

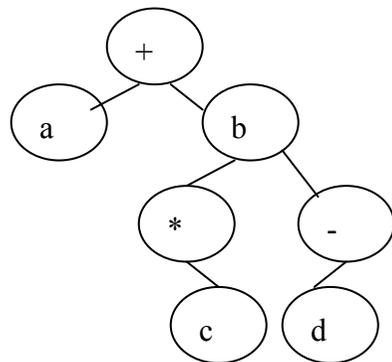
國立臺中第二高級中學 101 學年度第一學期第二次教師甄選 資訊科試題

請填寫准考證號碼 _____

一、選擇題：每格 2 分，共 60 分

1. 下圖中的二元樹(Binary Tree)經過後序(postorder)追蹤後，其順序為？

- (A)+ab*c-d (B) +b-d*ca (C) a+b*c-d (D) ac*d-b+



2. 將 a、b、c、d 依序放入堆疊(stack)中，取出兩個元素後，依序放入 e、f、g，再取出一個元素，並放入 h，請問此時堆疊中剩下的元素由上至下依序排列為何？

- (A) habfe (B) hfeba (C) hbaef (D) hefab

3. 下列那一種排序方式所需要的平均時間最短？

- (A) 堆積排序法(Heap Sort) (B) 插入排序法(Insertion Sort)
(C) 氣泡排序法(Bubble Sort) (D) 選擇排序法(Selection Sort)

4. 目前雲端運算(Cloud Computing)的服務類型不包括下列那一種？

- (A) 平台即服務(Platform as a Service, PaaS)
(B) 軟體即服務(Software as a Service, SaaS)
(C) 資料即服務(Data as a Service, DaaS)
(D) 基礎架構即服務(Infrastructure as a Service, IaaS)

5. 若 CPU 的速度為 5MIPS，則執行一個指令的平均時間為何？

- (A) 0.2μs (B) 0.5μs (C) 0.2ns (D) 0.5ns

6. 下列有關資訊安全的敘述，何者錯誤？

- (A) 對稱式加密法(Symmetric Encryption)中，加、解密雙方使用的金鑰是相同的
(B) 對稱式密碼學的加、解密時間效率比非對稱式密碼學為佳
(C) RSA 演算法是非對稱式加密法(Asymmetric Encryption)中常用的技術之一
(D) 數位簽章(Digital Signature)是以對稱式加密為基礎進行的驗證機制

7. 在一個有許多節點(node)的網路系統中，為了降低連線的成本，必需使用何種 Algorithm 來解決

- (A) Shortest Path (B) Minimum Spanning Tree
(C) Maximum Flow Minimum Cut (D) Amortized Analysis

8. 3-way handshaking protocol 是應用在下列那一方面

- (A) Network Transmission (B) Database Transaction (C) Data Encryption/Decryption
(D) Facial Recognition

9. 下列有關網頁、網站程式語言的敘述何者錯誤？

- (A) PHP 是在 server 端執行的程式語言 (B) Java Script 比 PHP 容易在網頁上產生動畫
(C) Java Script 比 PHP 容易讀、寫網站資料庫 (D) 瀏覽器無法執行 PHP 程式

10. 下列中文與英文縮寫之配對何者有誤？

- (A) 無線射頻識別：RFID (B) 電子資料交換：EDI (C) 人工智慧：AI (D) 憑證管理中心：PKI

11. 若 A 欲傳送資料給 B，如何使用公開金鑰技術，讓 B 相信資料確實為 A 所傳送？

- (A) 使用 A 的公鑰加密，再以 B 的私鑰解密
(B) 使用 B 的公鑰加密，再以 B 的私鑰解密
(C) 使用 A 的公鑰加密，再以 A 的公鑰解密
(D) 使用 A 的私鑰加密，再以 A 的公鑰解密

12. 以下那一種排程演算法，理論上能得到最短的平均等待時間？

- (A) 優先權(Priority) (B) 先到先做(FCFS) (C) 循環分配(RR) (D) 最短工作先做(SJF)

13. 為了要標示一本書的頁碼，排版工人總共用了 2989 個鉛字，請問這本書到底有幾頁？

- (A) 512 (B) 1024 (C) 1596 (D) 2048

14. 「無障礙網頁設計」是指下列哪一項網頁設計原則？

- (A) 內容完成使用中文表示 (B) 不設計身心障礙人士可能無法瀏覽的網頁內容
(C) 網頁中較艱澀的內容都標記注譯 (D) 網頁內容為為普遍級，各年齡層皆可瀏覽

15. 在 Microsoft Word 2003 環境中，若要使用二種不同格式的頁碼時，必須在不同頁碼之文件中插入下列何種符號？

- (A) 分節 (B) 分頁 (C) 欄 (D) 分段。

16. TCP、HTTP、IP 在 OSI 網路傳輸的七層協定中，由上而下的順序為

- (A) TCP -> IP -> HTTP (B) HTTP -> IP -> TCP (C) HTTP -> TCP -> IP
(D) IP -> TCP -> HTTP

17. 關聯式資料庫是以資料的什麼做為擷取資料的方式？

- (A) 位址 (B) 內容 (C) 指標 (D) 大小

18. 下列編碼中何者具有錯誤更正能力？

- (A) 漢明碼 (Hamming code) (B) 同位元 (Parity bit)
(C) 霍夫曼碼(Huffman code) (D) Unicode

19. 在一個有 Windows、Android、Mac OS 的龐大系統中，下列何者最適合用來開發 Cloud Computing？

- (A) Web's CGI (B) C# .Net (C) RPC on C/C++ (D) Java RMI

20. 每個標準 ASCII 字元、EBCDIC 及 Unicode 字元分別由多少位元所組成？

- (A) 7,7,16 (B) 7,8,16 (C) 16,8,7 (D) 16,8,8

21. 同位檢查(Parity Ckecking)是一項資料錯誤檢查的技術，下列何者不具有偶同位性？
(A) 110011110 (B) 101110101 (C) 010101001 (D) 011110100。
22. 50 倍速光碟機中之所謂 “倍數” 的基準資料傳輸速率為？
(A) 150 Kbit/sec (B) 150 KByte/sec (C) 300 Kbit/sec (D) 300 KByte/sec
23. 在一網路中，每一區段 (Segment) 傳輸媒介均有其最大的傳輸距離，超過該長度時訊號會衰減，因此需加裝何種裝置？
(A) Bridge (B) Router (C) Switching Hub (D) Repeater
24. 一般個人電腦內部所稱 cache 係指：
(A) DRAM (B) SRAM (C) SDRAM (D) EPROM
25. 十進制數值 50.875 以二進制數值表示，下列哪一項是正確的？
(A) 110010.111 (B) 110010.110 (C) 110100.111 (D) 110100.110。
26. 下列有關網路防火牆之敘述何者為誤？
(A)外部防火牆無法防止內部網路使用者對內部的侵害
(B)防火牆能管制封包的流向
(C)防火牆可以管制外部網路進入內部系統
(D)防火牆可以防止任何病毒的入侵。
27. 如我們使用的 B 類位址網路，網路遮罩的設定應為多少？
(A) 255.0.0.0 (B) 255.255.0.0 (C) 255.255.255.0 (D) 255.255.255.255。
28. 網路電子商務給生活帶來極大便利，下列何者是電子商務成功與否最重要的關鍵？
(A)隨時可推翻交易，保護消費者 (B)交易憑證的建立
(C)追蹤交易者真實身份，以昭公信 (D)交易後，仍可要求退貨
29. 下列那何者不屬於 Serial 的傳輸技術方式？
(A)Ethernet (B)IDE (C)USB (D)S-ATA
30. 若有一布林(Boolean)代數運算式為 $Z=X' Y' +X' Y+XY$ ，此運算式之最簡式為：
(A) $X'Y'$ (B) XY (C) $X+Y$ (D) $X'+Y$

二、問答題：共 40 分。(可不用照題號順序寫，但請務必清楚標明題號，並詳細填寫內容)

(一)、試以生活中實際問題，簡單設計一教學教材，讓學生可以利用文書處理軟體及試算表軟體來解決。(提示，例如可以某校各班進行減重比賽，每一位同學定期量體重，以試算表統計全班總減重成果，並加以排名，並將各班名次及總減重重量套印列印成獎狀。(10 分)

(二)、以 Flash 的 Action Script 來製作動畫時，若以 for loop 或 while loop 來改變物件的位置而形成移動的效果，播放出來的畫面只會看到最後一個畫面，中間移動的過程完全看不到。根據 Flash 的使用手冊也記載 確實有這個問題。請以 Action Script 的語言特性及多工或多執行緒的觀點，來解釋 Action Script 為何有這樣的限制。(提示：製作動畫在 Java 語言上必需以執行緒的方式才容易實作)(10 分)

(三)、比較「水平式思考」及「垂直式思考」，並各舉一實例。(10 分)

(四)、加密解密技術是 Data Security 的重要基礎，其中 RSA 加解密系統是一個已經證明非常安全的技術，RSA 是屬於非對稱式系統，使用 RSA 必須產生 public key 與 private key，才能完成資料的加解密動作。請根據 public key 與 private key 的特點，說明：
a. RSA 的加解密流程 (3 分)
b. RSA 相較於對稱式系統的最大優點 (2 分)
c. RSA 之所以非常安全的理論基礎 (重要原理即可，細節可不用寫) (5 分)