10-6-1 IKE 協定簡介(一)

- IKE (Internet Key Exchange) 協定簡介
- 協定功能
  - ISAKMP 僅提出協議架構，由 IKE 真正實現。
- 協定特性
  - 兩階段協商：(請參考 SSL 協議) - 資訊與網路安全技術
    - 第一階段：認證身分、協商安全套件、建立安全連線(產生通訊鑰匙)。
    - 第二階段：交換鑰匙材料，計算會議鑰匙。
  - 協商項目：
    - 加密演算法（Encryption Algorithm），如 DES。
    - 雜湊演算法（Hash Algorithm），如 MD5 或 SHA。
    - 認證方法（Authentication Method），如 HMAC。
    - Diffie-Hellman 演算法所需的訊息群組，如 MOPD。

10-6-1 IKE 協定簡介 (二)

- 協定特性
  - 認證或加密金鑰產生：(請參考 SSL 協議) - 資訊與網路安全技術
    - 預先共享金鑰（Pre-Shared Key）：雙方通訊之前利用其他管道，將秘密金鑰分配給雙方；一般大多採用 KDC 系統（如 Kerberos）系統來分配金鑰。
    - 會議金鑰（Session Key）：雙方利用 Diffie-Hellman 演算法，以互相交換鑰匙材料，所計算產生的金鑰。
    - 公開金鑰（Public key）：係利用憑證授權（CA）中心所發給的公鑰，互相認證彼此身份，並利用它傳遞『主密鑰』(Master Secret)。
  - 完全順向密鑰（ PFS ）
  - 虛擬亂數函數（PRF）