臺灣中小企業銀行 106 年度第二次新進人員甄選試題

甄選類別【代碼】：資訊系統管理人員【L1907】
綜合科目：含邏輯推理、作業系統（Windows /Unix）、資料庫系統(SQL、DB2)、網路基礎概論(TCP/IP)及資訊安全概論

＊入場通知書編號：＿＿＿＿＿＿＿＿

注意：①作答前先檢查答案卡（卷），測驗入場通知書編號、座位標籤號碼、報考類別等是否相符，如有不同應立即請監試人員處理。使用非本人答案卡（卷）作答者，不予計分。
②本試卷為 1 張雙面，【四選一單選選擇題 16 題，每題 1.25 分，合計 20 分】與【非選擇題共 4 大題，每題 20 分，合計 80 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**依標題指示之題號於各題指定作答區內作答**。
⑤**請勿於答案卡（卷）上書寫姓名、入場通知書編號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電子計算器(不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝(錄)影音、資料傳輸、通訊或類似功能)，但不得發出聲響；若應考人於測驗時將不符規定之電子計算器放置於桌面或使用，經勸阻無效，仍執意使用者，該節扣 10 分；該電子計算器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，未繳回者該節以零分計算。**

壹、四選一單選選擇題 16 題（每題 1.25 分）

【3】1. RSA 演算法是利用下列哪一個問題來設計的？
① $a^b \equiv c \pmod m$, 已知 a, c, m，欲求 b
② $y^2 = ax + b \pmod m$, 已知 a, x, b, m，欲求 y
③已知 e, pq 的值且 p 和 q 是質數，e 與$(p\text{-}1)(q\text{-}1)$互質，欲求 $e^{-1} \pmod{(p\text{-}1)(q\text{-}1)}$
④ $a(x) = 3x^3 + x^2 + x + 2$, 求 $GF(2^8)$之中的 $a^{-1}(x)$

【2】2.下列何者不適合作為多因素認證(multi-factor authentication)中的一個認證方式？
①檢查密碼
②要求使用者看扭曲過的驗證碼的圖形(CAPTCHA)，然後輸入
③將認證碼傳送到手機中，並要求限時輸入
④將認證碼傳送到電子信箱中，並要求限時輸入

【1】3.現行的 HTTPS 通訊協定使用何種方式對網頁資料進行加密傳輸？
①對稱式金鑰密碼法(symmetric encryption)
②非對稱式金鑰密碼法(asymmetric encryption)
③對稱式金鑰密碼法和非對稱式金鑰密碼法並用
④可能是對稱式金鑰密碼法，也可能是非對稱式金鑰密碼法

【3】4.對一個檔案進行加密與數位簽章後，仍不能提供下列何種安全需求？
①機密性
②完整性
③不可重用性
④不可否認性

【1】5.在 Unix 作業系統中有名的 chroot 程式可歸類為何種資安相關的應用？
①沙箱(sandbox)
②蜜罐(honeypot)
③防火牆
④ Rootkit

【2】6.電腦資料存取控制的安全是經由下列何種流程來確保？
①驗證→身份識別→授權
②身份識別→驗證→授權
③身份識別→授權
④驗證→授權

【3】7.下列哪一個 Linux 指令可以列出目前本機與其它連網設備的網路連線？
① man　② ls
③ netstat　④ ifconfig

【1】8 有關一次性密碼(one-time password)的說明，下列何者正確？
①只使用一次即丟棄的密碼
②一次性發給多個密碼
③第一次申請帳號時，臨時發給使用者的預設密碼
④這只是理論上的概念，無法實作出來

【2】9.殭屍網路(botnet)是進行下列哪一種資安攻擊所必備？
①勒索軟體(ransomware)攻擊
②分散式服務阻斷攻擊
③網路釣魚(phishing)
④帳號密碼暴力破解(brute-force attack)

【4】10.有關 SHA-2 的敍述，下列何者錯誤？
①是一種雜湊函數(hash function)
②是多對一函數
③是 SHA-1 的後繼者
④產生的訊息摘要(message digest)的長度固定是 224 位元

【3】11.有關訊息鑑別碼(message authentication code)的敘述，下列何者正確？
①一定包含數位簽章
②一定包含訊息摘要(message digest)
③一定經過金鑰加密
④一定與訊息分開傳送

【1】12.當一個瀏覽器試圖連線開啟 https://www.facebook.com/時，瀏覽器不會做下列哪件事？
①查出該網址對應的 IP 位址並保存在快取中
②與網頁伺服器建立加密的安全連線
③檢查網頁伺服器是否能夠提供有效的憑證
④使用 HTTP 通訊協定向網頁伺服器要求傳送網頁內容

【2】13.利用橢圓曲線密碼學(ECC)實作的演算法，是屬於下列何者？
①對稱式密碼法
②非對稱式密碼法
③可以是對稱式密碼法，也可以是非對稱式密碼法
④並非傳統對稱式或非對稱式密碼法，應屬於第三類

【4】14.在一封偽造的電子郵件中，一般來說下列何者最難做到？
①偽造發信人郵件地址
②偽造發送主機域名
③偽造發送人簽名檔
④偽造發送人電子簽章

【3】15.下列何種程式語言撰寫時可內嵌於 HTML 檔案之中，卻不會被瀏覽器看到程式碼？
① Java
② JavaScript
③ Microsoft ASP
④ Adobe Flash

【2】16.個人資料保護法規定被蒐集個資的當事人對於其個資有五項權利，下列何者不在其中？
①請求刪除
②請求損害賠償
③請求更正或補充
④請求製給複製本

【請接續背面】

貳、非選擇題四大題

第一題：

某書局今天雜誌只賣了 70 本 A 雜誌，60 本 B 雜誌和 50 本 C 雜誌。購買的客人有買 A 雜誌與 B 雜誌者 14 位，購買的客人有買 B 雜誌與 C 雜誌者 12 位，購買的客人有買 A 雜誌與 C 雜誌者 13 位；又三本雜誌都買的有 3 位且每一種雜誌每一位客人至多買一本。請推論有幾位客人到此書局買雜誌？（需寫出推論過程）【20 分】

第二題：

請回答下列 Windows/UNIX 作業系統相關問題：

（一）在 Windows 系統的命令提示字元下，請寫出登入管理者帳號，並以 wmic 移除所有包含 SQL 字串的軟體指令。【6 分】

（二）現 Windows 系統在 2017 年 09 月 10 日發生異常，請在命令提示字元下，撰寫找出該日 C 磁碟有被異動的所有檔案指令，並說明檔案有哪些時間屬性可以作為參考。【5 分】

（三）請撰寫 UNIX 系統找出佔據記憶體前五大程序的指令，並撰寫刪除單一程序的命令，且說明如何刪除所找出的程序。【9 分】

第三題：

TCP/IP 是網際網路(Internet)所採用的通訊協定，請回答下列問題：

（一）請說明 TCP 與 IP 的功能。【6 分】

（二）一般應用程式在網路上互傳資料時大都採用 TCP 及 UDP 兩種傳輸協定，請說明為何 TCP 比 UDP 複雜？在應用上兩者有什麼差異？【8 分】

（三）要將電腦連結上網際網路的時候，通常需要設定子網路遮罩(Subnet Mask)。請列舉出至少兩個理由說明為何網際網路需要有子網路的設計。【6 分】

第四題：

請撰寫以下 SQL 及 DB2 的指令：

（一）請將 BANK 資料表中的 BANK_ID 主鍵移除，並將 SWIFT_CODE 設定為主鍵的 SQL 指令。【5 分】

（二）欲查詢 CUSTOMER 及 STAFF 資料表中，BRANCH_NO 欄位值相同的資料應使用何種 SQL 指令？【5 分】

（三）請使用 SQL 指令查詢 CUSTOMER 資料表中的 BALANCE 欄位大於 100 萬元的筆數。【5 分】

（四）欲查詢 DB2 的 License，應使用何指令？【5 分】