# 第15章 網路管理與安全

一、選擇題

1. ( 4 ) 下列何者不是資訊安全的目標？ (1) Integrity (2) Confidentiality (3) Authentication (4) Stability
2. ( 4 ) 下列何者不是 PKI 的工作之一？ (1) 確認申請者身分 (2) 公布與管理公鑰 (3) 發出私鑰給申請者 (4) 架設光線網路
3. ( 2 ) 以下哪一個密碼相對最難破解？ (1) apple2 (2) r7&oXs! (3) 135790 (4) r7toXsu
4. ( 1 ) 若要證明文件由某人發附上何者： (1) 數位簽章 (2) 數位相片 (3) 簽名圖檔 (4) 印章圖檔
5. ( 2 ) 一般而言，用公鑰加密是為了什麼目的？ (1) 加速傳輸 (2) 保密 (3) 自動回應 (4) 確認身分
6. ( 2 ) 用下列何者對文件摘要加密而產生數位簽章？ (1) 公鑰 (2) 私鑰 (3) 簽名檔 (4) 輸入的密碼
7. ( 2 ) 以下關於數位簽章及電子簽章的說明何者有誤？ (1) 電子簽章必須依附在電子文件上 (2) 數位簽章的涵蓋面較電子簽章更廣, 在應用上更有彈性 (3) 電子簽章必須具備能藉以辨識簽署人身份的要件 (4) 電子簽章必須具備能藉以辨識電子文件真偽的要件
8. ( 2 ) 下列何者不是應用層的協定？ (1) SNMP (2) ICMP (3) HTTP (4) TELNET
9. ( 4 ) 依據密碼而決定權限的管理方式稱為： (1) share level (2) user level (3) tree level (4) account level
10. ( 1 ) 下列何者不是資訊安全管理的標準？ (1) ISO 9001 (2) ISO 27002 (3) BS 7799 (4) CNS 27001
11. ( 2 ) 「不可還原編碼函數」在防止下列何動作？ (1) 從原始文件推導出編碼文件 (2) 從編碼文件推導出原始文件 (3) 從原始文件推導出密碼 (4) 從原始文件推導出編碼規則
12. ( 4 ) 下列何者是對稱式加解密系統遇到的難題？ (1) 如何在中斷後可以續傳 (2) 如何確認對方收到 (3) 如何加速傳送 (4) 如何分享金鑰
13. ( 2 ) 非對稱式加解密系統所產生的兩把 key 稱為？ (1) first & second (2) public & private (3) single & double (4) secret & nonsecret
14. ( 4 ) 封包過濾防火牆運作於 TCP/IP 協定的哪一層？ (1) 應用層 (2) 網路層 (3) 連結層 (4) 以上皆是
15. ( 2 ) 如果要過濾郵件中的 .exe 檔, 必須使用哪一種防火牆？ (1) 封包過濾 (2) 應用層 (3) 以上皆非
16. ( 3 ) 哪一種防火牆不具備通透性？ (1) 封包過濾 (2) 應用層過濾 (3) 代理器 (4) 以上皆是
17. ( 2 ) SNMP 代理程式位於 (1) NMS (2) 被管理的網路裝置 (3) 網路線中
18. ( 4 ) 可到下列哪些地點申請自然人憑證？ (1) 區公所 (2) 戶政事務所 (3) 派出所 (4) 以上皆可
19. ( 2 ) 下列何者不是防火牆採用的作法？ (1) 過濾封包 (2) 檢查密碼 (3) 應用層過濾 (4) 代理器(proxy)
20. ( 1 ) Windows 防火牆的行為預設與下列何者設定有關？ (1) 網路位置 (2) IP 位址 (3) 電腦名稱 (4) 工作群組
21. ( 4 ) 在 Windows 選擇那個網路位置，可透過網路探索看到其他電腦？ (1) 公用網路 (2) 私人網路 (3) 工作場所網路 (4) 區域網路
22. ( 2 ) Windows 防火牆預設阻擋何種連線？ (1) 不請自來的對內連線 (2) 不請自來的對外連線 (3) 雙向連線 (4) 無線連線
23. ( 3 ) IPSec 的主要用途是？ (1) 取代 IPv4 (2) 解決 IP 位址不夠的問題 (3) 保護 IP 封包的安全性 (4) 加速傳輸速度
24. ( 2 ) 以下哪一項法律攸關資訊安全？ (1) 個人資料保護法 (2) 資通安全管理法 (3) 通訊保障及監察法 (4) 社會秩序維護法

二、問答題

1. 請說明代理器的作用？

ANS：代理器防火牆將內外網路完全隔絕, 當內部網路需要連線外部網路時 (例如要瀏覽外部網頁), 代理器防火牆收到內部網路的請求後, 會連到外部網路讀取該網頁, 然後再將該網頁轉送給內部的用戶端。所以代理器防火牆是內外網路的中間代理者, 所有連線都必須透過代理器防火牆來完成。  
  
代理器防火牆運作於應用層, 所以和應用層過濾防火牆相同, 可以針對各協定過濾字串或其他條件, 而且因為完全隔絕內外網路, 所以安全防護性更高。

2. 可遠端控制網路設備的通訊協定有那些？

ANS：Telnet、HTTP

3. 請簡述資料安全機制的四個目標分別為何？

ANS：

(1) 完整無誤 (Integrity)

確認從網路收到的資料是正確的, 途中沒有被篡改或變造。

(2) 身分驗證 (Authentication)

確認資料發送者的身分, 使發送者無法假冒他人身分發送資料。

(3) 不可否認 (Nonrepudiation)

使發送者無法否認這份資料是他所發出的。

(4) 資訊保密 (Confident iali ty)

確保資料在網路上傳遞時不會被他人竊知內容。

4. 網路資源存取的管理方式有那兩種？

ANS：一.共享層級(Share Level)。  
二.使用者層級(User Level)。

5. 防火牆的封包過濾功能, 屬於 OSI 哪個層級的運作？

ANS：傳輸層和網路層

6. IPSec 協定包含哪 3 種主要的的網路協定？

ANS：

ISAKMP協定主要用來決定加密與解密時所使用的密鑰

AH協定主要用來執行『身份驗證』與『完整性檢查』兩項工作。

ESP協定主要用來執行『身份驗證』和『資料加密』兩項工作。

7. 請說明「非對稱式金鑰加密」系統的優缺點。

ANS：其優點是可以增加安全性；缺點是會增加電腦的負荷。

8. 雜湊函數與雜湊值 (Hash Value) 之間的關係為何？

ANS：雜湊函數主要用來產生雜湊值 (Hash Value), 其關係如下圖所示：

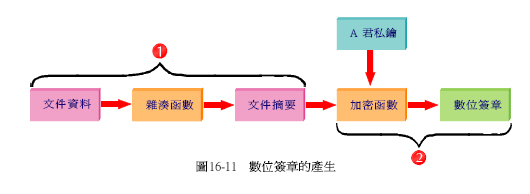


9. 請簡述數位簽章的產生流程？

ANS：

➊ 首先將電子文件經過雜湊函數處理, 產生一份文件摘要（也就是 16-5-5 所謂的雜湊值）。從先前對於雜湊函數的介紹, 我們可以知道無論這份電子文件有多大, 所產生的摘要都是同樣的長度, 而且無法從這份摘要反向推得文件內容。

➋ 再以傳送者的私鑰對摘要加密, 所產生的結果便是數位簽章。這裡要強調的是：不是對整份電子文件加密, 而是對摘要加密！換言之, 即使文件長度從 1KB 增加到 10MB, 因為所產生的摘要都是同樣長度, 所以這加密步驟所花費的時間並不會增加。



10. 傳送文件資料時附上數位簽章有那些好處？

ANS：證明這份文件確實是傳送者自己發出的, 而且文件內容沒有被篡改。