公開鑰匙認證協定 – 簡介

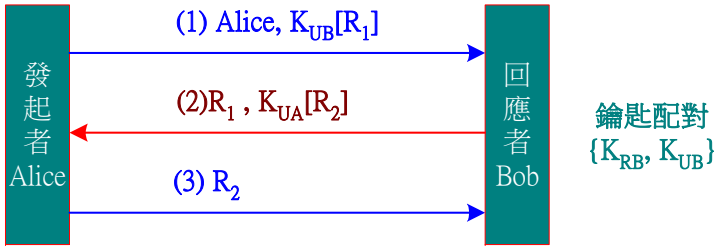
公開鑰匙認證協定的特性

用戶與系統皆必須擁有鑰匙配對(憑證)

- 開放性系統
- 系統安全要求較高的環境。
- 用戶與伺服器較複雜的環境。

鑰匙配對 $\{K_{RA}, K_{UA}\}$

單一伺服器



混合型密碼系統 (Hybrid Cryptosystem)

- 資料傳遞效率較高。

多用戶/多伺服器環境