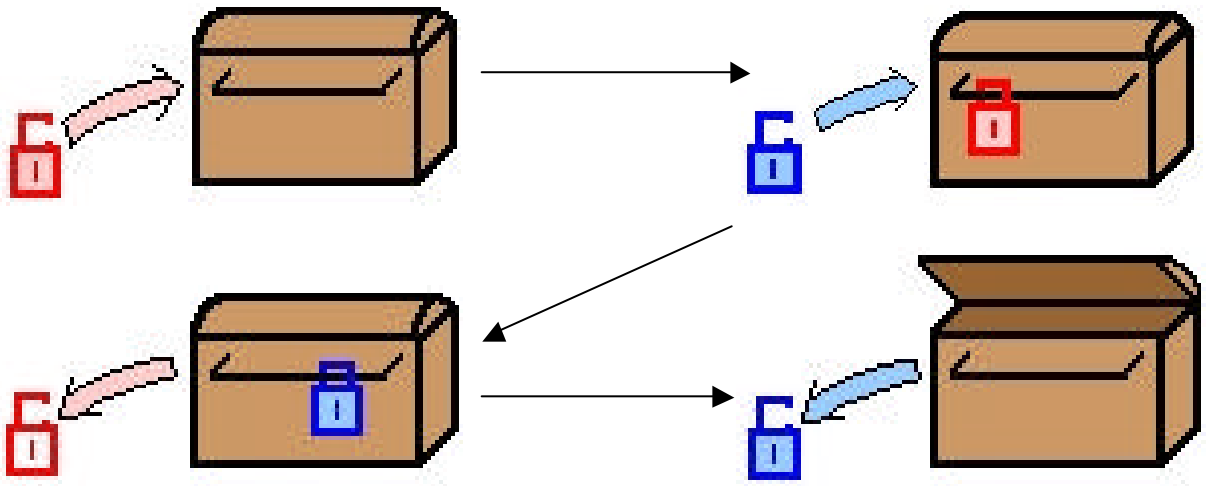
Double Cadenas:

L'idée est d'imaginer un système n'utilisant ***pas de clefs privées communes*** qu'il faille se communiquer auparavant. Chacun utilisera son algorithme, sa clef…

A/ Théorie:

Le système est très simple. Alice et Bob vont choisir chacun un algorithme, que l'on symbolisera par un cadenas : Alice mettra son message dans un coffre, fermé par son cadenas, et elle enverra le tout à Bob qui y mettra le sien. Puis celui ci renverra le coffre doublement cadenassé à Alice qui retirera son cadenas et renverra une dernière fois le coffre à Bob qui n'aura plus qu'à enlever le sien, ouvrir le coffre et lire le message.

Alice : **Bob :**



B/ Difficulté:

Vu ainsi, le système à l'air assez simple et très facile d'utilisation, mais, d'un point de vu plus mathématique, on se heurte à une difficulté qui est la commutation des 2 algorithmes. En effet, en nommant f, la fonction utilisée par Alice, et g, celle de Bob, l'échange complet du message aura consisté à lui appliquer la fonction $g^{-1} \circ f^{-1} \circ g \circ f$ mais rien ne nous dit que l'on obtiendra finalement le message initial, c'est à dire que cette application est l'identitée ! Il faut pour cela que les fonctions f et g commutent.

Or on a supposé qu'Alice et Bob n'ont pas communiqué entre eux auparavant. Il faut donc créer un catalogue de fonctions qui commutent, dans lequel les 2 interlocuteurs pourront piocher. D'un autre coté, il faut que ce catalogue soit suffisamment vaste, c'est à dire qu'il contienne un nombre de fonctions suffisamment grand, pour qu'un éventuel pirate n'ait pas trop de facilités à casser le code, par une attaque exhaustive, par exemple.