《資料處理概要》

試題評析

今年普考資料處理試題如同往常，資料庫佔了相當比重之分數，除此之外，網路、資料結構、資訊安全也各出現一題。

試題中第一題雖爲SQL題型，但爲較少出現之資料控制語言，但若有接觸者應不難回答；第三題資料結構較爲複雜，分數可能較難掌握，其餘二、四、五題同學們應可掌握得不錯。

估計一般同學本試題可能約在60分左右，程度較佳同學可在70~80分以上。

一、請利用SQL所提供的資料控制語言指令，寫出下列兩小題之語法：

(一) 授權User1、User2、User4等3位使用者對於Emp_view資料表享有SELECT、INSERT、DELETE之權力。（10分）

(二) 撤銷User3及User5等2位使用者對於Emp_view資料表執行INSERT及UPDATE之權力。（10分）

答：

(一)GRANT SELECT, INSERT, DELETE ON Emp_view TO User1, User2, User4

(二)REVOKE INSERT, UPDATE ON Emp_view FROM User3, User5

二、請說明關連式資料庫系統中的標準化格式與資料庫設計之間的關係。如何將資料庫，由2NF轉為3NF？（20分）

答：

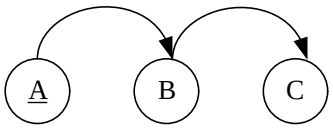
(一)關聯式資料庫的兩個重要資料整合性爲個體整合性限制，以及參考整合性限制；資料庫雖希望降低資料之重複性，但資料仍非完全未重複，如關聯之外鍵，必於其他關聯存在相對應的值；而外鍵與其參考之對象，資料格式應相同，否則較難管理亦容易產生不一致現象。建立標準化資料格式後，資料庫設計時，各關聯使用到之相同資訊，皆可使用標準之資料格式從事定義。

此外，標準化資料格式亦可限制資料之合法性，使資料內容符合資料庫設計時之規範，如身分證字號、員工編號等欄位之標準，不會出現不合法之資料，亦不會出現如多值屬性等不符合基本1NF之資料。

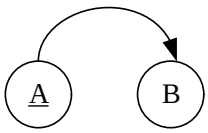
(二)2NF中，所有非主鍵之屬性已完全功能相依於主鍵，只要在該關聯中，找出所有遞移相依於主鍵之屬性，將其拆出，即可轉爲3NF。

如下例關聯R中，屬性C遞移相依於主鍵，將關聯拆爲R1、R2後，即滿足3NF。

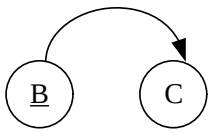
R:



R1:



R2:



三、假設有兩字串（strings）$A=A_0A_1A_2A_3\cdots A_n$及$B=B_0B_1B_2B_3\cdots B_m$，如何使用陣列找出兩字串中，最長的共同子字串？（20分）

答：

可使用二維陣列+遞迴方式實作。

陣列的大小需爲 $n \times m$，其中 n, m 分別爲輸入兩字串的長度。

題目中，兩字串分別爲$A=A_0A_1\cdots An$, $B=B_0B_1\cdots Bm$；

設L[i, j]爲$A= A_0A_1\cdots Ai$, $B= B_0B_1\cdots Bj$的最長共同子字串，其中$1\le i \le n$且$1\le j \le m$

則L[i, j] = 0 (if i = 0, or j = 0) //說明：若字串已走完，則共同字串爲零

= L[i-1, j-1] + 1，(if i , j > 0 and Ai = Bj) //說明：若兩字串該值相等，則將其加入陣列中，兩字串各推一步繼續判斷

= max(L[i, j-1], L[i-1,j]) if i , j > 0 and Ai ≠Bj //說明：若兩字串該值不相等，則A,B值分別推一步判斷最長共同子字串後，取兩者較長之陣列。

以遞迴方式重複尋找個子字串，即可得到A、B兩字串之最長共同子字串。

四、ISO將網路通訊協定分為那七層？請問一般市售的網路卡包含那些層的通訊協定？一台主機若無IP位址，是否可以經由其網路卡傳送網路訊息？為什麼？（20分）

答：

(一)ISO/OSI共分爲以下七層

1.實體層(Physical Layer)

在通訊頻道上傳輸原始位元資料。多在處理機械、電子和程序上的介面，以及實際傳輸的媒介。

2.資料鏈結層(Data Link Layer)

將資料傳送到線上，作網路上點對點(point-to-point)的錯誤控制(error control)及流量控制(flow control)。

3.網路層(Network Layer)

決定封包如何由原始點繞(route)至目的地，即從事路徑選擇(routing)及壅塞控制(congestion control)。網路層允許異質網路彼此間互相連結。

4.傳輸層(Transport Layer)

從事端對端(end-to-end)的錯誤控制(error control)及流量控制(flow control)，建立整條連線。

5.會議層(Session Layer)

從事記號管理(token management)及同步(synchronization)。負責端對端會談期間的連線，以及確保此期間資料傳輸的順暢。

6.展示層(Presentation Layer)

處理傳輸資訊的語法及語意(表現方式)。從事資料加密/解密，壓縮/解壓縮。

7.應用層(Application Layer)

虛擬網路終端機軟體的應用，使用者定義之服務，如WWW、HTTP、FTP、TELNET等。

(二)市售之網路卡一般使用TCP/IP協定，其中TCP於OSI的傳輸層，IP屬於OSI的網路層。

五、要讓公開金鑰密碼（Public-Key Cryptosystem）機制能順利地進行，一個公正且可信賴的認證中心（Certification Authority）是不可或缺的，請舉例說明公開金鑰密碼機制的運作流程，並說明為何需要認證中心的存在？（20分）

答：

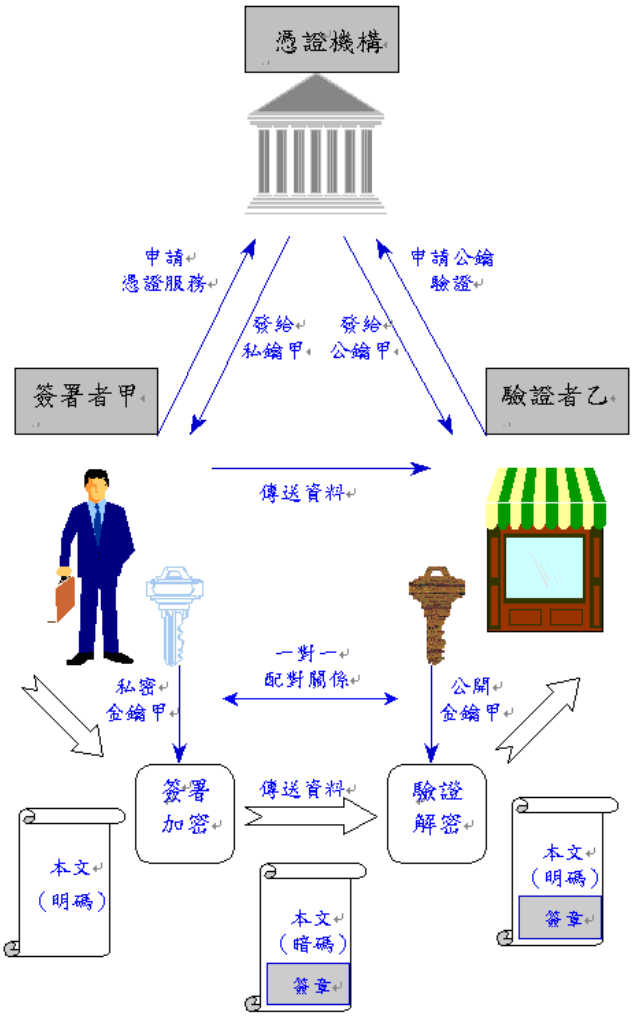
(一)運作流程

欲簽署憑證之一方(簽署者甲)，須先向CA提供資訊申請憑證服務，CA核定後發予其私密金鑰；欲驗證甲身分之驗證者乙，可向CA申請公鑰驗證，則CA將甲之公鑰發予驗證者。

之後，甲以其個人私鑰加密傳輸至乙方，乙方若能以甲之公鑰將內文解出，則可確認甲之身分。

此後雙方可以此對公私鑰進行資料傳輸。

運作流程圖示如下：



(二)所謂認證中心（Certification Authority，CA）指提供數位簽章製作及電子認證服務之機構。CA必須依據電子簽章法之相關管理規定及標準，提供相關憑證服務：包括審驗憑證申請人身分、資格與屬性，發給申請人私密金鑰，並且簽發公開金鑰憑證，以供驗證其公開金鑰及私密金鑰之配對關係，證明身分及確保安全。簡單言之，憑證機構便是扮演網路環境中的「戶政事務所」角色，負責個人身分審核並發給身分證明，以確保網路交易或資料傳輸時，雙方身份的確認，避免冒充身分之交易者。