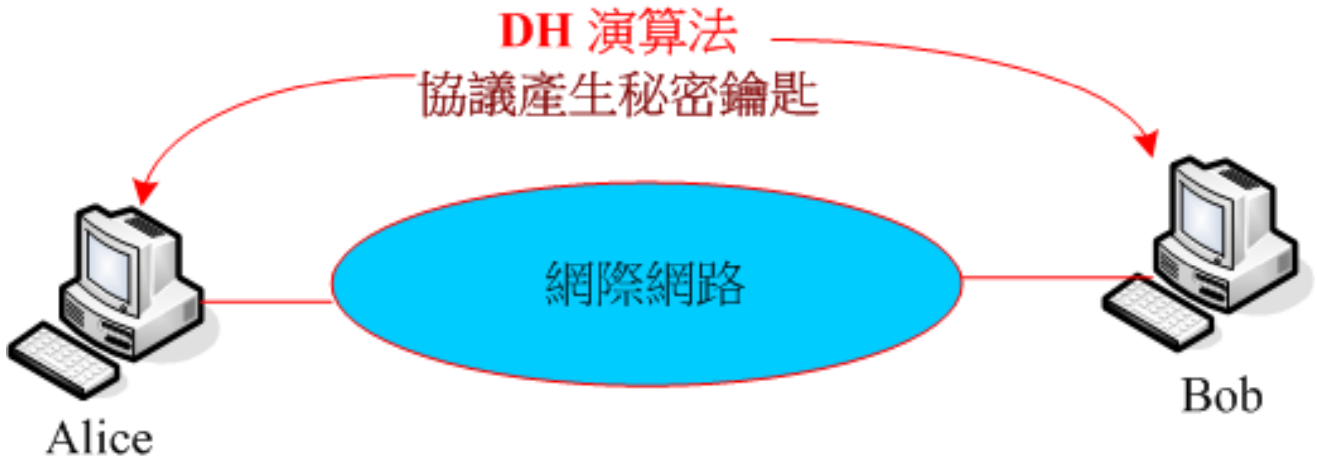
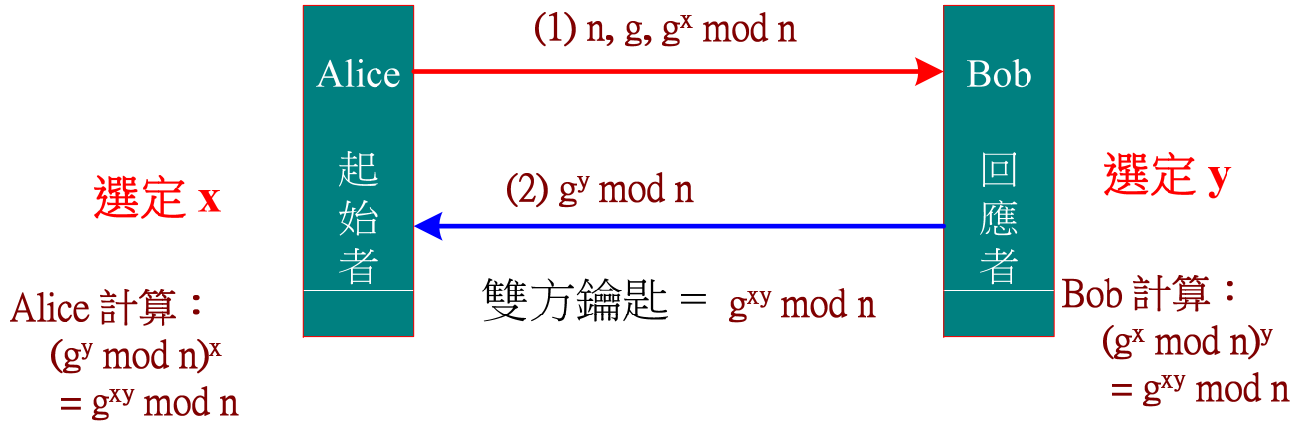
Diffie-Hellman 鑰匙交換

- **DH 演算法目的 – 產生秘密鑰匙**



Diffie-Hellman 鑰匙交換

- 鑰匙交換的運作程序
  - n 與 g 為公開值
  - 雙方各選一個較大的數值 x 與 y
  - 參數 g 與 n 可以由發起端(x) 或憑證內註明
  - 計算出『秘密鑰匙』：$g^{xy} \bmod n$



DH 演算法推論

- 驗證 Diffie-Hellman 演算法
  - Alice 選定：n = 47, g =3, x=8, 計算出：

    $g^x \bmod n = 3^8 \bmod 47 = 28 \bmod 47$

    訊息 (1) = {47, 3, 28}
  - Bob 選定：y =10 , 計算出：

    $g^y \bmod n = 3^{10} \bmod 47 = 17 \bmod 47$

    訊息 (2) = {17}
- Alice 計算會議鑰匙：

  $(g^x \bmod n)^y = g^{xy} \bmod n = 28^{10} \bmod 47 = 4 \bmod 47$
- Bob 計算會議鑰匙：

  $(g^y \bmod n)^x = g^{xy} \bmod n = 17^8 \bmod 47 = 4 \bmod 47$
- 會議鑰匙 k= 4