臺北自來水事業處及所屬工程總隊 103 年新進職員甄試試題

甄試類科：資訊處理(硬體)【F8903】　　甄試職別：一級業務員

專業科目二：資訊處理(二)【電腦網路、資料庫應用、資通安全】

＊請填寫入場通知書編號：＿＿＿＿＿＿＿＿

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 15 題，每題 2 分，合計 30 分】與【非選擇題 4 題；第一、二題每題配分為 15 分，第三、四大題每題配分為 20 分，合計 70 分】，總計 100 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非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採**橫式**作答，並請從答案卷內第一頁開始書寫，違反者該科酌予扣分，**不必抄題但須標示題號**。
⑤**應考人得使用符合簡章規定之電子計算器**，應考人測驗時於桌面上放置或使用不符規定之電子計算器，經勸阻無效，仍執意使用者，該科扣 10 分，電子計算器並由監試人員保管至該節測驗結束後歸還。
⑥**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 15 題（每題 2 分）

【1】1. MD5(Message-Digest Algorithm 5)屬於下列何種技術？
①產生訊息特徵碼的技術　②對稱式加密技術
③非對稱式加密技術　④對稱式解密技術

【3】2.如果 Alice 要將訊息以不被 Bob 以外的人知道的情況下傳送給 Bob，並且要讓 Bob 知道訊息是由 Alice 傳的，請問在非對稱式加解密的情境下，可以用下列何種方式做到？
① Alice 使用 Bob 的私密金鑰將訊息加密，並用自己的公開金鑰做簽章後傳給 Bob
② Alice 使用 Bob 的公開金鑰將訊息加密，並用自己的公開金鑰做簽章後傳給 Bob
③ Alice 使用 Bob 的公開金鑰將訊息加密，並用自己的私密金鑰做簽章後傳給 Bob
④ Alice 使用 Bob 的私密金鑰將訊息加密，並用自己的私密金鑰做簽章後傳給 Bob

【1】3.最近 Google+與 Facebook 等皆在其開放的 API 當中使用到 OAuth，有關 OAuth 之敘述，下列何者正確？
①讓 Facebook 等資源擁有者確認使用者同意某第三方應用程式可以存取使用者資料的協定
②讓 Facebook 等資源擁有者確認使用者擁有存取第三方應用程式權限的協定
③讓 Facebook 等資源擁有者辨識使用者透過授權的手機存取其資源的協定
④讓使用者能夠像 Facebook 等資源提供者註銷帳號的協定

【4】4.在網路安全中，常會使用到的 Snort 軟體，其可歸屬於下列哪一種技術的軟體？
①防火牆(Firewall)　②內容過濾(Content Filtering)
③記錄(Logging)　④入侵偵測系統(Intrusion Detection System)

【1】5.韓國在 2013 年 3 月爆發出史上最大的持續性滲透攻擊事件，下列何者為持續性滲透攻擊的正式英文縮寫？
① APT　② PA　③ PTT　④ PPT

【3】6.將兩顆相同的硬碟做鏡像儲存，是屬於下列何種技術？
① RAID 5　② RAID 4
③ RAID 1　④ RAID 0

【1】7.下列何項備援技術，是將相關的設備皆設定好，只要注入備援的資料即可提供服務？
①熱備援(Hot Site)　②冷備援(Cold Site)　③溫備援(Warm Site)　④混合備援(Mix Site)

【2】8.在以生物特徵進行身分辨識時，會存在 False Acceptance Rate，請問下列何者為 False Acceptance Rate 的定義？
①將授權的使用者鑑別成為沒有授權的使用者，因此使其無法存取
②將未授權的使用者鑑別成為另外一個被授權的使用者，因此使其在未經授權的情況下存取
③將授權的使用者鑑別成為另一個授權的使用者，雖然其仍可存取，但是在紀錄上發生錯誤
④將未授權的使用者鑑別成為另外一個未授權的使用者，因為仍然不能存取，所以沒有問題

【4】9.倘若 x = 0xAB，y=0xCD (0x 表示之後數字為 16 進位)，請問 x XOR y XOR x=？
①0xAB　②0x26　③0x62　④0xCD

【3】10.在談到雲端資料安全時，會要求雲端服務業者採用 OVF(Open Virtualization Format)格式的原因是：
①確保該服務提供者有提供相關的蒐證機制
②確保該服務提供者有做好相關資料的備份機制
③在需要的時候可將所建之虛擬機搬移到其他雲端服務業者
④確保該雲端服務業者有做好資料中心的實體安全防護機制

【2】11.在 DES 或 AES 等區塊式對稱式加密法中，如果資料的長度不是正好為加密演算法每次所要取區塊大小的倍數，則會運用到下列何種方法？
①加入 IV(Initialization Vector)值
②使用相對應的墊充(Padding)演算法
③將資料序列化(Serialization)
④最後一個不足規定區塊大小的資料不加密

【3】12.在使用 SSL 進行通訊時，通訊的雙方要取得對方的憑證，並確認是否有效，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)
④跨站腳本攻擊(XSS Attack)

【1】13.下列何種存取控制模型可以落實分工原則？
①角色導向存取控制模型(Role-based Access Control)
②命令式存取控制模型(Mandatory Access Control)
③隨意式存取控制模型(Discretionary Access Control)
④以屬性為基礎的存取控制模型(Attributed-based Access Control)

【2】14.在做滲透測試時，下列何者係用來取得受測方網路相關資訊的工具？
① tcpreply　② nmap
③ wget　④ cat

【3】15.當撰寫 AES 加密程式時，若使用 CBC 的模式，為了要讓在不同程式語言使用同一把金鑰對同一項資料進行加密有相同的數值，不需要確認哪個參數必須相同？
①墊充(Padding)演算法
② IV(Initialization Vector)
③需編碼資料的類型
④金鑰資料的位元排列順序與方式

【請接續背面】

貳、非選擇題四大題（第一、二題每題配分為 15 分，第三、四題每題配分為 20 分）

題目一：

請回答下列問題：

（一）形成超網(supernet)之區塊需符合之條件爲何？【3 分】

（二）將 8 個 Class C 網路（網路遮罩爲 255.255.255.0）合併。205.16.200.0、205.16.201.0、205.16.202.0、205.16.203.0、205.16.204.0、205.16.205.0、205.16.206.0、205.16.207.0 上述 8 個連續的 Class C 網路可以形成超網(supernet)，其網路遮罩爲何？網路位址爲何？【8 分】

（三）假設某位址爲 190.168.170.132/27，請問其網路位址(network address)爲何？【4 分】

題目二：

請說明 TCP/IP 參考模型的四個層次功能，並標示其各自對應到 OSI 組織定義的七層網路協定中的哪幾層？【15 分】

題目三：

請回答下列問題：

（一）何謂序列排程(Serial Schedule)？其優缺點爲何？【6 分】

（二）何謂可序列化排程(Serializable Schedule)？其目的爲何？【6 分】

（三）下面排程是否爲可序列化(Serializable)？若是，請列出一個與其等價(equivalent)之序列排程(serial schedule)。【8 分】

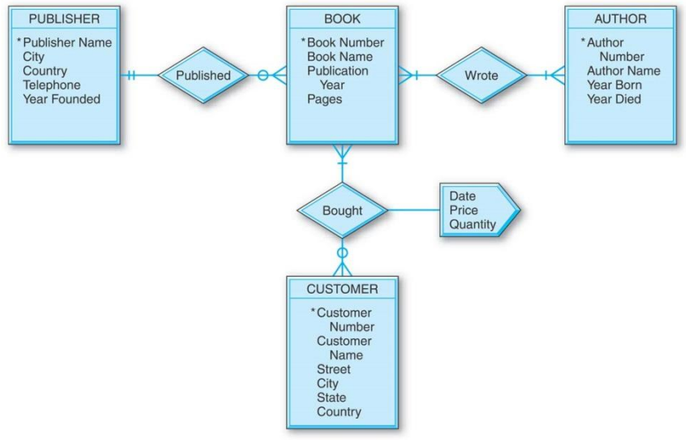
$\mathbf{r_1(x),w_1(x),r_3(y),w_2(y),w_3(z),w_1(y),w_2(z),r_1(y),r_1(z),w_2(m),c_1,c_2,c_3}$

題目四：

請回答下列相關問題：

（一）請說明當資料庫所有關聯裡的記錄都滿足哪些限制(constraint)時，就可稱該資料庫是“一致的”(consistent)？【12 分】

（二）請將書店資料庫 ER 圖(Entity-Relationship Diagram)（如圖四所示）轉換成爲關聯表格。共有 4 個表格 PUBLISHER、BOOK、AUTHOR 及 CUSTOMER，其欄位如下圖所示。【8 分】



【圖四】