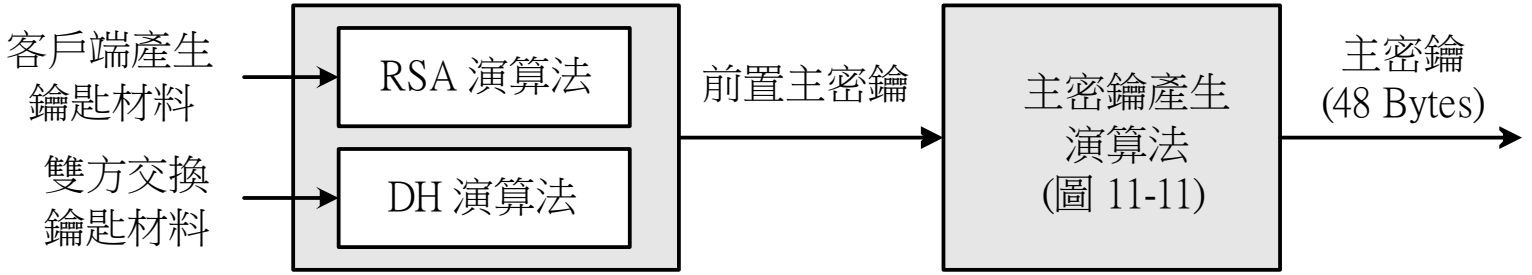
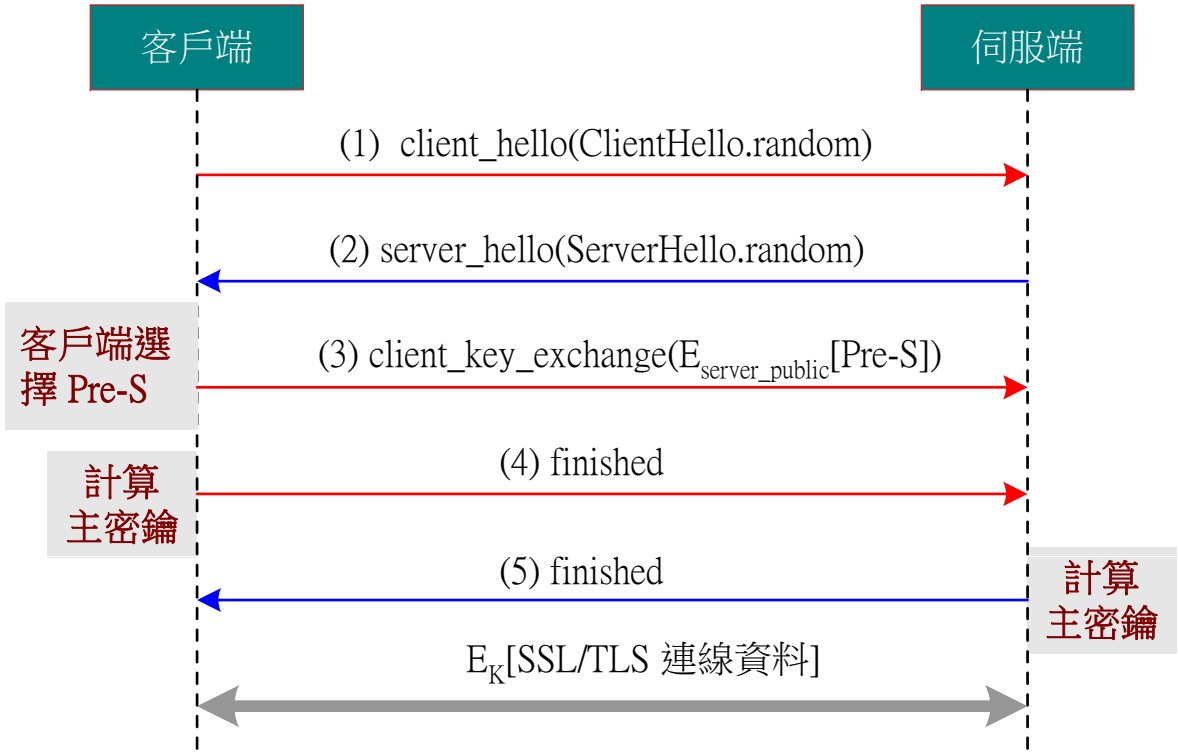
SSL 主密鑰產生

- **Pre-master Secret (48 Bytes) 產生方法：**
  - **RSA**：客戶端產生後，利用伺服端公鑰加密後，傳給伺服端，伺服端再用自己私鑰解密取得。
  - **DH**：雙方交換鑰匙材料製造出來。
- **48 Bytes 『主密鑰』(Master Secret)**
  - 產生各種鑰匙的基本元素。
- **主密鑰產生方法**



產生前置主密鑰 – RSA 演算法

- **RSA 演算法**
  - **客戶端產生 Pre-master Secret (48 bits)**
  - **前置主密鑰： K = f(Pre-S, CliebtHello.random, ServerHello.random)**



產生前置主密鑰 – DH 演算法

- **Diffie-Hellman 演算法**
  - **雙方交換鑰匙材料：**

    ServerDHParm = {dh_p, dh_g, dh_Ys} ≒ {n, g, g^x mod n}

    ClientDHParm = {dh-Yc} ≒ {g^y mod n}
  - **前置主密鑰：**

    Pre-master Secret = g^{xy} mod n
  - **MD5 訊息確認：**

    MD5_Hash = MD5(ClientHello.radom || ServerHello.radom || ServerParm)
  - **SHA 訊息確認：**

    SHA_Hash = SHA(ClientHello.radom || ServerHello.radom || ServerParm)

產生前置主密鑰 – DH 演算法

Diffie-Hellman 演算法 (2)