臺灣金融控股股份有限公司 109 年新進人員甄試試題

進用職等／甄試類別【代碼】：8 職等／電腦稽核人員【Q5902】

科目二：網路基礎概論、資訊安全概論及資料庫應用

＊入場通知書編號：＿＿＿＿＿＿＿＿

注意：①作答前應先檢查答案卡（卷），測驗入場通知書編號、座位標籤、應試科目是否相符，如有不同應立即請監試人員處理。使用非本人答案卡（卷）作答者，該節不予計分。
②本試卷為一張雙面，測驗題型分為【四選一單選選擇題 20 題，每題 1.5 分，共 30 分；非選擇題四大題，請參考各題配分，共 70 分】，合計 100 分。
③選擇題限以 2B 鉛筆於答案卡上作答，請選出一個正確或最適當答案，答錯不倒扣；以複選作答或未作答者，該題不予計分。
④非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採**橫式**作答，並請**依標題指示之題號於各題指定作答區內作答**。
⑤**請勿於答案卡（卷）上書寫應考人姓名、入場通知書編號或與答案無關之任何文字或符號。**
⑥本項測驗僅得使用簡易型電子計算器（不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝（錄）影音、資料傳輸、通訊或類似功能），且不得發出聲響。應考人如有下列情事扣該節成績 10 分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。
⑦**答案卡（卷）務必繳回，未繳回者該節以零分計算。**

壹、四選一單選選擇題 20 題（每題 1.5 分）

【4】1.非鍵屬性(Nonkey Attribute)藉由另一個非鍵屬性功能相依於主鍵，稱為下列何者？
①非鍵相依(Nonkey Dependency)
②部分相依(Partial Dependency)
③資料相依(Data Dependency)
④遞移相依(Transitive Dependency)

【4】2.請問建構資料庫時，可利用下列何種程序減少資料重複儲存的問題？
①結構化 ②物件化 ③模組化 ④正規化

【1】3.請問大數據單位 Terabyte (TB)為下列何者？
① 10^{12} byte ② 10^{15} byte ③ 10^{18} byte ④ 10^{21} byte

【2】4.請問關聯式運算(Relational Operations)的結果型態為何？
①數值(Numeric Value)
②表格(Table)
③資料屬性(Data Attributes)
④陣列(Array)

【1】5.在資料庫系統中，若其檔案中資料結構有更動時，用來處理此檔案的程式通常不需要加以變動，此為資料庫的何種特性？
①獨立性 ②完整性 ③分散性 ④安全性

【3】6.若要加快資料搜尋及排序的速度，我們可在資料表中經常作搜尋或排序的欄位上，設定下列何者？
①目錄 ②查詢 ③索引 ④標記

【2】7.請問關聯式資料庫查詢語言的理論基礎為下列何者？
① Normalization Theory
② Relational Algebra
③ Functional Dependency
④ Join Dependency

【2】8.一張實體關聯圖(Entity Relationship Diagram)係使用下列何種圖形來代表屬性？
①矩形 ②橢圓形 ③鑽石形 ④三角形

【2】9.下列何者不是資料庫交易(Transaction)的特性？
①單元性(Atomicity) ②完整性(Completeness)
③隔離性(Isolation) ④永久性(Durability)

【4】10.應用程式在處理資料時，常需要一連串的步驟一起處理完成，如果某一個步驟無法完成，則可利用下列資料庫管理系統的何種指令，協助其回復成原來未執行前的狀態？
① Committed ② Goback ③ Return ④ Rollback

【3】11.正規化資料庫到第三正規化會產生下列何種結果？
①資料表變少
②資料行變多
③資料不易重複
④查詢變得更容易

【4】12.在關聯式資料表中，表內所呈現的外來鍵(Foreign Key)欄位值，請問有何限制？
①須為唯一的(unique)，且不可為空值(null)
②須為唯一的(unique)，且可為空值(null)
③無須為唯一的(unique)，且不可為空值(null)
④無須為唯一的(unique)，且可為空值(null)

【4】13.請問實體關聯圖(Entity Relationship Diagram)是以下列何者為主？
①處理為主 ②流程為主 ③物件導向為主 ④資料為主

【1】14.在 SQL 語言中用來修改表格定義的指令為下列何者？
① ALTER TABLE
② CHANGE TABLE
③ MODIFY TABLE
④ UPDATE TABLE

【3】15.物件導向式之 UML 語言中，何種圖形可用於設計資料庫之結構？
①循序圖(Sequence Diagram)
②使用者案例圖(Use case Diagram)
③類別圖(Class Diagram)
④部署圖(Deployment Diagram)

【3】16.觸發程序(Trigger)在何時會執行程式？
①需要使用者自行呼叫
②資料查詢時會自動執行
③資料新增、修改或刪除時會自動執行
④需要前端應用程式的呼叫

【3】17.請問下列何者是兩個關聯之間的完整性限制？
①領域完整性限制
②實體完整性限制
③參考完整性限制
④鍵值完整性限制

【4】18.請問下列何者是對資料的新增、修改和刪除的語言？
① DDL (Data Definition Language)
② DCL (Data Control Language)
③ DQL (Data Query Language)
④ DML (Data Manipulation Language)

【2】19.對關聯式資料庫的關聯表 R 與 S 做 R JOIN S 之合併，若結果保留 R 中的每個值組(Tuples)，則此合併稱為下列何者？
① INNER JOIN
② LEFT OUTER JOIN
③ RIGHT OUTER JOIN
④ FULL OUTER JOIN

【4】20.在資料庫的實體關係模型中，如果一個實體 A 必須依賴另一個實體 B 的存在才能存在，當實體 B 不存在時，實體 A 亦不存在，這樣的實體 A 可以稱為是下列何種實體？
①子實體(Sub Entity)
②軟實體(Soft Entity)
③強實體(Strong Entity)
④弱實體(Weak Entity)

【請接續背面】

貳、非選擇題 4 大題

第一題：

請回答下列問題：

（一）基於 SNMP 協定所設計的網路管理軟體係位於網際網路四層協定（TCP/IP 協定）堆疊架構中之哪一層？請再列舉兩個運作於該層之網路協定。【5 分】

（二）若網路交換器(switch)未能在 MAC Table 中找到匹配（相同）的目的地(Destination) MAC 位址時，會如何處理該待轉送之訊框(frame)？再者，網路交換器處理待轉送訊框時，會自其標頭(header)中取出來源網卡位址(source MAC address)、連同輸入介面埠號儲存於其 MAC Table 中。請問此舉之作用（目的）為何？【6 分】

（三）當 IP 網路中的某個節點（主機或路由器）要傳送數據封包(packet)至下一個節點，但是原封包超過與下一個節點之鏈結(link)的最大傳輸單元(maximum transfer unit, MTU)時，該節點會對此封包做何處理？【4 分】

第二題：

請回答下列問題：

（一）已知四個連續的 Class C 網路「214.40.64.0，214.40.65.0，214.40.66.0，214.40.67.0」合併後構成一個超網絡(supernetwork)，此超網絡代表名稱及超網路遮罩(supernet mask)分別為何？【5 分】

（二）若已知一乙太網路群播硬體位址(Multicast MAC address)為「01:00:5E:0C:01:01」，則總計會有哪些 IP Multicast addresses 會轉換成與此相同的群播硬體位址？【10 分】

（三）目前的網際網路中，路由器(router)依據 IP 位址來轉送數據封包(packet forwarding)，但是除了參看 Source 及 Destination IP addresses 之外，還需要什麼資訊才能夠做出正確的判斷，以便將封包有效率的送至目的地網路(Destination IP network)？再者，路由器又為何需要此資訊？【5 分】

第三題：

請說明 Confidentiality、Integrity、Availability 和 Non-repudation 等四項資訊安全要素的意義或內涵。又 TLS(Transport Layer Security)可以提供前述四項要素中的哪幾項？【15 分】

第四題：

假設：

張三之 RSA 公鑰為(e_3, N_3)、而私鑰為 d_3 和

李四之 RSA 公鑰為(e_4, N_4)、而私鑰為 d_4，

其中 N_3 和 N_4 不相等且各為二整數的乘積，雙方都持有對方的公鑰。另有 H( )函數為 Sha256。請回答下列問題：

（一）以目前各國之安全標準而言，以 RSA 運作數位簽章功能時，通常 N_3 應至少幾位元？並列舉一項 N_3 的兩個因數應有特性。【4 分】

（二）張三要送一份資料 M(其大小為 16 Bytes)給李四，且希望只有李四能取得其內容，請寫出張三與李四各自的做法與運算過程（核心計算請列數學式）。【6 分】

（三）張三要送一份資料 M(其大小為 1G Bytes)給李四，而李四不但能判斷訊息內容為張三所送無誤，張三亦不能否認 M 為其所送，請設計一有效率的方法並寫出張三與李四各自的做法與運算過程（核心計算請列數學式）。【10 分】