《資料處理概要》

試題評析

第一題：本題屬網路中的資訊安全議題，近年來出現次數漸增，應屬正常準備之範圍，SSL和SET爲常見之機制，但如何辨析二者異同爲得分關鍵。
第二題：無線網路議題一直爲資訊類科之重要考點，此題難度較低，屬敘述性之問法，考生應可輕鬆答題。
第三題：鏈結串列爲資料結構中的基本題型，此題考串列反轉，對C程式語言有基本概念者應可輕鬆應對。
第四題：堆積樹屬於資料結構中高等樹的範圍，雖出現頻率較低，但觀念易懂，若有用心準備資料結構的考生應不難回答。
第五題：和往年相同，出現配分比例重的資料庫議題。此題屬SQL撰寫，但觀念簡單，熟悉Join的考生應可順利答題。

一、SSL（Secure Sockets Layer）為一提供應用程式通訊安全與信賴的協定，請說明：(一)SSL如何建立使用者與服務伺服器間的安全通道，尤其是秘密鑰匙（secret key）的建立方式？(二)SSL與SET的不同處為何？（20分）

答：

(一)此法最初是由Netscape所提出之機制，目的在於確保網路通訊的安全，該機制並非採單一加密方法，共運用RC4、RSA，以及MD5等三種方式，其中RC4和RSA皆屬加密演算法，但前者爲對稱式，後者爲非對稱式。MD5則負責完整性檢驗工作，詳細描述如下：

1.RC4

此演算法最初用以保護商業機密。採用對稱式架構，亦即加解密使用同樣的金鑰，因此使用時須特別保護此密鑰。雖不須額外的輔助機制即可運作，但金鑰交換的過程若有漏洞，將無法發揮保護的效果。運作時，效率較非對稱式佳。

2.RSA

和RC4不同，此演算法屬於非對稱式加密方法，加密和解密使用的金鑰不同，一般而言，加密時使用對方的公開金鑰(Public Key)，解密時藉由自身的私密金鑰(Private Key)。因此，該模式需額外獨立的第三方機構成立認證中心(Certificate Agent, CA)輔助統整與驗證公開金鑰的正確性與時效性。由於此機制較複雜，進行加解密動作時效率較差。

3.MD5

上述的RC4和RSA二演算法目的皆在於保護資料的機密性，但一套加密機制除機密性外，完整性亦爲十分關鍵之議題，MD5便負責此部分的工作，透過訊息摘要(Message Digest)檢驗傳輸過程中資料是否遭未經授權者加以修改。

就運作方式而言，SSL針對資料部分的加密採RC4，充分運用對稱式加解密的效率優勢，而傳送秘密金鑰時，再藉由RSA演算法保護秘密金鑰的安全性。此處採混和式架構之原因在於執行速度，若直接以RSA對資料進行加解密，所需時間會隨資料量增加而顯著成長。

傳輸秘密金鑰前，需先經由認證中心驗證公開金鑰之可用性，而後經由非對稱式加解密演算法完成傳輸，接收端藉由私密金鑰(Private Key)解密該訊息後便可獲得此次傳輸的秘密金鑰(Secrete Key)，解密前可先透過MD5驗證接收之密文是否具完整性，若經他人修改則可要求發送端重新傳輸，以確保後續資料傳輸的機密性。完成密鑰交換後，收送雙方往後皆可透過此密鑰進行資料加解密。

(二)SET全名爲安全電子交易(Secure Electronic Transactions)，由VISA和Mastercard二大信用卡公司共同推出的網際網路商業交易標準。主要用於確保網際網路信用卡交易的資訊安全，透過持卡者、商店憑證及數位簽章確認消費者和商家之身份。以下將針對目的、機密性、完整性、不可否認性以及隱私性等向度和SSL進行比較：

	SSL	SET
目的	確保一般資訊傳輸的機密性與完整性	保護電子商務交易各方的權益與隱私
機密性	秘密金鑰透過RSA保護，資料透過RC4保護	秘密金鑰透過RSA保護，資料透過DES保護
完整性	透過MD5達成	透過SHA-1達成
不可否認性	未提供	透過數位簽章達成
隱私性	未提供	採雙重簽章機制，使商家無法得知消費者資訊，收單者無法取得訂單內容

二、無線區域網路（Wireless LAN）將推動網際網路進一步的發展，請說明無線區域網路有何優勢？（10分）

答：

無線區域網路提供使用者不受拘束的最後一哩(Last Mile)服務，隨著技術的發展，逐漸衍生出眾多重要的服務，以下將就頻寬、便利性、穩定性、普及性及成本等因素分別探討：

(一)頻寬

早期無線網路頻寬較小，無法和有線網路相提並論，僅適用於極小量資料傳輸，但隨著無線區域網路的技術演進，目前802.11n標準藉由MIMO硬體架構的改變，在4x4天線架構下理論值可達540 Mbps，可媲美有線網路的規格。

(二)便利性

無線網路的特性在於傳輸介質爲電磁波，不需透過封閉式的線材，只需使用者進入訊號範圍即可，使用時亦不需受限於固定範圍，可於特定區間內自由活動，便利性佳。

(三)穩定性

無線區域網路發展之初，訊號穩定性仍舊不足，當連線至同一無線存取點的使用者數量過高時，常出現斷線或找不到網路的情況，但近年來針對通訊協定服務品質(Quality of Service)進行控管的機制日益進步，當管理者設定正確參數後，在大量使用者存取的情形下依然可維持一定的服務水準。

(四)普及性

時至今日，無線區域網路的普及性相當高，以台北市爲例，熱點覆蓋率已達九成，加上近日台北市政府開通的公共場所免費Wi-Fi上網，雖然頻寬僅512 Kbps，但此舉更將無線網路深入至民眾的日常生活。

(五)佈建成本

對於網路規畫者而言，成本是不可避免的先天限制。若欲佈建的範圍較大，且場地不易佈線時，許多規劃者便會使用無線網路作爲解決方案，因其建置之總成本較低，不需大費周章的更動既有的裝潢或硬體設備，不失爲一種良好的選擇。

【高分閱讀】
1.石濟，資料處理講義3-2，第二小節。
2.石濟，資料處理講義3-2，第三小節。

三、一個鏈結串列使用C語言宣告如下：

```
typedef struct node {
  int data;
  struct node *next;
} NODE;
```

假設現在已經產生一個共有n個節點的NODE的鏈結串列，已知變數pointer是指向該串列前端（head）之指標，請撰寫一程序將pointer所指向的串列，整個串列進行反轉。（15分）

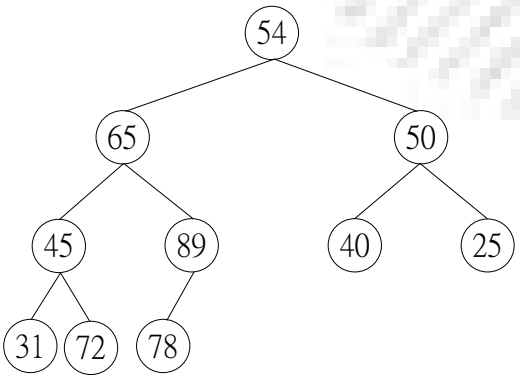
答：
下列程式將反轉原本由pointer所指向之串列順序

```
node *reverse(struct node *pointer, int n)
{
        struct node *end=pointer->next,temp;
        int i=0;
        pointer->next=NULL;
        for(i=1;i<n;i++)
        {
                temp=end;
                end=end->next;
                temp->next=pointer;
                pointer=temp;
        }
        return end;
}
```

【高分閱讀】
1.石濟，資料處理講義2-2 。

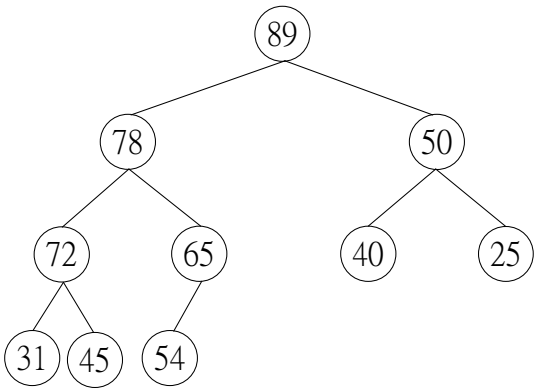
四、給定一個數列54, 65, 50, 45, 89, 40, 25, 31, 72, 78。（15分）
（一）畫出對應二元樹（Binary Tree）。
（二）請將這二元樹轉換成堆集樹（Heap Tree）。
（三）在使用堆集排序（Heap Sort）的前二個步驟後可輸出89和78兩數，請畫出在經過該二個步驟後的堆集樹。

答：
(一)
由上而下，由左至右依序加入節點至二元樹，結果如下所示：



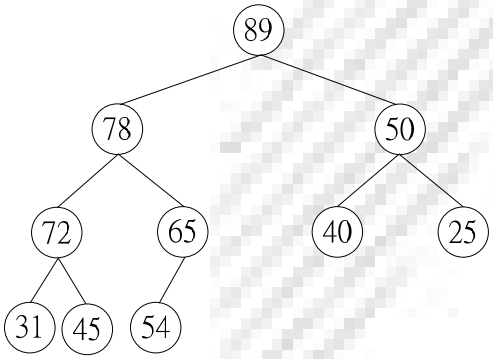
(二)
堆積樹(Heap)是一個完整二元樹，可分爲最大堆積樹(Max Heap)和最小堆積樹(Min Heap)，最大堆積樹意指所有父點之值皆大於等於子點之值，亦即樹根具最大值；相對的，最小堆積樹則表示所有父點之值皆小於等於子點之值，樹根具最小值。前題是建立二元樹時已將之設爲完整二元樹，故此處僅需將其結構改爲符合定義之形式。
調整的方式可分爲由上而下(Top down)或由下而上(Bottom up)二種，由上而下意指建立時，每次插入一節點

便調整一次，使之持續滿足heap的限制，但此處已建立完整二元樹，因此將使用由下而上的方式建立。此處以最大堆積樹爲例，如下所示：

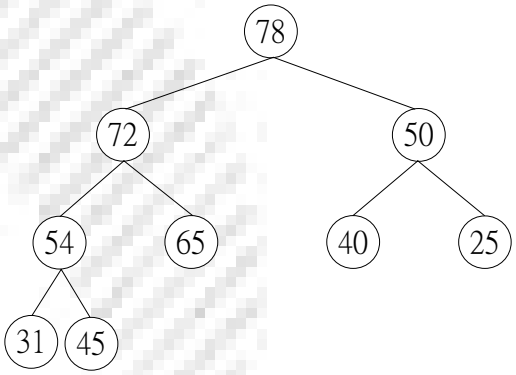


(三)每次將最大值，即樹根刪除，並將最後一個節點移至樹根處，整個結構再進行調整，過程如下：

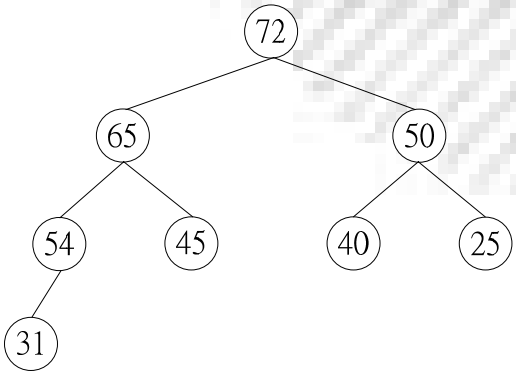
1.原始最大堆積樹



2.刪除89後



3.刪除78後



五、假設某圖書館之關聯資料庫中有七個關聯資料表，其資料綱要（data schema）如下，底線代表主要鍵。

BOOK (BookId, Title, PublisherName)
BOOK_AUTHORS (BookId, AuthorName)
PUBLISHER (Name, Address, Phone)
BOOK_COPIES (BookId, BranchId, No_Of_Copies)
BOOK_LOANS (BookId, BranchId, CardNo, DataOut, DueDate)

LIBRARY_BRANCH (BranchId, BranchName, Address)
BORROWER (CarNo, Name, Address, Phone)
寫出以下查詢之SQL：(40分)
(一)該圖書館的所有分館各擁有多少本書名為“三國演義”的書？
(二)現在那些借閱人在各分館借出“三國演義”這本書？
(三)現在那些借閱人在各分館有逾期未還的書？
(四)該圖書館擁有多少不同的書籍？

答：

(一)

SELECT BranchId, No_Of_Copies, COUNT(*) AS Number FROM BOOK, BOOK_COPIES, LIBRARY_BRANCH WHERE BOOK.Title = '三國演義' and BOOK.BookId = BOOK_COPIES.BookId and LIBRARY_BRANCH.BranchId = BOOK_COPIES.BranchId GROUP BY BranchId

(二)

SELECT Name, BranchId FROM BOOK, BOOK_LOANS, LIBRARY_BRANCH, BORROWER WHERE BOOK.Title = '三國演義' and BOOK_LOANS.BookId = BOOK.BookId and BOOK_LOANS.BranchId = LIBRARY_BRANCH.BranchId and BOOK_LOANS.CardNo = BORROWER.CardNo and BORROWER.DateOut<= getdate()

(三)

SELECT Name, BranchId, Title FROM LIBRARY_BRANCH, BOOK_LOANS, BOOK, BORROWER WHERE BOOK_LOANS.BookId = BOOK.BookId and BOOK_LOANS.BranchId = LIBRARY_BRANCH.BranchId and BOOK_LOANS.CardNo = BORROWER.CardNo and BORROWER.DueDate<= getdate()

(四)

假設同一出版社不會出版多本相同名字的書，則SQL可爲：
SELECT Title, PublisherName, COUNT(*) AS Number FROM BOOK, GROUP BY Title, PublisherName

【高分閱讀】
1.石濟，資料處理講義4-5，第一小節。
2.石濟，資料處理講義4-5，第二小節。