代號：41450
頁次：2－1

115年公務人員特種考試司法人員、法務部調查局調查人員及海岸巡防人員考試試題

考 試 別：調查人員
等　　別：三等考試
類 科 組：資訊科學組
科　　目：資料庫應用
考試時間：2 小時　　　　座號：＿＿＿＿＿＿

※注意：㈠禁止使用電子計算器。
㈡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。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、假設 T1、T2 與 T3 為三個不同的交易（Transactions）。且令 Read(X, A)為從資料庫中讀取資料項 X 的內容，並寫入本機變數 A 中。Write(A, X)為將本機變數 A 的內容，寫入資料庫的資料項 X 中。（每小題 10 分，共 20 分）

㈠現給定下列排程（Schedule）：

T1:	R(X, A),		W(A, X), R(Y, B),W(B, Y),	
T2:		R(X, A),W(A, X),R(Y,B),		W(B, Y)

試利用順序優先圖（Precedence Graph）方法，檢測此排程是否為可序列化排程（Serializable Schedule）。

㈡現給定下列排程（Schedule）：

T1:	R(X, A),R(Z, C),W(A, X),		W(C, Z),						
T2:		R(Y, B),		R(X, A),		W(B, Y),		W(A, X),	
T3:					R(C, Z),		R(Y, B), W(C, Z),		W(B, Y)

試利用順序優先圖（Precedence Graph）方法，檢測此排程是否為可序列化排程（Serializable Schedule）。

二、假設使用者 A 擁有一對 RSA 公鑰 AU 與私鑰 AR；使用者 B 也擁有一對 RSA 公鑰 BU 與私鑰 BR。若 A 欲透過網路將訊息 M 安全地傳送給 B：（每小題 10 分，共 20 分）

㈠請利用 RSA 加密法，設計一套能同時滿足鑑別性（Authenticity）、機密性（Confidentiality）、完整性（Integrity）及不可否認性（Non-Repudiation）之四安全原則的傳輸流程演算法，以安全完成該任務。

㈡請詳細說明您所設計的演算法，如何能有效達成上述四項資訊安全原則。

三、圖一為一個含有二個特殊化(specializations)的公司人員分類之 Enhanced Entity-Relationship Diagram, EERD)。

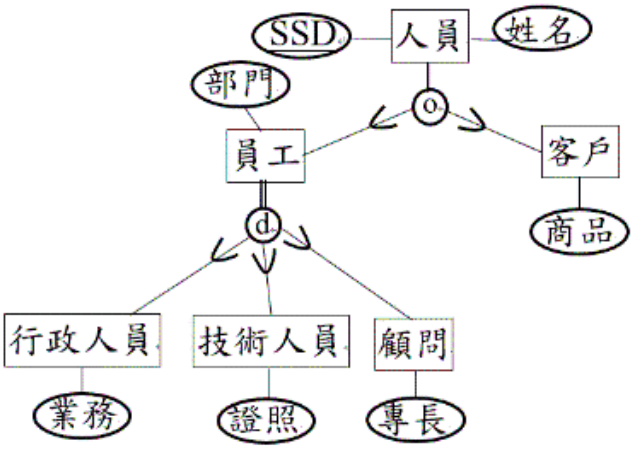
㈠針對圖一之 EERD，以下那些敘述是正確？（20 分）

1. 每一位人員必是員工或客戶。
2. 每一位員工必是行政人員、技術人員或顧問。
3. 可能有人員為員工，也為客戶。
4. 可能有員工為行政人員、為技術人員，也為顧問。
5. 可能有員工為行政人員、也為技術人員，但不為顧問。
6. 可能有人員為員工，但不為客戶。
7. 可能有人員不為員工，也不為客戶。
8. 可能有員工不為行政人員、不為技術人員，也不為顧問。
9. 可能有人員為行政人員，也為客戶。
10. 可能有人員為行政人員、為技術人員，也為客戶。

㈡請將圖一之 EERD 轉換成以關聯式資料庫之表格加以描述，並請結合子型態鑑別器（Subtype discriminator）PType 及 EType，為每位人員判斷其所對應之子類別，同時也正確標示出每一表格的 primary key。當中 PType 及 EType 兩個屬性，分別描述每位人員所屬類別，以及每位員工所屬類別。試列出將該 EERD 轉換後之最適當表格，並標出每一表格之 primary key。（18 分）

㈢試詳細說明如何表示 PType 及 EType 內容。（8 分）

㈣試寫一 SQL 程式片段，以查找出每一位員工之 SSD、姓名、所屬部門及職務類別（行政人員、技術人員、顧問）。（14 分）



圖一