中華郵政股份有限公司委託台灣金融研訓院辦理 99 年從業人員甄試試題

甄選類科：資訊安全(78407)　　**＊請填寫入場通知書編號：＿＿＿＿＿＿＿＿**

專業科目(2)：通訊與網路安全

注意：①本試卷為一張單面，共四大題問答(或申論)題(每大題配分 25 分)。
②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。
③應試人得自備使用簡易型電子計算機(簡易型電子計算機限僅有數字鍵 0～9 及＋－×÷√% = ⊡ ▶ +/- C AC CE TAX+ TAX- GT MU MR MC MRC M+ M- HMS M/EX 之功能，且不具財務、工程及儲存程式功能)；**若應試人於測驗時將不符規定之電子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；計算機並由監試人員保管至該節測驗結束後歸還。**
④答案卷務必繳回，否則該科以零分計算。

題目一：

請列舉並說明通訊網路開放系統應考慮的五項安全功能(security services)，以確保系統安全與資料的送達。【25 分】

題目二：

SSL(Secure Socket Layer)是目前被用來提供 Web 安全非常普遍的工具，請說明 SSL 包含哪些協定？【5 分】又請針對下列五項 Web 的安全威脅，說明 SSL 哪個特性(feature)可以予以防範：【每項 4 分】

(一)攻擊者以所有可能的密鑰(key)嘗試找出對稱式加解密法(symmetric encryption algorithm)使用的密鑰。

(二)SSL 在握手(handshake)交換訊息的初期，存在重送(replay)攻擊威脅。

(三)在密鑰(key)交換過程攻擊者介入，假扮成用戶端(client)，欺騙伺服端(server)，同時也假扮成伺服端欺騙用戶端。

(四)竊聽 HTTP 或其他應用訊息內的通行碼(password)。

(五)攻擊者使用偽造的 IP 位址欺騙主機(host)，使其接收假造的資料。

題目三：

請就 IETF(Internet Engineering Task Force)提出的 IPSec (Internet Protocol Security)的技術與觀念回答下列問題：

(一) IPSec 提供哪些功能？ 【6 分】

(二)傳輸模式(Transport model)與穿隧模式(Tunnel model)有何差異？ 【6 分】

(三)對同一點對點的通訊，若以兩個傳輸模式的 SA(Security Association)，結合 AH (Authentication Header)與 ESP(Encapsulating Security Payload)協定，請問應先執行 AH 協定或 ESP 協定比較理想？ 為什麼？ 【13 分】

題目四：

下表所列為三種以隨機亂數(nonce)達到挑戰/回應(Challenge/response)技術的方法，其中 N 表示使用者 A 所產生的隨機亂數、K 為使用者 A 與 B 共有的密鑰(shared key)、函數 f(Y)=Y+1、E(K, Y)表示以 K 為密鑰，對 Y 做對稱式加密。請回答下列子題：

(一)請分析說明此三種方法的功能。【9 分】

(二)請分析說明此三種方法的安全性。【9 分】

(三)三種方法就功能與安全性是否有優劣之分？若有，何者較優？為什麼？【7 分】

方法甲	方法乙	方法丙
(1)A→B：N (2)B→A：E(K,N)	(1)A→B：E(K, N) (2)B→A：N	(1)A→B：E(K, N) (2)B→A：E(K, f(N))