1er café 22 oct. 2009

- Pas de parole d'expert, retour d'expérience & échange entre membres d'un réseau
- ARAMIS : GO volontaires ; un serveur avec wiki ; sympa membres@aramis.resinfo.org
- Vous membres de l'Agrégation (Association?) Rhône-Alpes des Metiers de l'Informatique dans le Supérieur

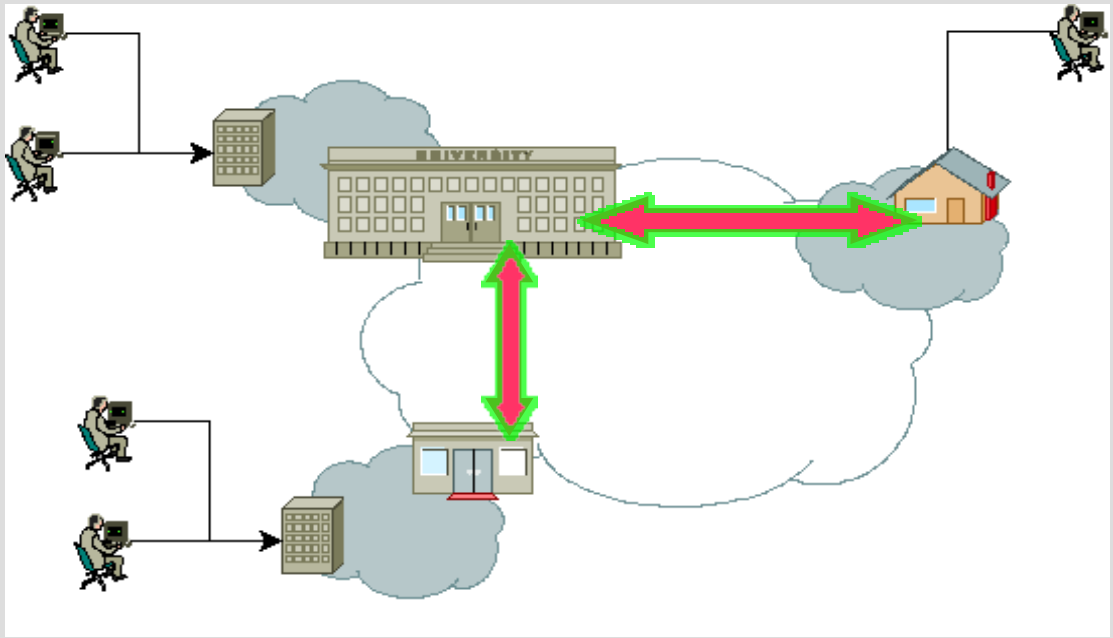
VPN

Principes des VPN

Rappels sur les outils existants

Exemple de VPN, SSH a l'ISC

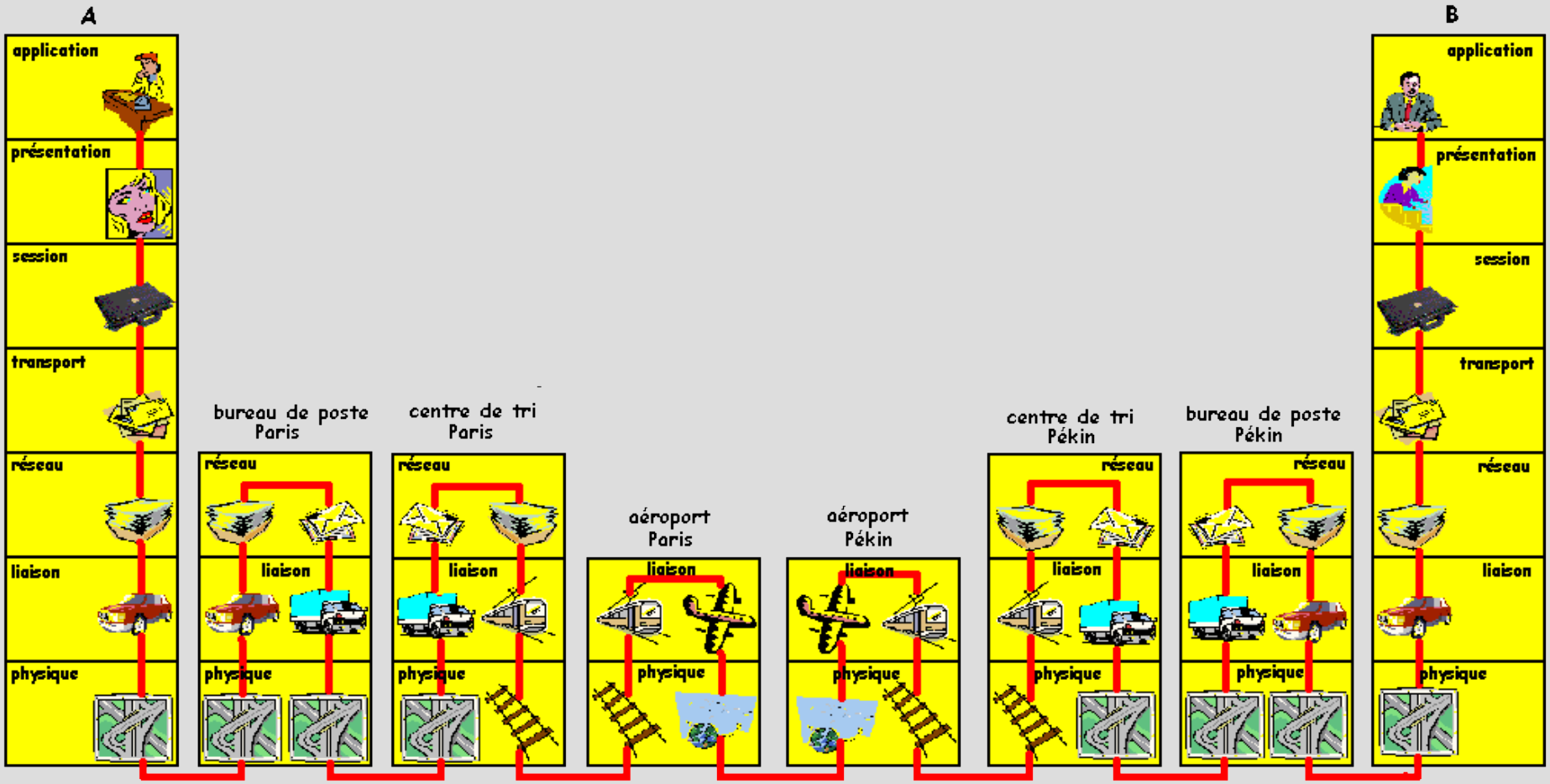
Cas d'utilisation des VPN



Protection d'un lien

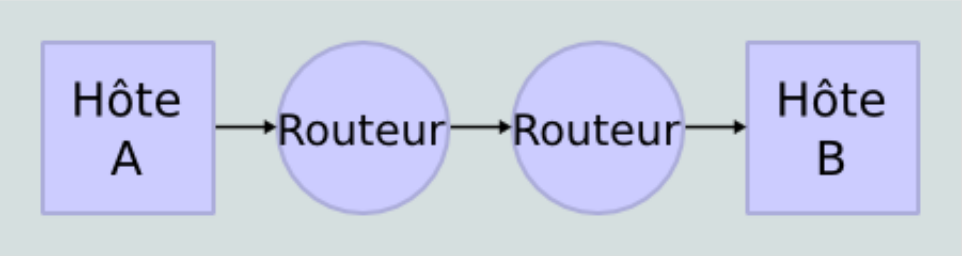
- Site - Site
- Site - Usagers

Réseaux : Modèle en couche OSI

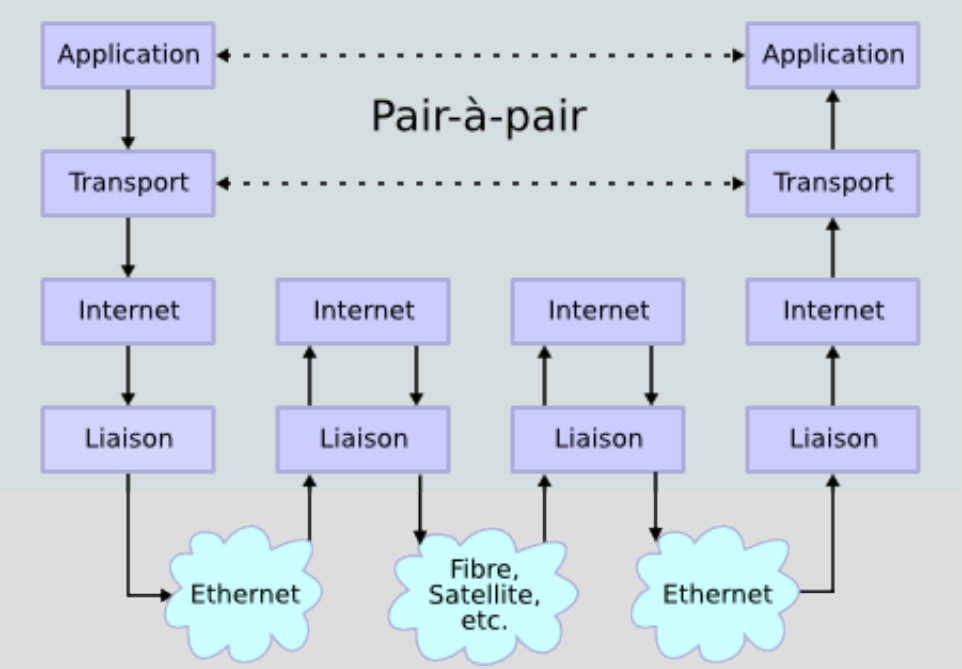


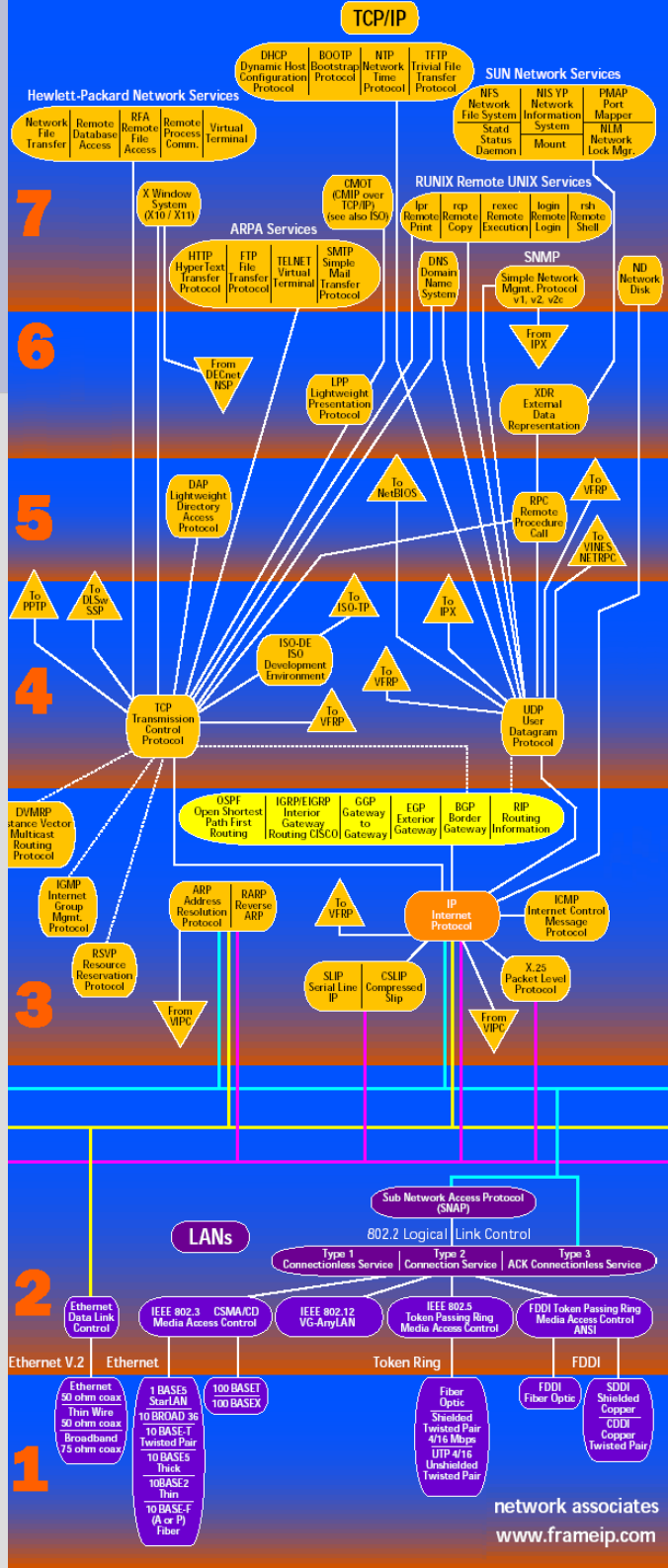
Couches TCP-IP

Connection réseau

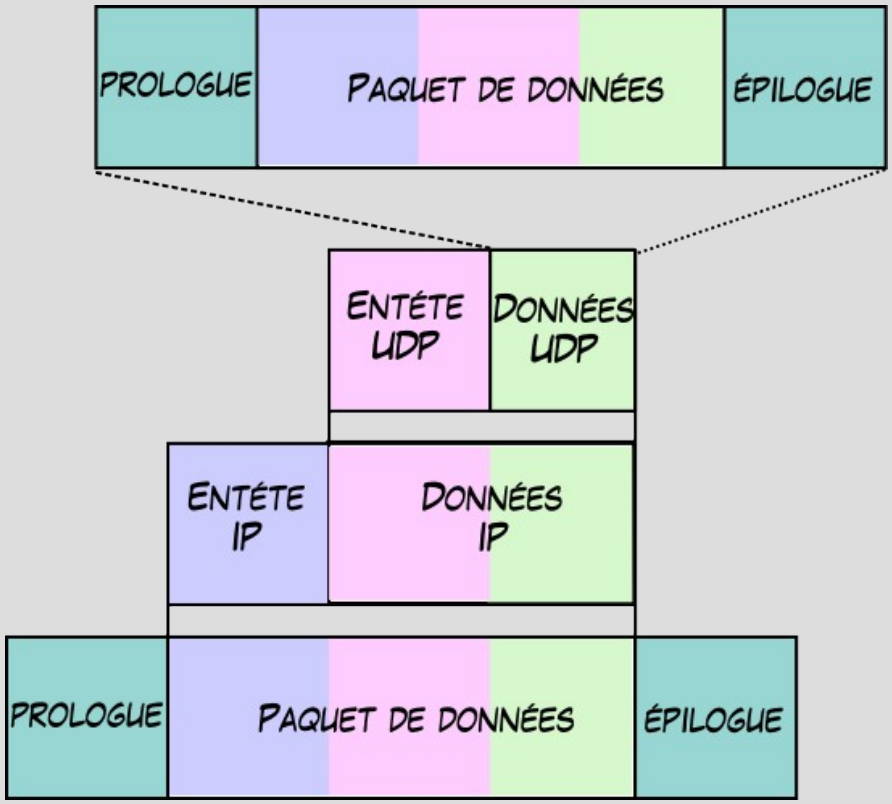


Piles de connections





Encapsulation



Par exemple
PPTP dans UDP

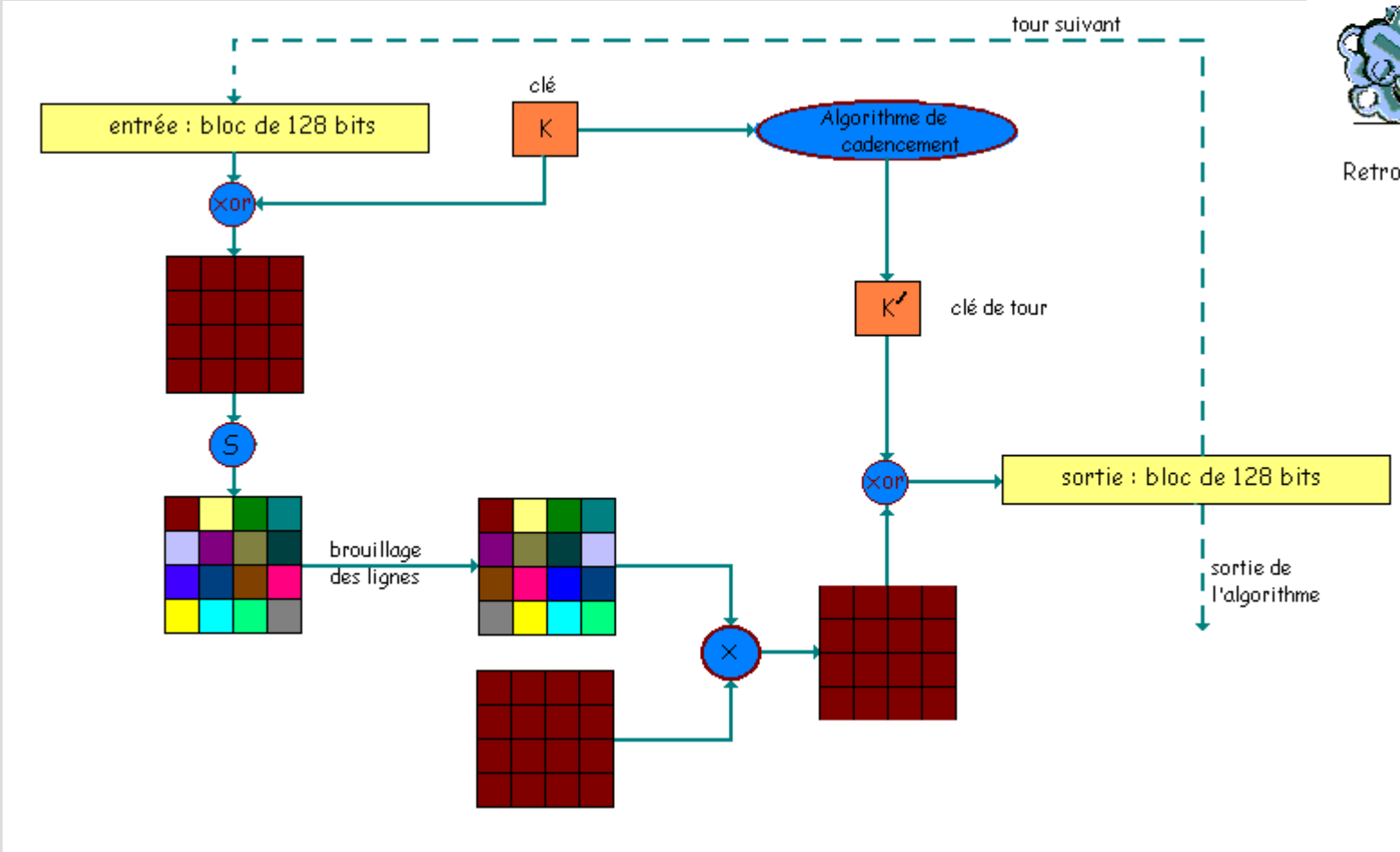
Interface virtuelle (TUN, L2TP, etc...)

Capsulons :
TCP dans ICMP, IP dans DNS... Etc.

Chiffrer l'encapsulé ?

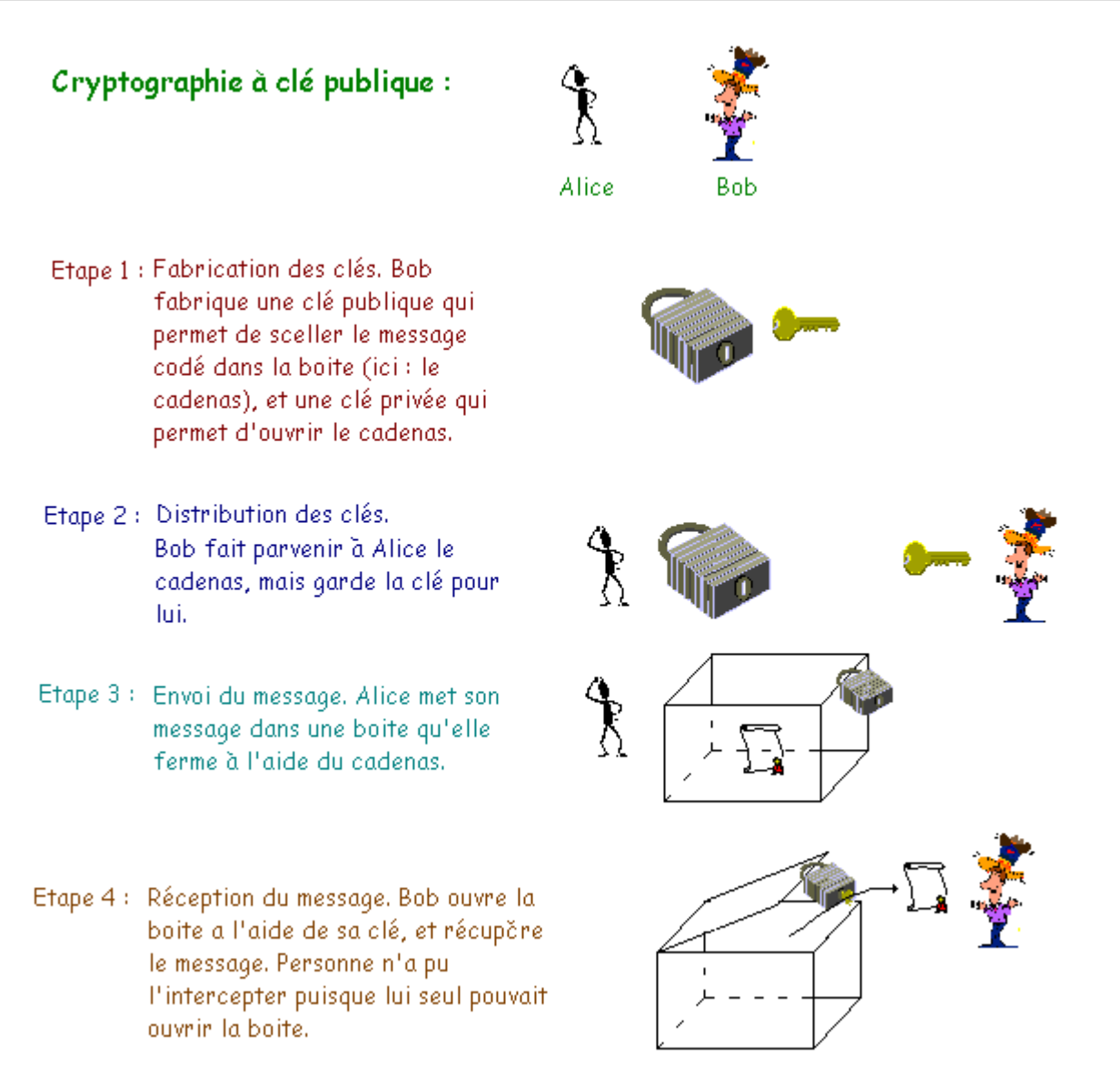
Cryptographie symétrique

Opérations rapides : substitution & transposition
Une clée à partager
Ex: DES, Blowfish, AES ...



Retrouvez la bonne clé parmi 2^{128}!

Cryptographie asymétrique



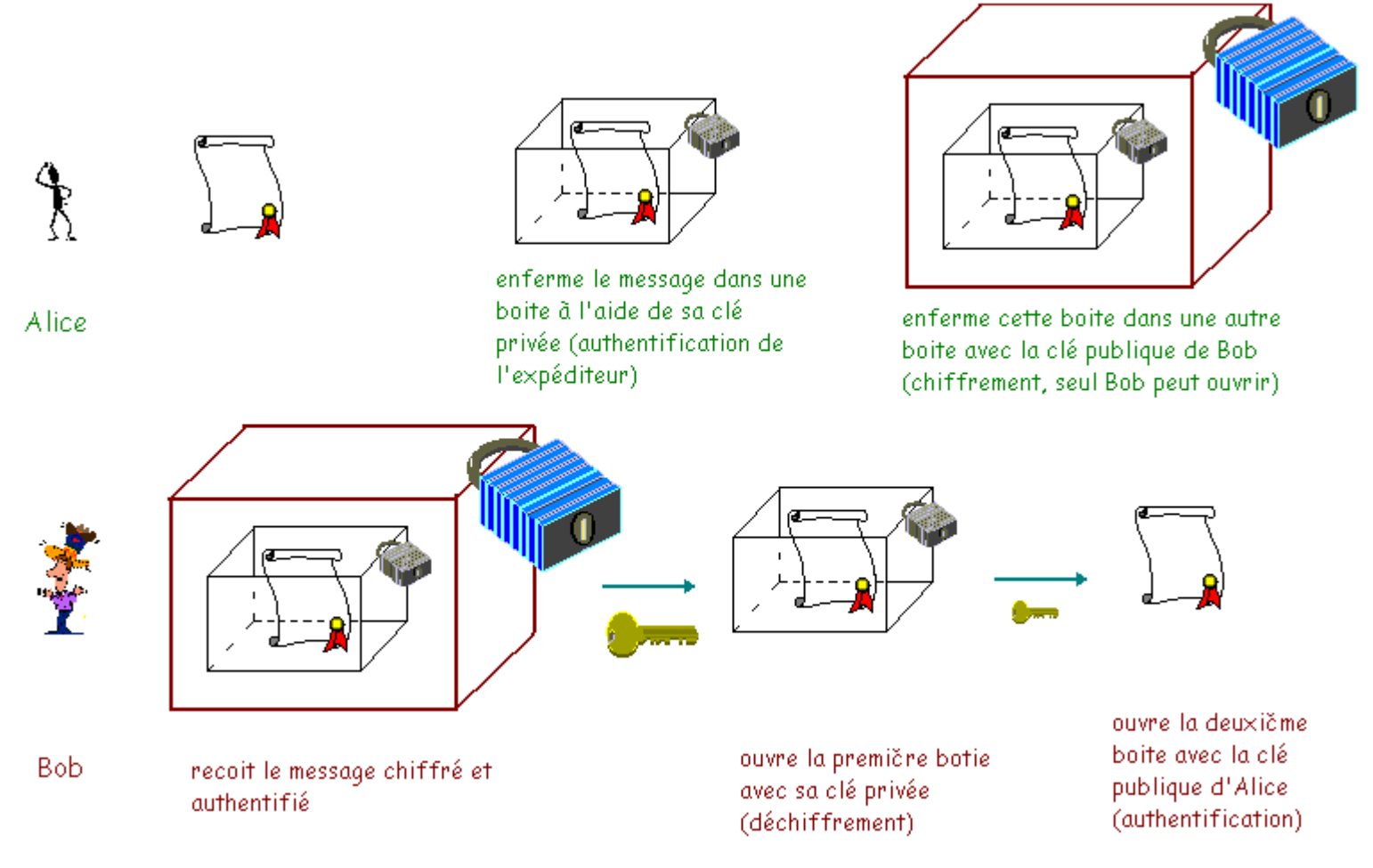
Opérations lentes

- tests de primalité
- génération nombre premier

Exemple :

- Rivest Shamir Adleman,
- Digital Signature Algorithm (ElGamal)

Signature électronique



Certificats

- Conteneurs de clefs pour la cryptographie asymétrique
- Infrastructure de gestion associée => Prix ?

Outils Open Source VPN

- Au niveau de l'OS : GRE, IPSec
- L'ancêtre : vtun
- Le moderne : OpenVPN
- Jouons aux légos stunnel + ppp
- Un couteau suisse OpenSSL