

《資料處理》

試題評析：

今年考題除了第二題在答題上較為複雜外，其餘題目之議題同學們應皆有涉獵，資訊安全、Java/C語言、資料庫皆為近幾年常見之考題，一般同學應在40分左右，程度較佳者可拿到50分以上。

一、要保護Web網站的安全，必須考慮可能存在於Web Server、Browser及Web applications 的安全漏洞，請舉例說明這些可能存在的安全漏洞為何？應如何防範這些漏洞對Web網站所造成的安全威脅？（20分）

答：

(一)可能安全漏洞

1. 網頁上的惡意程式、間諜程式：例如惡意之ActiveX， Javascripts。
2. 線路竊聽(Wire tapping， sniffing)：透過在通訊線路上搭線之方式竊取傳送之資料。
3. 攻擊程式撰寫不嚴謹之網站：如SQL Injection， 嵌入不合法之程式語法。
4. 阻斷服務 (Denial-of-Service， DoS)：在一段期間內透過大量且密集的封包傳送，達到使被攻擊的網站無法處理，以致許多正常想要連上該網站的用戶，都被阻絕在外，連不上該網站。
5. 主機假冒(Spoofing)：假冒合法機器以欺騙受攻擊的主機，取得其信任，進而取得其所需資源或權限。方式如：硬體位址(ARP)假冒、IP位址假冒、TCP連線假冒、路徑資訊假冒、主機名稱假冒、服務假冒等。
6. 潛入系統禁區(Trap doors)：破壞密碼，非法侵入機密領域，例如非法連結後端資料庫伺服器。
7. 實體安全防護不足：如機房、門禁措施不足。

(二)防範措施

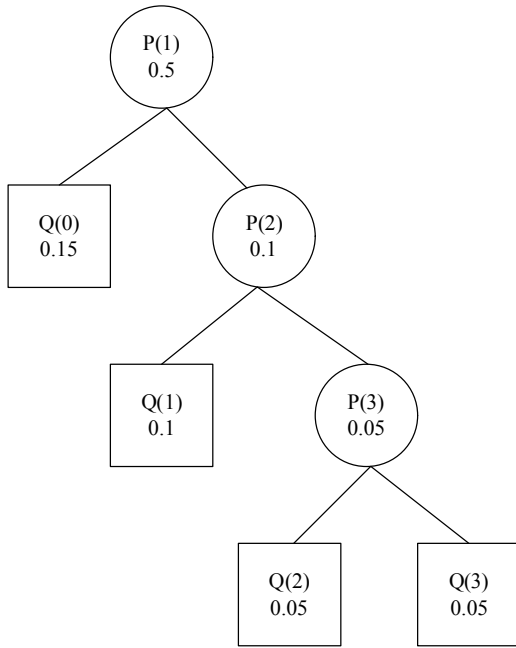
1. 安裝防火牆：對網路流經的通訊進行掃描，它能過濾掉部分的電腦病毒及一些駭客對本地網路的攻擊。此外，防火牆也可以透過防止由特定節點流出任何內部通訊，或禁止一些來自特殊網站的瀏覽，以達到保護內部區域網路及個人電腦的目的。
2. 資料加密：透過SSL等網路加密方式，對網路上傳輸之資料從事加密，避免資料遭攔截、竊聽。
3. 電子簽章：網路交易透過電子簽章確認雙方身份，避免主機假冒。
4. 強化員工訓練、實體安全防護。

二、請說明何謂最佳化二元搜尋樹 (Optimal Binary Search Tree)？何種應用 (application) 適合使用最佳化二元搜尋樹為其資料結構？請以下列例子說明如何建立其對應之最佳化二元搜尋樹： $P(1)=0.5, P(2)=0.1, P(3)=0.05, Q(0)=0.15, Q(1)=0.1, Q(2)=0.05$ and $Q(3)=0.05$ 。（20分）

答：

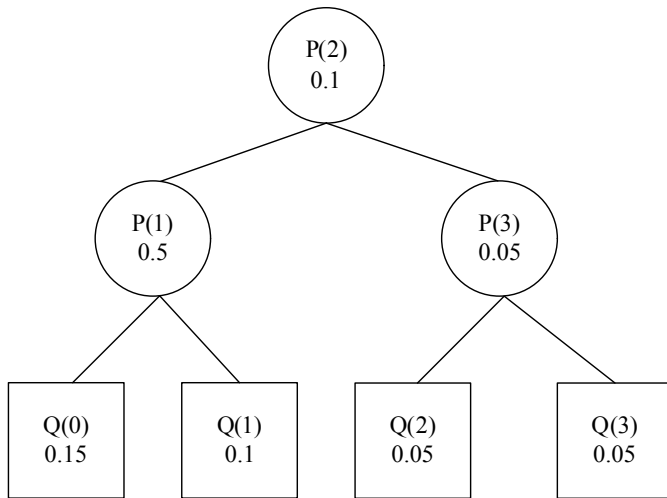
- (一)最佳化二元搜尋樹 (Optimal Binary Search Tree)，就是要找出搜尋成本最小的二元搜尋樹，其中每個節點各有其出現權重，代表其會被查詢到的次數(機率)。最佳化二元搜尋樹就是要找出最佳的樹狀結構，使這些元素安排到適當位置後，每個元素查詢次數乘以元素深度總和(即查詢花費總和)，和需為最小。
- (二)在樹狀結構不會改變，且每筆之資料搜尋機率(即權重)已知時，最佳化二元搜尋樹可將資料之平均搜尋成本降至最低。
- (三)題目之例子共有以下五種可能二元搜尋樹狀結構，其中第一種之成本總和最小，故其為最佳化二元搜尋樹。

1.



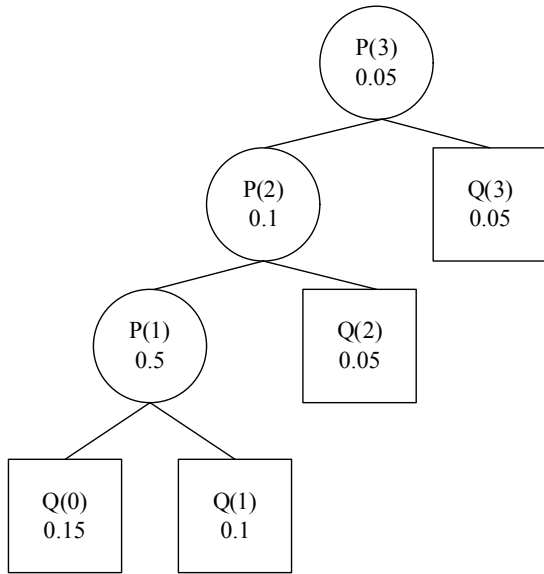
$$\text{成本} = (0.5 + 0.1 \times 2 + 0.05 \times 3) + (0.15 + 0.1 \times 2 + 0.05 \times 3 + 0.05 \times 3) = 1.5$$

2.



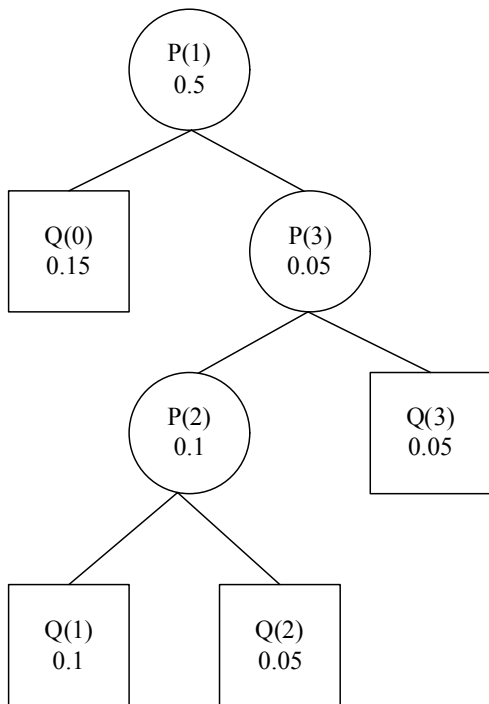
$$\text{成本} = (0.5 \times 2 + 0.1 + 0.05 \times 2) + (0.15 \times 2 + 0.1 \times 2 + 0.05 \times 2 + 0.05 \times 2) = 1.9$$

3.



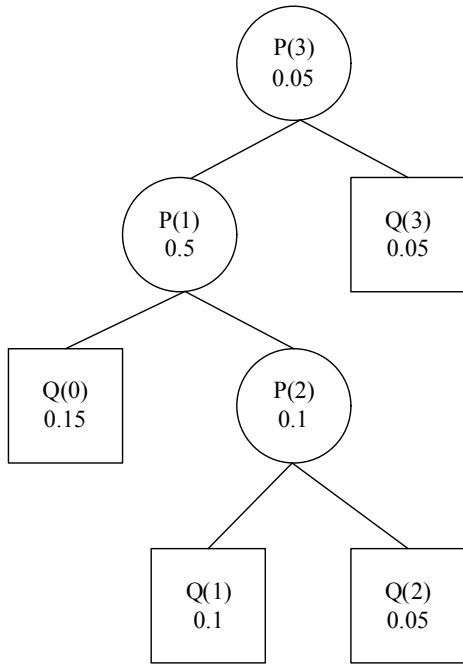
$$\text{成本} = (0.5 \times 3 + 0.1 \times 2 + 0.05) + (0.15 \times 3 + 0.1 \times 3 + 0.05 \times 2 + 0.05) = 2.65$$

4.



$$\text{成本} = (0.5 + 0.1 \times 3 + 0.05 \times 2) + (0.15 + 0.1 \times 3 + 0.05 \times 3 + 0.05 \times 2) = 1.6$$

5.



成本=(0.5*2+0.1*3+0.05)+(0.15*2+0.1*3+0.05*3+0.05) = 2.15

三、 $F(n)=F(n-1)+2F(n-2)-F(n-3)$, $n \geq 3$, $F(0)=0$, $F(1)=1$, $F(2)=2$ 。請用C語言或JAVE語言，撰寫一非遞迴式 (non-recursive) 的副程式，用以計算 $F(n)$ 的值。並請計算 $F(12)=?$ (20分)

答：

(一)

```

Public void Func (int n) {
    int[] F = new int[n];

    F [0] = 0;
    F [1] = 1;
    F [2] = 2;

    for(int i = 3; i < n; i++)
        F [i] = F [i-1] + 2F [i-2] - F [i-3] ;

    for(int i = 0; i < n; i++)
        System.out.println("F[" + i + "] = " + F[i] );
    }
}
    
```

(二)

```

F [0] = 0;
F [1] = 1;
F [2] = 2;
F [3] = F[2]+2F[1]-F[0] = 2+2*1-0 = 4;
F [4] = F[3]+2F[2]-F[1] = 4+2*2-1 = 7;
...
F[12] = 441 + 2*244 - 136 = 793

```

四、請先說明下列程式 (sysdate為系統當前時間) 對Oracle資料庫提供了什麼樣的安全性措施，之後再請詳細敘述三種可用來保護資料庫系統的安全技術或流程。(20分)

```

CREATE OR REPLACE TRIGGER table 1
BEFORE INSERT OR UPDATE OR DELETE ON table 2
BEGIN
  IF (TO_CHAR(sysdate, 'DY') IN ('SAT', 'SUN'))
    OR (TO_NUMBER(Sysdate, 'HH24') NOT BETWEEN 8 AND 17)
  THEN RAISE_APPLICATION_ERROR (-20506, '')
  ENDIF;
END;

```

答：

- (一)題目之程式為維護一個資料庫觸發(trigger) table1，內容為當table2有任何資料要被新增、修改、或刪除前，若當時為週六日或下班時間(非8:00~17:00)，則拋出一系統錯誤。
此觸發程式可確保table2資料不會在非上班時間被任意修改。
- (二)常見之資料庫安全技術如
- 1.資料加密：將特殊敏感或機密資料從事加密，避免具權限之使用者可任意存取該資料。
 - 2.權限控管：透過帳號密碼以及資料庫權限設定，管理各使用者可存取之資料內容。
 - 3.存取控制：透過如Stored Procedure、Trigger等方式過濾機密資料，使用者僅可存取特定資料表格、景觀、或符合特定條件下之資料(如上述之辦公時間限制)。

五、利用下列Bookstores、Books及Order等資料表，請分別寫出利用關聯式代數 (Relational algebra) 及關聯式計算(Relational calculus)來完成訂購「紅樓夢」的書局名稱“name”與所在城市“city”之查詢。(20分)

Bookstores				Books				Order		
no	name	rank	city	id	bookname	author	publisher	no	id	quantity
1	射手書局	20	高雄	1	三國演義	羅貫中	古文出版社	1	1	20
2	天秤書局	10	臺中	2	西遊記	吳承恩	河洛出版社	1	2	30
3	水瓶書局	20	臺南	3	水滸傳	施耐庵	中庸出版社	1	4	30
4	巨蟹書局	30	臺北	4	未央歌	鹿橋	臺灣商務	1	5	20
5	獅子書局	50	新竹	5	紅樓夢	曹雪芹	春秋出版社	2	2	15
				6	道德經	老子	大唐出版社	2	3	65
								2	6	50
								3	1	40
								3	5	25

答：

(一)關聯式代數

$$\pi_{\text{name, city}}(\text{Bookstores} \bowtie \text{Order} \bowtie (\sigma_{\text{bookname}='紅樓夢'}(\text{Books})))$$

(二)關聯式計算

以值組導向關聯式計算為例：

Range of BS is Bookstores;

Range of B is Books;

Range of O is Order;

name, city where BS.no=O.no and B.id=O.id and B.bookname='紅樓夢';