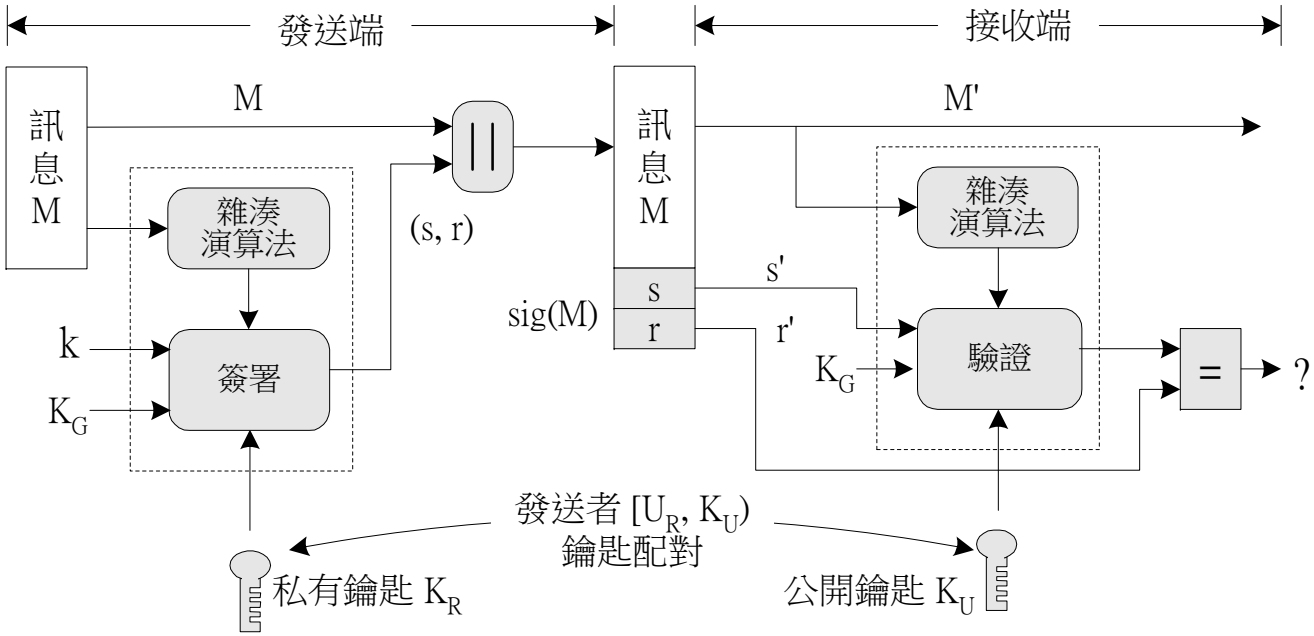
DSS 數位簽章架構

- 數位簽章標準 (Digital Signature Standard, DSS)
  - DSA (Digital Signature Algorithm)演算法、1994 年 NIST 標準：
  - K 亂數、Kg公共鑰匙、私有鑰匙、公開鑰匙
  - SHA-1 演算法
  - Sig(M) = {s, r}



DSA 演算法

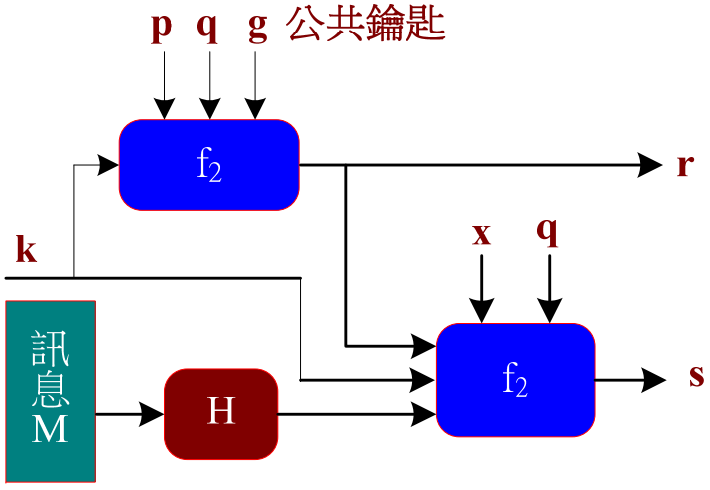
- **數位簽章演算法 (Digital Signature Algorithm, DSA)**
  - 雜湊演算法：**SHA-1**
  - 簽章演算法： **(並非採用加密演算法)**
    - 私有鑰匙：簽署人的私有鑰匙。
    - 公共鑰匙 K_G：公開共同使用。
      - p ：質數，且 $2^{L-1} < p < 2^L$； $512 < L < 1024$
      - q ：160 位元長的質數
      - g ： $g = h^{(p-1)/q} \bmod p$
    - **隨機亂數：k , 0 <k < q**

DSA 演算法 (2)

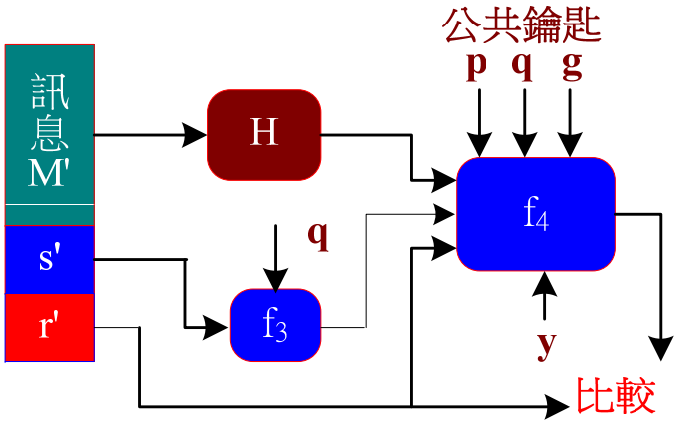
- **DSA 簽署函數：{r, s}**
  - **r =** $(g^k \bmod p) \bmod q$
  - $s = [k^{-1} (H(M) + xr)] \bmod q$，x 為發送者的私有鑰匙。
  - k= random number

- **DSA 確認函數：Ver(M', r', s')**
  - **w =** $(s')^{-1} \bmod q$
  - $u1 = [H(M')w] \bmod q$
  - $u2 = (r')w \bmod q$
  - $v = [(g^{u1} y^{u2}) \bmod p] \bmod q$，其中 y 為發送者的公開鑰匙
  - 倘若 v = r'，則認證成功（訊息與簽章皆正確）；否則，訊息將遭受竄改或鑰匙不對。

(a) DSA 簽署函數



(b) DSA 確認函數



DSA 安全考量

- **DSA 安全性考量**
  - 暴力攻擊法：鑰匙長度越長越安全。
  - 如同 **RSA** 演算法