(3) Principe Cryptographie à clé publique.

- 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 privé de decryptage.

⇒ B publiera une clé publique k_{pub} et gardera une clé privé k_{pr}

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

A		B
	$\xleftarrow{k_{pub}}$	$k = (k_{pub}, k_{pr})$
$e_{k_{pub}}(x) = y$	$\xrightarrow{y}$	$x = d_{k_{pr}}(y)$.

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

A		B
	$\xleftarrow{k_{pub}}$	k_{pub}, k_{pr}
Choisir une clé k_{DES}.		
$y = e_{k_{pub}}(k_{DES})$	$\xrightarrow{y}$	$k_{DES} = d_{k_{pr}}(y)$
Crypter message x par DES:		
$z = DES_{k_{DES}}(x)$	$\xrightarrow{z}$	$x = DES^{-1}_{k_{DES}}(z)$.