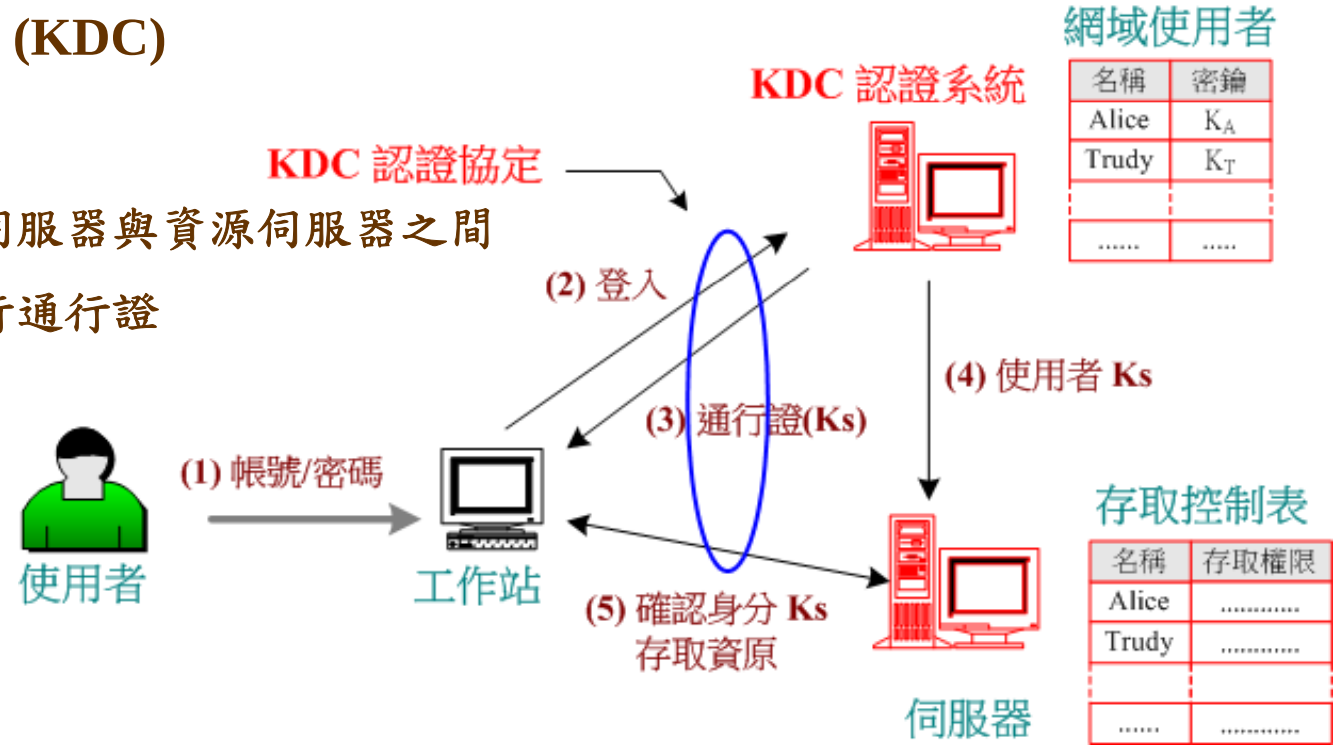
認證協定與系統簡介

- 認證系統
  - 集中式用戶認證 – 網域使用者
  - 分配通訊鑰匙 (KDC)
- 認證協定：
  - 工作站、認證伺服器與資源伺服器之間
  - 用戶認證、發行通行證
  - 通訊鑰匙認證



認證協定與系統簡介

KDC 認證協定 (KDC Authentication Protocol)

- 確認使用者身份
- 發給『通行票』：$E_{KB}[ID_A \| K_S]$
  - 伺服器的主密鑰 (E_{KB}) 加密
  - 會議鑰匙：K_S
- 認證協定：
  - 基本認證協定
  - Needham-Schroeder 認證協定
  - 公開鑰匙認證協定
- **Kerberos 認證系統：**
  - 秘密鑰匙系統
  - 公開鑰匙系統