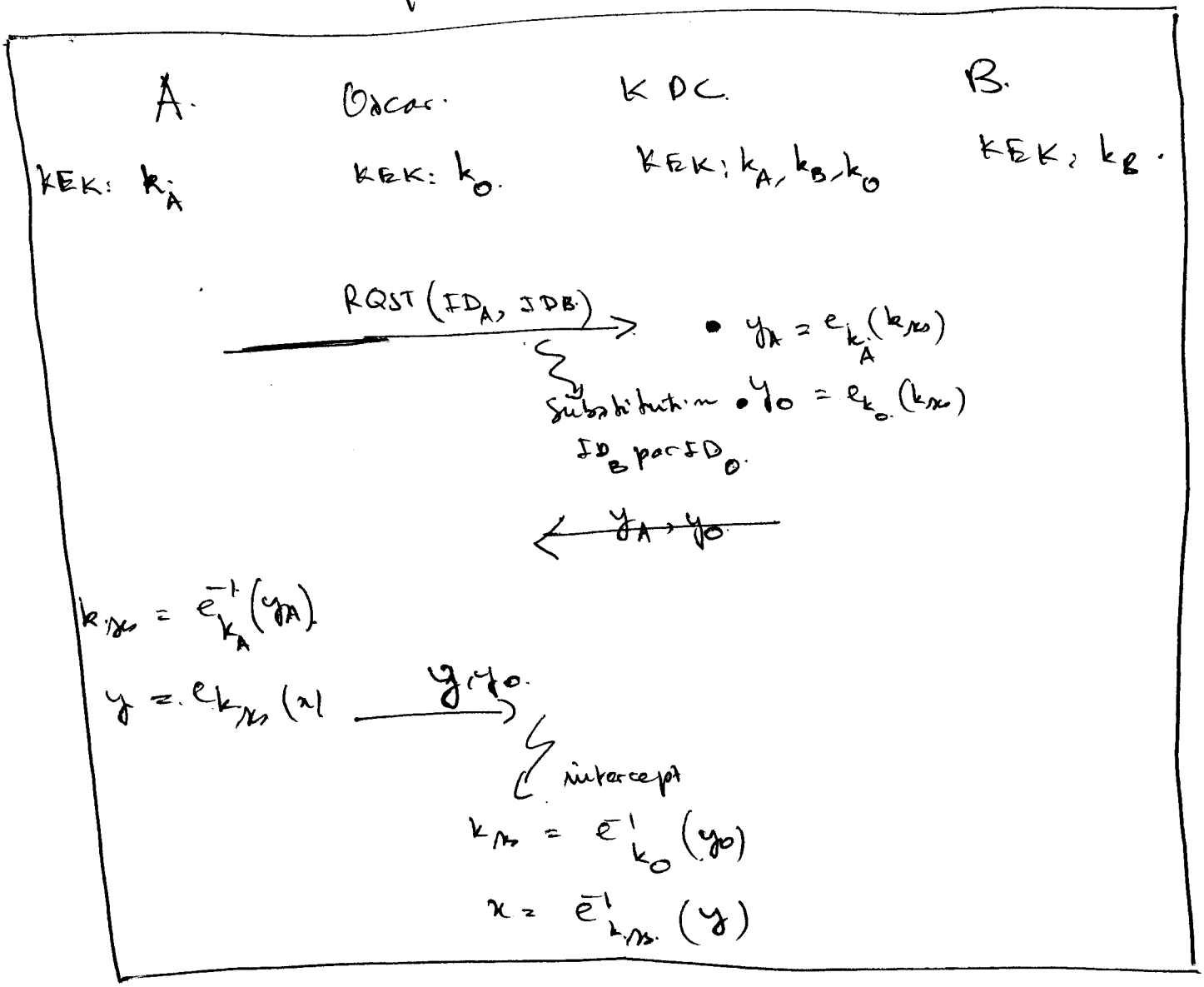
→ Remarque le Protocole KDC1 est fait pour empêcher une attaque par rejeu lorsque Oscar a accès à l'une de clés et au KDC. Entrée systématiquement k_{AB} à A et à B.

Une autre attaque de KDC1 est :



➡ Le système Kerberos permet de parer à ces attaques en confirmant la clé (voir page 340 de Paar et al), par utilisation de challenge — Réponse.