- Le problème de n utilisateurs.

Ainsi le graphe de connexion est K_n. et deux participants qq. i et j partage une clé secrète k_{ij}. ($\Rightarrow \frac{n(n-1)}{2}$ clés).
D'où aussi pour utilisateur i de stocker $n-1$ clés.

§ 5.2. Etablissement de clés utilisant la cryptographie symétrique.

Même avec la crypto-symétrique, on peut réaliser le transport de clés (voir §1). à l'aide d'un centre de distribution (Ex: système embarqué; cell phone) de clés (KDC: Key Distri. Center).

- K.D.C. !

Chaque utilisateur U partage au début une clé k_U notée KEK (Key Encryption Key) pour communiquer secrètement entre U et KDC.
Supposons que A demande une communication secrète avec B:
Le KDC répond par $y_A = e_{k_A}(k_{sess})$; $y_B = e_{k_B}(k_{sess})$;
donc KDC crypte le k_U par les demandeurs: