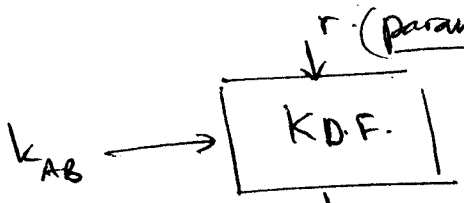
• Clés éphémères et dérivation de clés

• Dans certains applications (Internet, mobile phone), la durée d'une clé est limitée. Au lieu de recalculer la clé secrète chaque fois, on dérive des clés en utilisant une fonction KDF. (Key derivation function) :



KDF est one-way.

Une réalisation possible est le protocole avec r = nonce.

(numerical value used once) généré par l'une des parties participantes :

KDF avec Nonce.

A	B
	• générer r nonce.
	$\xleftarrow{r}$
• dériver clé : $k_{ses} = e_{k_{AB}}(r)$	• dériver clé $k_{ses} = e_{k_{AB}}(r)$.

$e_{k_{AB}}$ peut être DES, AES, ...

Rq • on peut aussi utiliser $k_{ses} = HMAC_{k_{AB}}(r)$ au lieu de r, soit encore la valeur d'un compteur :

$$k_{ses} = HMAC_{k_{AB}}(cpt).$$