

114年公務人員普通考試試題

類 科：統計
科 目：資料處理概要
考試時間：1 小時 30 分

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

一、某一公司的採購資料如下所述：

每一位客戶包含有屬性客戶編號、姓名、電話、地址。在客戶中，客戶編號具有唯一性。

每一張訂單包含有屬性訂單編號、購貨日期。在訂單中，訂單編號具有唯一性。每一張訂單裡的每一項產品都有其訂購數量之屬性。

每一項產品包含有屬性產品編號、產品名稱、單價。而在產品中，產品編號具有唯一性。

每一位客戶可能都沒下過訂單，也可能下過多張訂單。

每一張訂單必定為某一位客戶且也僅能為一位客戶所下訂的。

每一張訂單包含有至少一項以上產品；每項產品可能被多張不同訂單所訂購過，也可能未被任何訂單所訂購過。(每小題 10 分，共 40 分)

(一)試依上述說明，為該公司畫出一實體關聯圖 (Entity Relationship Diagram, ER Diagram)。該實體關聯圖需標出每一實體的名稱、屬性、主鍵屬性 (Key attribute)、每一關係 (Relationship) 及其基數性 (cardinality)。

(二)試為該實體關聯圖 (ER Diagram)，決定出最簡化之各關聯表格。需描述出每一表格的名稱、屬性 (attribute)、主要鍵 (primary key) 及外來鍵 (foreign key)。

(三)試寫出一 SQL 程式片段，為每一張訂單所採購之每一項產品，列印出該訂單編號、產品名稱及採購金額。

(四)試寫出一 SQL 程式片段，為每一張訂單列印出該訂單編號及該訂單所採購總金額。

二、 L_1 為一由小而大排序之資料串列， L_2 為一由大而小排序之資料串列，其分別含有 N_1 與 N_2 筆資料，且 $N_1, N_2 \gg 0$ ：(每小題 10 分，共 20 分)

(一)請設計出一最佳演算法，以能最快速查詢一資料 D 是否存在於資料串列 L_1 或 L_2 內。

(二)並求出該演算法之時間複雜度 (請越精確估算越佳)。

三、請撰寫一演算法，透過堆疊(stack)以計算出一後序式數學運算式(Postfix Expression) (例如"E=23*5+")之結果。假設運算式中只含加、減、乘、除(+, -, *, /)四種運算子(operator)，及0, 1, ..., 9十種運算元(operand)。(10分)

四、應用適當的密碼學機制，可確保資料的機密性(confidentiality)、完整性(integrity)、鑑別性(authenticity)、不可否認性(non-repudiation)之安全目標。

(一)試解釋何謂機密性、完整性、鑑別性、不可否認性。(8分)

(二)若A欲將機密資料D，透過網路傳送給B。請透過雜湊(Hash)函式及RSA加密法，設計一資料加密機制，以確保機密資料之機密性、完整性、鑑別性。(10分)

(三)若A欲將一電子合約D，透過網路傳送給B簽章。請透過雜湊(Hash)函式及RSA加密法，設計一數位簽章機制，以確保電子合約之機密性、完整性、鑑別性、不可否認性。(12分)