RSA 安全考量

- **RSA 安全性考量**
  - 生日攻擊法：雜湊碼越長越安全。
  - 暴力攻擊法：鑰匙長度越長越安全：
    - 一年內使用至少 **1024 bits** 以上。
    - 一年以上至少 **2048 bits** 以上。
- **採用 RSA 數位簽章時必須注意事件：**
  - 執行數位簽章與文件加密的鑰匙，不可以使用同一對公鑰與私鑰配對。
  - 執行數位簽章時，必須針對文件的雜湊值加密，而不可以直接對文件明文加密。
  - 不可以對亂數做數位簽章。
  - 不同鑰匙配對之間不可以有相同的模數（**n**）。
  - 必須將明文填補（亂數或 **0**）到與模數（**n**）相同長度之後，再執行數位簽章。
  - 需加密的文件，必須先做數位簽章，再做訊息加密。