中五資訊及通訊科技練習卷

中五　資訊及通訊科技　｜　時限：75 分鐘　｜　總分：100 分　｜　共 24 題

1. IPv4 子網劃分與可用主機數（18 分）

可用主機數目 = $2^n - 2$（n 為主機位元，扣除網絡位址與廣播位址）。

1. (a) 網絡 192.168.10.0/26：求每個子網的位址數目、可用主機數目，以及由 192.168.10.0/24 可劃出多少個 /26 子網。

答案：主機位元 = 32 − 26 = 6，位址數目 = 2^6 = 64；可用主機 = 64 − 2 = 62。由 /24 劃出 2^(26−24) = 4 個 /26 子網。

2. (b) 網絡 10.0.0.0/22：求子網遮罩、位址數目及可用主機數目。

答案：遮罩 = 255.255.252.0（22 個 1 後接 10 個 0）。主機位元 = 10，位址數目 = 2^{10} = 1024，可用主機 = 1024 − 2 = 1022。

3. (c) 主機位址 172.16.5.130/27：求網絡位址、廣播位址及可用主機範圍。

答案：區塊大小 = 2^(32−27) = 32。130 ÷ 32 = 4 餘 2，故網絡位址 = 172.16.5.128，廣播位址 = 172.16.5.159，可用範圍 172.16.5.129 至 172.16.5.158。

4. (d) 由 192.168.1.0/24 劃分，需要至少 5 個子網、每個子網至少 25 部主機，求最合適的前置長度並說明理由。

答案：25 部主機需 5 個主機位元（$2^5 - 2 = 30 \geqslant 25$）；用 /28 只有 $2^4 - 2 = 14$ 部，不足。故前置長度 = 32 − 5 = /27（255.255.255.224），可劃出 $2^3 = 8$ 個子網，滿足至少 5 個的要求。

2. TCP/IP 分層與協定（16 分）

答案須寫出層名及協定名稱。

5. (a) 列出 TCP/IP 模型四層，每層舉一個協定。

答案：應用層（HTTP、DNS、SMTP）、傳輸層（TCP、UDP）、互聯網層（IP、ICMP）、網絡存取層（Ethernet、IEEE 802.11）。

6. (b) 比較 TCP 與 UDP 的四項差異（連接方式、可靠性、開銷、典型用途）。

答案：TCP 為連接導向、可靠（確認、重傳、按序交付）、標頭較大開銷高，用於網頁與檔案傳輸；UDP 無連接、不保證送達、標頭小開銷低、延遲低，用於語音、直播及 DNS 查詢。

7. (c) 某段網絡 MTU 為 1500 bytes，IP 標頭 20 bytes、TCP 標頭 20 bytes，求 MSS 及有效負載佔整個訊框的百分比。

答案：MSS = 1500 − 20 − 20 = 1460 bytes；佔比 = 1460 ÷ 1500 × 100% = 97.33%。

8. (d) 簡述 TCP 三次握手的三個步驟及其作用。

答案：客戶端送 SYN（含初始序號）→ 伺服器回 SYN-ACK（確認並送自己的序號）→ 客戶端回 ACK。作用是雙方確認收發能力、同步初始序號，建立可靠連線後才傳資料。

3. 資料庫正規化與 SQL 查詢（18 分）

SQL 答案須用標準語法；正規化須指出相依關係。

9. (a) 分別說明第一（1NF）、第二（2NF）、第三（3NF）正規化的要求。
答案：1NF：每格只存單一原子值，無重複群組；2NF：符合 1NF，且非主鍵欄位完全依賴整個主鍵（消除部分相依）；3NF：符合 2NF，且非主鍵欄位之間無相依（消除遞移相依）。

10. (b) 表 Enrol(student_id, student_name, class_code, class_teacher)：指出兩項相依問題，並拆成 3NF 的表結構。
答案：student_name 只依賴 student_id（部分相依，若主鍵為 student_id 加 class_code）；class_teacher 只依賴 class_code（遞移相依）。拆為 Student(student_id, student_name, class_code)、Class(class_code, class_teacher)、Enrol(student_id, class_code)。

11. (c) 寫出 SQL：列出平均分高於 70 分的班別及其平均分。
答案：SELECT class_code, AVG(score) AS avg_score FROM Enrol GROUP BY class_code HAVING AVG(score) > 70;（查核樣本資料下只有 A1，平均 80.33 分。）

12. (d) 寫出 SQL：列出每位學生姓名及其班別老師姓名（兩表連接）。
答案：SELECT s.name, c.teacher FROM Student s JOIN Class c ON s.class_code = c.class_code;（查核樣本資料回 5 行。）

4. 演算法複雜度與排序比較（16 分）

須寫出所用的計算式。

13. (a) 在一萬零二十四個元素的已排序陣列中，線性搜尋與二分搜尋的最壞情況比較次數各為多少？（元素數目取 1,048,576）
答案：線性搜尋最壞 = n = 1048576 次；二分搜尋最壞 = $\lceil \log_2 \ n \rceil = \lceil \log_2 \ 1048576 \rceil = 20$ 次。

14. (b) 對 1024 個元素，泡沫排序最壞比較次數為 $n(n-1)/2$，合併排序約為 $n \log_2 \ n$，分別計算並比較。
答案：泡沫排序 = $1024 \times 1023 \div 2 = 523776$ 次；合併排序 $\approx 1024 \times 10 = 10240$ 次。兩者相差約 51 倍，元素越多差距越大。

15. (c) 陣列 [42, 17, 68, 9, 55, 23, 71, 34]，以最後元素為基準做一次 Lomuto 分割，寫出分割後的陣列及基準所在索引。
答案：基準 = 34。由左至右把小於或等於 34 的元素換到前面，最後把基準交換到分界位置：結果 = [17, 9, 23, 34, 55, 68, 71, 42]，基準在索引 3，左邊全部 ⩽ 34、右邊全部 > 34。

16. (d) 把 $O(n^2)$、$O(n \log n)$、$O(\log n)$、$O(1)$ 由增長最慢排到最快，並各舉一例。
答案：$O(1)$（陣列按下標取值）< $O(\log n)$（二分搜尋）< $O(n \log n)$（合併排序）< $O(n^2)$（泡沫排序）。n 越大，高階項主導實際執行時間。

5. 數碼檔案大小與壓縮（16 分）

1 MiB = 1,048,576 bytes；1 MB = 1,000,000 bytes。

17. (a) 一幅 1920 × 1080、24 位元色深的未壓縮點陣圖，求檔案大小（MiB 及 MB）。
答案：每像素 24 bits = 3 bytes；總量 = 1920 × 1080 × 3 = 6220800 bytes = 5.93 MiB ≈ 6.22 MB。

18. (b) 一段 44.1 kHz、16 位元、立體聲、長 3 分鐘的未壓縮 WAV，求檔案大小。
答案：每秒 = 44100 × 2 bytes × 2 聲道 = 176400 bytes；3 分鐘 = 180 秒；總量 = 31752000 bytes = 30.28 MiB ≈ 31.75 MB。

19. (c) 一行索引色像素為 WWWWBBBBWWWWWWBBB（每像素 1 byte），用（顏色, 次數）每組 2 bytes 的行程編碼（RLE），求壓縮後大小及壓縮比。
答案：行程 = (W,4)(B,4)(W,6)(B,3)，共 4 組 × 2 bytes = 8 bytes；原本 17 bytes，壓縮比 = 17 ÷ 8 = 2.125。顏色越集中，RLE 越有效。

20. (d) 比較有損與無損壓縮，各舉一例並說明適用情況。
答案：無損壓縮解壓後與原檔完全相同（PNG、ZIP、FLAC），適合文字、程式碼、醫療影像；有損壓縮捨棄部分資料換取更高壓縮率（JPEG、MP3、H.264），適合相片、音樂、影片，但要避免反覆壓縮累積失真。

6. 資訊保安與相關法規（16 分）

答案須指出技術名稱及作用。

21. (a) 比較對稱與非對稱加密，各舉一種演算法及一項用途。
答案：對稱加密用同一條金鑰加解密（AES），速度快，適合大量資料如磁碟與 HTTPS 會話資料；非對稱加密用公鑰加密、私鑰解密（RSA），適合金鑰交換與數碼簽署，但運算較慢。

22. (b) 說明數碼簽署如何同時提供完整性與不可否認性。
答案：寄件人先對訊息計雜湊（SHA-256），再用自己的私鑰簽署該雜湊值；收件人用寄件人公鑰驗簽並重算雜湊，兩者相同即證明內容未被篡改（完整性），而只有私鑰持有人能產生該簽署（不可否認性）。

23. (c) 列舉三種常見網絡攻擊手法，並各寫一項對應防禦措施。
答案：釣魚電郵（防禦：核對寄件網域、啟用多重認證）；暴力破解密碼（防禦：長密碼加帳戶鎖定與 MFA）；中間人攻擊（防禦：強制 HTTPS 並驗證憑證）。

24. (d) 就香港《個人資料（私隱）條例》（第 486 章）六項保障資料原則，說明與機構收集及使用顧客資料最相關的兩項，並各舉一例。
答案：第 1 原則（收集目的及方式）：須為合法目的、與目的直接有關、足夠但不超乎適度，並告知用途；例：試堂登記只收集姓名與電話。第 3 原則（使用）：除獲資料當事人同意或法律准許，資料只可用於收集時所述目的；例：未經同意不得把名單轉交第三方推銷。

TutorZone 中五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。