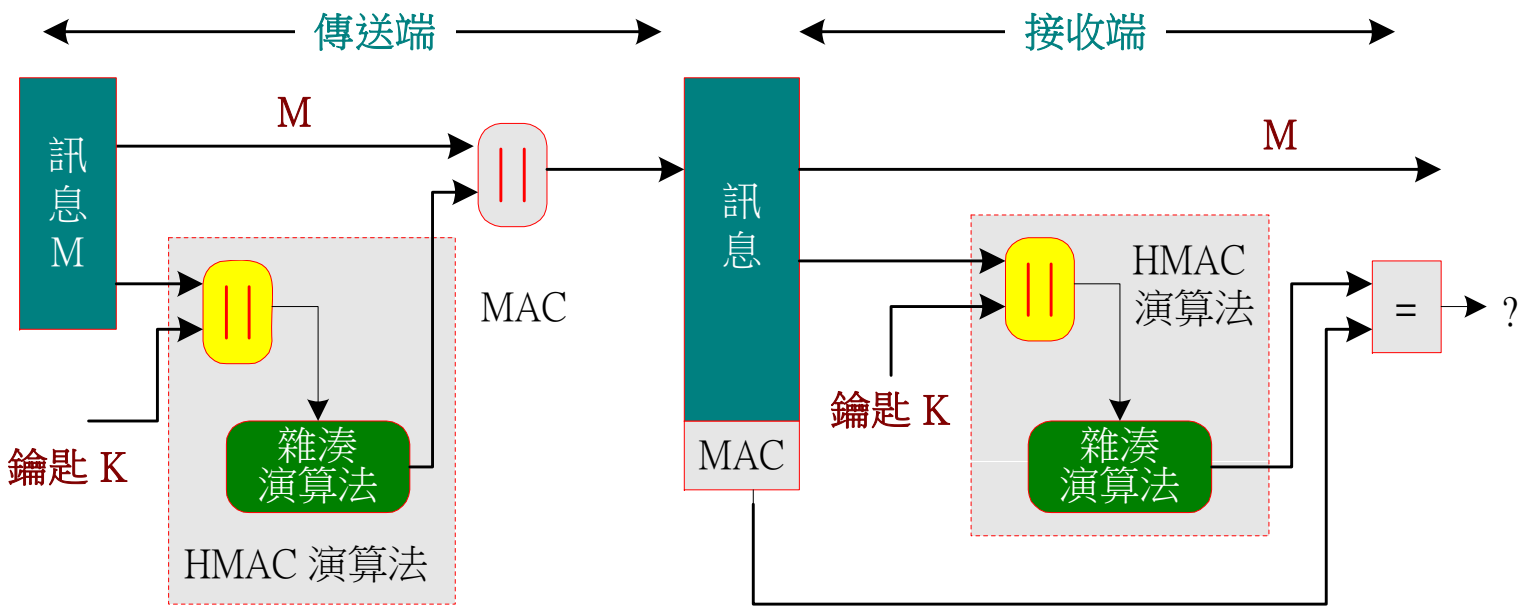
HMAC 演算法

- **Hash Message Authentication Code (HMAC)**
  - **RFC 2104 標準**
  - **可嵌入多種雜湊演算法：MD4、MD5 與 SHA-1**
  - **加入『秘密鑰匙』**

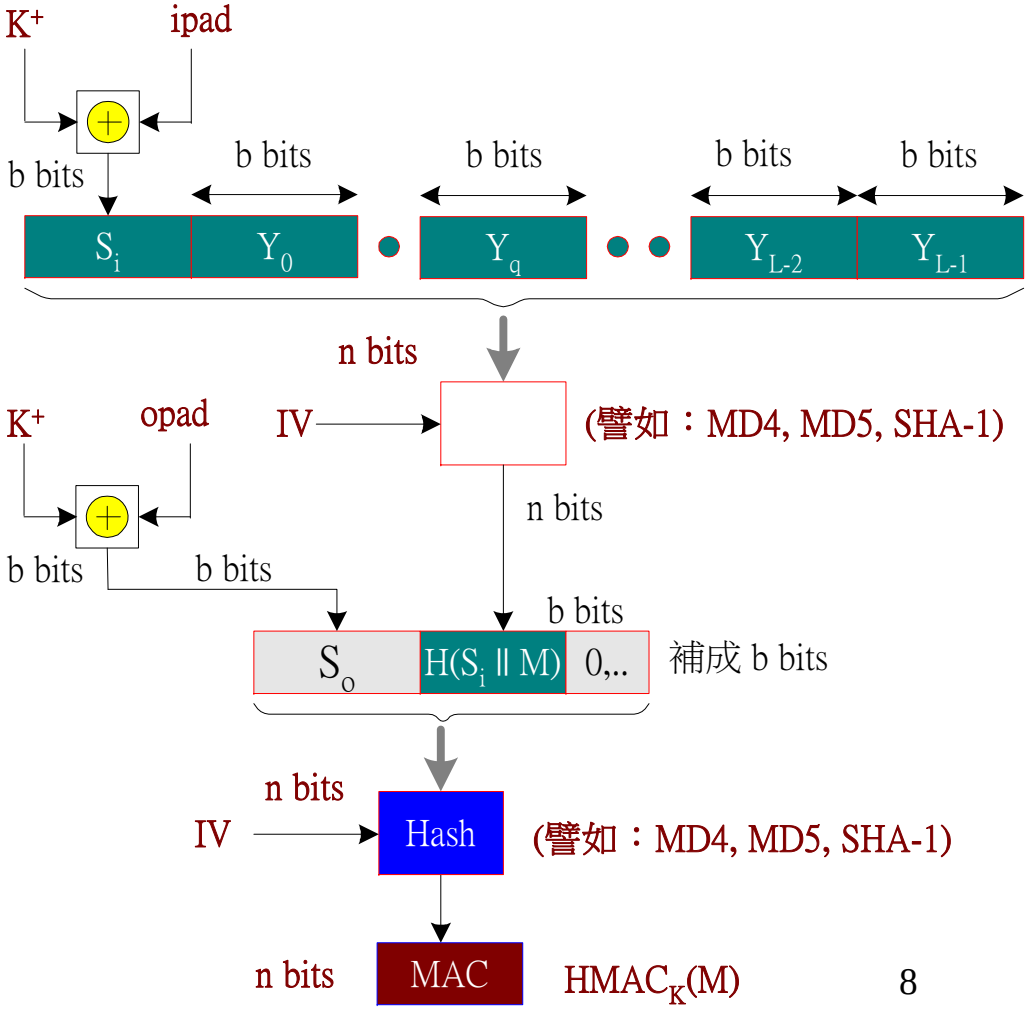


HMAC 設計概念

- 依照 RFC 2104 所述：
  - 能在不修改現有的雜湊演算法之下，將它嵌入 HMAC 演算法之內。
  - 當需要更快速的雜湊演算法時、或是新的雜湊演算法被發展出來的時候，我們希望能容易地更新內嵌的雜湊演算法。
  - 當雜湊演算法被嵌入 HMAC 演算法之內後，期望能維持它原來的執行速度，以免造成執行效能大幅滑落。
  - 可以簡單的使用鑰匙。
  - 希望所嵌入的雜湊演算法能滿足一些合理的條件，並且可以根據這些條件分析該 HMAC 的安全強度。

HMAC 架構

- $HMAC_K(M) = H[(K^+ \oplus opad) \| H[(K^+ \oplus ipad) \| M]]$
- 鑰匙 K 以 0 補滿 512 bits
- ipad：將 00110110 重複 b/8 次
- opad：將 01011100 重複 b/8 次



HMAC 的安全性

- 可能攻擊方法：
  - 暴力攻擊法：強力搜尋出所植入的秘密鑰匙。
  - 生日攻擊法：找出此雜湊函數的碰撞訊息。