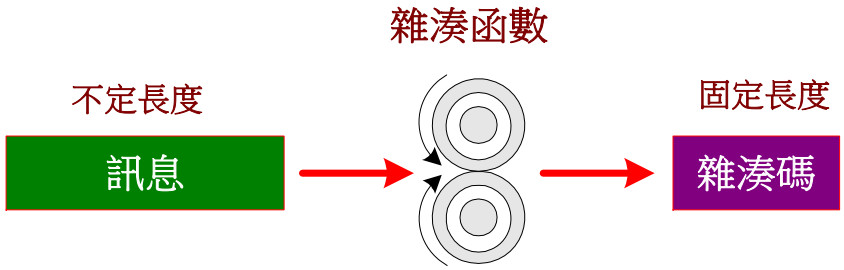
雜湊函數簡介

- 雜湊函數 (Hash Function)
- 數位指紋 (Digital Fingerprint)
  - 定義：
    - 明文：M
    - 雜湊函數：H
    - 雜湊值：h = H(M)



  - 雜湊函數必須具備之功能：
    1. 對任意長度的訊息輸入，產生固定長度的雜湊值輸出。
    2. 可 H(M)，並可經由硬體或軟體來實現。
    3. 『單向雜湊』（One-way Hash）之特性。
    4. 對於訊息 M_1，在計算上是無法找出另一個訊息 $M_2 \neq M_1$，使得 $H(M_1) = H(M_2)$。
    5. 若 $H(M_1) = H(M_2)$，則 $M_1 = M_2$，若 $H(M_1) \neq H(M_2)$，則 $M_1 \neq M_2$。
  - 『弱雜湊函數』(Weak Hash Function)：滿足 1~ 4 條件
  - 『強雜湊函數』(Strong Hash Function)：滿足 1 ~ 5 條件

簡單的雜湊函數

- **CRC (Cyclic Redundancy Code)**
- **Bitwise-XOR**
- **不符合弱雜湊函數 ：**
  - **可以找出 $M_2 \neq M_1$，使得 $H(M_1) = H(M_2)$。**