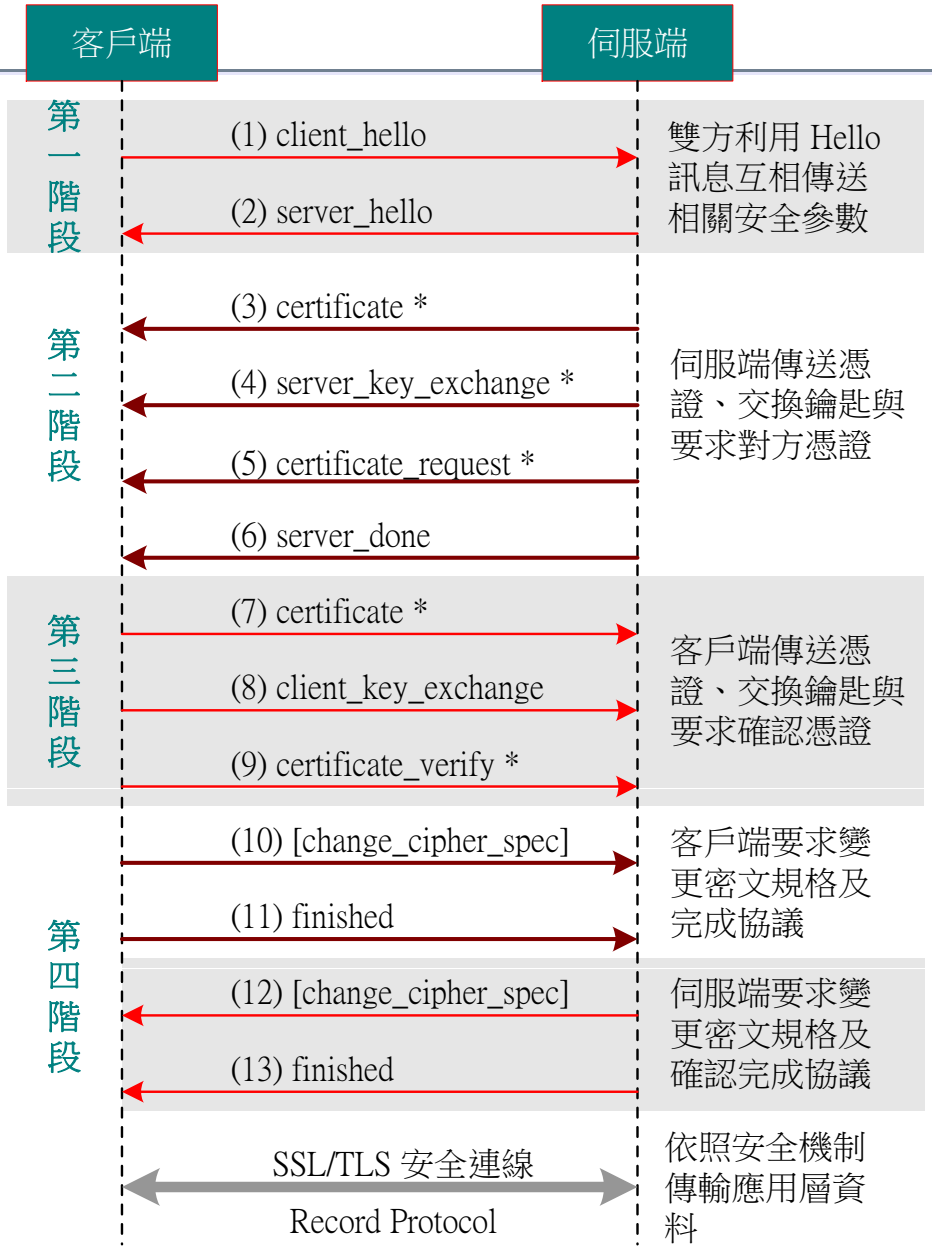
SSL 握手協定運作



備註：有星號 (*) 表示選項訊息

SSL 第一階段：協商安全套件

- 安全套件
  - RSA 密碼系統
  - 匿名的 Diffie-Hellman
  - 固定的 Diffie-Hellman
  - 暫時的 Diffie-Hellman
  - Fortezza
- 協商項目：
  - 加密演算法：RC4, RC2, DES, 3DES
  - MAC 演算法：MD5, SHA-1
  - 密文型態：Stream/Block Cipher
  - 可否出口：True or False
  - 雜湊碼大小：0, 16, 20 Bytes
  - 鑰匙材料：二進位亂數
  - IV Size：CBC Operating Only

SSL 第二、三階段協商

- SSL 第二階段：伺服器確認與鑰匙交換
- SSL 第三階段：客戶端確認與鑰匙交換
  - 鑰匙材料：
    - RSA：48 bits Pre-master Secret
    - 暫時或匿名 Diffie-Hellman：包裝於訊息。
    - 固定 Diffie-Hellman：包裝於憑證內。

SSL 第四階段協商：完成

- 第四階段：完成
  - 客戶端送出『變更密文規格』、伺服端回應『完成』
  - 產生安全參數如下：
    - Client writ MAC Secret
    - Server write MAC Secret
    - Client write key
    - Server write key
    - Client write IV
    - Server write IV