

教育部受託辦理115學年度 公立高級中等學校教師甄選

資訊科技科 試題

作答注意事項

1. 本試題共兩部分：選擇題 36 題，及綜合題 3 大題，共計 100 分。
2. 選擇題請用2B軟心鉛筆在答案卡劃記，綜合題限用藍色、黑色原子筆或鋼筆在答案本上作答，但繪圖時得使用黑色鉛筆。
3. 本科「不可以」使用電子計算器。

第一部分：選擇題 (共 40 分)

一、單選題 (每題 1 分，共 32 分)

- (C) 1. 某一電腦其記憶體位址由十六進制的 2000 到 DFFF 總共佔多少個位址？ (A)16K (B)32K (C)48K (D)64K。
- (B) 2. 小鹿同學在瀏覽器中輸入網址，結果卻回傳了一個「403 Forbidden」的訊息，這是 http 回應狀態代碼中的那種類別？ (A)伺服器錯誤回應 (B)用戶端錯誤回應 (C)重新導向訊息 (D)資訊回應。
- (D) 3. 下列有關 RGB、CMYK 及 HSB 的敘述何者錯誤？ (A)RGB (255,255,0) 表示黃色 (B)RGB 混色方式稱為加色法 (C)CMYK 分別表示青色、洋紅色、黃色及黑色，其數值都介於 0%到 100% (D)HSB 數值都介於 0%到 100%。
- (B) 4. 在 OSI 七層模型中，關於各層的功能敘述，何者正確？ (A)資料連結層 (Data Link Layer) 負責跨路由器的路徑選擇，並以封包 (Packet) 作為其資料傳輸單位 (B)傳輸層 (Transport Layer) 將資料切分為區段 (Segment)，並提供 TCP 與 UDP 等傳輸模式 (C)網路層 (Network Layer) 主要負責將資料封裝成框架 (Frame)，並加上實體位址 (MAC Address)，以確保資料能準確送達區域網路內的特定設備 (D)會議層 (Session Layer) 主要負責資料的加密、壓縮與格式轉換，以確保不同系統間的資料呈現一致。
- (D) 5. 在下列 IEEE 802.11x 的無線通訊協定，依理論上的傳輸速度，由快到慢排序，何者正確？ ①802.11a ②802.11ac ③802.11ad ④802.11b
(A)③②④① (B)④①②③ (C)①②③④ (D)③②①④。
- (A) 6. 有一系統使用 8 位元 2 的補數來表示一個整數，則整數可表示的範圍為多少？
(A)-128 到+127 (B)-128 到+128 (C)-127 到+127 (D)-127 到+128。
- (C) 7. 一個 IP 網段使用子網路遮罩 255.255.255.192，在此網段實際上可以使用的 IP 個數是多少？ (A)30 (B)32 (C)62 (D)64。
- (D) 8. 大明從雲端硬碟檔案中，下載了一個約 400MB 的檔案，總共花費了 20 秒，請問大明所使用的網路下載速度為何？ (A)20Mbps (B)40Mbps (C)80Mbps (D)160Mbps。
- (C) 9. 有關 TCP/IP 及 OSI 通訊協定的說明，下列何者錯誤？ (A)表達層負責對傳送的資料進行壓縮、解壓縮或是加解密 (B)傳輸層的通訊協定主要有 TCP 及 UDP，TCP 會確認資料是否正確送達接收端 (C)ICMP 是應用層的協定，負責傳輸錯誤訊息 (D)172.27.172.16 屬於 Class B 等級的私有 IP (Private IP)，要透過 NAT 技術才能連上 Internet。
- (B) 10. 有關「電子商務安全機制」的敘述，下列何者正確？ (A)使用安全資料傳輸層 SSL (Secure Socket Layer) 機制來傳輸交易資料，只需商家申請憑證，程序簡便，也能防止消費者盜刷的行為 (B)在進行網路銀行或信用卡線上交易時，銀行端經常會採用一次性密碼 OTP (One-Time Password) 來提升交易安全 (C)SSL 與 SET 都可確保資料傳輸的隱密性與完整性、不可否認性，且 SSL 的安全性比 SET 高 (D)傳輸層保全 TLS (Transport Layer Security) 與 3D-Secure 相同，都是 SSL 的改良版本，可應用於 E-mail 的安全防護。
- (D) 11. 學校某部八核心電腦的資料匯流排有 8 Bytes、位址匯流排有 32 位元、控制匯流排有 8 bits，執行一個指令需要 16 個時脈週期，一個時脈週期為 0.25ns，下列敘述何者正確？ (A) CPU 內頻為 2.5 GHz (B)若要傳送 CPU 讀取硬碟的訊號可由位址匯流排

負責，其最大定址空間為 4GB (C)八核心 CPU 表示有八個處理器，可利用平行運算提高效率 (D) CPU 處理速度為 250 MIPS。

- (B) 12. 有關軟體開發程式的敘述，下列何者正確？ (A)React Native 是由 Meta 公司推出，主要用來開發 Windows 環境下的軟體 (B)App Inventor 目前由 MIT 維護，不須安裝，透過瀏覽器就可在線上使用 (C)Xcode 是適合在 Windows 環境下撰寫不同程式語言，如 C++、JAVA 等 (D)Eclipse 主要用來開發 VB 應用程式。
- (D) 13. 下列關於 Office 的敘述何者錯誤？ (A)Word 中選取整個表格再按 Del 鍵，只能刪除表格內容，無法刪除整個表格 (B)在 Excel 中，有一儲存格中的內容為「國文、英文、數學」，如要以『、』為分隔符號，將「國文」「英文」「數學」分散到三個儲存格，可使用「資料剖析」功能 (C)在 Word 中可在頁尾插入圖片；但 PowerPoint 不行 (D)在 Excel 中，若儲存格的內容為文字且長度超過儲存格寬度，會以#####顯示。
- (D) 14. 下列關於 Office 的敘述何者錯誤？ (A)在 Word 中，樣式功能可以定義一套文字色彩、大小、段落間距…等格式的規則，以便於快速使文件擁有統一的格式 (B)在 Word 中，更新表格內運算公式的值，需要按下快速鍵 F9 (C)在 Excel 儲存格中輸入'123.56，則預設對齊方式為靠左對齊 (D)將文件的某一段分成二等欄，結果會自動產生「分欄符號..... 」符號。
- (D) 15. 關於 MAC 位址、IP 位址與網域名稱，下列敘述何者正確？ (A)每張網路卡只有 1 個 MAC 位址，一台電腦僅能插 1 張網路卡 (B)1 個公有 IP 僅可對應 1 個虛擬 IP (C)每個網域名稱僅能對應 1 個公有 IP 位址 (D)每個 MAC 位址可對應多個虛擬 IP 位址，而多個虛擬 IP 位址能對應 1 個公有 IP 位址。
- (A) 16. 下列何者是合法的 Public IP 位址，可通過防火牆 (Firewall) 管制，直接在 Internet 上流通？ (A) 8.9.10.11 (B) 100.254.255.256 (C) 255.255.255.0 (D) 127.0.0.1。
- (A) 17. 在數位簽章 (Digital Signature) 的標準運作流程中，發送方與接收方需結合雜湊函數與非對稱加密技術。下列關於此流程的敘述，何者正確？ (A)發送方先對原始訊息進行雜湊運算以產製訊息摘要，再使用發送方的私鑰對該摘要進行加密，此加密後的結果即為數位簽章 (B)接收方於驗證簽章時，需使用接收方本人的公鑰將簽章解密，並與原始訊息經雜湊運算後的結果進行比對 (C)雜湊函數的主要作用是將任意長度的訊息轉換為固定長度的訊息摘要，且接收方可透過摘要逆向還原出原始訊息內容 (D)數位簽章雖然能提供身分鑑別與不可否認性，但由於未對原始訊息進行加密，因此無法確保資料的完整性。
- (B) 18. 下列關於 CPU 指令週期 (Instruction Cycle) 的敘述，何者錯誤？ (A)CPU 執行指令的循環順序為：擷取→解碼→執行→儲存 (B)擷取階段是由控制單元根據指令暫存器的位址，將指令從記憶體讀入程式計數器中 (C)指令擷取後，程式計數器會自動加 1 (或增加一個指令長度)，以指向下一個等待執行的指令位址 (D)在執行階段，主要由算術邏輯單元 (ALU) 負責運算，並將結果存入累加器或暫存器中。
- (C) 19. 關於堆疊 (Stack) 與佇列 (Queue) 之特性、運作邏輯與應用，下列敘述何者正確？ (A)堆疊遵循先進先出 (FIFO) 原則，適合應用於印表機的文件排程 (B)佇列遵循後進先出 (LIFO) 原則，瀏覽器中的回上一頁功能之紀錄即具有佇列特色 (C)在程式實作上，佇列通常從後端 (Rear) 新增資料並從前端 (Front) 移除；而堆疊的插入與刪除則固定在同一端 (Top) 進行 (D)若對一初始為空的堆疊依序執行 Push(A)、Push(B)、Pop()、Push(C)、Pop()，最終留在堆疊中的元素為 C。

- (C) 20. 將下列時間複雜度依優劣的情況排序，何者正確？ ① $O(n)$ ② $O(\log_2 n)$ ③ $O(1)$ ④ $O(n!)$ ⑤ $O(n^2)$ ⑥ $O(n \log_2 n)$
(A)③②⑥①④⑤ (B)③②⑥①⑤④ (C)③②①⑥⑤④ (D)③②①⑥④⑤。
- (A) 21. 下列排序演算法中，哪些屬於非穩定的排序 (Unstable Sort)？ ①氣泡排序法 ②選擇排序法 ③合併排序法 ④快速排序法
(A)②④ (B)③④ (C)②③ (D)①③。
- (D) 22. 在圖形的追蹤 (Graph Traversal) 有兩種常用的方法，一個為深度優先搜尋 (Depth First Search, DFS)，另一種為廣度優先搜尋 (Breadth First Search, BFS)，試問在對圖形做 BFS 時，通常會使用到何種資料結構？ (A)樹 (Tree) (B)堆積 (Heap) (C)堆疊 (Stack) (D)佇列 (Queue)。
- (A) 23. 在 Linux 作業系統中，欲顯示某一文字檔的內容，可以使用下列哪一個指令？
(A)cat (B)type (C)ls (D)edit。
- (D) 24. 程序 (Process) 是作業系統正在處理中的程式，它具有多種狀態，下列關於程序的敘述，何者正確？ (A)程序允許進入主記憶體中等待被分配 CPU 時間來執行，屬於等待狀態 (B)程序已經獲得 CPU 時間，並正在執行其指令，屬於建立狀態 (C)程序正在等待外部資源，如等待 I/O 操作結束，屬於結束狀態 (D)程序完成等待外部資源後，終止中斷，屬於就緒狀態。
- (B) 25. 請利用氣泡排序法 (Bubble Sort) 將陣列中的資料：80, 50, 30, 90, 20, 70, 10, 40, 60，由左至右且由小到大排列，第三次排序後的順序為何？
(A)50, 30, 20, 10, 40, 60, 70, 80, 90 (B)30, 20, 50, 10, 40, 60, 70, 80, 90
(C)20, 30, 50, 10, 60, 40, 70, 80, 90 (D)10, 20, 30, 40, 50, 60, 70, 80, 90。
- (A) 26. 在多程序 (Process) 運作中，下列何者不是發生死結 (deadlock) 的充分必要條件？
(A)搶占 (preemption)：系統資源可被強制從一個行程中退出 (B)持有和等待 (hold and wait)：一個行程可以在等待時持有系統資源 (C)互斥 (mutual exclusion)：資源只能同時分配給一個行程，無法多個行程共享 (D)循環等待 (circular waiting)：一系列行程互相持有其他行程所需要的資源。
- (C) 27. 下列何者是區塊鏈「智慧合約」的正確描述？ (A)交易驗證與確認的過程 (B)保障區塊鏈資料庫數據準確和保密的主要核心 (C)將合約中的交易條款或商業規則內嵌在區塊鏈系統，在交易的環節中適時地執行 (D)網路上共享的資產帳簿，所有參與者都能有與自己完全相同副本的帳簿。
- (B) 28. 在人工智慧領域中，下列關於 AI 代理 (AI Agent) 的敘述，何者正確？ (A)核心價值在於超越傳統語言模型的語言理解力，能提供更精準的問答回覆 (B)具備自主性與目標導向，能進行任務規劃並具備調用外部工具以執行操作的能力 (C)運算架構受限於特定硬體，必須在高性能圖形處理器 (GPU) 上才能運行 (D)僅限於具備實體驅動裝置的機器人系統，不涵蓋純軟體環境中的代理程式。
- (C) 29. 在一個包含 n 個相異整數的陣列中進行二分搜尋，下列敘述何者正確？ (A)若陣列長度 $n=100$ ，則無論目標值位於陣列中的哪個位置，二分搜尋法找到目標值所需的比較次數皆固定為 $\log_2 100$ 次 (B)當資料量增加為原本的 2 倍時，二分搜尋法在最差情況下的比較次數也會隨之增加 2 倍 (C)若陣列數列為 [2, 5, 8, 12, 19, 25, 31, 38, 42, 50, 61, 74, 88]，以二分搜尋法搜尋目標值「12」，若採中間偏左索引方式，需經過 4 次比較即可找到目標 (D)若陣列長度 $n=1000$ ，則最差情況下僅需約 11 次比較。

- (D) 30. Jacky 在執行商業委託案期間，針對不同授權類型的工具軟體進行了處置。根據各類軟體的授權規範與法律原則，下列哪一項行為完全合法且不具侵權風險？ (A)將免費軟體 (Freeware) 進行內容調整，更動其商標識別與名稱後，以個人名義重新提供給同業好友下載使用 (B)將自由軟體 (Free Software) 組件整合至收費產品中交付客戶，以商業機密為由，拒絕揭露該組件的來源資訊與原始授權說明 (C)使用共享軟體 (Shareware) 進行專案產出，於 30 天試用期屆滿後，因軟體功能未受限制，遂判定可不支付授權費並持續用於商業接案 (D)取得標註為公共領域 (Public Domain Software) 的原始檔案，經由個人專業加工與優化後，將該衍生版本視為個人設計產出，並販售予廣告公司營利。
- (B) 31. 某電信公司準備在 A、B、C、D、E 五個節點之間佈設海底電纜。各節點間的連接成本如下表所示。若因特殊安全需求，規定佈線方案中「必須包含 C-D」這段線路，請問在連接所有節點且路徑不形成迴圈的前提下，最低總成本為多少百萬元？
(A) 26 (B) 34 (C) 35 (D) 36。

節點連接	單位 (百萬元)	節點連接	單位 (百萬元)
A - C	5	B - E	10
A - D	7	C - E	8
B - C	9	D - E	6
B - D	8	C - D	15

- (B) 32. 某 AI 模型在訓練集表現極佳，但在新資料上表現明顯下降，此現象最可能為何？
(A)欠擬合 (Underfitting) (B)過擬合 (Overfitting) (C)強化學習失敗 (D)硬體效能不足。

二、複選題 (每題 2 分，全對才給分，共 8 分)

- (BD) 33. Sophie 是一間大型電商平台的數據分析師，她正試圖利用各種機器學習 (Machine Learning) 演算法來優化平台的營運效率。關於她所採用的演算法與對應的應用情境，下列哪些敘述是錯誤的？
(A)關聯性分析 (Apriori)：可用於分析購買咖啡豆的顧客，通常也會同時購買牛奶，進而優化網頁的交叉銷售推薦組合。
(B)分群 (K-means)：屬於一種監督式學習，Sophie 必須先手動標記出哪些顧客是高消費族群，系統才能將其他數據準確歸類。
(C)分類 (KNN)：可用於郵件系統的垃圾信過濾，透過已標記的歷史郵件特徵，來預測新收到的信件是否屬於垃圾郵件。
(D)線性迴歸 (Linear Regression)：主要用於處理非連續性的類別資料，例如將客戶自動區分為喜歡運動與喜歡閱讀兩個群體，不涉及數值預測。
- (AB) 34. Alex 是一位跨境電商創辦人，他正試圖導入多種生成式 AI (Generative AI) 工具以優化營運流程。關於他所接觸到的工具特性、分類與技術風險，下列哪些敘述是正確的？
(A)當 Alex 需要撰寫多國語言商品描述、產出客服對話劇本或進行長篇市場報告摘要時，可採用 ChatGPT、Claude 或 Gemini 等文字生成工具。
(B)Midjourney 與 DALL-E 屬於圖像生成工具，其核心技術在於將抽象的文字描述轉化為具體的視覺影像，在技術分類上屬於文字轉圖像 (Text to Image) 應用。
(C)若 Alex 的開發團隊使用 GitHub Copilot，該工具能透過分析上下文自動補全程式碼





、撰寫註解或修正邏輯錯誤，這在分類上屬於程式碼生成，能有效提升軟體開發效率。
(D)生成式 AI 若產出看似合理但與事實不符的資訊，稱為幻覺 (Hallucination)，這主要是因為輸入提示詞 (Prompt) 長度不足導致的運算溢位或硬體存取錯誤，通常只要增加指令字數即可完全消除此現象。

- (AB) 35. Fiona 為了強化電商平台的資料安全，她正與技術團隊討論如何針對會員個資與交易封包進行加密處理。根據對稱式與非對稱式加密的特性比較，下列哪些敘述是正確的？
D
- (A)當需要針對伺服器內大量的商品圖檔與歷史訂單進行快速加密時，選擇對稱式加密較為合適，因為其加密速度快，適合處理大規模資料。
(B)在多方通訊的情境下，非對稱式加密能有效解決金鑰管理問題，使用者只需妥善保管自己的私鑰，並將公鑰自由分發給任何需要傳送加密訊息給他的人。
(C)非對稱式加密的缺點在於金鑰管理極其困難，因為每增加一位不同的通訊對象，系統就必須為該對象維護一把獨有的專屬金鑰，導致金鑰總數隨用戶量激增。
(D)對稱式加密的優勢在於運算邏輯簡單且速度快；而非對稱式加密雖然運算複雜且較慢，但能解決金鑰傳輸安全問題。
- (AB) 36. 關於作業系統 (Operating System) 的資源與記憶體管理機制，下列哪些敘述是正確的？
- (A)緩衝區 (Buffer)：主要配置於實體記憶體 (RAM) 中作為暫存媒介，協調 CPU 處理速度與低速外部設備 (如磁碟或印表機) 間的傳輸速率差異。
(B)虛擬記憶體 (Virtual Memory)：允許程式定址空間大於實際物理記憶體，其運作本質是將部分輔助儲存空間 (如硬碟) 作為物理記憶體的延伸，以支援大型程式執行。
(C)多元處理 (Multi-processing)：指系統將所有工作任務拆分為微小片段，並限制在單一的 CPU 核心內輪流完成運算，以確保資料的運作順序。
(D)中斷機制 (Interrupt)：為維護系統穩定，硬體設備發出請求後，必須等待 CPU 完整執行完當前應用程式的運算週期，才能獲得處理權限。

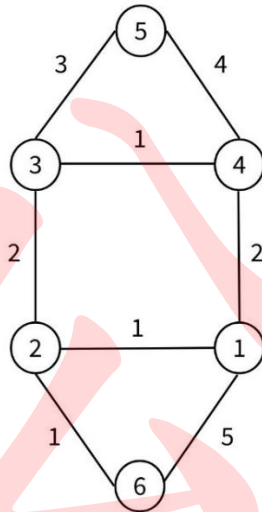
第二部分：綜合題 (共 60 分)

一、填充題 (共 36 分)

1. 創用 CC (Creative Commons) 是作者用來向公眾宣告作品的授權範圍，由四個標章組成 (1) 6 (2 分) 種授權條款，其四個標章說明如下：

標章	姓名標示(BY)	(2) <u>禁止改作(ND)</u> (2 分)	(3) <u>相同方式分享(SA)</u> (2 分)	非商業性(NC)
				
說明	必須標示原作者	不得改作此作品	若改作此作品，必須沿用原授權條款	不得用於商業目的

2. 如下圖一所示之具有加權值的圖形，最小花費擴張樹的加權值之和為(4) 8 (2分)。



圖一

3. IPv6 的 localhost IP 為(5) ::1 或 0000:0000:0000:0000:0000:0000:0000:0001 (2分)。
4. 作業系統為了管理程序的執行順序，通常會採用工作排程的方式。常見的排程方法包括 FCFS、SJF、RR 和 Priority。根據下表所列的 A、B、C、D 四個程序及其處理時間，且若四個程序到達時間皆為 0。(RR：執行時間片段為 4ms)

程序	優先順序	到達順序	執行時間
A	1	3	9 ms
B	4	1	4 ms
C	2	2	8 ms
D	3	4	5 ms

- (1)若作業系統採用「SJF」的排程演算法，請問這四個程序的平均等待時間為(6) 7.5 (2分) 毫秒？
- (2)若作業系統採用「Priority」的排程演算法，請問這四個程序的平均等待時間為(7) 12 (2分) 毫秒？
- (3)若作業系統採用「RR」的排程演算法且執行時間片段為 4ms，請問這四個程序的平均等待時間為(8) 12.25 (2分) 毫秒？
5. 在資通安全責任等級分級辦法中，等級 D 級之各機關應辦事項，所有人員（含主管）每年應接受(9) 3 (2分) 小時以上之資通安全通識教育訓練。
6. 某一加密系統之運算規則為：先將明文 (plaintext) 的英文字母依序轉換為對應序號 (如：A=1, B=2, ..., Z=26)，並代入下列公式求得密文之字母序號。(註：若運算結果為 0，則該序號對應之字母為 Z)

$$\text{密文序號} = (\text{明文序號} + 13) \bmod 26$$

根據上述規則，已知一組密文 (ciphertext) 為 FZVYR，請問原始的明文訊息 (message) 應該為何？(10) SMILE (2分)

7. 若有一數列為「9, 10, 6, 3, 8, 16, 15」，請以第一個數字「9」作為根節點，並依照數列順序逐一插入建立二元搜尋樹。請在下表中分別寫出前序走訪及後序走訪的結果數列。

走訪類型	結果數列
前序走訪	(11) <u>9, 6, 3, 8, 10, 16, 15</u> (2 分)
中序走訪	3, 6, 8, 9, 10, 15, 16
後序走訪	(12) <u>3, 8, 6, 15, 16, 10, 9</u> (2 分)

8. 有一個 Python 程式片段如下，請寫出執行後輸出的答案：(13) 8 (3 分)

```
total = 0
for i in range(1, 6):
    if i == 2:
        continue
    if i == 5:
        break
    total += i
print(total)
```

9. 有一個 C++ 程式片段如下，請寫出執行後輸出的答案：(14) 19 (3 分)

```
#include <iostream>
using namespace std;
int main() {
    int a[] = {12, 5, 8, 3, 7, 4, 9, 15, 1, 6};
    int sum = 0;
    int k = 4;
    for (int i = 0; i < 10; i++) {
        if (a[i] < a[k]) {
            sum = sum + a[i];
        }
    }
    cout << sum;
    return 0;
}
```


10. 有一個 Python 程式片段如下，請寫出執行後輸出的答案：(15) 7 (3 分)

```
grid = [  
    [13, 27, 42],  
    [38, 15, 36],  
    [51, 24, 19]  
]  
x = grid[1][1] % 2  
y = grid[2][2] // 4  
z = grid[1][0] % 3  
print(x + y + z)
```

11. 有一個 Python 程式片段如下，請寫出執行後輸出的答案：(16) 23 (3 分)

```
def rec(n):  
    if n <= 2:  
        return n-1  
    else:  
        return rec(n-1) + rec(n-2) + 3  
print(rec(4) + rec(5))
```

二、名詞解釋 (每題 2 分，共 8 分)

1. Quantum Computer
2. Edge Computing
3. Deepfake
4. NPU (Neural Processing Unit)

三、問答題 (每題 4 分，共 16 分)

1. 在網頁設計中，表單資料的傳遞最常使用的就是 get 與 post 兩種方法，請比較 get 與 post 的差別？
2. 何謂資料隱碼 (SQL Injection)？如何避免其發生？
3. 請詳細說明什麼是資訊安全三要素？
4. 請問「物聯網 (IoT)」的三層架構為何？並請簡述其意義及功能。