中華郵政股份有限公司 110 年職階人員甄試試題

職階／甄選類科【代碼】：專業職（一）／資安與網路管理(1)【S0206】、資安與網路管理(2)【S0207】

第二節／專業科目（2）：通訊與網路安全概要

＊入場通知書編號：＿＿＿＿＿＿＿＿

注意：①作答前先檢查答案卷，測驗入場通知書編號、座位標籤、應試科目等是否相符，如有不同應立即請監試人員處理。使用非本人答案卷作答者，該節不予計分。
②本試卷為一張單面，非選擇題共 4 大題，每題 25 分，共 100 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**依標題指示之題號於各題指定作答區內作答**。
④**請勿於答案卷上書寫姓名、入場通知書編號或與答案無關之任何文字或符號。**
⑤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)，且不得發出聲響。應考人如有下列情事扣該節成績 10 分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。
⑥**答案卷務必繳回，未繳回者該節以零分計算。**

第一題：

常見的網路安全威脅有哪些？請寫出並簡述至少 5 個常見的安全威脅。【25 分】

第二題：

請回答下列問題：

（一）請說明 TLS (Transport Layer Security)可達成哪些安全保護？【5 分】

（二）請說明 TLS 協定使用哪些密碼學機制？另說明使用這些機制的目的。【20 分】

第三題：

雙因素認證(Two-Factor Authentication, 2FA)方法被廣泛使用於網路服務登入流程中，目前常見的 2FA 有使用一次性密碼產生器、利用電子郵件與利用簡訊等三種方式。請回答下列問題：

（一）請簡述題目中所述三種方式的登入流程。【15 分】

（二）一次性密碼產生器必須要讓登入系統與用戶可同時產生完全相同的密碼，請舉出一種實作方法並簡述其原理。【5 分】

（三）常見於登入頁面上的驗證碼測試(CAPTCHA)是否也和帳號／密碼組成雙因素認證？請簡述原因。【5 分】

第四題：

現今大部分的網路連線都要求訊息加密，請回答下列問題：

（一）加解密過程中可能使用雜湊函數(Hash Function)。雜湊函數是有廣泛用途的一種函數，但密碼學所使用的雜湊函數相較於一般的雜湊函數有何種額外條件要滿足？【12 分】

（二）雜湊函數可與對稱式金鑰密碼法(symmetric-key cipher)結合來產生訊息驗證碼(Message Authentication Code, MAC)。MAC 可否用來確認發送者的身分，也就是實作資訊安全中的不可否認性(non-repudiation)？其理由為何？【6 分】

（三）雜湊函數還可與非對稱式金鑰密碼法(asymmetric-key cipher)結合來產生數位簽章(Digital Signature)。請簡述接收者如何利用數位簽章來確認加密者身分。【7 分】