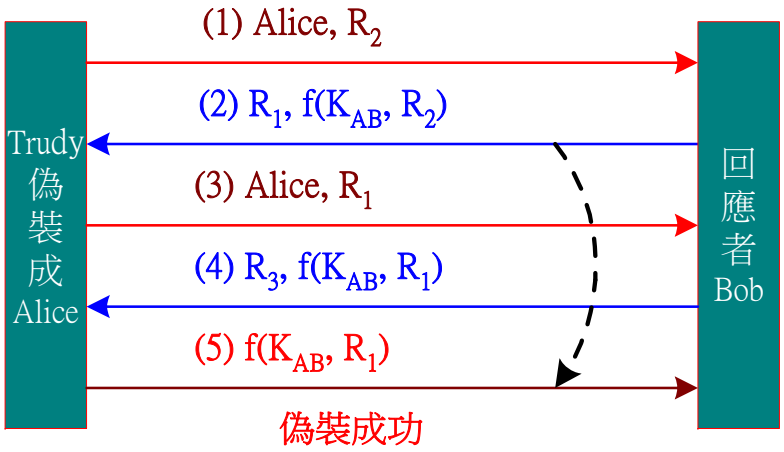
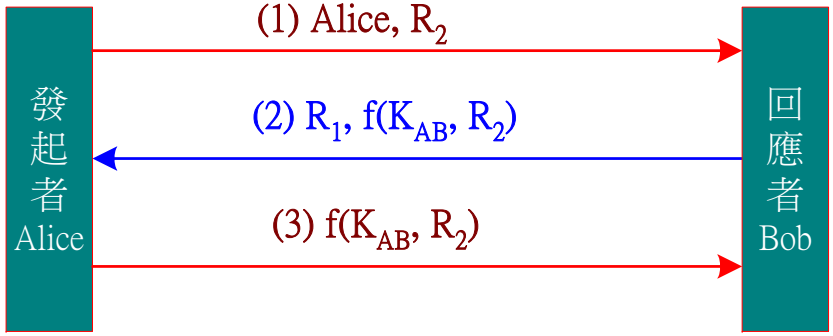
相互密鑰認證 – 破解技巧

- 破解技巧
  - 反射攻擊法：



  - 密碼猜測攻擊法：
    - 由訊號 (1) 的 R2 與訊號 (2) 的 f(KAB, R2)
    - 由訊號 (2) 的 R1 與訊號 (3) 的 f(KAB, R1)
    - 分解及猜測出密碼



相互密鑰認證－改良型

- 改良型的共享密鑰認證
  - 回應者確認(3) 無誤後，再回應 (4)。