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／網路通訊【B6207】

專業科目(2)：網路通信與資通安全

＊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：

資訊安全是使資訊不受各種廣泛的威脅之保護，以確保營運持續性、降低營運風險至最低、得到最豐厚的投資報酬率及最大商機。

（一）資訊安全主要係保存資訊之 C、I、A 性質，請說明此 3 種性質各為何意？【9 分】

（二）請針對小題（一）中之各種性質，分別就資料及網路，各提出 1 項保護措施。【12 分】

（三）資訊安全另有一重要性質為不可否認性(Non-repudiation)，有部分現在的加解密技術可達成股票網路交易的不可否認性。請寫出該技術名稱及描述其如何完成此目標。【4 分】

題目二：

資料加解密經常使用 RSA 及 Diffie-Hellman 演算法，請回答下列問題：

（一）請問此 2 種演算法所共同解決之問題為何？【5 分】

（二）請問此 2 種演算法之安全性各基於何種數學難題上？【6 分】

（三）請問此 2 種演算法各使用之金鑰為對稱式(symmetric)或非對稱式(non-symmetric)金鑰？【6 分】

（四）請描述 Diffie-Hellman 演算法如何會受中間人(man-in-the-middle, MiM)攻擊？【8 分】

題目三：

請回答下列資訊安全相關問題：

（一）請說明何謂 Cross-Site Scripting (XSS) 及其攻擊手法為何？【9 分】

（二）請分別描述 worm（蠕蟲病毒）和 botnet（殭屍病毒）的定義與傳染途徑。【16 分】

題目四：

請回答下列(1)VLAN (Virtual Local Area Network)；(2)超網(Supernet)；(3)網路位址(network address)之相關問題：

（一）請說明 VLAN 基本原理及其特性，並說明其所用的技術有哪些？【12 分】

（二）假設某超網的第一個位址為 204.16.32.0，其超網遮罩為 255.255.248.0。請問這個超網有多少區塊？最後一個位址為何？【8 分】

（三）假設某位址為 166.198.170.82/27，請問其網路位址為何？【5 分】