

等 別：三等考試

類 科：資訊處理

科 目：電腦網路

考試時間：2小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

- 一、循環冗餘檢驗 (Cyclic Redundancy Check, CRC) 是普遍被使用的鏈接層錯誤偵測技術。假設資料 D 的長度為 k bits，檢驗碼 R 的長度為 n bits， n 小於 k ， G 為生成多項式 (Generator Polynomial)，長度為 $n+1$ bits。請輔以公式說明 CRC 的運作原理。(20 分)
- 二、試述 TLS 與 SSL 的英文全名及彼此間之關連，並說明它們的主要功能與最常見之應用。(15 分)
- 三、Fast Retransmit 與 Fast Recovery 為 TCP 之改善機制，試述兩種機制之目的各為何？並說明兩者如何動作。(20 分)
- 四、某機關採購一批物品，打算公開招標，並利用網路進行電子投標。為了保密與公平，採用公開金鑰密碼 (Public Key Cipher) 技術。請說明這技術之操作方法為何？(10 分) 它有何存在風險，如何解決？(5 分)
- 五、下列為無線網路中常見之術語，請寫出它們的英文全名。(每小題 3 分，共 15 分)
 - (一) OFDM
 - (二) MIMO
 - (三) WiMAX
 - (四) VANET
 - (五) 3GPP
- 六、請說明在 WiFi 網路環境下，一個無線主機 (Wireless Host) 從開始尋找擷取點 (Access Points, APs) 到連線上 Internet 之過程。若有不同尋找擷取點之過程請一併說明。(15 分)