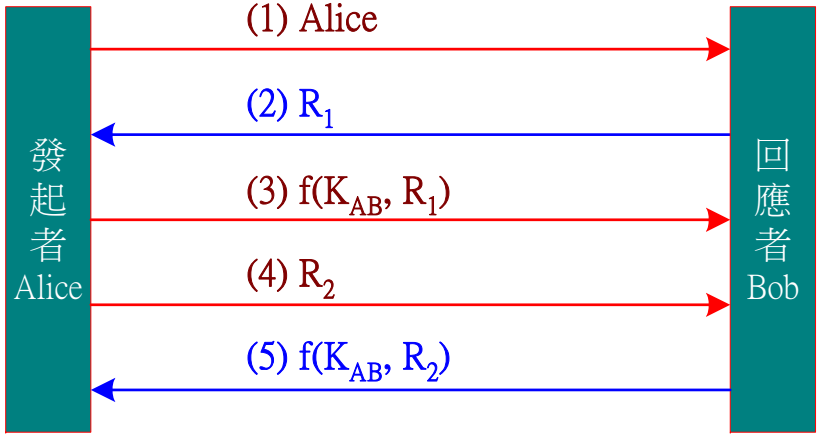
相互認證協定

- **相互認證(Mutual Authentication) 協定**
  - 通訊雙方互相確認對方的身份
  - 機制：
    - 相互共享密鑰認證
    - 相互公開鑰匙認證

相互共享密鑰認證 – 運作程序

- 相互共享密鑰認證
  - 雙方確任對方所持的共享密鑰是否相同。
  - 『盤問/回應』(Challenge/Response) 機制。
  - 基本運作程序：



  - 簡化運作程序：