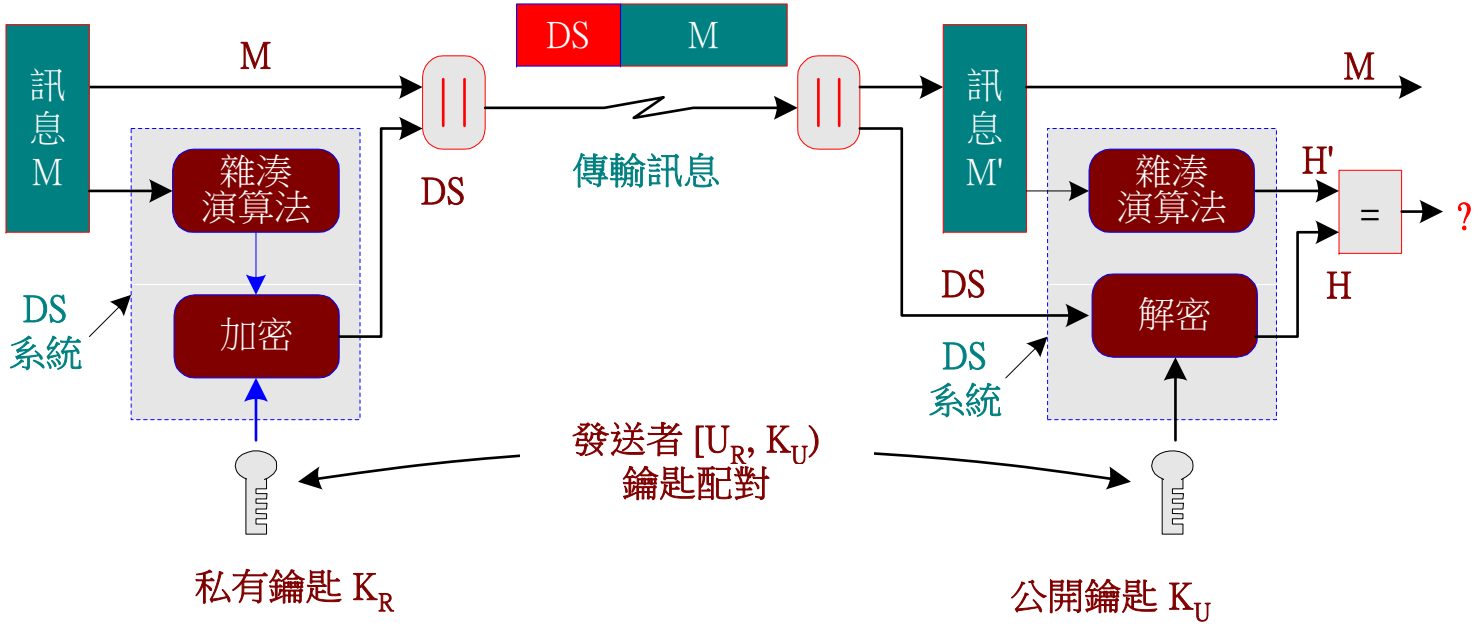
RSA 數位簽章架構

- RSA 數位簽章
  - RSA 公司發行
  - 可嵌入各種雜湊演算法：
  - MD4、MD5、SHA-1



RSA 數位簽章演算法

RSA 密碼演算法

- 選出兩個較大的質數 p 和 q、計算兩個質數的乘積 $n = p \times q$。
- 計算出小於 n 且與 n 互質的整數個數 $\psi(n) = (p-1)(q-1)$。
- 選出一個質數 e（一般可固定為 3），$1 < e < \psi(n)$；使 e 與 $\psi(n)$ 互質，亦即 $\gcd(\psi(n), e) = 1$。
- 計算出 $d = e^{-1} \bmod \psi(n)$。
- 公開鑰匙 $K_U = \{e, n\}$。 私有鑰匙 $K_R = \{d, n\}$。

RSA 簽章演算法

- 傳送訊息： M、雜湊演算法：H
- 加密演算法：$E_K[M] = (M)^d \bmod n$、解密演算法：$D_K[C] = (C)^e \bmod n$
- 傳送端計算雜湊碼：H(M)、數位簽章：$Sig(M) = E_{KR}[H(M)] = (H(M))^d \bmod n$
- 接收訊息：M’、接收端計算雜湊碼：H(M’)
- 驗證簽章：$Ver(Sig(M)) = D_{KU}[E_{KR}[H(M)]] = ((Sig(M))^e \bmod n = H(M)$
- 如果 H(M) = H(M’)，則確認成功；否則確認失敗。