《資料處理》

試題評析

今年考題命題範圍涵蓋資料庫、系統分析及物件導向三個領域，但卻沒有出現網路方面的題目，以試題難度來說，考題內容比往年困難，今年考生不易作答，除第三、五題較容易之外，其餘三題均不易作答，預估今年得分比往年低，中間考生可能有45分，實力佳者應可有60分以上。

依據近幾年試題範圍及目前資訊運用趨勢來看，建議本科的準備方向可針對資料庫(含交易管理)、網際網路(含電子商務)、物件導向、傳統系統分析等四個領域。

第一題：物件導向的四種類別區分，對多數考生來說可能很陌生。

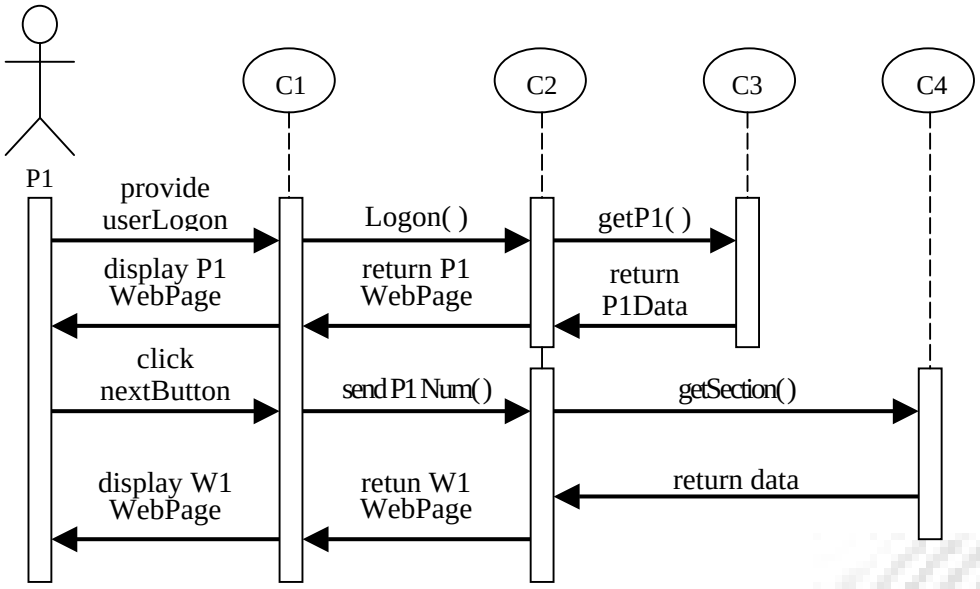
第二題：資料庫安全題目，看似簡短，實則是電腦駭客入侵的安全漏洞，屬網站架設資料庫須注意的實務應用，一般考生甚難作答。

第三題：黑箱及白箱測試是系統分析一般性題目，在其他特考中常見。

第四題：資料庫並行交易屬資料庫進階運用，內容則延續93年度兩階段鎖定的提醒，考生應有所準備。

第五題：RAID常見於資料庫復原所採用的儲存技術，觀念易懂，但對高等級的RAID5、6不易區分清楚。

一、請分別說明下列物件導向模式(object-oriented paradigm)四種類別(classes)之作用：entity classes，interface classes，abstract classes，control classes？下圖中的類別（C1至C4）分別屬於那一類別？請說明為什麼。（20分）



答：

(一)entity classes：實體類別，是問題領域類別的設計識別碼，換言之，它來自領域模型。這些物件通常是被動的，因爲必須等到有事件發生時它們才會執行某些作業。另外，它們通常也是永續存在的類別。例如本題中的C3、C4。

(二)interface classes：介面類別，是經過專門設計，出現在系統自動化邊界上的類別。在桌上型系統中，這些類別指的是視窗類別以及與使用者介面相關的所有其他類別。例如本題中的C1。

(三)abstract classes：抽象類別，一種不能初始化的類別(即不能建立物件)，存在的目的只是爲了讓子類別能夠繼承它的屬性、方法及關聯。

(四)control classes：控制類別，存在於邊界類別與實體類別之間。換言之，它的責任是擷取來自於邊界類別物件的訊息，並將他們傳給正確的實體類別物件。它扮演的角色有點類似交換機或控制器，位於檢視層與領域層之間。例如本題中的C2。

二、請舉例說明下列程式有何安全上之漏洞？並說明如何修補該安全漏洞。（20分）

```
Dim sq1
Sq1=”SELECT*FROM WebUsers WHERE Username=’ ” & username &”’
        AND password=’ ” & password &”’ ”
Set rs=Conn.OpenRecordset(sq1)
If not rs.eof()then
  ‘connect successfully’
end if
```

答：

本題屬於SQL Injection題型，是從安全的角度來看駭客是如何攻擊資料庫，以及防範之道。

(一)

1.本題原意：是一個典型用於登錄到web site的檢驗機制，通過select語句和資料庫進行匹配，如果匹配成功，則使用者可允許存取資料。

2.安全漏洞：利用改變一個SQL語句成爲另外一種，以本題爲例，可將一個簡單查詢變成了2個查詢。

(1)下例語句看起來沒有什麼問題，但是如果駭客的密碼輸入如下時(請特別注意密碼部份)：

輸入Username爲：Bob

輸入password爲：Aa OR ‘A’ = ’ A’

(2)若原程式中並不對輸入做任何檢查與過濾，則輸入後相對應的SQL語句意思將變成：

```
SELECT *
FROM WebUsers
WHERE Username=’ Bob’ AND password=’ Aa’ OR ‘A’ = ‘A’
```

(3)注意結尾的‘A’ = ’ A’ ，這條語句的結果值是TRUE(真)，由於SQL Injection之故，本處已失去了密碼鑑別作用。駭客只須輸入他們知道的任何用戶名稱就可以完成登錄，已不須要密碼。

(二)修補之道：

驗證用戶的輸入值，重點在於解析查詢語句，要注意原程式裡對參數值的分析，特別是單引號、注釋符號等的過濾，以避免原來的查詢語句被駭客加註其他查詢語句，例如先前舉例的OR語句等。

三、黑箱(Black-Box)測試及白箱(White-Box)測試可用來驗證資訊系統之正確性及完整性，請說明這兩種測試方法的差異性，並舉一實例設計所需之測試案例(test cases)解釋測試流程。（20分）

答：兩者差異及舉例如下

(一)白箱測試

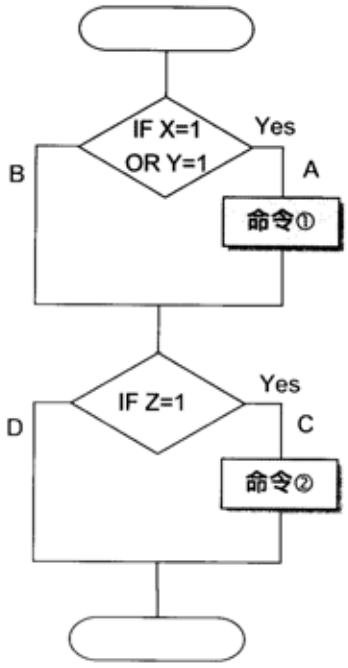
1.方法：追蹤整個系統功能模組內部執行作業指令和決策判斷的方式，根據程式指令與處理邏輯，編造各種可能狀況之測試資料。

2.舉例說明：在下例中可依流程內流設定三個測試案例

(1)X=1, Y=2, Z=1 =>可測試複合條件1及條件2，執行分支A、C

(2)X=2, Y=1, Z=1 =>可測試複合條件1及條件2，執行分支A、C

(3)X=2, Y=2, Z=2 =>可測試複合條件1及條件2，執行分支B、D



(二)黑箱測試

1.方法：不追蹤模組內的指令，只比較輸入和輸出的結果。

2.舉例說明：在下例用來確定年月日錯誤的測試案例

有效類別	無效類別
1999/12/31	1999/12/32
2000/01/01	2000/01/00
2000/02/29	2000/02/30
2000/12/31	XXXX/YY/ZZ

四、考慮二個交易(transaction)T及Q，其內容如下：

Transaction T:
Bank&Withdraw(A, 4);
Bank&Deposit(B, 4);

Transaction Q:
Bank&Withdraw(C, 3);
Bank&Deposit(B, 3);

A, B, C分別表示三個用戶之銀行帳號，Withdraw（提款）及Deposit（存款）並非atomic operation，都包含read operation及write operation。

若同時(concurrent)處理二個交易(transaction)T及Q，請用T及Q的執行過程說明可能會發生的問題？並提出解決方法。（20分）

答：

(一)本題交易T及交易Q不滿足可循序性(serializable)，分析如下

1.題意說明Withdraw及Deposit都包含read(以R表示)及write operation(以W表示)。

2.交易T及交易Q共同使用資料B，亦即不必在意資料A及資料C，只需妥善處理資料B引起的衝突(conflict)問題。

3.交易T的Bank&Deposit(B,4)可簡化成$R_T(B)$、$W_T(B)$

4.交易Q的Bank&Deposit(B,3)可簡化成$R_Q(B)$、$W_Q(B)$

5.若仔細交錯安排$R_T(B)$、$W_T(B)$、$R_T(B)$、$W_T(B)$可得到六種可能次序，本處僅以一種交錯方式來舉例說明：在此處依序爲$R_T(B)$、$R_T(B)$、$W_T(B)$、$W_T(B)$，將出現兩次衝突(conflict)，分別是$R_T(B)$、$W_T(B)$及$W_T(B)$、$W_T(B)$次序時，因此交易T及交易Q不滿足可循序性(serializable)。

時間點	交易T	交易Q
T_1	$R_T(B)$	
T_2		$R_Q(B)$
T_3	$W_T(B)$	
T_4		$W_Q(B)$

(二)解決方法

1.可採取兩階段鎖定(Two-phase Locking)方法，指交易以兩個階段來進行資料鎖定(Lock)與解除鎖定(Unlock)。

2.上例將成爲

時間點	交易T	交易Q
T_1	請求$R_T(B)$的S鎖定	
T_2	取得$R_T(B)$的S鎖定	
T_3	$R_T(B)$	
T_4		請求$R_Q(B)$的S鎖定
T_5	$W_T(B)$	
T_6	COMMIT	取得$R_Q(B)$的S鎖定
T_7		$R_Q(B)$
T_8		$W_Q(B)$
T_9		COMMIT

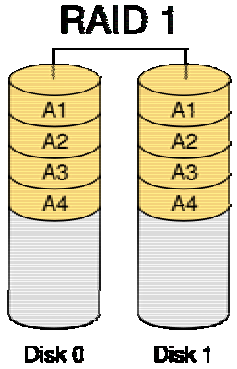
3.結論：運用兩階段鎖定(Two-phase Locking)法，可充許交易T及交易Q仍可採用交錯方式來執行交易T的Bank&Withdraw(A,4)、及交易Q的Bank&Withdraw(C,3)，僅需對交易T的Bank&Deposit(B,4)及交易Q的Bank&Deposit(B,3)進行鎖定。

五、RAID(Redundant Array of Independent Disks)技術用來提高資訊儲存設備之可靠度(reliability)，請說明RAID 1(Disk mirroring)、RAID 5(Byte interleaf with parity checking)、RAID 6(Byte interleaf with double parity checking)之差異性？並舉例說明何種資訊需使用何種RAID技術。（20分）

答：

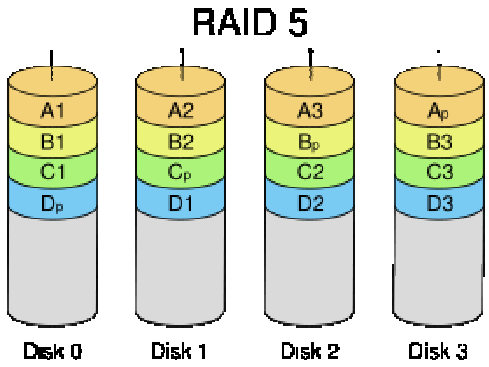
(一)三者的差異說明

1.RAID 1(Disk mirroring)：在主硬碟上存放數據的同時也在鏡像硬碟上寫一樣的數據。當主硬碟損壞時，鏡像硬碟則代替主硬碟的工作。因爲有鏡像硬碟做數據備份，所以RAID 1的數據安全性在所有的RAID級別上來說是最好的。

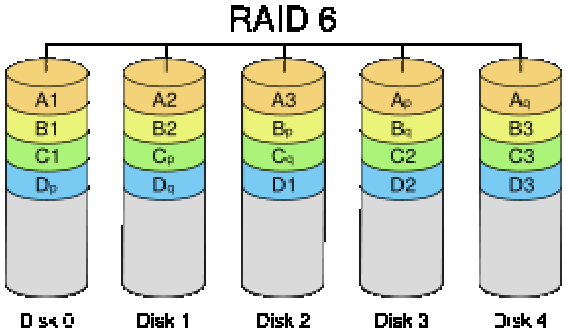


2.RAID 5(Byte interleaf with parity checking)：使用Disk Striping(硬碟分割)技術，RAID 5不對存儲的數據進行備份，而是把數據和相對應的奇偶校驗信息存儲到組成RAID5的各個磁碟上，並且奇偶校驗信息和相對應

的數據分別存儲於不同的磁碟上。當RAID5的一個磁碟數據發生損壞後，利用剩下的數據和相應的奇偶校驗信息去恢復被損壞的數據。



3.RAID 6(Byte interleaf with double parity checking)：與RAID 5相比，RAID 6增加了第二個獨立的奇偶校驗資訊塊。兩個獨立的奇偶系統使用不同的演算法，資料的可靠性非常高，即使兩個磁碟同時失效也不會影響資料的使用。但RAID 6需要分配給奇偶校驗資訊更大的磁碟空間。但較差的性能和複雜的實施方式使得RAID 6很少得到實際應用。



(二)舉例說明使用時機

1.RAID1：適用於要求高數據安全性，且容許較低磁碟利用率的資訊。

2.RAID5：適用於適合於小資料塊和隨機讀寫的資料。RAID 5可以爲系統提供數據安全保障，但保障程度要比Mirror低而磁碟空間利用率要比Mirror高。

3.RAID 6：適用於要求比RAID5更高的資料的可靠性，但需占用比RAID5更多的磁碟空間，但實施方式複雜。