DSE ICT 練習卷：電腦系統、數據通訊與程式編寫

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

甲部：電腦系統與數據表示（32 分）

甲部全部題目必答，須展示計算步驟。

1. (a) 將二進位數 1011 1101 轉換為十進位值。(b) 將同一個數轉換為十六進位。(c) 將十六進位 3F 轉換為八位二進位數。(d) 說明電腦為何採用二進位而非十進位表示數據。

答案：(a) 1011 1101 = 128 + 32 + 16 + 8 + 4 + 1 = 189。(b) 每四位一組：1011 為 B、1101 為 D，故十六進位為 BD。(c) 3F = 0011 1111，即 00111111。(d) 數位電路只有高、低兩種穩定狀態，二進位可直接對應導通與截止，電路簡單、抗噪聲能力強，亦便於用邏輯閘實現算術與邏輯運算。

2. 一幅 1920 × 1080 像素、色深 24 位元的未壓縮點陣圖像：(a) 求其檔案大小（以 KiB 表示）；(b) 以 MiB 表示，取兩位小數；(c) 若無損壓縮後大小為原來的四成，求壓縮後的位元組數；(d) 說明改用 8 位元索引色為何能大幅縮小檔案。

答案：(a) 檔案大小 = 像素數 × 每像素位元數 ÷ 8 = 1920 × 1080 × 3 = 6,220,800 位元組 = 6,075 KiB。(b) 除以 1,048,576 得 5.93 MiB。(c) 壓縮後 = 6,220,800 × 0.4 = 2,488,320 位元組。(d) 索引色每個像素只需 8 位元記錄調色盤索引，較 24 位元真彩色少三分之二；同時同一色塊可用相同索引值表示，令相鄰像素更易被無損壓縮。

3. 一個 24 MiB 的檔案經標稱 8 Mbps 的寬頻連線傳送，實際吞吐量只有標稱值的六成。(a) 求實際吞吐量（Mbps）；(b) 求傳送所需時間（秒）；(c) 若先把檔案壓縮至原本一半大小，傳送時間為多少秒；(d) 指出兩項影響實際吞吐量的因素。

答案：(a) 實際吞吐量 = 8 × 0.6 = 4.8 Mbps。(b) 檔案大小 = 24 × 8 = 192 Mbit，時間 = 192 ÷ 4.8 = 40 秒。(c) 壓縮後為 96 Mbit，時間 = 96 ÷ 4.8 = 20 秒。(d) 網絡擁塞程度、線路誤碼引致的重傳、伺服器回應速度，以及同一網絡的使用者數目。

4. 某處理器時脈為 3.2 GHz，平均每個指令需 4 個時脈週期。(a) 求每秒可執行的指令數，並以 MIPS 表示；(b) 若時脈改為 2.6 GHz 而每指令仍需 4 個週期，MIPS 為多少；(c) 說明加大快取記憶體如何提升實際效能。

答案：(a) 每秒指令數 = 3,200,000,000 ÷ 4 = 800,000,000，即 800 MIPS。(b) 2,600,000,000 ÷ 4 = 650,000,000，即 650 MIPS。(c) 快取記憶體把常用指令與數據放在處理器附近，縮短平均記憶體存取時間，減少管線停頓，故實際完成指令數提高。

乙部：數據通訊、網絡與網絡安全（36 分）

乙部全部題目必答，數值答案須附單位。

5. 網絡 192.168.10.0/24 須平均劃分為四個子網路。(a) 求每個子網路的前置碼長度；(b) 求每個子網路可用的主機位址數目；(c) 寫出子網路遮罩；(d) 寫出第一個子網路的網路位址與廣播位址。

答案：(a) 借兩位主機位元，前置碼為 /26。(b) 每個子網路共有 64 個位址，扣除網路位址與廣播位址，可用 62 個。(c) 子網路遮罩為 255.255.255.192。(d) 第一個子網路網路位址為 192.168.10.0，廣播位址為 192.168.10.63。

6. 一段 30 秒的立體聲音頻以 44.1 kHz 取樣、16 位元量化錄製，並未壓縮。(a) 求檔案大小（位元組）；(b) 以 MiB 表示，取兩位小數；(c) 若改為單聲道並把取樣率減半，檔案大小為原來的百分之幾；(d) 說明有損壓縮在音頻應用的取捨。

答案：(a) 大小 = 44,100 × 2 × 2 × 30 = 5,292,000 位元組。(b) 除以 1,048,576 得 5.05 MiB。(c) 單聲道令資料減半，取樣率減半再減半，合計為原來的 25%。(d) 有損壓縮捨棄人耳較難察覺的高頻與遮蔽成分，換取大幅縮小檔案；代價是無法還原原始波形，重複編碼會累積失真。

7. 執行以下虛擬碼，寫出 total 的最終值，並列出每次迴圈結束後 total 的值。total ← 0；for i ← 1 to 5；total ← total + i × i；end for；輸出 total。

答案：迴圈依次加入 1、4、9、16、25。每次迴圈後 total 依次為 1、5、14、30、55，最終值為 55。

8. 資料表 Orders 有欄位 order_id、customer 與 amount，記錄為：(1, A, 120)、(2, B, 680)、(3, C, 450)、(4, D, 900)、(5, E, 300)。(a) 寫出找出 amount 大於 500 的記錄數目的 SQL 語句；(b) 求該結果的記錄數目；(c) 求符合條件記錄的 amount 總和；(d) 說明主鍵的作用。

答案：(a) SELECT COUNT(*) FROM Orders WHERE amount > 500;(b) 符合條件的記錄為第 2 及第 4 行，共 2 條。(c) 總和 = 680 + 900 = 1,580。(d) 主鍵唯一識別每一行記錄，不允許重複或空值，並可作為其他資料表的外鍵引用，確保實體完整性。

丙部：程式編寫、數據庫與系統開發（32 分）

丙部全部題目必答，虛擬碼答案須逐步列出。

9. 比較對稱式加密與非對稱式加密，並說明數位簽章如何同時提供來源認證與資料完整性。答案須指出兩類加密的金鑰使用方式及其效能差異。

答案：(a) 對稱式加密以同一把金鑰加密與解密，運算快，適合大量資料，但金鑰分發困難。(b) 非對稱式加密以公鑰加密、私鑰解密，解決金鑰分發問題，但運算較慢。(c) 數位簽章先用雜湊函數（例如 SHA-256）求訊息摘要，再以發送者私鑰加密摘要；接收者以發送者公鑰驗證，能確認來源身分，並在內容被更改時驗證失敗。(d) 實務上以非對稱式加密交換短期對稱金鑰，再以對稱式加密傳輸主體資料。

10. 在一個已排序、含 1000 個元素的陣列中搜尋目標值。(a) 線性搜尋在最壞情況下需要多少次比較；(b) 二分搜尋在最壞情況下最多需要多少次比較；(c) 說明二分搜尋為何要求資料事先排序。

答案：(a) 最壞情況要檢查全部元素，共 1,000 次比較。(b) 每次比較把搜尋範圍減半，最多 10 次比較，因為 2 的 10 次方為 1,024，已覆蓋 1,000 個元素。(c) 二分搜尋靠比較中間元素判斷目標位於左半或右半，若資料未排序，這個判斷不成立，可能丟棄目標所在的區間。

11. 說明系統開發生命週期（SDLC）的五個主要階段，並指出系統分析階段最常進行的一項資料收集活動及其用途。

答案：(a) 五個階段為系統分析、系統設計、系統實施、系統測試與系統維護，部分模型在分析之前加可行性研究。(b) 系統分析階段最常進行訪談與問卷調查，用以收集現有系統的運作問題與使用者需求，作為編寫需求規格書的依據。(c) 各階段並非單向：測試或維護階段發現的缺陷會令流程回到設計或分析，形成迭代。

12. 說明第一、第二及第三正規化形式分別要消除什麼問題，並指出 IaaS、PaaS 與 SaaS 三種雲端服務模式在責任分工上的分別。

答案： ⒜ 第一正規化形式要求每格只存單一值，消除重複群組與多值欄位。⒝ 第二正規化形式要求非主鍵欄位完全依賴整個複合主鍵，消除部分依賴。⒞ 第三正規化形式要求非主鍵欄位之間不存在傳遞依賴，消除由其他非主鍵欄位決定的冗餘。⒟ IaaS 只提供虛擬機器與儲存，客戶自行管理系統與應用；PaaS 另提供執行環境與中介軟件，客戶只部署應用；SaaS 直接提供可用的應用服務，客戶只管理帳戶與資料。

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。