

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。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、(一)一個 QPSK (Quadrature Phase Shift Keying) 的星座圖 (signal constellation)，四點的座標分別在(1,1), (1,-1), (-1, 1)和(-1, -1)。請問如果依據這樣的參數設計，在一個鮑率 (baud) 為 1200 的通信系統，所得到的資料速率 (data rate) 是多少 bps？並說明理由。(5分)
- (二)一個全雙工 QAM-64 (Quadrature Amplitude Modulation) 的數據機 (modem) 總共使用了多少個頻率？並說明理由。(5分)
- (三)請針對下面幾個面向，比較線路交換 (circuit-switched) 網路以及封包交換 (packet switched) 網路之不同。(10分)
1. 需要呼叫建立 (call setup) 與否
 2. 是否有專屬實體路徑 (dedicated physical path)
 3. 每個封包是否走相同的路徑
 4. 封包是否依所傳送的順序到達
 5. 可能遭遇壅塞的時間點
- 二、(一)比較資料鏈結層 (data link layer) 與傳輸層 (transport) 的功能特性，各舉出兩個相同點，以及兩個不同點。(10分)
- (二)為什麼路由 (routing) 的計算，是網路層 (network layer) 的工作，而不是在傳輸層或資料鏈結層？(10分)
- 三、(一)假設在一個 slotted ALOHA 網路裡，只有三個工作站 A, B, C。而每個工作站在一個時槽 (time slot) 裡會傳送訊框 (frame) 的機率，分別是 $P_A=0.2$, $P_B=0.3$, $P_C=0.4$ 。則工作站 A 的吞吐量 (throughput) 約是多少？整個系統的吞吐量又是多少？(10分)
- (二)請比較 WiFi 及藍牙 (Bluetooth) 的媒介存取協定 (medium access control protocol) 主要的不同點？至少舉出兩點。(10分)
- 四、(一)比較 pure ALOHA、non-persistent CSMA、1-persistent CSMA、p-persistent CSMA 之間的不同。(13分)
- (二)CSMA/CA 的 CA (Collision Avoidance) 碰撞避免的策略為何？舉兩個策略並說明之。(12分)

等 別：三等考試
類 科：資訊處理
科 目：電腦網路

五、(一)假設 Bob 要傳送一份機密的文件給 100 個人，使用的是非對稱金鑰 (asymmetric-key) 方式確保機密性 (confidentiality)，請問需要使用到幾把金鑰？請說明理由。(3 分)

(二)數位簽章 (digital signature) 可否提供：(並請說明理由)(6 分)

1. 訊息認證 (message authentication)
2. 機密性 (confidentiality)
3. 不可否認性 (nonrepudiation)

(三)下列那一個(或那幾個)是一種機密性 (confidentiality) 的攻擊？(並請說明理由)(6 分)

1. 窺探 (snooping)
2. 偽裝 (masquerading)
3. 否認 (repudiation)