《資料處理》

試題評析	今年地特題目相對來說題目較少，在正常情況下考生應該會有更多作答時的思考時間，且多數題目考點明確無多餘的變化，我認為今年考題相較往年來說為相對簡單的一年。當然試卷第二題的SQL我認為若考量實際執行層面是有難度的，因為在不同SQL與法版本中可能會有不同的答案，但無法確定出題者是否有考量到此點。然而除此點外，整體而言試卷難度不高，各題申論成分較少且皆屬於有正確標準答案的試題類型，因此可以預期準備充分的同學可以獲得相當不錯的成績。

一、加密系統是面對資訊安全威脅的一項資訊技術防護措施。

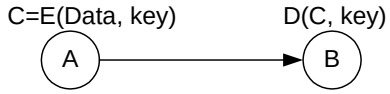
(一)請說明對稱性加密與非對稱性加密的區別。（10 分）

(二)請以https 協定的SSL/TLS 為例，說明私鑰（Private Key）與公鑰（Public Key）的運作方式。（15 分）

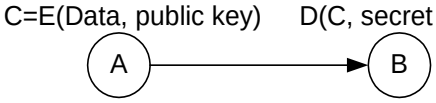
試題評析	此題為資訊安全中的理論題，考題為常見資料加密方法中對稱與非對稱式金鑰的基礎理論與一個另一個常見的網路通訊安全協定SSL，考題難度上基本上不難，同學只須注意敘述答題方式即可，此類題目建議以條列式回答為佳
考點命中	【高點・高上資料處理講義】第二回，黃浩哲編撰，頁206~209。

答：(一)

1.對稱式金鑰(Symmetric key)：收送方擁有相同的私鑰(private key)，加解密使用相同鑰匙，適合用於大量資料加解密，例如：DES、IDEA



2.非對稱性金鑰(Asymmetric key)：加解密使用不同鑰匙；公鑰用來加密，私鑰用來解密，適合用於少量資料加解密，例如：RSA



(二) SSL 是數位信封的應用，是目前最被普及利用的安全機制，主要的安全防護程序如下：

1.Server 端(例如 Amazon)將自己由 CA 所發給的電子憑證傳送給Client 端(例如消費者的PC)

2.Client 端的 Browser(例如 IE)，其儲存有世界主要 CA 的公鑰，可利用此來解開 Server 的電子憑證，取得其內部的企業資訊與其公鑰。

3.Client 端的 IE 會隨機產生一個對稱式的秘密金鑰，SSL 利用此金鑰對內文加密，再利用 Server 端的公鑰對秘密金鑰加密，形成數位信封。

4.Client 端將密文與數位信封(亦即利用企業公鑰加密保護的秘密金鑰)，一起傳送給 Server。

5.Server 端以自己的私鑰解開數位信封內的秘密金鑰，再以秘密金鑰解開內文。

二、請透過下列三個有關期中考的資料表（Tables），使用SQL 查詢“王教授”的課程編號ID為“A123”課程，其班級總分與最後一名的學生姓名。（t 代表Teacher 資料表名稱；s 代表Student 資料表名稱；e 代表Exam 資料表名稱）。（25 分）

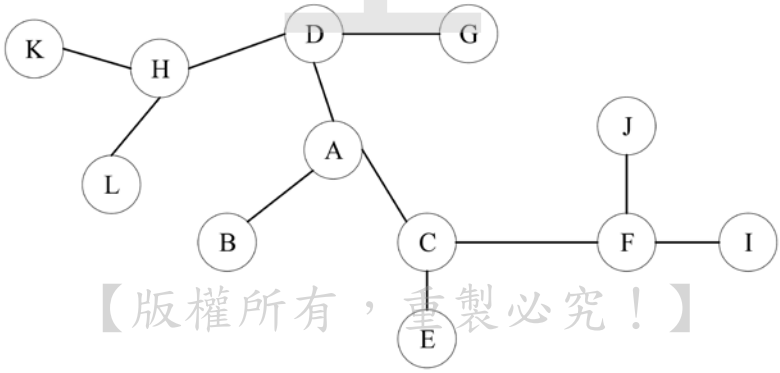
Teacher [TeacherID , TeacherName , ClassID]
Student [StudentID, StudentName, ClassID]
Exam [ExamName, StudentID, Subject, Score]

試題評析	此題幾乎每年必考的資料庫語法實作題，我認為若排除題目本身有缺陷的情況則屬於較難的類型，因為提議中所敘述的"班級總分"與"學生姓名"在SQL聚合語法中是邏輯上衝突的，因此實務要達成題目要求結果需藉由多個JOIN創造額外的Table來規避掉SQL聚合函數限制的問題，同學在回答類似考題時須特別注意此類衝突，因為邏輯上可能很簡單，但實際上直覺的SQL語法可能無法得到正確結果。
考點命中	【高點・高上資料處理講義】第三回，黃浩哲編撰，頁92~96、頁98~102

答：

```
SELECT TOP 1 Main.ClassToatl AS 班級總分, Main.StudentName AS 學生姓名
FROM (Student AS s
INNER JOIN Teacher AS t
ON s.ClassID=t.ClassID
INNER JOIN Exam
ON s.StudentID=e.StudentID) AS Data
INNER JOIN
 (SELECT t2.ClassID, SUM(e2.Score) AS ClassToatl
 From Exam AS e2
 INNER JOIN Student AS s2
 ON  e2.StudentID=s2.StudentID
 INNER JOIN Teacher AS t2
 ON s2.ClassID=t2.ClassID
 WHERE t2.TeacherName LIKE '王教授' AND t2.ClassID LIKE 'A123'
 GROUP BY t2.ClassID) AS TotalClassScore
ON Data.ClassID=TotalClassScore.ClassID AS Main
ORDER BY Main.Score ASC;
```

三、在人工智慧與機器學習領域，狀態空間表示一個問題的所有可能解的集合，如下圖所示。請從狀態A 開始，以字母排序的先後順序，用兩種常用的演算法：廣度優先搜尋（Breadth-First Search, BFS）與深度優先搜尋（Depth-First Search, DFS），分別列舉搜尋的結果。（25分）



試題評析	此題為資料結構中圖形演算法的實作題，題目除考深度與廣度搜尋外並未加入過多的變化，因此難度來說相當簡單，同學僅需照提議要求排出搜尋順序即可，作答時須注意題目中有要求深度/廣度一致時要以字母為優先順序。
考點命中	【高點・高上資料處理講義】第二回，黃浩哲編撰，頁74~75、頁93。

答：

BFS：{ABCDEFGHIJKL}

DFS：{ABCEFIJDGHKL}

四、請列舉“This is a book”中間有空格的連續字串，經過下列程式執行後，兩個printf 的輸出內容。（25 分）

```
#include <stdio.h>
#include <string.h>

void reverse(char str[], int start, int end) {
    char temp;
    while (start < end) {
        temp = str[start];
        str[start] = str[end];
        str[end] = temp;
        start++;
        end--;
    }
}

int main() {
    char str[] = "This is a book";
    int len = strlen(str);

    reverse(str, 0, len - 1);
    printf("%s\n", str);

    int word_start = 0;
    for (int i = 0; i < len; i++) {
        if (str[i] == ' ') {
            reverse(str, word_start, i - 1);
            word_start = i + 1;
        }
    }

    reverse(str, word_start, len - 1);
    printf("%s\n", str);
    return 0;
}
```

試題評析	此題為程式實作題，相較於以往要求同學寫出程式碼，今年的考題則要求同學列出結果即可，因此以同樣25分配分來說難度是相對簡單許多，建議同學在解此類題目時可以盡量將每行程式碼執行後結果列出，如此在答題與檢查上會更加簡單。
考點命中	【高點・高上資料處理總複習講義】，黃浩哲編撰，頁16~20。

答：

第一個Printf輸出：”koob a si sihT”

第二個Printf輸出：” book a is This”