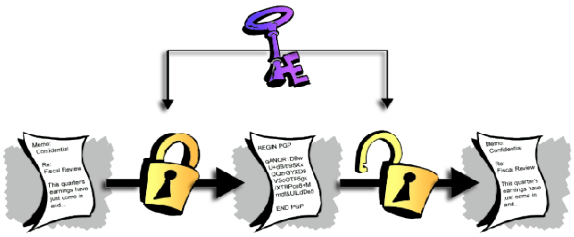
printemps des sciences
Science et ville 14-20 mars 2005

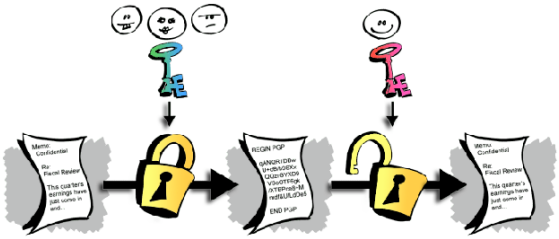
La carte d'identité électronique

DÉPARTEMENT D'INFORMATIQUE
Rémy Drijkoningen – Maurice Schubert – Paty Ilunga



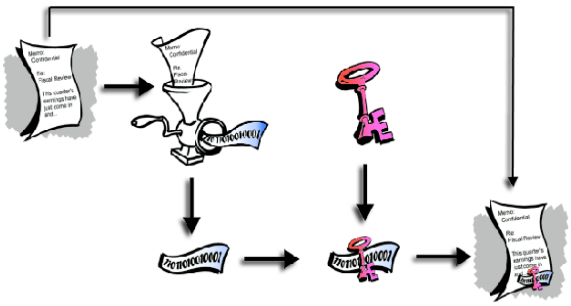
Chiffrement symétrique

Un système de chiffrement est dit symétrique s'il utilise la même clé pour chiffrer et déchiffrer.



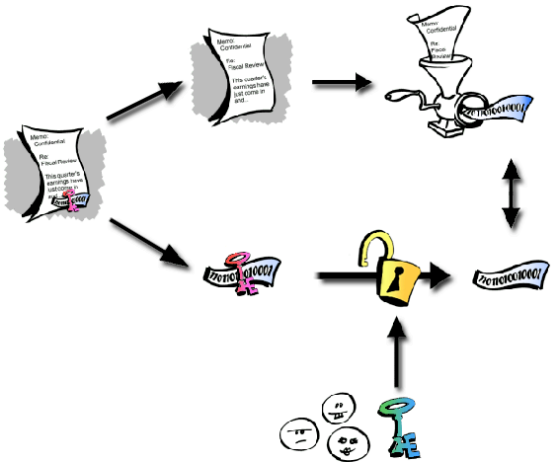
Chiffrement asymétrique

Un système de chiffrement est dit asymétrique s'il utilise deux clés complémentaires pour chiffrer et déchiffrer. L'une des deux est généralement tenue secrète, l'autre pouvant être distribuée. Tout document chiffré avec l'une n'est déchiffrable qu'avec l'autre, et réciproquement.



Signature digitale

- Analogue à la signature papier.
- Dépend du signataire et du document; elle n'est donc pas transférable d'un document à un autre.
- Une empreinte du message est chiffrée à l'aide de la clé privée et forme alors la signature unique du message pour ce signataire.



Vérification d'une signature digitale

Lorsqu'une personne reçoit le document signé, elle vérifie que la signature une fois déchiffrée (à l'aide de la clé publique), correspond bien à l'empreinte du message reçu.

FACULTE DES SCIENCES
UNIVERSITE LIBRE DE BRUXELLES