FACULTE DES SCIENCES

CLEFS PUBLIQUES ET CLEFS PRIVEES

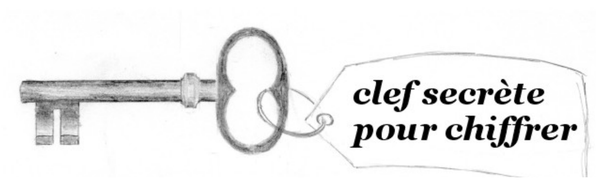
Deux sortes de systèmes de cryptage

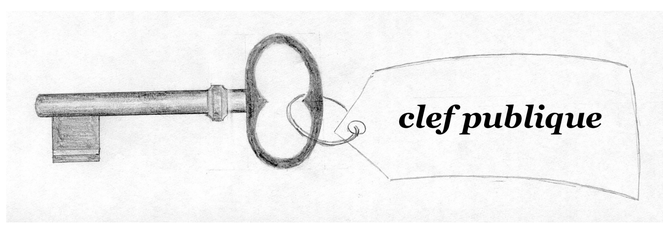
Symétrique

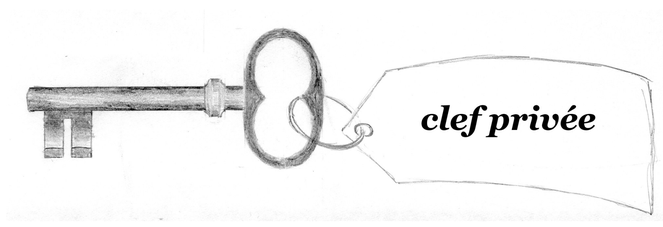
Même clef pour chiffrer et déchiffrer le message.
Utilisé jusqu'à nos jours.
Problème : Transmission de la clef de façon sûre.

Asymétrique

Une clef pour chiffrer et une autre pour déchiffrer.
Inventé en 1977 par Diffie et Hellman.
Avantage : La clef pour déchiffrer ne doit pas être envoyée.

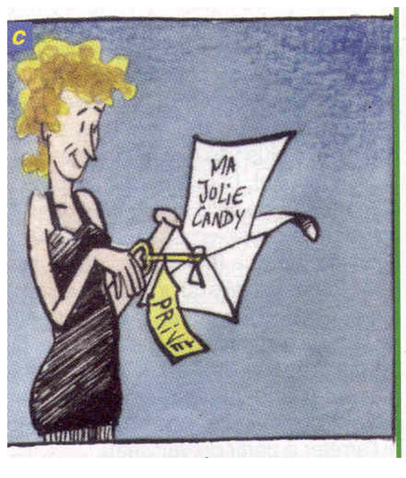






Regardons de plus près le système asymétrique...

Deux sortes de clefs



Clef publique

La clef est connue par toute personne qui veut envoyer un message chiffré.

Clef privée

La clef est connue uniquement par le destinataire, qui peut ainsi déchiffrer le message reçu.

Cryptage simultané

Problème: RSA trop lent.
Solution : On crypte le message avec un système symétrique (DES, AES) et uniquement la clef avec un système asymétrique (RSA).