中六資訊及通訊科技練習卷：網絡與數據傳輸、加密與網絡安全、數據庫與 SQL、演算法與程式編寫、系統開發與測試、科技倫理與可持續運算

中六　資訊及通訊科技　｜　時限：75 分鐘　｜　總分：100 分　｜　共 24 題

第一部分 網絡與數據傳輸

甲部：每題 4 分，共 16 分。

1. 一個 480 MB 的檔案經一條標稱 100 Mbps 的連線傳送，實際有效頻寬只有標稱值的 80%。求傳送所需的時間（秒）。

答案：有效頻寬 = 100 × 0.8 = 80 Mbps，即 80 ÷ 8 = 10 MB s⁻¹；時間 = 480 ÷ 10 = 48 s（以 bit 計：480 × 8 × 10^6 ÷ 80 × 10^6 = 48 s）。

2. 一幅 3000 × 2000 像素、每像素 24 位色的未壓縮點陣圖，求檔案大小（MB）。若以無損方式壓縮後體積減少 70%，求壓縮後大小（MB）。

答案：像素數 = 3000 × 2000 = 6 000 000；總位元 = 6 000 000 × 24 = 144 000 000 bit；÷ 8 = 18 000 000 byte = 18.0 MB；壓縮後 = 18.0 × 0.3 = 5.4 MB。

3. 一個 IPv4 網絡使用 /26 前綴。求該子網可用主機數目、子網遮罩（點分十進制）及廣播位址（以 192.168.10.64/26 為例）。

答案：主機位元 = 32 − 26 = 6，位址數 = 2^6 = 64，可用主機 = 64 − 2 = 62；遮罩 = 255.255.255.192；網段 192.168.10.64 – 127，廣播位址 = 192.168.10.127。

4. 一個 60 MB 的檔案經 50 Mbps 連線傳送，連線來回時間（RTT）為 40 ms，需要兩次來回才完成握手。假設忽略其他延誤，求總傳輸時間（秒）。

答案：傳輸時間 = 60 × 8 ÷ 50 = 9.6 s；握手延誤 = 2 × 0.04 = 0.08 s；總時間 = 9.6 + 0.08 = 9.68 s。

第二部分 加密與網絡安全

乙部：每題 4 分，共 16 分。

5. 比較對稱與非對稱加密在密鑰分發上的差別：10 名用戶兩兩通訊，各需多少條密鑰？並各舉一項效能上的優缺點。

答案：對稱加密每人共用一條密鑰：10 × (10 − 1) ÷ 2 = 45 條；非對稱每人一對公私鑰：2 × 10 = 20 條。對稱運算快但密鑰分發困難（n 人需 n(n−1)/2 條）；非對稱密鑰分發容易但運算慢，故實務上用非對稱交換會話密鑰，再以對稱加密傳資料。

6. RSA 取質數 p = 61、q = 53，公開指數 e = 17。求 n、φ(n) 及私鑰 d，並以明文 m = 65 驗證加解密。

答案：n = 61 × 53 = 3233；φ(n) = 60 × 52 = 3120；由 e · d ≡ 1 (mod 3120) 得 d = 2753（17 × 2753 = 46801 = 15 × 3120 + 1）。加密：c = 65^17 mod 3233 = 2790；解密：2790^2753 mod 3233 = 65，還原成功。

7. 某系統密碼由大寫、小寫字母及數字組成（共 62 個字元），長度固定 8 位。求可能組合總數；若攻擊者每秒可試 10 億個組合，求平均破解時間（以日為單位，取一位小數）。

答案：組合數 = 62^8 = 2.183e+14 ≈ 2.18×10^{14} ；全部試完需 218,340 s；平均（一半）= 1.3 日。故須加長度、加鹽及限制嘗試次數。

8. 某公司有 500 名員工，釣魚測試中 3% 的人點擊了假連結。計算點擊人數，並說明防火牆與員工培訓在防禦上分別針對哪些風險。

答案：點擊人數 = 500 × 3% = 15 人。防火牆過濾未經授權的埠與流量，阻擋外部掃描與部分惡意連線；但釣魚郵件多用正常埠（80/443），故須靠培訓、郵件過濾與多重認證，並以「四眼原則」處理匯款要求。

第三部分 數據庫與 SQL

丙部：每題 4 分，共 16 分。

9. 解釋主鍵、外鍵與正規化的作用，並說明為何未正規化的表會產生更新異常。

答案：主鍵唯一識別每筆記錄且不可為空；外鍵參照另一表的主鍵以維持參照完整性；正規化（1NF→2NF→3NF）消除重複組與部分 / 傳遞相依。未正規化時同一事實重複儲存，改一處漏改另一處即造成更新異常，刪除一筆又可能連帶丟失其他資料。

10. 資料表 Marks 有 5 筆分數：72、58、91、45、84。寫出求平均分的 SQL，並算出結果。

答案：SELECT AVG(score) AS avg_score FROM Marks; 合計 = 350，平均 = 350 ÷ 5 = 70.0。若要四捨五入至整數可用 ROUND(AVG(score), 0)，並可用 WHERE 加條件篩選。

11. 現有 Student(student_id, name) 與 Enrol(student_id, class_code)。寫出 SQL 列出每班學生人數，只顯示多於 20 人的班別，並按人數由多至少排序。

答案：SELECT class_code, COUNT(*) AS n FROM Enrol GROUP BY class_code HAVING COUNT(*) > 20 ORDER BY n DESC; 要點：JOIN 只為取姓名，計人數用 Enrol 已足夠；篩選聚合結果用 HAVING，不可用 WHERE；ORDER BY 放最後。

12. 一張有 1,000,000 筆記錄的表，全表掃描每筆比較約 10 微秒；用 B-tree 索引只需 20 次節點讀取，每次 5 毫秒。求兩者平均查詢時間及速度比。

答案：全表掃描平均掃 500,000 筆：500,000 × 10 μs = 5.0 s；索引：20 × 5 ms = 100 ms = 0.1 s；速度比 = 5.0 ÷ 0.1 = 50 倍。但索引會增加寫入成本與儲存空間，且對低選擇性欄位效益有限。

第四部分 演算法與程式編寫

丁部：每題 4 分，共 16 分。

13. 在 1,000,000 個已排序項目中，線性搜尋平均比較多少次？二分搜尋最多比較多少次？求兩者之比。

答案：線性搜尋平均 500,000 次；二分搜尋最多 $\lceil \log_2 \ 1{,}000{,}000 \rceil = 20$ 次；比 = 500,000 ÷ 20 = 25,000 倍。二分搜尋要求資料已排序，插入新資料需維持排序。

14. 氣泡排序對 12 個項目作最壞情況（完全逆序）排序，共需多少次比較？若每次比較與交換合計 1 微秒，求所需時間。
答案：比較次數 = $n(n-1)/2 = 12 \times 11 \div 2 = 66$ 次；時間 $\approx 66\ \mu s = 0.066$ ms。時間複雜度 $O(n^2)$，資料量倍增時比較次數約增四倍，故大數據應用改用 $O(n \log n)$ 的排序。

15. 以遞迴定義計算 fib(10) 的樸素演算法共會被呼叫多少次？並說明為何改用備忘錄法可大幅減少。
答案：fib(10) 的呼叫次數（含本身）= 177 次，因為同一個 fib(k) 被重複計算多次，時間複雜度約 $O(1.6^n)$。備忘錄法把已算結果存入陣列或字典，每個 k 只算一次，複雜度降為 $O(n)$，fib(10) 只需約 10 次計算加查表。

16. 比較 $O(1)$、$O(\log n)$、$O(n)$、$O(n \log n)$、$O(n^2)$ 在 $n = 1024$ 時的運算次數，並指出哪一種最不適合處理大型輸入。
答案：$O(1) = 1$；$O(\log n) = 10$；$O(n) = 1{,}024$；$O(n \log n) = 10{,}240$；$O(n^2) = 1{,}048{,}576$。$O(n^2)$ 最不適合：n 增至 10 倍時運算量增 100 倍，實際會超時；故選演算法先看增長的階，再看常數與記憶體。

第五部分 系統開發與測試

戊部：每題 4 分，共 16 分。

17. 列出系統開發生命週期（SDLC）的主要階段，並說明「需求分析」做得不好會如何影響後期成本。
答案：階段：可行性研究→需求分析→系統設計→編碼實作→測試→推行轉換→維護檢討。需求階段的錯誤在設計、編碼、測試各階段被放大，越後期才發現，修改要重做設計與測試，成本最高；故須與用戶確認需求並以原型驗證。

18. 某判斷邏輯有 3 個互相獨立的條件。以白盒測試的「條件組合覆蓋」計，最少需要多少個測試案例？並說明黑盒測試與白盒測試的分別。
答案：每個條件有真 / 假兩種，組合數 = 2^3 = 8 個案例。白盒測試看程式內部結構與路徑，由開發者設計；黑盒測試只看輸入與輸出是否符合規格，由測試者或用戶按需求設計，兩者互補。

19. 比較瀑布模型與敏捷開發，並說明在需求經常改變的項目中為何多用敏捷。
答案：瀑布模型按階段順序推進，每階段完成才進下一階段，文件齊全但難回頭，適合需求穩定的項目；敏捷以短迭代交付可用版本，每個衝刺後檢視與調整，客戶持續參與，故需求常變時能及早修正方向，風險分散但要求團隊自律與持續溝通。

20. 說明用戶驗收測試（UAT）的目的與做法，並解釋版本控制（如 Git）在團隊開發中的作用。
答案：UAT 由實際用戶按業務情境執行，確認系統符合需求才可上線；做法包括以真實資料跑主要流程、記錄缺陷並簽署驗收。版本控制保存每次修改與作者，可分支平行開發、合併變更、必要時回退，避免檔案互相覆蓋，並留下可追溯的修改紀錄。

第六部分 科技倫理與可持續運算

己部：每題 5 分，共 20 分。

21. 比較自由及開放源碼軟件（FOSS）與專有軟件的授權、成本與風險，並各舉一個適用情境。
答案：FOSS（如 GPL、MIT）可自由使用、修改及再發佈，無授權費，源碼可審計，但需自負支援與維護；專有軟件收取授權費、封閉源碼，供應商負責支援與更新，但易受廠商鎖定。學校教學平台可用 FOSS 降低成本，金融核心系統多選專有軟件以取得合約保障。

22. 列舉《個人資料（私隱）條例》六項保障資料原則中的四項，並說明學校應如何處理學生資料。

答案：六項原則：①收集目的及方式合法相關而不過度；②準確及保留不超過所需時間；③使用限於原定目的（除非同意）；④保安措施；⑤政策公開；⑥查閱與改正權利。學校應只收集教學所需資料、加密儲存、限制存取、訂明保留期，並向家長說明用途與查閱途徑。

23. 說明以大數據或機器學習作決策時，偏見可能從何而來，並提出兩項減低風險的措施。

答案：偏見源頭：①訓練資料本身有歷史歧視或取樣偏差；②特徵選擇把受保護屬性（性別、族裔）間接編碼；③標籤由人決定而帶主觀；④模型在黑盒下難以解釋，錯誤難察覺。措施：審核資料分佈與代表性、以不同群組分別評估準確率與誤判率、保留人工覆核與申訴機制、公開模型卡與決策依據。

24. 某數據中心的 IT 設備耗電 400 kW，總耗電 500 kW。求 PUE；若全年不停運作（8 760 小時）、每度電排放 0.6 kg 二氧化碳，求年排放量（公噸）。並提出一項降低 PUE 的方法。

答案：PUE = 500 ÷ 400 = 1.25；年用電 = 500 × 8 760 = 4,380,000 kWh；排放 = 4,380,000 × 0.6 = 2,628,000 kg = 2,628 公噸。降 PUE：改用自然冷卻（如冷通道封閉、提高送風溫度）、餘熱回收或虛擬化提高使用率。

TutorZone 中六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。