財團法人金融聯合徵信中心 103 年新進人員甄試試題

甄試類別【代碼】：資訊人員【F4501】

科目二：資訊專業科目(電腦網路、資料庫概論與資通安全)

＊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本試卷為一張單面，共有四大題之非選擇題，各題配分均為 25 分。
③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**。
④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，該科扣 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。
⑤**答案卷務必繳回，未繳回者該科以零分計算。**

題目一：

請回答下列問題：

（一）假設某一金融機構已配置一組“C 級”(Class C)網段，其網路位址(network address)為 210.68.8.0。現擬進行子網路(subnet)分割以滿足四個部門使用，各部門所需求之 IP 數量依序為 120, 60, 30, 30 個網址，如下表所列，請問：

①依序分割後的子網路位址為“210.68.8.x/y”，則各部門的 x 與 y 值應各自為何？【8 分】

②於各分割後之子網路範圍內，各部門之 IP 位址數量又各自為何？【4 分】

使用部門	IP 需求數	x	y	IP 分配數
壽險部	120			
證券部	60			
信託部	30			
創投部	30			

（二）企業機構為防範內部網路遭受駭客(hacker)非法入侵而被散播電腦病毒(virus)或惡意攻擊(attack)系統，為此常架設防火牆(firewall)設備以避免後端網路系統被癱瘓。請問若為此防火牆設定封包過濾(packet filtering)存取規則，其基本的過濾準則以何為依據？【13 分】

題目二：

請回答下列問題：

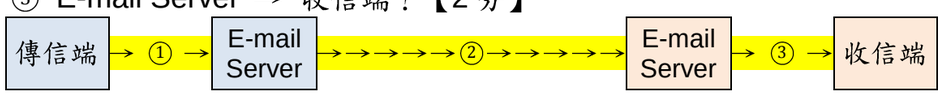
（一）使用簡易的網路指令 ping，例如 ping 210.68.8.68，請問藉此指令之執行可得知何種訊息？【6 分】

（二）用戶端經由電子郵件伺服器(e-mail server)得於網際網路上傳收電子郵件，請問於下列所示的三階段郵件傳收中，各階段所適用的郵件存取協定應各自為何：POP3 或者 SMTP？

① 傳信端 → E-mail Server？【2 分】

② E-mail Server → E-mail Server？【2 分】

③ E-mail Server → 收信端？【2 分】



（三）於網際網路中路由器(router)需執行效率佳的路由協定(routing protocols)，例如 OSPF, BGP 與 RIP，以順利傳遞封包(packets)至指定的 IP 目的端主機，請問：

① OSPF 之中文（或英文）全名為何？【3 分】

② OSPF,BGP 與 RIP 之中，何者係屬於“自治系統間”(Inter-AS, inter-autonomous system)之路由協定？【3 分】

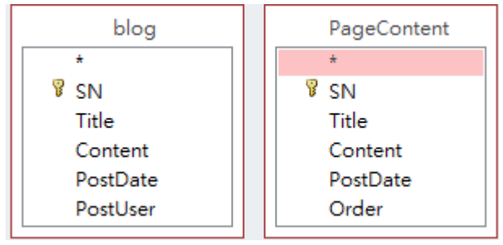
（四）通訊協定 IEEE 802.11g, 802.11b, 802.11n 係用於無線區域網路(wireless LAN)，請問：

①於上述三項協定中，何者可支援的資料傳輸率為最大？何者又為最小？【4 分】

② IEEE 802.11b/g 協定係採用 CSMA/CA 以提高封包傳輸成功率，請問 CSMA/CA 之中文（或英文）全名為何？【3 分】

題目三：

請根據下圖兩個資料表回答問題：



（一）請問在資料表 blog 中，以 SN 為主鍵與使用 Title（標題）、PostUser（作者）為主鍵的差異為何？請以部落格文章舉例說明。（註：SN 為自動編號）【15 分】

（二）請嘗試寫一 SQL 查詢語法，使用 union 查詢兩表格並指定四個必須欄位，其中需對 Title 進行搜尋關鍵字“測試”，並照 PostDate 反向排序，且注意搜尋結果需可以顯示標題，並對應原表格的資料。【10 分】

題目四：

假設張三和李四兩人已共同擁有一長效密鑰(long-term key)K_{AB}，下面協定試圖使張三和李四相信他們已共同建置一新(fresh)的共同密鑰(shared session key)K'_{AB}。請據此回答下列問題：

1.張三給李四：張三,N_A

2.李四給張三：$E(K_{AB},[N_A, K'_{AB}])$ //以密鑰對$[N_A, K'_{AB}]$加密

3.張三給李四：$E(K'_{AB}, N_A)$ //以密鑰對$[N_A, K'_{AB}]$加密

（一）請以張三和李四各自的角度去分析說明為什麼執行完此協定後，張三和李四相信他們彼此已共同建置一新(fresh)的共同密鑰 K'_{AB}。【16 分】

（二）假設張三啟動此協定試圖與李四建立共同密鑰，但是當他執行此協定步驟 1 之後駭客王五從中截斷，請說明王五如何透過一些輔助的通訊步驟可以成功假冒為李四與張三進行協定各項步驟，最後張三誤認其與李四（王五假冒）在進行建立共同密鑰。亦即第（一）小題張三的“相信對方是李四”是有瑕疵的。【5 分】

（三）請修正此協定強化後使其可杜絕第（二）小題駭客的假冒攻擊。【4 分】