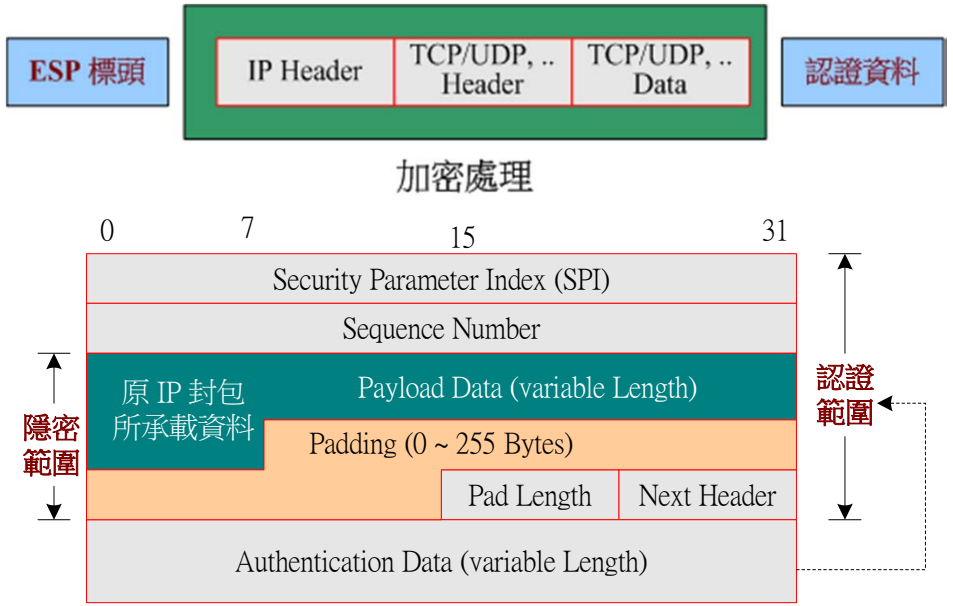
10-4-1 IPSec ESP 協定簡介 (一)

- 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
  - AES、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

10-4-1 IPSec ESP 協定簡介 (二)

- **ESP 封包封裝**
  - **ESP 標頭 (ESP Header)**
    - 安全參數索引 (SPI)
    - 序號 (Sequence Number)
  - **承載資料 (Payload Data)**
    - 含填補 (Padding)
    - 加密範圍
  - **ESP 標尾 (ESP Trailer)**
    - 填補長度 (Pad Length)
    - 下一個標頭 (Next Header)
    - 認證資料 (Authentication Data)



10-4-1 IPSec ESP 協定簡介 (三)

- ESP 加密及認證演算法
  - 依雙方 SA 協議而定
  - 密碼系統
    - 3DES、AES、、
  - 認證演算法
    - HMAC-MD5
    - HMAC-SHA-1