* **Chiffrement symétrique** :

Le navigateur et le serveur utilise la même clé pour encrypter et décrypter les données transférées

La clé symétrique est échangée entre le serveur et le navigateur au début de la connexion.

**Problème** :

Un pirate qui se trouve au milieu entre serveur et client peut pirater la clé et décrypter le contenu des données échangés.

* **Chiffrement asymétrique** :

Clé publique : utilisé pour crypter les donnés

Clé privée : utilisé pour décrypter les données (doit être bien sauvegarder)

Le serveur crée une clé publique et une clé privée et envoie la clé publique vers le navigateur. Ce dernier utilise cette clé pour encrypter la clé symétrique et la renvoyer vers le serveur. Si le pirate se trouve au milieu il ne peut pas décrypter la clé symétrique car il ne possède pas la clé privée et comme ça on n’a pas de problème.

**Problème** :

Le pirate peut jouer le rôle de proxy entre le client et le serveur.

Lorsque le navigateur demande connexion le pirate répond avec un clé publique généré par le pirate avec son clé privée. Le navigateur utilise cette clé pour encrypter la clé symétrique et l’envoyer cette fois au pirate et comme ça le pirate joue le rôle de proxy.

* **Le certificat** :

Le navigateur ne va pas accepter aucune clé publique s’il n’est pas signé ou certifié.

Pour que la clé publique de serveur soit acceptée elle doit être signé par CA (certificat authority).

CA : c’est un serveur que tout le monde fait confiance

Qu’une clé soit signée il faut :

* Soit Attaché à un nom de domaine (ex : Banque.tn) : CA va demander une preuve que vous été le propriétaire de ce nom de domaine.
* Si c’est bon CA va signer votre clé

Lorsque le navigateur recoit la clé signée il va vérifier la liste des certificats.

Les certificats sont mis à jour dans votre navigateur.

* A la place d’échange de clé public on parle maintenant de l’échange de certificat qui contient la clé publique.

Empreinte : hasher certificat content.

La signature : on va signer l’empreinte avec clé privé qui va chiffrer les données et un clé public qui va déchiffrer les données.