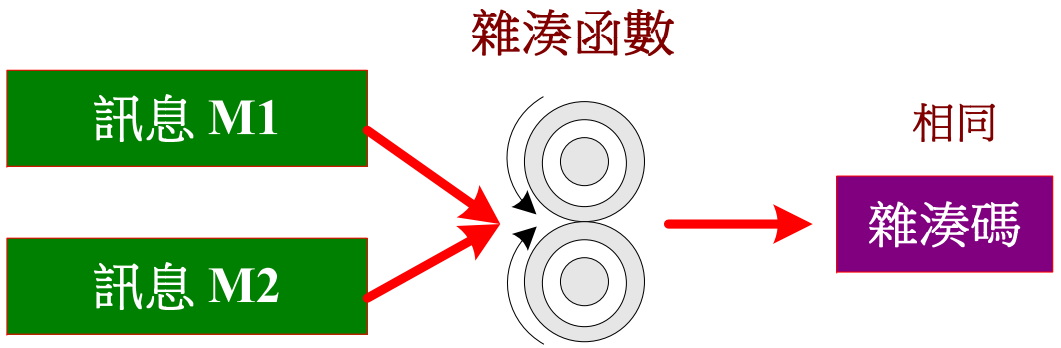
破解雜湊函數

- 破解雜湊函數的基本原理
  - 偽造訊息，使其與原來訊息的雜湊值相同



破解雜湊函數

- 生日攻擊法 (Birthday Attack)
  - 攻擊者已得到一份經由簽署者簽署過的文件，簽署方式是明文後面加上已加過密的雜湊值。
  - 攻擊者依照該文件的明文格式，修改其內容，並製造出其它偽造明文。
  - 攻擊者針對此明文產生 2^{32} 個不同的變形，一定可以找出相同雜湊值的偽造明文。
  - 攻擊者將偽造的明文與原來簽署的雜湊值結合起來，一併送出。
  - 經由接收者檢視後（利用簽署者的公開鑰匙），認為該明文的確是由簽署者所發沒錯。
- 中途相遇攻擊法 (Meet-in-the-Middle Attack)
  - 一個區塊接一個區塊的偽造