IPSec ESP 協定簡介

- 封裝安全承載協定 (Encapsulation Security Payload, ESP)
  - 將原封包重新包裝成一個新的封包
  - 提供隱密性、資料來源認證、非連接方式的完整性、以及反重播攻擊能力。
  - 具有傳輸模式與通道模式
  - 利用封包序號來防禦重播攻擊
  - **DES-CBC** 加密
  - **HMAC-MD5, HMAC-SHA-1** 認證
  - 通道模式才具有『有限度的流量機密性』的功能
  - 可配合 **AH** 協定使用