中華郵政股份有限公司 100 年第 2 次從業人員甄試試題

職階／甄選類科【代碼】：營運職／資訊安全【B6209】
專業科目(2)：通訊與網路安全

＊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。
④**切勿在答案卷上署名簽章或書寫非必要之文字、編號、符號或自備稿紙書寫，違者該科答案卷即認無效，並以零分計算。**
⑤應試人得自備使用簡易型電子計算機(須不具財務、工程及儲存程式功能且按鍵不得發出聲響)，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，若經勸阻無效，仍執意使用者，扣除該科目成績 10 分，計算機並由監試人員保管至該節測驗結束後歸還。
⑥**答案卷務必繳回，未繳回者該科以零分計算。**

題目一：

請針對公開金鑰基礎建設(Public Key Infrastructure)相關概念，回答下列問題：

（一）電子憑證管理中心(Certificate Authority)主要職責為何？【6 分】

（二）檢驗一電子憑證之有效性時，應檢驗哪些事項？【9 分】

（三）請寫出利用電子憑證在網路上鑑別某一特定使用者身分之方法步驟。【10 分】

題目二：

請就虛擬私有網路(Virtual Private Networks)相關概念，回答下列問題：

（一）什麼是虛擬私有網路？【3 分】

（二）列舉虛擬私有網路四項優點。【8 分】

（三）以虛擬私有網路技術處理封包技術，對應在 ISO 七層網路架構來分類，主要可以分為哪幾層？【6 分】

（四）虛擬私有網路技術必須達到一定程度的安全性，所建構出之虛擬的私有網路，才值得企業去使用。請就安全性相關之觀點，列舉四項虛擬私有網路必須滿足的要求。【8 分】

題目三：

請回答下列問題：

（一）解釋中間人攻擊(Man-in-the-middle Attack)如何損害基本的資訊安全服務，如可用性(Availability)、私密性(Confidentiality)及完整性(Integrity)？【9 分】

（二）Alice 和 Bob 兩人欲透過不安全的通訊管道互相傳遞資訊，請解釋雙方在採用對稱式密碼法(Symmetric Cipher)與非對稱式密碼法(Asymmetric Cipher)時，兩人總共需要幾把金鑰？各金鑰的用途為何？【8 分】

（三）TLS(Transport Layer Security)使用對稱式密碼法的金鑰做為會議金鑰(Session Key)，卻用非對稱式密碼法傳送它。這種作法相較於只使用對稱式密碼法或非對稱式密碼法，有哪些優點？【8 分】

題目四：

Kerberos 是目前相當普及的驗證與授權的網路安全技術，請說明：

（一）認證伺服器(Authentication Server)與票據授權伺服器(Ticket Granting Server)在使用者要求認證或授權時扮演什麼角色？【8 分】

（二）Kerberos 如何進行相互驗證(Mutual Authentication)功能？【10 分】

（三）相互驗證是否可以抵禦中間人攻擊？【7 分】