

注意：①作答前須檢查答案卡(卷)入場通知書編號、桌角號碼、應試類別是否相符，如有不同應立即請監試人員處理，否則不予計分。

②本試卷為一張雙面，測驗題型分為【四選一單選選擇題 30 題，每題 2 分，合計 60 分】與【非選擇題 2 題，每題 20 分，合計 40 分】。

③選擇題限以 2B 鉛筆於答案卡上作答，請選出最適當答案，答錯不倒扣；未作答者，不予計分。

④非選擇題限用藍、黑色鋼筆或原子筆於答案卷上採橫式作答，不必抄題但須標示題號；請從答案卷內第一頁開始書寫，違反者該科酌予扣分。

⑤請勿於答案卡(卷)書寫應考人姓名、入場通知書號碼或與答案無關之任何文字或符號。

⑥本項測驗僅得使用簡易型計算機(不具任何財務函數、工程函數功能、儲存程式功能)，但不得發出聲響；若應考人於測驗時將不符規定之計算機放置於桌面或使用，經勸阻無效，仍執意使用者，該科扣 10 分；該計算機並由監試人員保管至該節測驗結束後歸還。

⑦答案卡(卷)務必繳回，未繳回者該科以零分計算。

### 壹、四選一單選選擇題 30 題 (每題 2 分)

【4】1.下列何者的值一定可以允許重複？

- ①候選鍵(Candidate Key) ②主鍵(Primary Key) ③超鍵(Super Key) ④外來鍵(Foreign Key)

【3】2.有關第三階正規化，下列敘述何者錯誤？

- ①所有屬性皆完全功能相依於主鍵 ②不允許多重值屬性和組合性屬性的存在  
③具有遞移相依性 ④尚未進行去除功能相依性的作業

【4】3. SQL 欲進行 update 時，下列哪一關鍵字是用來指定欲更改的欄位名稱及給予該欄位新值？

- ① update ② where ③ order by ④ set

【1】4.欲讓一資料庫新使用者進行驗證身分的程序，應採用下列哪一 SQL 指令？

- ① CREATE USER ② ALLOW USER ③ INSERT USER ④ ADD USER

【4】5.下列選項何者非 SQL 的預存程式(Store Procedure)所提供的優點？

- ①提升資料庫安全性 ②可將 T-SQL 程式模組化，提供不同使用者使用  
③降低網路負載 ④可攜性佳

【2】6.請問  $ANS = 25 + \&O22 + \&H33$ ，變數 ANS 最後的值會是：

- ① 80 ② 94 ③ 97 ④ 100

【1】7. Visual Basic 中，控制項的資料繫結無法透過哪一元件完成？

- ① DataReader ② BindingSource ③ TableAdapter ④ DataSet

【3】8.下列哪一項屬性可以判斷此目錄屬性為記憶卡儲存裝置？

- ① ReparsePoint ② Compressed ③ Temporary ④ Device

【4】9.下列 Function 宣告方式，何者錯誤？

- ① Function Test(By Val X, By Val Y) As String  
② Function Test(By Val X As Single, By Val Y As Single)  
③ Function Test(By Val X As Single, optional By Val Y As Single=0) As String  
④ Function Test(optional By Val X As Single, By Val Y As Single) As Single

【3】10.下列何者不是表單控制項的方法？

- ① Close() ② Show() ③ Display() ④ Hide()

【2】11.有關 Java 的敘述，下列何者錯誤？

- ①一個 Java 程式主要是由一群物件(Object)所構成  
②物件會藉由呼叫其他物件的型別(Type)來相互溝通  
③型別是由類別(Class)或者是介面(Interface)來定義  
④Java 是屬於物件導向的程式語言

【3】12.下列何者為不合法的 JAVA 識別字？

- ① int\_a; ② int\_\$;  
③ int 7q; ④ int a\_very\_detailed\_identifier;

【3】13.有關 Java 例外處理的寫法，下列敘述何者錯誤？

- ①使用 try 來撰寫陳述句 ②使用 catch 來撰寫例外處理  
③使用 find 來撰寫檢查敘述 ④使用 finally 來撰寫一定會處理的區塊

【3】14.下列程式碼的結果是什麼？

```
public class Boxer1 {
    Integer i;
    Integer x;
    Boxer1(Integer y)
    {
        x=y+i;
        System.out.println(x);
    }
    Public static void main(String[] args)
    {
        new Boxer1(new Integer(4));
    }
}
```

- ① 4 會顯示在命令列 ②編譯失敗，因為第 6 行程式碼有錯誤  
③執行時產生 NullPointerException ④編譯失敗，因為第 9 行程式碼有錯誤

【2】15.下面 JAVA 程式片段，執行的結果為何？

```
Int x=1;
Int y=2;
y=(++x)+(y++);
System.out.println(y);
```

- ① 3 ② 4 ③ 5 ④ 6

【3】16.在建立資訊安全管理制度時會採取 PDCA 模式，下列何者不是 PDCA 的程序？

- ①規劃(Plan) ②執行(Do) ③改變(Change) ④行動與回應(Act)

【4】17.下列何者不是行動裝置管理(Mobile Device Management, MDM)方案的主要功能？

- ①遠端資料抹除 ②遠端機器鎖定 ③越獄或破解偵測 ④遠端協助故障排除

【1】18.下列哪一應用程式弱點最不容易透過檢查使用者輸入來檢查？

- ①不當資訊揭露(Information Leakage) ②SQL 隱碼(SQL Injection)  
③CSRF(跨站要求偽造) ④XSS(跨站指令碼攻擊)

【3】19. A 和 B 在進行網路通訊時，進行交互認證(Mutual Authentication)，主要是要預防：

- ①重送攻擊(Replay Attack) ②資料竊取(Eavesdropping)  
③中間人攻擊(Man-in-the-middle Attack) ④SQL 隱碼攻擊(SQL Injection)

【3】20.容量規劃(Capacity Management)的控制措施，主要是針對下列哪個安全目標？

- ①機密性 ②完整性 ③可用性 ④隱私

【3】21.假設有 6 個人有需要兩兩間彼此通訊，但他們使用對稱式密碼法，因此一次只會與另一人通訊，且每次的通訊內容即使其他人攔截後仍無法解密，那麼這 6 個人總共至少需要使用多少把不同的金鑰？

- ① 6 ② 12 ③ 15 ④ 30

【1】22.假設有 6 個人有需要兩兩間彼此通訊，但他們使用非對稱式密碼法，一次只會與另一人通訊，且每次的通訊內容即使其他人攔截後仍無法解密，那麼這 6 個人總共至少需要使用多少把不同的私密金鑰？

- ① 6 ② 12 ③ 15 ④ 30

【1】23.下列哪一種特性是蠕蟲類型惡意程式所特有，但卻是其他類型的惡意程式沒有的？

- ①不須人為介入就可以自我複製 ②危害本機系統  
③經由網路散布複製後的本體 ④在主機開啟後門

【3】24.下列哪一種軟體內含弱點特徵資料庫，可以用來進行弱點掃描？

- ① hping ② wireshark ③ nessus ④ nmap

【2】25. Triple DES 顧名思義，加密和解密時會執行三次的 DES。若以 E()和 D()各別代表 DES 的加密和解密函數，p 代表明文，則以下哪個組合是 Triple DES 的加密方法？

- ① E(E(E(p))) ② E(D(E(p))) ③ E(E(D(p))) ④ D(E(D(p)))

【1】26.下列哪一個是公開金鑰密碼法？

- ① ElGamal ② Rijndael ③ Blowfish ④ Twofish

【2】27.一次性通行碼(one time password)可以防止下列哪一種攻擊？

- ①服務阻斷攻擊 ②重送攻擊 ③偽裝攻擊 ④生日攻擊

【4】28.已知 107 是質數，請利用費馬小定理(Fermat's little theorem)計算  $27^{323} \bmod 107$  之值為何？

- ① 1 ② 10 ③ 47 ④ 100

【2】29.數位簽章可以提供哪些功能？

- ①達成機密性和資料完整性 ②同時作為認證用途與達成不可否認性  
③確保機密性與不可否認性 ④確保電子商務、電子公文系統的可用性

【2】30.在 Kerberos 協定中，客戶端要求認證以取得服務時，一開始發送的明文要求中，包含了訊息生成時間以及一個隨意值(nonce)來防禦重送攻擊，而認證伺服器的回應中則會包含以客戶端金鑰對這個隨意值加密後的結果。為什麼這樣做就可以防禦重送攻擊？

- ①因為攻擊者重送客戶端的要求時，認證伺服器會發現相同的隨意值而偵測出攻擊
- ②因為攻擊者重送伺服器以前的回應時，客戶端會發現解開來的隨意值不同而偵測出攻擊
- ③因為攻擊者重送客戶端的要求時，認證伺服器會比對時間與隨意值是否和最近已收到的要求一樣，若發現有一致的情形，伺服器就偵測出攻擊而丟棄該要求
- ④這樣做還不能防禦重送攻擊，還要加上後續的步驟才可以

## 貳、非選擇題二大題（每大題 20 分）

### 題目一：

請寫出以下程式執行結果：

(一) 請根據以下資料表與 SQL 指令寫出結果。【10 分】

| 學生    |    |     | 電話    |            |
|-------|----|-----|-------|------------|
| 學號    | 姓名 | 班級  | 學號    | 電話         |
| 98001 | 王五 | 3 班 | 99001 | 0212345678 |
| 99001 | 張三 | 3 班 | 99001 | 0912123456 |
| 99002 | 李四 | 4 班 | 99002 | 072234567  |
|       |    |     | 98001 | 031234567  |

```
SELECT * FROM 學生 s INNER JOIN 電話 t ON s.學號=t.學號
```

(二) 請寫出以下 JAVA 程式的執行結果。【10 分】

```
public class main {
    public static int A[] = {1,2,3,4,5,6,7,8,9};
    public static void main(String args[]) throws IOException
    {
        main a = new main();
        a.sort(1);
        for (int i = 0; i < a.A.length;i++)
            System.out.print(a.A[i*2%9]);
    }
    public void sort(int i)
    {
        if (i < A.length - 1)
        {
            if (A[i+1] > A[i])
            {
                int C = A[i];
                A[i] = A[i+1];
                A[i+1] = C;
            }
            sort(i+1);
        }
    }
}
```

### 題目二：

若你管理的單位擬新增 WiFi 網路提供同仁以及來訪者使用，請分析下列幾種作法對於資訊安全防護的效果與限制。

- (一) 隱藏 SSID。【4 分】
- (二) 過濾 MAC 位址。【4 分】
- (三) 開啟 WEP 加密。【4 分】
- (四) 開啟 WPA/WPA2 加密。【4 分】
- (五) 使用網頁登入系統管理帳戶。【4 分】