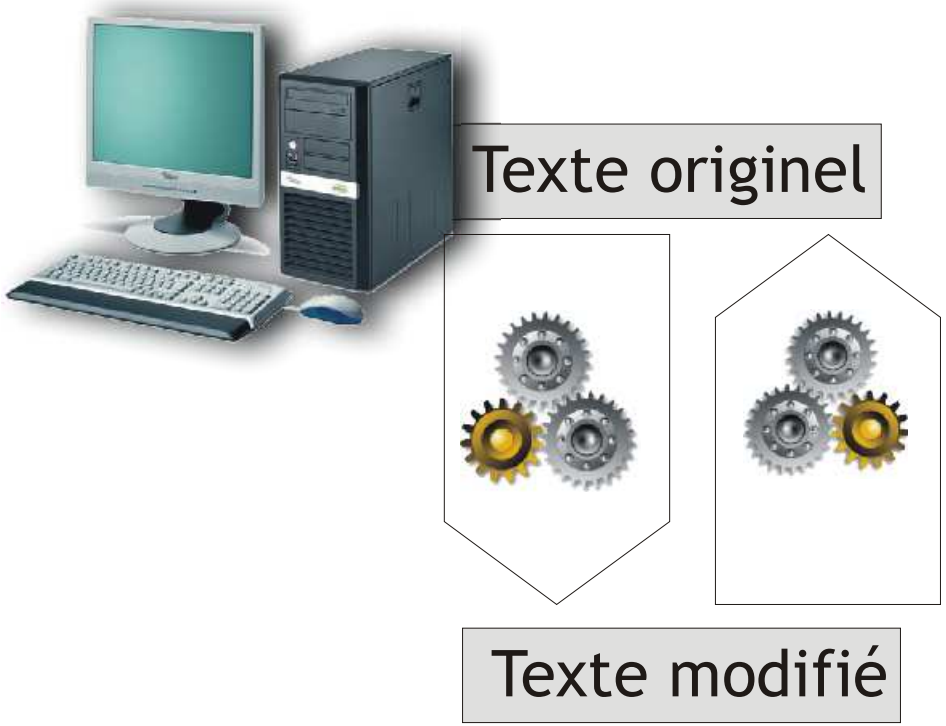
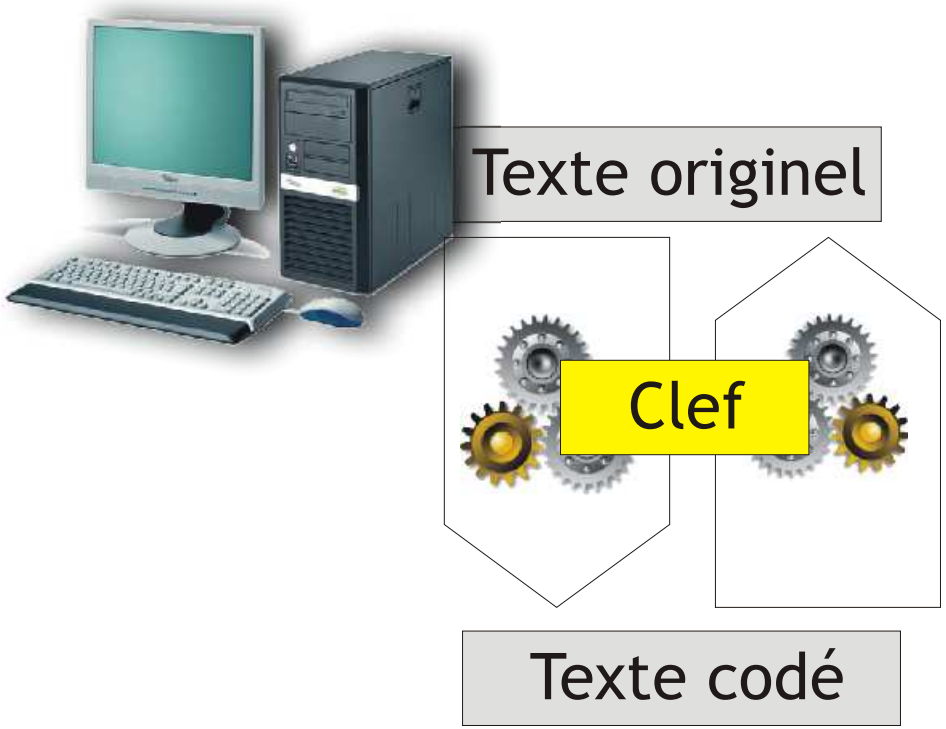
✓ **Algorithmes de chiffrement faibles (facilement cassables) :**

- ROT13 (rotation de 13 caractères, sans clé)
- Chiffre de César (décalage de trois lettres dans l'alphabet sur la gauche)
- Chiffre de VIGENERE (introduit la notion de clé)



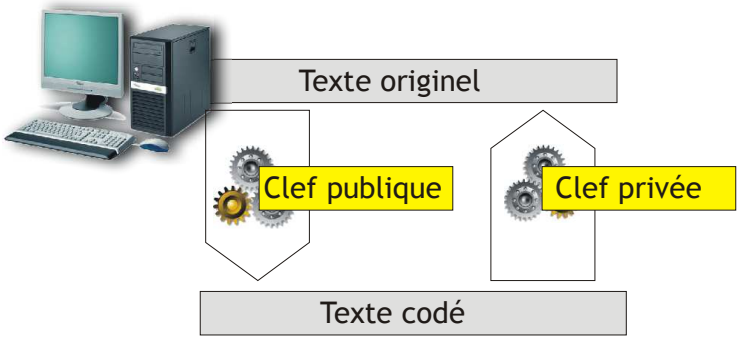
✓ **Algorithmes de cryptographie symétrique (à clé secrète) :**

- Chiffre de Vernam (le seul offrant une sécurité théorique absolue, à condition que la clé ait au moins la même longueur que le message, qu'elle ne soit utilisée qu'une seule fois à chiffrer et qu'elle soit totalement aléatoire)
- DES (Data Encryption Standard) en 1977
- 3DES (Triple DES) en 1999
- AES (Advanced Encryption Standard) en 2000
- RC4 (Rivest Cipher 4) en 1987 (Rivest est le concepteur) puis RC5, RC6…
- MISTY1 (Mitsubishi Improved Security Technology) en 1995

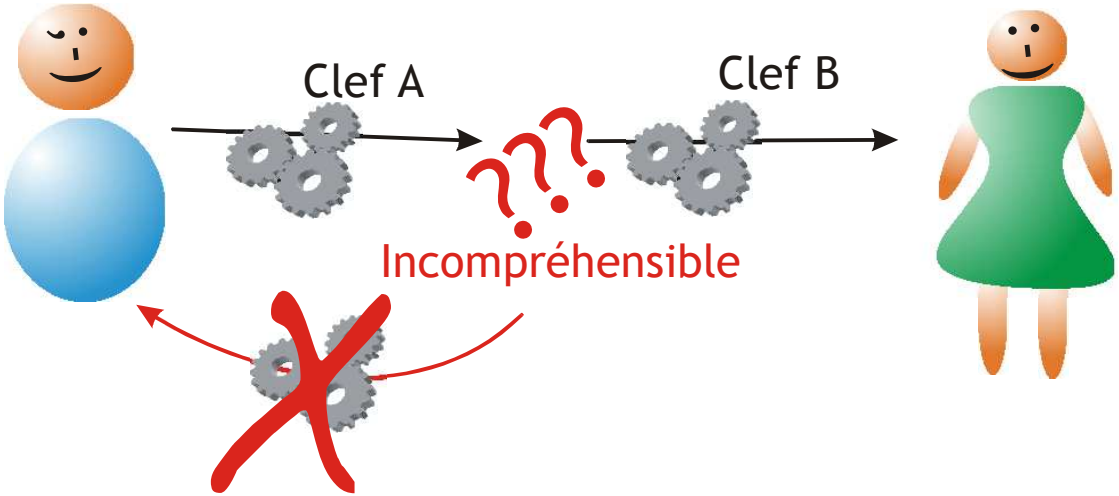


✓ **Algorithmes de cryptographie asymétrique (à clé publique et privée)**

- RSA (chiffrement et signature)
- DSA (signature)
- Protocole d'échange de clés Diffie-Hellman (échange de clé)
- Des logiciels permettent l'encryptage des données pour envoi groupé : PGP GnuPG (libre et en opensource)



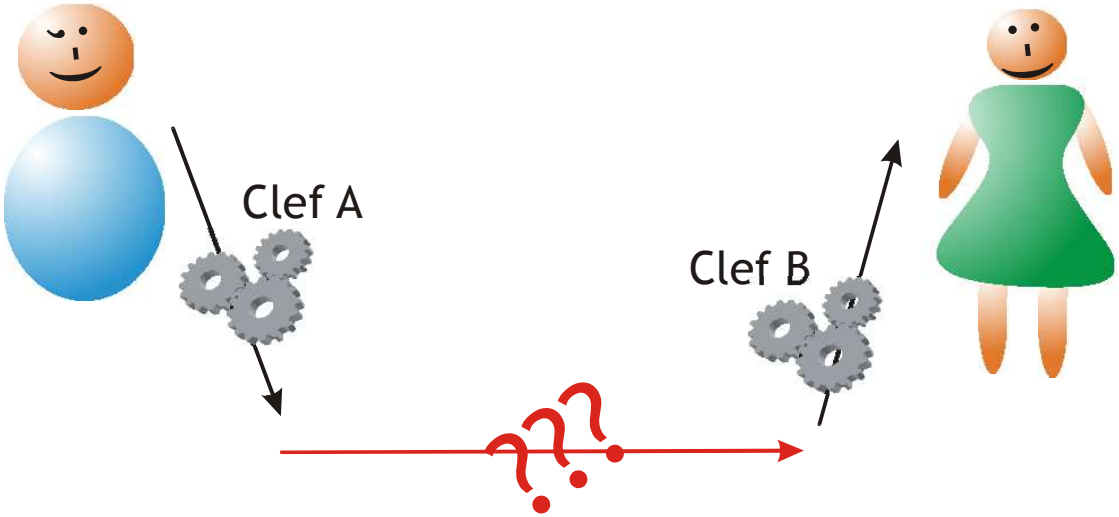
SSL - chiffrement SSL



Le principe de chiffrement utilisé dans le SSL.

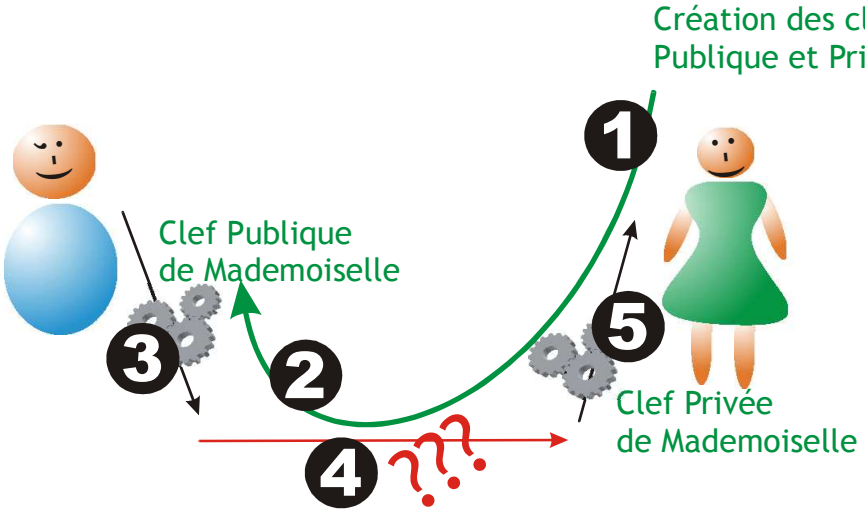
Le concept est de crypter les données de telle manière qu'il n'est pas possible de remonter en arrière.

Le nombre de bits de sécurité sont souvent
64 bits : **18446744073709551616** clefs possibles
128 bits : **3,40e+38** clefs possibles

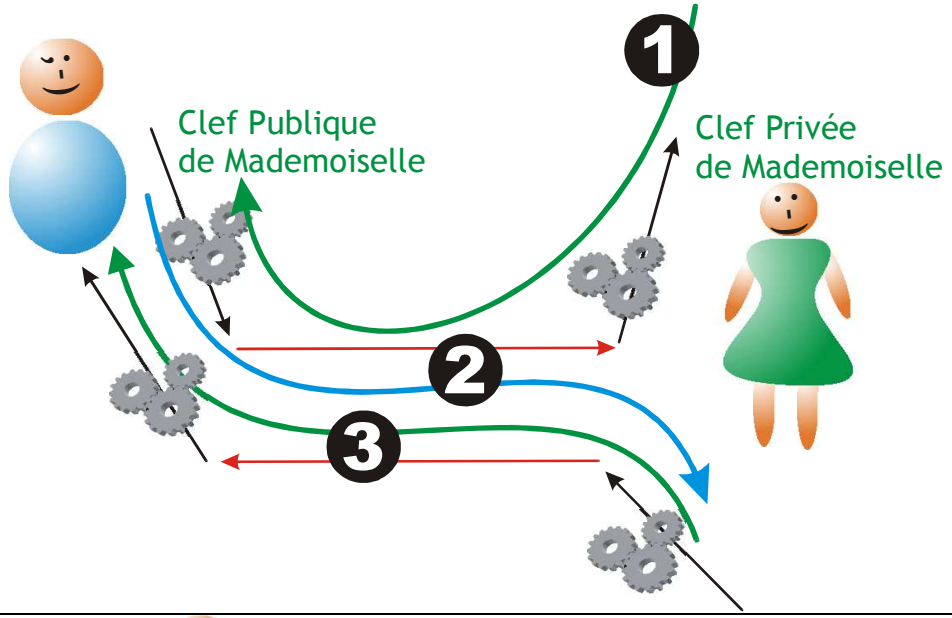


Durant le transport, les données ne sont pas réversibles.

Toutefois, comment faire pour que Monsieur connaisse la clef qui fonctionne avec Mademoiselle ?



1. Mademoiselle crée un couple de clefs de codage décodages.
2. la clef Publique de Mademoiselle est transmise à Monsieur qui pourra lui parler « codé ». Tout ce qui sera codé ne pourra être décodé qu'avec la Clef Privée (donnée à personne).
3. Monsieur envoie les données cryptée illisible (même pour lui d'ailleurs)
4. Les pirates (ou Madame) ne pourront pas comprendre la communication. Par contre, les pirates peuvent parler à Mademoiselle (ou cas où ils auraient récupéré la Clef de l'étape 2).
5. Grâce à la Clef Privée, Mademoiselle comprend la communication.



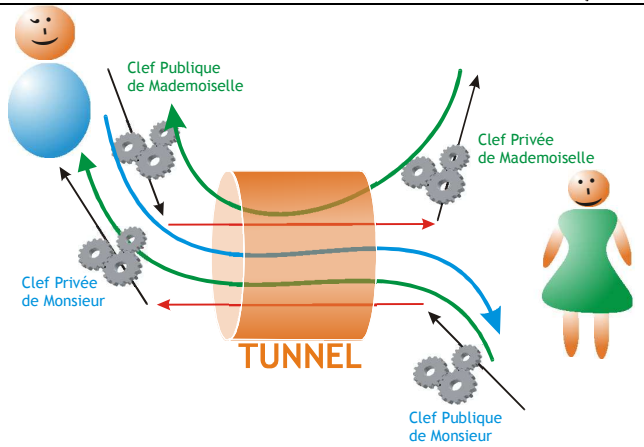
La connexion se fait dans les 2 sens.

1. Mademoiselle crée le couple de Clef pour que Monsieur code et qu'elle puisse décoder.

2. Toutes les communications de Monsieur sont codées. Il en profite d'ailleurs pour donner sa clef Publique à lui afin de Mademoiselle puisse, à son tour, lui parler en codé.

3. Les communications de Mademoiselle sont, elle aussi, codées.

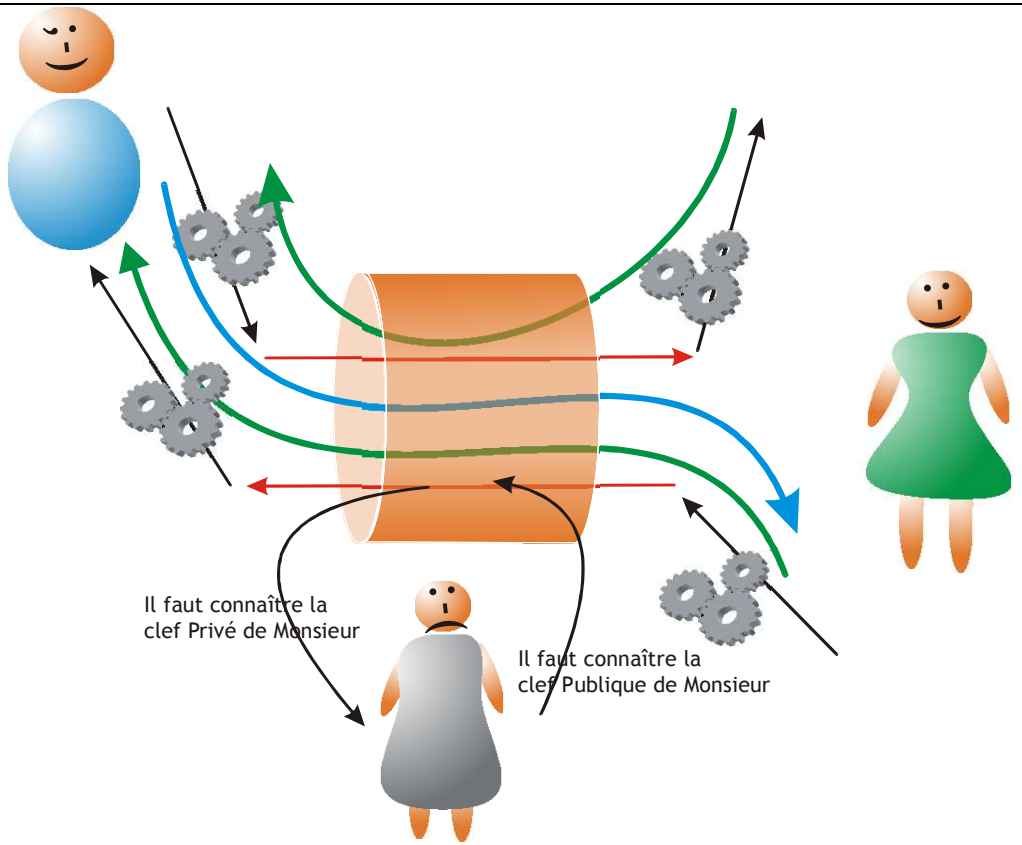
La communication est codée dans les 2 sens avec les clefs qui permettent de coder mais pas celle qui permettent le décodage.



Cette procédure de codage découpé s'appelle un TUNNEL crypté à encodage asymétrique.

Cette méthode permet de crypter les communication mais ne garantit pas l'authentification des 2 communicants.

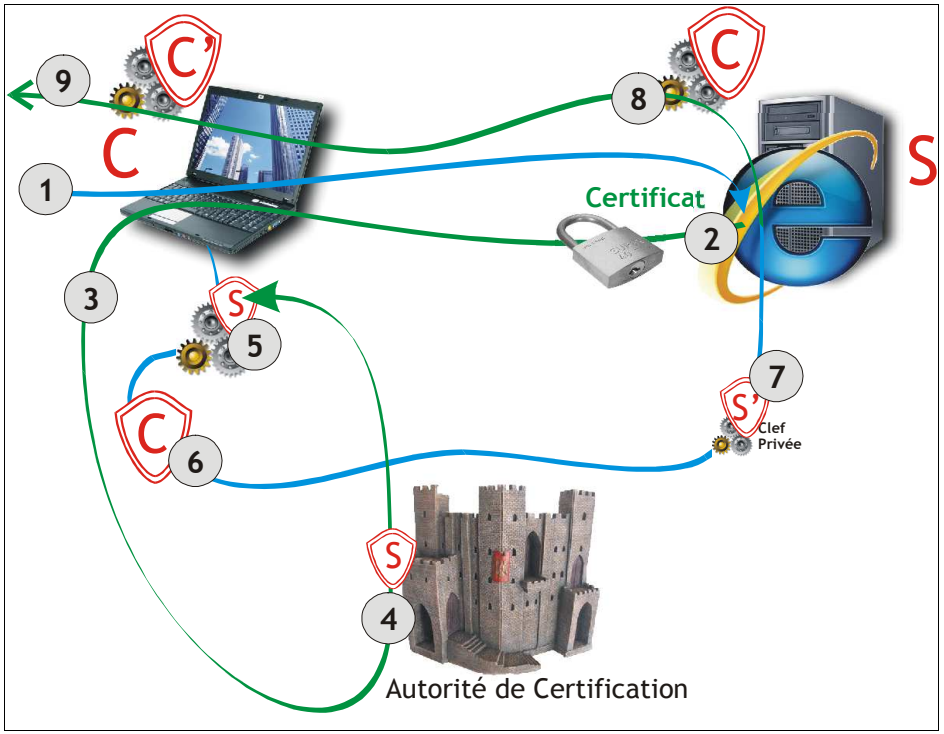
Il est donc possible de communiquer avec ce niveau de cryptage avec Madame au lieu de Mademoiselle !
Si les premiers échanges sont trompés (usurpés), la communication sera cryptée avec le pirate !



Pour qu'un pirate récupère une donnée, il lui faudra un certificat. Pour qu'il puisse parler dans la conversation, il lui faudra un second certificat.

Mais, dans tous les cas, il lui faut la clef privée pour comprendre ce qui se dit.

Or, dans le VPN, nous verrons que le mécanisme est encore plus complexe.



1. demande d'accès au site sécurisé
2. le site envoie son Certificat
3. le client se connecte à l'autorité de certification
4. dans le certificat transmis se trouve la clef Publique (appelée clef privée)
5. dorénavant, le client se servira de la clef pour crypter ses envois au serveur
6. le client se sert de la clef pour envoyer sa clef publique au serveur
7. le serveur décrypte par sa clef privée les données provenant du client
8. le serveur crypte avec la clef publique du client les données en SSL
9. le client décrypte avec sa client privée les données du serveur

Le Certificat :

Le principe est donc de commencer la communication sécurisée en transmettant le certificat (au lieu de la clef Publique).

Ce certificat possède plusieurs informations dont la clef Publique du communicant.

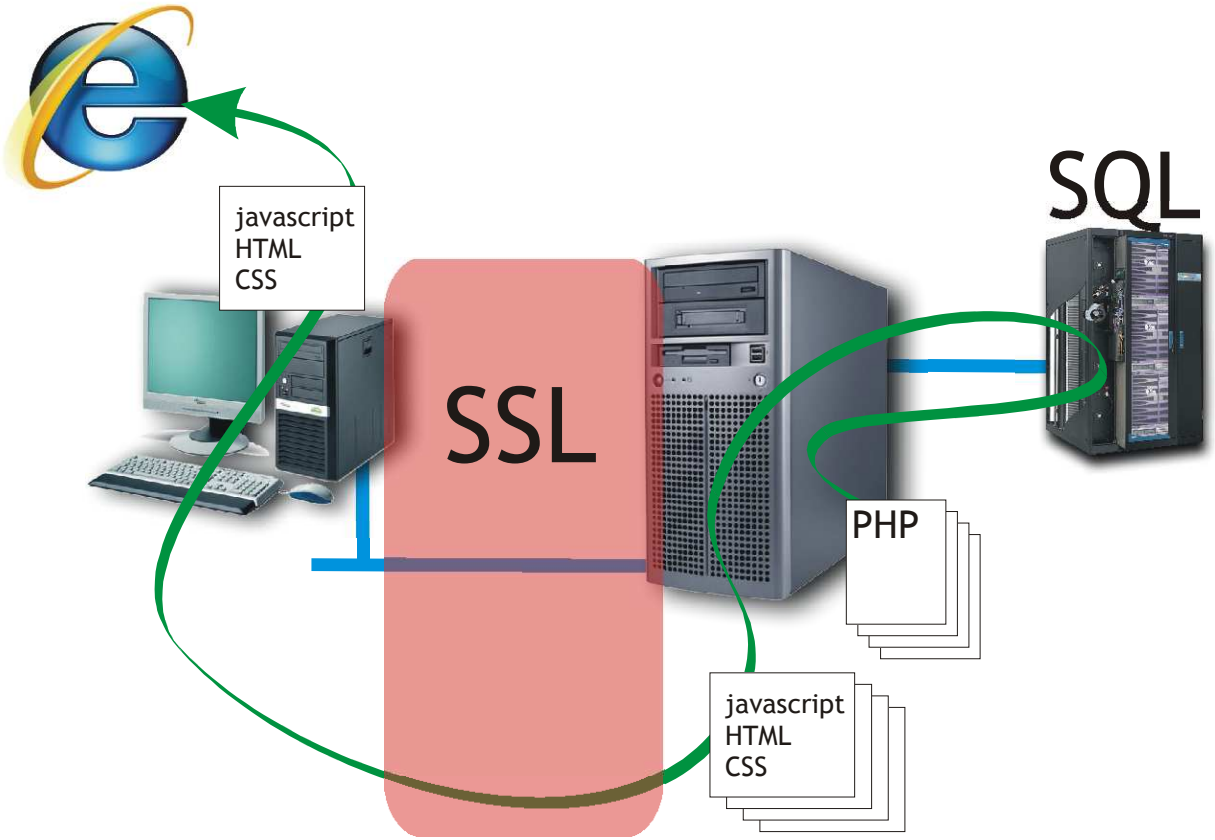
Il ne possède pas la clef privée !

Même si le pirate récupère la clef du certificat, cela ne lui sera d'aucun secours puisqu'il faut la clef privée pour comprendre la communication.

Attention, dans le certificat, nous trouvons une « clef privée » : il s'agit d'une « clef personnelle » (la clef publique) – il s'agit d'une erreur de traduction qui provoque souvent des incompréhension dans le fonctionnement du SSL.

Ici, nous ajoutons encore une difficulté au pirate : avoir le certificat + les clefs privées !

Le tunnel SSL d'un Site internet



La connexion se fait par canal (Tunnel) SSL.
Les applications sont identiques, mais le transport est sécurisé.