son message avec cette clé et envoie le message chiffré au destinataire.
> - Le destinataire utilise sa clé privée pour déchiffrer le message.

Remarques :

- Pas besoin de partager une clé à l'avance comme dans les chiffrements symétriques.
- La sécurité repose sur le fait qu'il est quasi impossible de retrouver la clé privé à partir de la clé publique.
- Le chiffrement asymétrique le plus connu actuellement est le **chiffrement RSA** qui s'appuie sur la difficulté qu'ont les ordinateurs actuels à **factoriser** des grands nombres entiers en produit de deux nombres premiers.
- Hélas, les chiffrements asymétriques sont beaucoup plus gourmands en ressources que les chiffrements symétriques équivalents.
- On peut **signer numériquement** un message en le chiffrant avec sa clé privée que l'on est le seul à détenir. Le destinataire pourra chiffrer le message reçu avec notre clé publique et s'il obtient un message intelligible, il pourra être certain que nous sommes bien l'émetteur.

4) Protocole HTTPS (= HTTP + TLS)

- Le but est de réunir le meilleur des deux mondes : On commence la communication par un chiffrement asymétrique (qui ne nécessite pas de rencontre préalable), le temps de s'échanger une clé de chiffrement symétrique, puis on continue en chiffrement symétrique (beaucoup moins gourmand en calculs).
- Le chiffrement permet la **confidentialité** et l'**intégrité** des communications mais pas l'**authentification** : Si Alice veut communiquer avec Bob mais que ses messages sont interceptés dès le début par un pirate qui se fait passer pour Bob, elle ne s'en rendra pas forcément compte. TLS prévoit donc un mécanisme d'authentification à l'aide de **certificats** signés par des **autorités de certification** auxquelles Alice et Bob font confiance tous les deux (ou plutôt leurs navigateurs ;-).