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）。

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）。

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）。

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）。

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。

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。

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）。

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。

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。

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。

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。

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。

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。

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。

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。

16. 比較 O(1)、O(log n)、O(n)、O(n log n)、O(n²) 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。

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。

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。

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。

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。

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。

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。

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。

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。
