

CH08

是非題

- (○) 1. 資料機密性通常透過資料加密來達成。
- (○) 2. 對稱式加密演算法的執行效率，一般而言，較非對稱式加密演算法來得好。
- (×) 3. 在密碼長度相同的情況下，非對稱式的加密演算法較對稱式加密演算法來得安全。
- (○) 4. 使用非對稱式金鑰演算法進行加密，只有擁有私密金鑰的使用者，可以順利地進行解密。
- (×) 5. 網站的網址只要是使用 https 的協定傳輸，就一定是安全無虞的。
- (×) 6. 手機所使用的 A5 演算法，是一種對稱式的區塊加密演算法。
- (○) 7. RSA 演算法是基於因數分解的困難度設計而成的。
- (×) 8. 只要不知道密碼，就永遠都無法得知被加密保護的密文。
- (○) 9. 憑證 (certificate) 的目的是用以證明公開金鑰的擁有者以及其背書者是
否正確。
- (×) 10. 雜湊函數的輸出與輸入內容的長度成比例。

選擇題

- (A) 1. 下列何種對稱式演算法是美國國家標準技術局自 2001 年起採用的加密標準?
- (A)AES (B)BES (C)CES (D)DES
- (C) 2. 若要在公開場合交換密碼,我們可使用下列何種演算法進行交換?
- (A)RSA (B)ElGamal (C)Diffie-Hellman (D)BlowFish
- (B) 3. 阻斷服務攻擊(DoS)的進階版 DDoS,其字首 D 的意義為何?
- (A)Daniel (B)Distributed (C)Denial (D)Distributor
- (D) 4. 下列何者不是常見的無線網路傳輸相關的加密機制?
- (A)WEP (B)TKIP (C)WPA (D)WAP
- (C) 5. 下列哪種應用和非對稱式加解密演算法無關?
- (A)RSA (B)DSA (C)DES (D)ElGamal
- (B) 6. RSA 演算法是基於計算何種問題的困難度設計而成?
- (A)離散對數 (B)因數分解 (C)二次剩餘 (D)橢圓曲線

填充題

1. 基於效率考量,數位簽章通常不直接對內容進行簽章,而是針對內容的 雜湊值 進行簽章。
2. 我們可以使用 雜湊函數 來檢查資料是否遭到修改。
3. 駭客自製介面精美的偽冒網站,以吸引使用者提供其帳號密碼等個人資訊。這種攻擊我們稱為 (網路)釣魚。
4. 表面上沒有惡意,卻暗地裡在電腦主機上開啟後門的程式,我們常常稱其為 特洛伊木馬 (Trojan horse)。

5. 我們可以透過 加密 的方式，避免資料在網路傳輸時遭到監聽。
6. 目前常見的無線網路連線常用的安全加密機制為 WEP 以及 WPA。

簡答題

1. 請列舉 3 種常見的對稱式金鑰加密演算法。

【詳解】

DES、AES、IDEA、RC5 等。

2. 區塊加密的對稱式加密演算法常常需要配合操作模式如 CBC、CTR 等運作，其主要原因為何？

【詳解】

其主要原因是避免使用相同的密碼與相同的演算法，對相同的資料進行加密時，產生相同的密文。透過初始向量 (IV)、密文以及加密資料的 XOR 運算，可以提升加密資料安全性。

3. 請列舉 2 種常見的雜湊演算法。

【詳解】

MD5、SHA1、SHA256 等。

4. 我們在建置高可用性的系統時，常常使用「心跳」(heartbeat) 機制。請簡述心跳機制的做法。

【詳解】

心跳機制讓二個系統之間，互相偵測另一個系統是否還是在正常運作中。簡單的說，心跳機制就是讓二台主機之間定期交換一個特定的探測訊息。如果其中一方發現另一個系統沒有回應時，就可以判斷系統異常而啟動備援，接手工作的機制。

CH09

是非題

1. C 語言寫出來的程式，比組合語言寫出來的程式，可攜性較低。

【解答】 ×

2. LISP 常被用來撰寫人工智慧的應用。

【解答】 ○

3. 在類別中，我們可以定義資料和行為。

【解答】 ○

4. 我們常利用指標，來表示不確定大小的資料。

【解答】 ○

5. 在 PASCAL 裡，我們利用 repeat 指令來表示執行固定次數的迴圈。

【解答】 ×

選擇題

1. C 語言是屬於哪一種語言：

(A)高階語言 (B)低階語言 (C)自然語言 (D)組合語言

【解答】 (A)

2. 下列何者為最早提出來的高階語言：

(A)JAVA (B)C (C)FORTRAN (D)BASIC

【解答】 (C)

3. 下列何者為物件導向程式語言：

(A)C++ (B)PROLOG (C)ADA (D)PASCAL

【解答】 (A)

4. 下面哪一項資料型態，是處理一序列具有相同型態的資料：

(A)字元 (B)陣列 (C)結構 (D)浮點數

【解答】 (B)

5. 在呼叫一個程序時，若是直接把真實參數的值，指定給正式參數，則這種方法我們稱作：

(A)以值傳遞 (B)以位址傳遞 (C)以名傳遞 (D)以上皆非

【解答】 (A)

填充題

1. 專為商業資料處理而開發設計出來的語言，為 _____ 程式語言。

【解答】 COBOL

2. 一般程式語言提供的數字型態，包含了 _____、_____、_____和 _____等。

【解答】 整數、長整數、浮點數、雙精準數

3. if 指令提供了邏輯判斷式的寫法，也就是，如果 _____指令後面接著的運算式被判斷為真，則程式會繼續執行 _____指令後面的運算式，否則執行 _____指令後面的運算式。

【解答】 IF、Then、Else

4. PASCAL 裡的"begin"指令和"end"指令，對應到 C 語言裡的 _____符號和 _____符號。

【解答】 { 符號和 }

5. 在流程圖裡，用以表示決策的運算式，是用 _____表示；用以表示計算的敘述式，是用 _____表示。

【解答】 菱形框、長方框

問答題

1. 宣告一個結構，來表示公司裡一個員工的相關資料。

【詳解】

以下宣告一個員工，具有姓名、地址、職稱、薪水等資料。

```
struct employee {  
    char (6) name;  
    char (20) address;  
    char (10) title;  
    int salary;  
};
```

2. 利用 C 語言裡的"while"指令，計算整數 1 到 100 的和。

【詳解】

```
i = 1; x = 0;
while ( i <= 100 )
{
    x = x + i;
    i = i + 1;
}
```

3. 列出定義一個程序時，所需要提供的四項資訊。

【詳解】

程序在定義時，必須提供下列資訊：

1. 程序名稱
2. 程序本體，含變數宣告和命令敘述
3. 正式參數（Formal parameter）宣告
4. 程序回傳的資料型態

4. 說明全域變數和局部變數的差別。

【詳解】

全域變數（Global variable）能被全部的程式碼使用到；而局部變數（Local variable）只能被一部分程式碼使用到，通常定義在程序中。

5. 請上網查詢有關 JAVA 程式語言的特性。

【詳解】

完整的資料可以由美國 Sun 公司所提供的網站 <http://java.sun.com> 所取得。

6. 列舉物件導向程式語言的特性。

【詳解】

具有封裝特性的物件，為程式的核心。

7. 撰寫一個程序"sum"，其中定義一個整數參數"n"，然後該程序會回傳"1"加到整數"n"的和。

【詳解】

```
int sum(int n)
{
    int i = 1, x = 0;
    while ( i <= n )
    {
        x = x + i;
        i = i + 1;
    }
    return(x);
}
```

8. 撰寫一個程序"sum"，其中定義一個整數參數"n"，然後該程序會回傳"1"加到整數"n"的和。但是必須判斷參數"n"是否為正整數，若小於 0 的話則程序直接回傳 0。

【詳解】

```
int sum(int n)
{
    int i = 1, x = 0;
    if (n < 0)
        return(0);
    while ( i <= n )
    {
        x = x + i;
        i = i + 1;
    }
    return(x);
}
```

9. 討論在什麼情況下，程序需要用到「以位址傳遞」的方式。

【詳解】

希望改變原本真實參數的值。

10. 上網查詢目前 COBOL 程式語言發展的近況。

【詳解】

相關的資料可由 <http://www.cobolportal.com> 查詢到。

CH10

一、是非題

1. 陣列裡元素的資料型態可以不同。

【解答】 ×

2. 在程式執行時，陣列裡註標比較小的元素，會比註標大的元素更快拿到。

【解答】 ×

3. 環狀佇列是採用「先進先出」的順序。

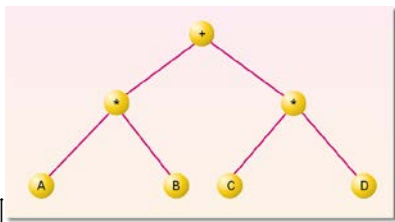
【解答】 ○

4. 環狀佇列裡宣告的每一個空間，都可以填入資料。

【解答】 ×

5. 樹只有一個根節點。

【解答】 ○



6. 在圖中的二元樹，其樹高為 3。

【解答】 (○)

二、選擇題

1. 以下何者代表 C 語言裡的空指標：

(A)null (B)nil (C)empty (D)not

【解答】 (A)

2. 以下何者的邏輯順序和實體順序不一定相同：

(A)鏈結串列 (B)一維陣列 (C)二維陣列 (D)以上皆是

【解答】 (A)

3. 以下哪種資料結構是採用「後進先出」的順序：

(A)陣列 (B)佇列 (C)堆疊 (D)環狀佇列

【解答】 (C)

4. 從根節點到樹中所有葉節點的最長可能路徑，稱作樹的

(A)高度 (B)階層 (C)根節點 (D)葉節點

【解答】 (A)

5. 在二元樹的探訪順序中，先探訪父節點、再探訪左子節點、最後探訪右子節點，稱作

(A)前序法 (B)中序法 (C)後序法 (D)循序法

【解答】 (A)

三、填充題

1. 假設系統在記憶體裡記錄多維陣列的方法，是先從第一列開始，然後接著記錄第二列，這種方式稱作_____。

【解答】 以列為主

2. 根據 C 語言的語法，若在宣告一個變數時前面加上_____符號，則該變數就是指標變數。

【解答】 *

3. 所謂的二元樹，就是每一個節點最多只有_____個子節點。

【解答】 2

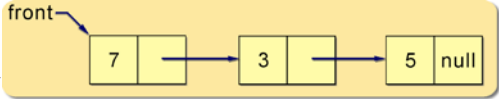
4. 將一個算數運算式以樹狀結構表示，此樹稱作_____。

【解答】 運算樹

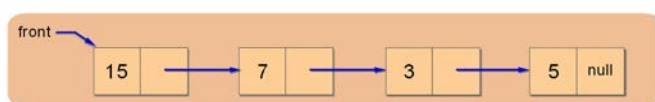
5. 在程序的本體中，又呼叫到自己本身，稱作_____程序。

【解答】 遞迴

四、問答題

1. 根據圖的鏈結串列，執行「insert(front, 15)」，畫出執行後的鏈結串列。

【詳解】



2. 利用第 7-3 節的堆疊宣告，改進程序"push"，要求在加入資料前，先判斷堆疊是否還有空位置。

【詳解】

```
void push (int data){
    if (top < 9)
    {
        top = top + 1;
        stack[top] = data;
    } else
    {
        printf("The stack is full.");
    }
}
```

3. 利用第 7-3 節的堆疊宣告，改進程序"pop"，要求在取出資料前，先判斷堆疊內是否有資料。

【詳解】

```
int pop( ){
    if (top >= 0)
    {
        top = top -1;
        return stack[top+1];
    }
    else
    {
        printf("The stack is empty.");
    }
}
```

4. 利用第 7-3 節的佇列宣告，改進程序"put"，要求在加入資料前，先判斷佇列是否還有空位置。

【詳解】

```
void put (int data){
    if (rear < 9)
    {
        rear = rear + 1;
        queue[rear] = data;
    } else
    {
        printf("The queue is full.");
    }
}
```

5. 利用第 7-3 節的佇列宣告，改進程序"get"，要求在取出資料前，先判斷佇列內是否有資料。

【詳解】

```
int get(){
    if (rear > front )
    {
        front = front +1;
        return queue[front];
    } else
    {
        printf("The queue is empty.");
    }
}
```

6. 討論何時使用陣列，何時使用鏈結串列。

【詳解】

如果資料不確定有多少，且時常動態增減，則較適宜使用鏈結串列。

7. 根據第 7-2 節 node 和 front 的定義，撰寫一個程序叫作 RemoveHead，把參數 front 指到的鏈結串列的第一個節點移除，然後回傳該節點所表示的資料（data）。

【詳解】

```
int RemoveHead(struct node *front)
{
    struct node *temp;
    temp = front;
    front = front->next;
    return(temp->data);
}
```

8. 討論何時使用堆疊，何時使用佇列。

【詳解】

如果我們希望先遇到的資料先處理，則使用佇列。反之，若希望先遇到的資料後處理，則使用堆疊。

9. 討論何時針對二元樹做後序法的探訪。

【詳解】

如果我們希望處理資料的順序，是先處理左子節點，接著是右節點，最後才處理父節點的話，則適用後序法。

CH11

填充題

1. 從 n 個數中找出最大數，最少要用 _____ 次比較。

【解答】 $n-1$

2. 給定 n 個數，請將它們由小排到大，稱為 _____ 問題。

【解答】 排序

3. _____ 排序法將數列切成兩部分：已排序數列及未排序數列，每次從未排序的數列中挑出最小的數，將它移到未排序數列的最前面。

【解答】 選擇

4. _____ 排序法將數列切成兩部分：已排序數列及未排序數列，每次將未排序數列中的第一個數，插入到已排序數列中，使得插入後的已排序數列仍然維持由小排到大的性質。

【解答】 插入

5. _____ 排序法將數列切成兩部分：已排序數列及未排序數列，每次從未排序數列中的最後一個數看起，如果它比前面的數小，則往前移，一直看到未排序數列的第一個數為止。

【解答】 泡沫

簡答題

1. 12 個金幣，有一個假的，只知和其他標準金幣重量不同，請用天平秤三次，就把假的金幣找出來，並確認它比較重或比較輕。（每次稱有三種可能性：大於、等於及小於，可用一個樹狀圖來描繪各種可能性）

【詳解】

有兩種方式，第一種可先四個和四個秤；第二種可先三個和三個秤。兩種方式展開的樹狀圖都可在秤三次情況下，找出假金幣。

2. 給定數列 23、12、58、85、72、98、13、37，請以課本介紹的兩個方法，找出其中的最大數及最小數，把你的作法記錄下來。

【詳解】

第一種方法逐一比較得最大數 98；第二種方法兩兩比較，98 會勝出。

3. 給定數列 23、12、58、85、72、98、13、37，請以課本介紹的方法，找出其中的最大數及第二大數，把你的作法記錄下來。

【詳解】

第一種方法逐一比較得最大數 98，再從剩下的 23、12、58、85、72、13、37 找出第二大數 85；
第二種方法兩兩比較得 98 最大，再從曾輸過 98 的 85、72、37 中找出第二大數 85。

4. 給定一個數列，請設計一個可找出前三大數的演算法。

【詳解】

兩兩比較找出最大數，再從曾輸過最大數的那些數中找出第二大數，再從曾輸過最大數和第二大數的數中找出第三大數。

5. 給定數列 23、12、58、85、72、98、13、37，請以「選擇排序法」將它由小排到大，記錄你的過程。

【詳解】

```
23  12  58  85  72  98  13  37
12 || 23  58  85  72  98  13  37
12  13 || 58  85  72  98  23  37
12  13  23 || 85  72  98  58  37
12  13  23  37 || 72  98  58  85
12  13  23  37  58 || 98  72  85
12  13  23  37  58  72 || 98  85
12  13  23  37  58  72  85  98
```

6. 給定數列 23、12、58、85、72、98、13、37，請以「插入排序法」將它由小排到大，記錄你的過程。

【詳解】

```
23  12  58  85  72  98  13  37
12  23 || 58  85  72  98  13  37
12  23  58 || 85  72  98  13  37
12  23  58  85 || 72  98  13  37
12  23  58  72  85 || 98  13  37
12  23  58  72  85  98 || 13  37
12  13  23  58  72  85  98 || 37
12  13  23  37  58  72  85  98
```

7. 給定數列 23、12、58、85、72、98、13、37，請以「泡沫排序法」將它由小排到大，記錄你的過程。

【詳解】

```
23 12 58 85 72 98 13 37
12 || 23 13 58 85 72 98 37
12 13 || 23 37 58 85 72 98
12 13 23 || 37 58 72 85 98
12 13 23 37 58 72 85 98
```

8. 給定數列 23、12、58、85、72、98、13、37，請以「快速排序法」將它由小排到大，記錄你的過程。

【詳解】

```
23 12 58 85 72 98 13 37
13 12 23 85 72 98 58 37
...
12 13 23 37 58 72 85 98
```

9. 給定數列 23、12、58、85、72、98、13、37，請以「合併排序法」(merge sort)將它由小排到大，記錄你的過程。(雖然本章沒介紹作法，但讀者可到圖書館找演算法相關書籍，以本章建立的基礎，應有辦法理解這個方法)

【詳解】

先以合併排序法排 23、12、58、85，得 12、23、58、85；再以合併排序法排 72、98、13、37 得 13、37、72、98。再將 12、23、58、85 及 13、37、72、98 依序合併得 12、13、23、37、58、72、85、98。

10. 給定數列 12、13、23、37、58、72、85、98，請以「二元搜尋法」找看看 85 在不在這數列中，也找找看 18 在不在這數列中，記錄你的過程。

【詳解】

找看看 85 在不在這數列中？先比較 85 和 37，因為 85 比較大，所以找後面部分；再比較 85 和 72，85 仍然比較大，再找後面部分；比較 85 和 85 時，回答 85 在這數列中。

找找看 18 在不在這數列中？先比較 18 和 37，因為 18 比較小，所以找前面部分；比較 18 和 13，18 比較大，所以比較後面的部分；此時只剩 23 和 18 比，並不相等，所以回答 18 不在這數列中。

11. 請解釋動態規劃技巧的解法三步驟。

【詳解】

動態規劃技巧有三個主要部分：遞迴關係 (recurrence relation) 用來定義最佳答案、列表式運算 (tabular computation) 用來找最佳答案的值及路徑迴溯 (traceback)，將最佳答案的組合列出。

12. 以 LCS 的方法，找 PROFESSOR 和 CONFESSION 這兩個序列的最長共同子序列。

【詳解】

OFESSO

13. 「旅行推銷員問題」和「小偷背包問題」這兩個問題，你有沒有想到好解法呢？

【詳解】

自由發揮。

14. 請計算 $1000n$ 、 $100n \log_2 n$ 、 $10n^2$ 、 n^3 及 2^n ，在 $n = 1$ 、 100 、 10000 及 1000000 時的值各為多少，把它們的大小關係列出來。

【詳解】

$1000n$ 剛開始會輸，但隨著 n 的增長，很快就會勝出； 2^n 很快就暴增了。

15. 已知 128 個金幣中有一假金幣（假的較輕），請問用天平最少秤幾次可以得知那一個是假金幣？

【詳解】

如果每次都盡可能平分成三堆，一定至少有兩堆金幣個數相同，把那相同個數的兩堆拿來秤，如果有一堆比較輕，那一堆一定包含那個假金幣，否則金幣就在沒秤的那一堆，再把包含假金幣的那堆依同樣作法盡可能平分成三堆做下去，…。128 個金幣平均分成三堆，三堆個數分別為 43、43、42，把那 43 個的兩堆拿來秤，如果一樣重，則假金幣在 42 個的那堆，否則比較輕的就包含假金幣，此時我們的問題大小已從 128 降到 42 或 43，比剛剛分兩堆的策略只降到 64 有效多了，所以這樣總共要秤幾次呢？最糟情況是：128、43、15、5、2，共 5 次，也就是

$\log_3^{128} = 5$ 次。

CH12

一、是非題

1. 撰寫程式的原則是保持程式碼清楚易懂，亦即維持良好的可讀性。

【解答】 ○

2. 可信賴的程式是指寫出能夠跑出正確結果的程式即可。

【解答】 ✕

3. 軟體品質認證只有 CMMI 可作為選擇。

【解答】 ✕

4. 開發不熟悉的專案，如果採用螺旋式模型，可以逐步學習擴大以完成專案。

【解答】 ○

5. 軟體的生命週期是指從購買日期開始使用授權有一定的日期限制，生命週期結束必須再買授權。

【解答】 ✕

6. 軟體專案中，必須負責與客戶討論，理解客戶需求的人員是專案管理人(PM)。

【解答】 ○

7. CMMI 的五個等級中，以第五級代表最成熟的軟體公司。

【解答】 ○

8. 軟體發展中，風險發現的越早，所付出的成本越低。

【解答】 ○

9. 如果軟體發展進度落後，多加派人手進行發展即可順利解決問題。

【解答】 ✕

10. CMMI 中第四級所強調的精神在於所有的事情都能夠先經過定義才進行。

【解答】 ✕

11. 程式撰寫之初，程式研發人員(RD)必須針對市場的需求進行分析，撰寫市場需求文件(MRD)。

【解答】 ✕

12. CMMI 是由康乃爾(Cornell)大學協助美國聯邦政府針對軟體承包商的開發能力所制定的評估標準。

【解答】 ✕

二、選擇題

1. 在軟體開發生命週期中，哪個階段所需要的花費通常最多：

(A)需求分析 (B)設計 (C)編碼 (D)維護

【解答】 (D)

2. 將行為和資料一起直接定義在物件上的性質，稱作以下何者

(A)封裝 (B)階層 (C)類別 (D)繼承

【解答】 (A)

3. 在 UML 提供的圖形工具中，描述系統中有哪些類別的圖，稱作以下何者

(A)使用情況圖 (B)類別圖 (C)活動圖 (D)實作圖

【解答】 (B)

4. 在 UML 提供的圖形工具中，顯示使用者和系統之間的互動，稱作以下何者

(A)使用情況圖 (B)類別圖 (C)活動圖 (D)實作圖

【解答】 (A)

三、填充題

1. 測試工程師(QA)測試程式時如果已經知道整個流程架構，然後針對流程進行測試稱為_____。

【解答】 白箱測試

2. 軟體生命週期的五大過程為：分析、_____、編碼、_____、_____。

【解答】 設計、測試、維護

3. 軟體發展中，除了程式碼之外，為了日後運作順利，必須撰寫_____以利後人維護或改版。

【解答】 文件

4. CMMI 的五個等級中從低至高分別是初級、可重複的、_____、_____、最佳化。

【解答】 已定義的、量化管理

5. 物件所包含的特性包括_____、_____、封裝。

【解答】 屬性、方法

6. UML 的全名為_____。

【解答】 Unified Modeling Language

7. _____圖可顯示系統架構內所設計的軟體元件和硬體元件，以及元件之間的互動。

【解答】 實作

四、簡答題

1. 上網查詢目前提供 UML 的軟體工具有哪些。

【詳解】

Object by design, Visio, Rational Rose 等。

2. 比較瀑布式模型和物件導向分析設計的不同。

【詳解】

瀑布式模型提出的進行流程是線性的，也就是從需求分析開始依序進行每一階段。雖然要求大量的文件說明階段的進行，但是對軟體的維護仍然需要付出龐大的代價。

物件導向模式，則提供良好的模組化觀念，把相關資料的處理程序都定義在一起（也就是直接定義在物件上），並且提供遞迴的設計過程。如此一來，若是日後要維護的時候，我們可以很輕易的找出要修改的地方，而不會淹沒在龐大的程式碼中。另外，我們修改的地方，也會被侷限在局部的程式碼中，比較不會發生因為修改舊的錯誤，而產生新錯誤的問題。

CH13

是非題

1. 一般的程式語言，都提供了詳盡的資料分析工具。

【解答】 ✕

2. 關聯主要是由「列」和「欄」所組成。

【解答】 ○

3. 一個關聯的主鍵只能由一個屬性所構成。

【解答】 ✕

4. 外來鍵表示了兩個關聯間的關係。

【解答】 ○

5. Access 是微軟公司所發展出來的資料庫軟體。

【解答】 ○

6. 在 XPath 中，我們可用符號 '/' 代表二元素間具有父子關係。

【解答】 ○

選擇題

1. 下面哪一項是利用一般程式語言建立資料管理系統時，可能面臨的問題：

(A)資料的重複與不一致 (B)資料難以存取 (C)資料的限制難以修改 (D)以上皆是

【解答】 (D)

2. 目前市面上的商用資料庫軟體，大多是建立在什麼模式之上：

(A)網路模式 (B)關聯式模式 (C)階層模式 (D)物件導向模式

【解答】 (B)

3. 假設有一些屬性，他們的屬性值在整個關聯裡都永遠不會重複，我們稱這些屬性為：

(A)主鍵 (B)外來鍵 (C)綱要 (D)資料列

【解答】 (A)

4. 下面哪一項是 Access 資料庫裡的物件：

(A)資料表 (B)查詢 (C)報表 (D)以上皆是

【解答】 (D)

5. 在 Access 裡若要輸入一長段文章，我們可選用的資料型態為：

(A)自動編號 (B)備忘 (C)文字 (D)數字

【解答】 (B)

6. 下列哪個子句，不在 XQuery 中被定義：

(A)for (B)let (C)where (D)select

【解答】 (D)

7. 以下何者是用來規範任一份 XML 文件中可以出現那些元素，以及各元素出現的順序等？

(A)SOAP (B)DTD (C)DOM (D)XPath

【解答】 (B)

8. 以下何者將 XML 檔案分解成個別的元素、屬性等，然後以它們為節點表示成一個有順序的標籤樹？

(A)SOAP (B)DTD (C)DOM (D)XPath

【解答】 (C)

9. 在 XPath 中，以下哪個符號是用來代表二元素間具有父子關係？

(A) '/' (B) '/' (C) '[' (D) '['

【解答】 (B)

10. 若一家超商從交易行為中，利用資料探勘的技術找出的資訊為：「顧客買麵包時通常會買牛奶」，則此項資訊屬於以下何者：

(A)關聯規則 (B)分群 (C)分類 (D)以上皆是

【解答】 (A)

填充題

1. 資料庫的查詢語言，根據其功能的不同，又可細分為 _____ 和 _____ 兩大部分。

【解答】 資料定義語言、資料處理語言

2. 關聯裡的每一筆資料，我們稱作 _____。

【解答】 資料列

3. 在 Access 裡的【建立資料表】視窗中，若想要更改欄位名稱，我們可以選取某個欄位，然後按滑鼠右鍵，選擇 _____，再輸入想要的欄位名。

【解答】 更改欄名

4. 在 Access 裡要設定表格的外來鍵，必須利用 _____ 關聯圖。

【解答】 資料庫

5. 在 Access 裡利用【設計查詢】設計 SQL 查詢句時，針對要輸出的欄位，我們必須將該欄位的 _____ 方塊選取起來。

【解答】 顯示

6. XML 的全名為_____。

【解答】 Extensible Markup Language

7. 所謂的元素，就是由一個_____到對應的_____為止，包含其中的所有內容。

【解答】 開始標籤、結束標籤

8. DOM 的全名為_____。

【解答】 Document Object Model

9. 若我們以一個關聯規則描述兩個物品，通常我們會以此規則的_____度來表示此二個物品是否經常被購買，並以_____度用來表示這兩個物品是否很有關聯。

【解答】 支持度（support）和信心度（confidence）

10. 進行資料探勘，通常需要的三個步驟，依序為_____、_____和_____。

【解答】 資料管理與準備、建立模型以分析資料、輸出結果

簡答題

1. 請列出資料庫管理者（DBA）的職責。

【詳解】

- A.決定哪些資料包含在資料庫內，且設定資料彼此之間的關聯
- B.設計資料存放在硬碟裡面的架構
- C.建立使用者帳號
- D.執行安全的控管
- E.週期性的資料維護，譬如：將資料備份、確定硬碟空間是否足夠、監控系統的效率並做適當的調整

2. 根據表 13-1 的學生關聯，假設我們要找出姓名「施小龍」同學的系別和排名，請列出對應的 SQL 查詢句。

	系別	年級	學號	姓名	地址	監護人	排名
1	資工系	4	B9901	王雅蕙	台北市	王爸爸	1
2	資工系	4	B9902	劉維新	台中市	劉大新	11
3	資工系	4	B9903	張自強	高雄市	張善良	21
4	電機系	4	B9904	施小龍	台北市	施大龍	7
5	電機系	4	B9905	林正當	台中市	林正正	2
6	電機系	4	B9906	鄭順利	高雄市	鄭大順	15
7	資工系	4	B9907	林紹興	台北市	林爸爸	13
8	資工系	4	B9908	洪志堅	台北市	洪媽媽	6
9	資工系	4	B9909	陳柏豪	台北市	陳阿姨	30
10	資工系	4	B9910	張建設	高雄市	張成功	4

【詳解】

```

SELECT 系別，排名
FROM student
WHERE 姓名 = '施小龍'

```

3. 根據表 13-4 的成績關聯，假設我們找出所有修習課程「程式語言」的同學學號和其總成績，請列出對應的 SQL 查詢句。

學號	課程	作業	期中考	期末考	總成績
B9901	資料庫	65	90	73	80
B9901	程式語言	0	33	49	40
B9902	程式語言	84	48	36	70
B9904	資料庫	71	51	38	60
B9904	程式語言	53	68	78	71
B9905	作業系統	59	41	79	65

【詳解】

```

SELECT 學號，總成績
FROM enroll
WHERE 課程 = '程式語言'

```

4. 根據表 13-1 的學生關聯和表 13-4 的成績關聯，假設我們找出在修習課程「程式語言」的同學中，期末考成績小於 60 分的同學姓名、地址、和其監護人，請列出對應的 SQL 查詢句。

	系別	年級	學號	姓名	地址	監護人	排名
1	資工系	4	B9901	王雅蕙	台北市	王爸爸	1
2	資工系	4	B9902	劉維新	台中市	劉大新	11
3	資工系	4	B9903	張自強	高雄市	張善良	21
4	電機系	4	B9904	施小龍	台北市	施大龍	7
5	電機系	4	B9905	林正當	台中市	林正正	2
6	電機系	4	B9906	鄭順利	高雄市	鄭大順	15
7	資工系	4	B9907	林紹興	台北市	林爸爸	13
8	資工系	4	B9908	洪志堅	台北市	洪媽媽	6
9	資工系	4	B9909	陳柏豪	台北市	陳阿姨	30
10	資工系	4	B9910	張建設	高雄市	張成功	4

學號	課程	作業	期中考	期末考	總成績
B9901	資料庫	65	90	73	80
B9901	程式語言	0	33	49	40
B9902	程式語言	84	48	36	70
B9904	資料庫	71	51	38	60
B9904	程式語言	53	68	78	71
B9905	作業系統	59	41	79	65

【詳解】

```

SELECT 姓名，地址，監護人
FROM student，enroll
WHERE 課程 = '程式語言' and
      期末考 < 60 and
      student.學號 = enroll.學號

```

5. 自訂適當的標籤，將表 13-1 的學生關聯裡的全部資料列，表示成一個格式正確的 XML 文件。

	系別	年級	學號	姓名	地址	監護人	排名
1	資工系	4	B9901	王雅蕙	台北市	王爸爸	1
2	資工系	4	B9902	劉維新	台中市	劉大新	11
3	資工系	4	B9903	張自強	高雄市	張善良	21
4	電機系	4	B9904	施小龍	台北市	施大龍	7
5	電機系	4	B9905	林正當	台中市	林正正	2
6	電機系	4	B9906	鄭順利	高雄市	鄭大順	15
7	資工系	4	B9907	林紹興	台北市	林爸爸	13
8	資工系	4	B9908	洪志堅	台北市	洪媽媽	6
9	資工系	4	B9909	陳柏豪	台北市	陳阿姨	30
10	資工系	4	B9910	張建設	高雄市	張成功	4

【詳解】

<Students>

<Student major = "資工系" year = "4" id = "B9901">

<Name> 王雅蕙 </Name>

<Address> 台北市 </Address>

<Guardian> 王爸爸 </Guardian>

<Rank> 1 </Rank>

</Student>

<Student major = "資工系" year = "4" id = "B9902">

<Name> 劉維新 </Name>

<Address> 台中市 </Address>

<Guardian> 劉大新 </Guardian>

<Rank> 11 </Rank>

</Student>

<Student major = "資工系" year = "4" id = "B9903">

<Name> 張自強 </Name>

<Address> 高雄市 </Address>

<Guardian> 張善良 </Guardian>

<Rank> 21 </Rank>

</Student>

<Student major = "電機系" year = "4" id = "B9904">

<Name> 施小龍 </Name>

<Address> 台北市 </Address>

<Guardian> 施大龍 </Guardian>

<Rank> 7 </Rank>

</Student>

<Student major = "電機系" year = "4" id = "B9905">

<Name> 林正當 </Name>


```

    <Address> 台北市 </Address>
    <Guardian> 林正正 </Guardian>
    <Rank> 2 </Rank>
</Student>
<Student major = "電機系" year = "4" id = "B9906">
    <Name> 鄭順利 </Name>
    <Address> 高雄市 </Address>
    <Guardian> 鄭大順 </Guardian>
    <Rank> 15 </Rank>
</Student>
<Student major = "資工系" year = "4" id = "B9907">
    <Name> 林紹興 </Name>
    <Address> 台北市 </Address>
    <Guardian> 林爸爸 </Guardian>
    <Rank> 13 </Rank>
</Student>
<Student major = "資工系" year = "4" id = "B9908">
    <Name> 洪志堅 </Name>
    <Address> 台北市 </Address>
    <Guardian> 洪媽媽 </Guardian>
    <Rank> 6 </Rank>
</Student>
<Student major = "資工系" year = "4" id = "B9909">
    <Name> 陳柏豪 </Name>
    <Address> 台北市 </Address>
    <Guardian> 陳阿姨 </Guardian>
    <Rank> 30 </Rank>
</Student>
<Student major = "資工系" year = "4" id = "B9910">
    <Name> 張建設 </Name>
    <Address> 高雄市 </Address>
    <Guardian> 張成功 </Guardian>
    <Rank> 4 </Rank>
</Student>
</Students>

```

6. 簡述 XML 目前已知的重要應用。

【詳解】

資料交換的標準、複雜文件的儲存格式和網際服務等

7. 上網查詢 ebXML 定義了那些標籤。

【詳解】

請至網站<http://www.ebxml.org>參考完整定義。

8. 想想看，資料探勘的技術可以如何應用在你的日常生活中，提高你工作的效率。

【詳解】

讀者可自行發想。

CH14

是非題

1. 電子商務是指使用網際網路進行商業交易的商務型態。

【解答】 ○

2. 對稱式加密系統使用同一鑰匙來加密及解密。

【解答】 ○

3. 凡是能夠連上網的地方，就有電子商務的存在，這是電子商務的全球標準特性。

【解答】 ✕

4. 數位學習包括數位內容、數位平台及數位服務。

【解答】 ○

5. 電子商務中，交易金額最大的是 C2C 商務的範疇。

【解答】 ✕

6. Enigma 是第一個加密解密的機器。

【解答】 ○

7. RSA 是非對稱加密系統中一重要演算法。

【解答】 ○

8. SSL 提供安全連線，每一次建立連線都使用同一密碼進行加密。

【解答】 ✕

9. 電子商務具有多元與互動的特性，能夠提供給使用者平面文字或電視媒體無法提供的訊息。

【解答】 ○

10. 惡意搶先以他人公司名稱註冊網域名稱的人稱為網路小偷。

【解答】 ✕

11. RSA 加密演算法是利用給定某一很大的數字，要求得特定的因數 P、Q 不易之特性。

【解答】 ○

12. M-commerce 是指以無線數位裝置來完成交易的行動商務。

【解答】 ○

13. 一個安全的電子商務環境應包含完整性、不可否認性、確實性、機密與隱私性，及可得性等特質。

【解答】 ○

14. 公鑰加密除了安全可靠之外，也擁有加解密計算快速的特性。

【解答】 ×

填充題

1. 電子商務依交易對象分類可分成 B2B、_____、_____。

【解答】 B2C、C2C

2. 生活上用來證明身分的是身分證，網路上用來證明身分的是_____。

【解答】 自然人憑證

3. 非對稱式加密系統中的一對鑰匙分別稱為_____及_____。

【解答】 公鑰、私鑰

4. 針對使用者的消費喜好或者過往的消費紀錄，傳達不同的產品內容或服務，稱之為_____。

【解答】 客製化

5. 入口網站分成兩種類型，分別是水平式及_____，其中後者指的是專門提供某個領域的資訊產品或服務。

【解答】 垂直式

6. _____是指用數位的方式來輔助學習，或是提供學習的平台。

【解答】 數位學習

7. _____定律是指網路的價值與使用人口成正比，也就是說，具有規模與報酬呈現正向循環。

【解答】 梅特卡夫

8. _____可以兼顧對稱式加密系統的快速與非對稱式加密系統的安全。

【解答】 數位信封

9. 電子商務是否能蓬勃發展一大關鍵在於_____，如果沒有辦法讓使用者放心地交易，電子商務發展將大受限制。

【解答】 安全

10. 有些網站專門負責幫使用者處理交易或者業務，稱為_____。例如 104 人力銀行幫忙企業及應徵者找雇員或工作。

【解答】 交易中間人

11. 雜湊函數可產生固定長度的雜湊(hash)，雜湊亦可稱為_____。

【解答】 訊息摘要

CH15

一、是非題

1. 人工智慧是這一兩年才被提出來的新技術。

【解答】 ×

2. 經驗法則有時成立，有時不成立。

【解答】 ○

3. 資料探勘可以分析使用者的消費行為。

【解答】 ○

4. 小畫家是用來看 DVD 的。

【解答】 ×

5. PowerDVD 主要是用來繪圖。

【解答】 ×

二、選擇題

1. 下列何者不是人工智慧裡重要的技術：

(A)知識表示 (B)邏輯系統 (C)經驗法則搜尋 (D)數值分析

【解答】 (D)

2. 下列何者是人工智慧常用的程式語言：

(A)LISP (B)C (C)C++ (D)FORTRAN

【解答】 (A)

3. 下列何者不是影像的副檔名：

(A)BMP (B)WAV (C)JPG (D)TIF

【解答】 (B)

4. 下列何者不是壓縮檔的副檔名：

(A)BMP (B)ZIP (C)RAR (D)GZ

【解答】 (A)

5. 下列何者不是音樂檔的副檔名：

(A)MP3 (B)WAV (C)MP+ (D)GIF

【解答】 (D)

三、填充題

1. _____是近年來媒體的寵兒，它是多種資訊傳輸媒介或多個不同型態的資訊。

【解答】 多媒體

2. 能夠類似專具有處理特殊問題的系統，我們稱作_____系統。

【解答】 專家

3. 人和機器溝通的工具，稱作_____語言；而人和人之間使用的，則是_____語言。

【解答】 程式、自然

4. 影像是最常見的媒體型態，在電腦中，它是以資料矩陣的方式表示。矩陣中的每一個元素，稱為一個_____。

【解答】 像素

5. 24 個位元（紅、綠、藍各八個位元）則能表現出 $2^{24} = 16777216$ 種顏色，又稱為_____。

【解答】 全彩

6. 由感應器接收訊號，然後線路連結將訊號傳進電腦，透過程式進行分析判斷，稱為_____。

【解答】 電腦視覺

7. 電腦視覺的_____步驟，其主要目的是去除沒有幫助的資訊。

【解答】 潤飾

8. M. L. Minsky 發表的_____論，該方法先將大量相關資訊輸入電腦，再將這些資訊按照情形，來定義為選擇性的條件或是強制性的條件。

【解答】 框架（Frame）

9. 幾年前，IBM 一部很有名的電腦_____，曾打敗過當時世界排名第一的西洋棋大師。

【解答】 深藍

10. 自然語言（Natural Language），是指_____之間溝通所使用的語言。

【解答】 人類

四、簡答題

1. 什麼是媒體呢？什麼是多媒體？

【詳解】

什麼是媒體呢？它的可能解釋包括了「用來傳播資訊的媒介」(如教室裡老師所使用的黑板、粉筆、白板筆、單槍投影機、麥克風以及學生的筆記本、隨身聽等)或「利用媒介來傳送的資訊本體」(如黑板上的文字及投影片上的圖像等不同資訊型態所表達的意念)。多媒體乃是運用兩個以上的媒介或資訊型態來傳遞資訊。

2. 目前市面上常見的影像編輯軟體有哪些？

【詳解】

目前市面上常見的影像編輯軟體有：PhotoImpact、Photoshop、小畫家、Microsoft Photo Editor 及 ACDSee 等。

3. 常見的影像檔副檔名有哪些？

【詳解】

幾個常見的影像檔副檔名有：GIF、JPG、PNG、BMP、TIF、EPS 和 TGA 等。

4. 常見的影音播放軟體有哪些？

【詳解】

常見的影音播放軟體，包括：Windows Media Player、Apple 公司的 QuickTime、訊連科技的 PowerDVD、享受網路上即時播放的 RealPlayer（RealOne Player）。

5. Lena 到底是誰呢？

【詳解】

她是《花花公子》1972 年 11 月份的女郎，來自瑞典。1973 年時，有位南加大的學者設計了一個新的影像處理方法，想應用在有光澤的臉部圖片上，就在苦尋不得其果之際，有位同學帶著一份近期的《花花公子》走進實驗室，其中 Lena 這張美女圖正中該學者的下懷，因為它具備了可用來測試影像處理效果的各種重要特性。沒想到這張美女圖魅力驚人，從此成為影像處理領域最具公信力的測試基準，展開了極為出色的「Lena 王朝」。

6. 請簡述電腦視覺的處理過程的五大步驟。

【詳解】

電腦視覺的處理過程有五大步驟：潤飾(conditioning)、下標籤(labeling)、群組化(grouping)、解析(extracting)、比對(matching)。

7. 請簡述你所認知的人工智慧。

【詳解】

所謂的人工智慧（Artificial Intelligence），顧名思義，就是「人工」形成的「智慧」。一般就生物學的角度，人類是具有智慧的最高等生物，而電腦則只是一個服從命令的機器。人工智慧的研究，就是希望使電腦系統也具有人類的知識，和學習、推理的能力，以便電腦可以自行判斷來解決不同的問題。

8. 你認為電腦有智慧嗎？

【詳解】

自由發揮。

9. 「杜林試驗」(Turing test)如何進行呢？

【詳解】

杜林(Alan Turing)曾提出了如何決定電腦是否會「思考」的方法，他跳脫了哲學層次的說法，而是以模擬遊戲來進行，這個稱為「杜林試驗」(Turing test)的方法是這樣進行的：有兩個人和一部電腦，其中一個人扮演質詢者的角色；另一個人和電腦待在與質詢者不同的房間。質詢者可以問他們各式各樣的問題，但他並不知道誰是電腦及誰是另一個人，如果在一連串問題之後，電腦讓質詢者誤以為它是另一個人，它就算通過杜林試驗，就某個角度看，它是會思考的。杜林有關這個測試的論文，被視為人工智慧研究領域的基石。

10. 上網查詢有關資料探勘的最新研究成果。

【詳解】

資料探勘主要的研究成果來自於統計學家和資訊學家，非常值得好好地探勘一番。

11. 何謂資料壓縮？為什麼我們要做資料壓縮，有什麼好處呢？

【詳解】

資料壓縮是透過編碼的技術，來降低資料儲存時所需的空間，等到我們要用時，再做解壓縮的動作即可。資料經過壓縮後，除了需要較少的儲存空間外，當我們在網路上傳輸時，所需的傳輸時間也較短。

12. 提出你所能想到的資料壓縮技巧。

【詳解】

只要有立論基礎即可。

13. 有個克里特島的人說：「所有克里特島人的每句話都是謊言。」這句話有矛盾嗎？

【詳解】

可以肯定的是，這個克里特島人說的這句話不是真話，因為如果是真話的話，會有這句話也是謊話的矛盾。

14. 請寫一個自我矛盾的句子。

【詳解】

此句乃謊言。

15. 試述以小畫家擷取局部影像的技巧。

【詳解】

因為小畫家(Paint)在 Windows 的附屬應用程式中都有安裝，所以用它做基本的影像處理非常方便。然而，有時因為影像的解析度高，使得擷取局部影像大小超過整個螢幕，這時就必須靠一點小技巧才能裁剪出我們所要的局部影像。首先，以【全選】選擇整個影像，接著按下滑鼠左鍵，移動影像，直到所要擷取影像左上角已被搬至小畫家畫面的左上角為止，此時擷取影像的左邊和上邊已決定。接著將螢幕滾動到全部影像的最右下角，將滑鼠移到右下藍點上面(右邊及下邊也各有一個藍點)，按下不放，並往左上移動到所要擷取影像的右下角，這樣就大功告成，以【另存新檔】將擷取影像存到另一個檔案。