

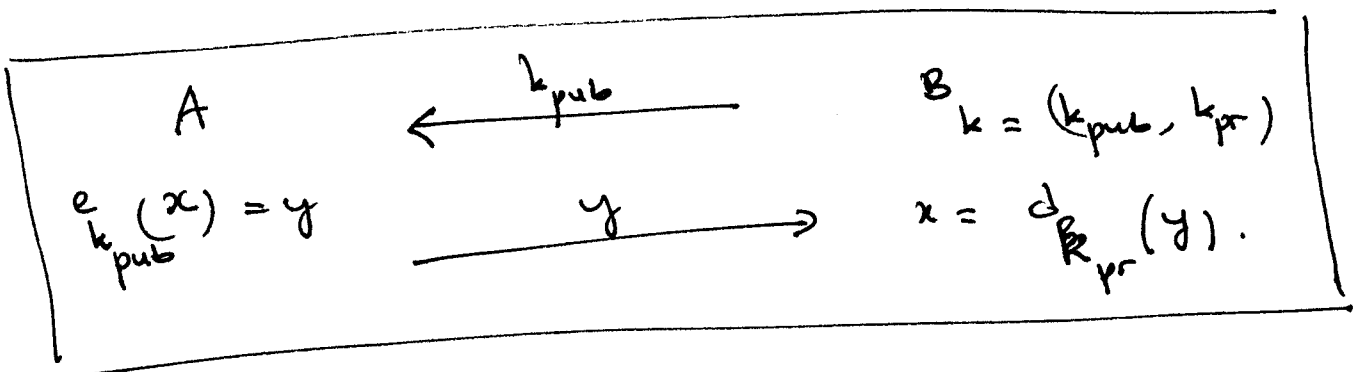
(3) Principe cryptographie à clé publique.

(3.2)

- Supposons que A veut envoyer un message chiffré à B;  
il n'est pas nécessaire que la clé de cryptage soit secrète,  
et il suffit que B possède une clé privée de decryptage.

$\Rightarrow$  B publiera une clé publique  $k_{pub}$  et garde une clé

$\Rightarrow$  la clé de B est  $k = (k_{pub}, k_{pr})$ .



- Exemple de transport d'une clé de chiffrement symétrique par l'utilisation d'un cryptosystème à clé publique.

