# 中六資訊及通訊科技練習卷：網絡、數據傳輸與網絡保安

中六（S6）　資訊及通訊科技　｜　時限：75 分鐘　｜　總分：100 分　｜　共 12 題

## 甲部：數據傳輸與網絡定址（32 分）

回答全部題目，答案須寫在指定位置。

**1. 資料：一個大小為 24 MB 的檔案，經一條頻寬為 8 Mbps 的網絡連線傳送。假設沒有其他流量。(a) 計算理想的傳輸時間（以秒為單位）。（2 分）(b) 解釋實際傳輸時間通常比理想值長的兩項原因。（4 分）**

答案：(a) 24 MB = 24 × 8 = 192 Mbit；192 ÷ 8 = 24 秒。（2 分，列式 1 分、答案及單位 1 分）(b) 網絡有其他人共用頻寬，實際可用頻寬低於標稱值；封包標頭與重傳開銷；路由器與交換器的處理及排隊延誤；每次連線的來回延遲。（4 分，每項 2 分）

**2. 比較光纖與雙絞線兩種傳輸媒體。(a) 分別指出光纖在頻寬與抗電磁干擾兩方面的優勢，並各加一句說明。（4 分）(b) 指出光纖的一項限制，並說明在校園主幹網絡中選用光纖的理由。（4 分）**

答案：(a) 頻寬：光纖以光訊號傳送，頻寬遠高於雙絞線，可支援 10 Gbps 以上；抗干擾：光訊號不受電磁干擾影響，亦不向外輻射，適合電磁環境複雜的場所。（4 分，每項 2 分）(b) 限制：成本較高，接駁與熔接需要專門設備和技術人員。理由：校園主幹需長距離傳送大量資料，光纖低衰減、高頻寬可減少主幹瓶頸，長遠維護成本較低。（4 分）

**3. 一個網絡使用 192.168.10.0/26 作為子網位址。(a) 計算每個子網可分配給主機使用的位址數目。（4 分）(b) 寫出第一個子網的網絡位址與廣播位址。（4 分）**

答案：(a) 主機位數 = 32 − 26 = 6，共 64 個位址，扣除網絡位址與廣播位址，可用 62 個。（4 分，列式 2 分、答案 2 分）(b) 網絡位址 192.168.10.0；廣播位址 192.168.10.63。（4 分，每項 2 分）

**4. (a) 分別說明對稱加密與非對稱加密在使用金鑰上的差異。（3 分）(b) 解釋 HTTPS 連線為何同時使用該兩種加密方式。（4 分）(c) 說明數位證書在 HTTPS 連線中的作用。（3 分）**

答案：(a) 對稱加密用同一條金鑰加密與解密，雙方須事先共享金鑰；非對稱加密用一對金鑰，公開金鑰加密、私人金鑰解密。（3 分）(b) 非對稱加密用於在握手階段安全交換一條臨時對稱金鑰；對稱加密速度快，適合大量資料傳輸，故握手後改用對稱金鑰加密內容，兼得安全與效率。（4 分）(c) 數位證書由受信任的憑證機構簽發，證明伺服器公開金鑰與網域名稱的綁定；瀏覽器據此驗證伺服器身分，防止中間人冒充。（3 分）

## 乙部：保安技術與無線網絡（36 分）

計算題須列出計算步驟，並註明單位。

**5. 某系統以 4 位數字作為個人識別碼（PIN）。(a) 計算可能的 PIN 總數。（3 分）(b) 若改為 8 位字元，每位可為大寫字母、小寫字母或數字，計算組合總數並與 (a) 比較，解釋為何後者更難被暴力破解。（6 分）**

答案：(a) 10^4 = 10,000 個。（3 分）(b) 每位 26 + 26 + 10 = 62 個選擇，共 62^8 = 218,340,105,584,896 個組合，約為 (a) 的 2.18 × 10^10 倍；組合數量大幅增加，使逐一嘗試所需的時間變得不可行。（6 分，組合式 2 分、數值 2 分、解釋 2 分）

**6. 一個公司網絡在互聯網與內部網絡之間設置防火牆，另設非軍事區（DMZ）放置對外網頁伺服器。(a) 說明防火牆如何依據規則過濾封包。（4 分）(b) 指出入侵偵測系統（IDS）與入侵防禦系統（IPS）的一項分別。（2 分）(c) 解釋把網頁伺服器放在 DMZ 而非內部網絡的好處。（3 分）**

答案：(a) 防火牆按來源與目的位址、埠號及協定比對規則，符合允許規則的封包放行，其餘丟棄；並可記錄連線日誌。（4 分）(b) IDS 只偵測並發出警報，不主動阻擋；IPS 偵測到攻擊行為後可直接攔截或中斷連線。（2 分）(c) 網頁伺服器一旦被攻破，攻擊者只處於 DMZ，未能直接接觸內部資料庫與員工電腦，可限制入侵的影響範圍。（3 分）

**7. 資料：一個網頁需要下載 4 個資源，每個 1.5 MB；連線頻寬為 12 Mbps；每個請求的來回延遲為 80 毫秒。(a) 計算純傳輸時間（以秒為單位）。（4 分）(b) 計算包含延遲的總載入時間，並解釋內容傳遞網絡（CDN）如何縮短此時間。（5 分）**

答案：(a) 4 × 1.5 = 6 MB = 48 Mbit；48 ÷ 12 = 4 秒。（4 分，列式 2 分、答案及單位 2 分）(b) 總時間 = 4 + 4 × 0.08 = 4.32 秒。（2 分）CDN 把資源快取到接近使用者的伺服器，縮短每次請求的來回路徑與延遲，並可分散流量，減少主伺服器的排隊時間。（3 分）

**8. 一位使用者在咖啡店連接免費無線網絡，並登入網上銀行。(a) 指出此情境下兩項資料外洩風險。（4 分）(b) 提出三項減低風險的措施，並各加一句說明。（5 分）**

答案：(a) 免費網絡可能由他人架設，可作中間人截取資料；同一網絡上其他使用者可能嗅探未加密的封包；偽冒熱點可誘使裝置自動連線。（4 分，每項 2 分）(b) 使用 VPN 加密全部流量；確認網址為 HTTPS 並檢查憑證；關閉自動連線及檔案共享，只用自己熟悉的網絡處理銀行交易；啟用雙重認證。（5 分，每項約 1 至 2 分）

## 丙部：應用比較與成本分析（32 分）

比較題須以分項方式作答。

**9. 比較 TCP 與 UDP 兩種傳輸層協定，並各舉一個適用應用。（8 分）**

答案：TCP 提供連線導向、可靠、有序的傳送，含確認與重傳，代價是開銷與延遲較大，適合網頁瀏覽、檔案下載與電郵。UDP 不建立連線、不保證送達，開銷小、延遲低，適合串流影片、語音通話與線上遊戲。（8 分，每協定 4 分）

**10. 一家中小企考慮把客戶資料由本地伺服器遷移到雲端服務。(a) 指出兩項好處。（4 分）(b) 指出兩項風險，並各提出一項對應措施。（4 分）**

答案：(a) 免卻前期硬件投資，按用量付費；服務商負責維修、擴充與備份，可快速增加容量；員工可從不同地點存取。（4 分，每項 2 分）(b) 風險：資料存放於第三方，涉及私隱與合規問題；網絡或服務商故障會令業務中斷。措施：加密靜態資料並簽訂資料處理協議；採用多重備份及訂明服務水平的合約。（4 分）

**11. 資料：某公司每月收到 40 封釣魚郵件，其中 5% 令員工點擊並造成平均每次 120,000 元損失。推行保安培訓後，成功率降至 1%，培訓成本為每月 30,000 元。計算推行前後的每月預期損失、節省金額及淨得益，並判斷培訓是否值得。（8 分）**

答案：推行前：40 × 5% × 120,000 = 240,000 元。（2 分）推行後：40 × 1% × 120,000 = 48,000 元。（2 分）節省 240,000 − 48,000 = 192,000 元；扣除培訓成本 30,000 元，淨得益 162,000 元。（2 分）淨得益為正數且數額可觀，故培訓值得推行；惟仍須配合技術過濾與定期演練。（2 分）

**12. (a) 指出物聯網（IoT）裝置兩項常見的保安弱點。（4 分）(b) 解釋 3-2-1 備份策略的內容及其好處。（4 分）**

答案：(a) 出廠預設密碼或弱密碼，使用者極少更改；固件長期不更新，存在已知漏洞；裝置運算能力有限，難以執行強加密。（4 分，每項 2 分）(b) 保存三份資料副本，使用兩種不同儲存媒體，其中一份存放於異地；好處是單一媒體損壞、勒索軟件加密或場地事故時仍可還原資料。（4 分）

---

TutorZone 中六（S6）資訊及通訊科技練習卷｜題目與文章為原創，並非任何學校或出版社的教材。