# 109 年公務人員高等考試三級考試試題

類 科：資訊處理
科 目：資通網路

一、請比較說明下列各組名詞有何不同：(每小題 5 分，共 20 分)
㈠OC-3 和 OC-3c
㈡transmission rate 和 propagation rate
㈢in-band signaling 和 out-of-band signaling
㈣connection oriented service 和 connectionless service

【解題關鍵】
《考題難易》：★★
《破題關鍵》題目均出自前兩章，掌握各項資通網路基本名詞即可解題。

擬答：

㈠同步光纖網路(SONET, Synchronous Optical NETwork)由美國 Bellcore(現為 Telcordia Technologies, 原為貝爾實驗室)開發，光學載波（OC）是在一個有許多確定水平的 SONET 光纖網路中的一組訊號頻寬。它通常表示為 OC-n，其中，n 是一個倍數因子，表示是基本速率 51.84Mbps 的多少倍，因此 OC-3 即指傳輸速度 155.52Mbps。而 OC-3c 中的"c"是指串接(concatenated)，將 3 個 STS-1(OC-1) 訊框(frames)串接成一個如同單一 OC-3 類似的串流(stream)。

㈡傳輸速率(transmission rate)是在給定的時間段內可以從一個地方發送到另一個地方的數據總量。傳播速率(propagation rate)則是在給定的時間段內可以從一個點到達另一個點的數據總量。

㈢帶內訊號(in-band signaling)是資料控制與資料傳輸通過同一連接進行，使用此種方式的協議包括 HTTP 和 SMTP。帶外訊號(out-of-band signaling)則是資料控制與資料傳輸通過不同連接進行。例如 FTP 等協議使用的頻外控制，FTP 在一個連接上發送控制信息，其中包括用戶標識、密碼、PUT / GET 命令，而資料傳輸則透過另一個獨立的並行連接。

㈣連接導向服務(connection oriented service)傳遞資料之前入須先建立連結（connection），然後才能開始傳送資料，資料傳送結束後也必須將連結取消，這種服務方式以電話系統為代表。無連接導向服務(connectionless service) 不必事先建立連接即可傳送，這種服務方式以郵遞為代表。

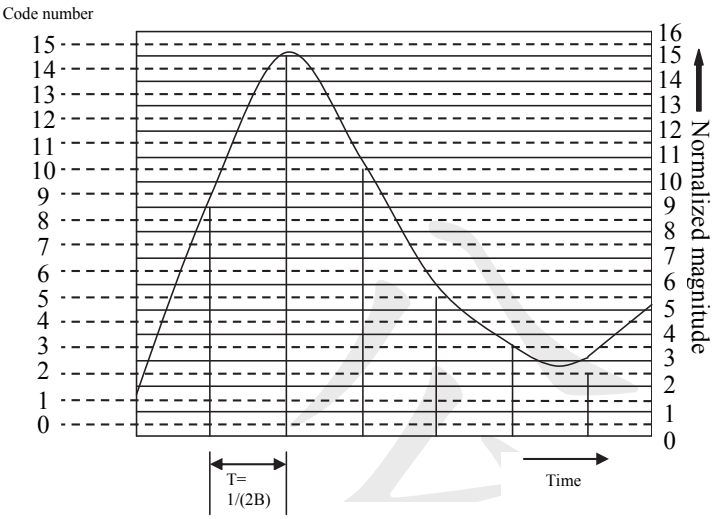
二、請說明搏碼調變(pulse code modulation, PCM)與取樣理論(sampling theory)的原理。(20 分)

【解題關鍵】
《考題難易》：★
《破題關鍵》PCM 基本概念題，掌握 PCM 操作方式即可解題。

擬答：

搏碼調變（Pulse code modulation, PCM）是一種類比訊號的數位化方法。PCM 將訊號的強度依照同樣的間距分成數段，然後用獨特的數位記號（通常是二進位）來量化，常被用於數位電信系統上。例如在一個 4KHz 的頻道上以每秒 8000 次的頻率取樣，分別以 7 或 8 位元的方式表示。利用 PCM，任何複雜類比訊號，都可以透過傅立葉轉換（Fourier Transform）分解為許多頻率不同、振幅不等的弦式訊號的疊加，接著可以被取樣和量化，利用正弦波在每段固定時間內被取一次樣，即 x 軸的刻度。而每一個樣本則依照某種運演算法，選定它們在 y 軸上的位

置。這樣便產生完全離散的輸入訊號的替代物，很容易編碼成為數位資料，以作保存或操縱。如下圖表示在此單位時間內，共取樣 7 次，第 1 次取樣得到值為 1.2，經量化(採無條件捨去小數)為 1，故可編碼為 0001；其餘均可以此類推。




| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PAM value | 1.2 | 9.0 | 15.1 | 10.1 | 5.2 | 2.8 | 2.7 |
| Quantized code number | 1 | 9 | 15 | 10 | 5 | 2 | 2 |
| PCM code | 0001 | 1001 | 1111 | 1010 | 0101 | 0010 | 0010 |

Ref：Stalling

三、依據項農理論(Shannon theory)，欲使一條 100 kHz 的傳輸線達到 T1 載體(carrier)的傳輸速率(transmission rate)，其信號雜訊比(signal-to-noise ratio, SNR)應為何？(附註：$\log_{10}2 = 0.301$) (20 分)

【解題關鍵】

《考題難易》：★★★

《破題關鍵》項農理論公式計算題，記得 T1 速率再掌握項農理論公式代入即可求得，但計算過程較為繁複。

擬答：

T1 是北美與日本 TDM 載波的標準，其規格稱為 DS-x，其中 T1 可將 24 個語音頻道多工在一起，各在 125 微秒內傳送一個 bytes，外加一個加框位元，因此 T1 的速率為（24*8+1）*8000=1.544Mbps。

根據項農理論(Shannon theory)，資料傳送速率=$H\log_2$（1+S/N），其中 H 為傳輸頻寬，S/N 為信號雜訊比，因此 00 kHz 的傳輸線最大資料傳送速率=$100k* \log_2$（1+S/N）=1.544M

此時 $\log_{10}$（1+S/N）/ $\log_{10}2$=15.44，故 $\log_{10}$（1+S/N）=4.64744

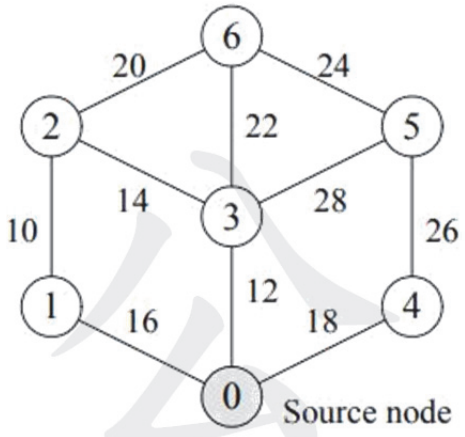
因此 $1+S/N = 10^{4.64744}$

$SNR=S/N=10^{4.64744}-1$

四、請將下列無方向連接圖(undirected connected graph)，依子題之說明，起始節點為節點 0，建構一最小費用擴張樹(minimum cost spanning tree)。(註：圖中圓圈標示節點(node)號碼，連線(link)旁標示費用；作答時必須標示加入連線的順序)(每小題 10 分，共 20 分)

㈠採用 Kruskal's algorithm 不含任何限制條件。

㈡採用 Kruskal's algorithm 含限制條件：每一分支(branch)最多含 3 段連線(link)。




【解題關鍵】

《考題難易》：★★

《破題關鍵》Kruskal 最小費用擴張樹實作題，掌握 Kruskal 演算法操作過程即可解題，第二小題稍有變化但只要小修 Kruskal 演算法即可求解。

擬答：

㈠由於 Kruskal's algorithm 是將費用由小到大排列後依次考量，只要不產生 cycle 即選用，因此選取過程如下：

*1.* 費用 10 的 link(1-2) 由於未產生 cycle 故選用

*2.* 費用 12 的 link(0-3) 由於未產生 cycle 故選用

*3.* 費用 14 的 link(2-3) 由於未產生 cycle 故選用

*4.* 費用 16 的 link(0-1) 由於產生 cycle 故不予選用

*5.* 費用 18 的 link(0-4) 由於未產生 cycle 故選用

*6.* 費用 20 的 link(2-6) 由於未產生 cycle 故選用

*7.* 費用 22 的 link(3-6) 由於產生 cycle 故不予選用

*8.* 費用 24 的 link(5-6) 由於未產生 cycle 故選用。此時已經選取需要的 6 條連線，故結束。

㈡此時演算法是將費用由小到大排列後依次考量，只要不產生 cycle 且合於限制條件即選用，因此選取過程如下：

*1.* 費用 10 的 link(1-2) 由於未產生 cycle 且合於限制條件故選用

*2.* 費用 12 的 link(0-3) 由於未產生 cycle 且合於限制條件故選用

*3.* 費用 14 的 link(2-3) 由於未產生 cycle 且合於限制條件故選用

*4.* 費用 16 的 link(0-1) 由於產生 cycle 故不予選用

*5.* 費用 18 的 link(0-4) 由於未產生 cycle 且合於限制條件故選用

*6.* 費用 20 的 link(2-6) 未產生 cycle 但不合限制條件(分支 0-3 將含 4 段連線)故不予選用

*7.* 費用 22 的 link(3-6) 未產生 cycle 但不合限制條件(分支 0-3 將含 4 段連線)故不予選用

*8.* 費用 24 的 link(5-6) 由於未產生 cycle 且合於限制條件故選用。

*9.* 費用 26 的 link(4-5) 由於未產生 cycle 且合於限制條件故選用。此時已經選取需要的 6 條連線，故結束。

五、2020 年 5 月台灣中油股份有限公司發生嚴重資安事件，請說明：(每小題 10 分，共 20 分)

㈠本事件屬何種病毒的攻擊，請針對此類病毒說明之。

㈡面對該類病毒，是否有預防策略，理由為何？

【解題關鍵】

《考題難易》：★★

《破題關鍵》掌握勒索病毒基本觀念即可解題，參考 107 普考資管與資通安全概要中類似題。

擬答：

㈠中油在 2020 年 5 月 4 日至 5 日期間，接連遭到駭客入侵並將勒索病毒植入公司系統、個人電腦以及伺服器等資訊設備，造成重要檔案無法開啟、系統停擺，同時公司也被要求交付贖金，因此本次事件屬勒索病毒攻擊，這是一種特殊的惡意軟體，屬於阻斷存取式攻擊，可以將受害者的電腦鎖起來，或是系統性的加密受害者硬碟上的檔案後。要求受害者繳納贖金以取回對電腦的控制權，或是取回受害者根本無從自行取得的加密金鑰。勒索病毒通常透過木馬病毒的形式傳播，將自身為掩蓋為看似無害的檔案。也可以透過路過式下載（隱藏式下載、偷渡式下載、強迫下載,網頁掛馬）攻擊，瀏覽惡意網頁或惡意廣告就會中毒。

㈡其預防策略：

1. 重新檢視企業網路防護機制，觀察企業 VPN 有無異常登入行為或異常網路流量，留意具有軟體派送功能的系統是否異動。
2. 加強監控企業網域中的特定權限帳號。
3. 更新防毒軟體病毒碼，留意防毒軟體所發出的警告。
4. 建立備份機制，並且離線保存。