104 年特種考試地方政府公務人員考試試題

等 別：三等考試
類 科：資訊處理
科 目：電腦網路

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。

【擬答】：

循環冗餘碼(CRC ,Cyclic Redundancy Code);或稱多項式碼(Polynomial Code)
用來解決同位檢查法只能檢查奇數個錯誤的問題，對於如通訊傳輸時經常發生的連續性錯誤(Burst error)相當合適。

㈠CRC 碼的產生

1.將欲傳送之資料位元串看成是只含有 1 或 0 的多項式的表示法。
2.傳接雙方協定出一個生成多項式(Generator polynomial)，將資料位元串多項式除以此一生成多項式，得一餘式。
3.將此餘式接在資料位元串多項式之後，即可得到欲傳資料的 CRC 碼。

㈡CRC 的檢查與解碼

將接收到的資料視為多項式除以協定之生成多項式，若能整除，即表示正確傳送，此時只要將資料後段的餘式去除即可得到資料。反之則表示發生錯誤。
例如欲傳資料為: k bits　　1101011011
生成多項式　　: n+1 bits　　10011
可以用下圖求得 n bits 的檢驗碼(餘數)為 1110

```
             1100001010
          ____________
10011 ) 11010110110000
        10011
         10011
         10011
          00001
          00000
           00010
           00000
            00101
            00000
             01011
             00000
              10110
              10011
               01010
               00000
                10100
                10011
                 01110
                 00000
                  1110
```

因此傳送的整體資料框架是 11010110111110

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。

【擬答】：

㈠TLS(Transport Layer Security)

是在網際網路上提供安全保密的通訊協定，利用秘密鍵加密演算法在網際網路上提供端點身份認證與通訊保密，為諸如網站、電子郵件、網上傳真等等數據傳輸進行保密。提供連接安全性中具有私有與可靠的特性。其中私有是指其以對稱加密進行資料加密（DES 、RC4 等）。對稱加密所產生的金鑰對每個連接都是唯一的，且此金鑰基於另一個協定（如握手協定）協商。可靠則指資訊傳輸中使用金鑰的訊息驗證碼(Message Authentication

Code,MAC)進行資訊完整性檢查。運用安全雜湊功能（ SHA、MD5 等）於 MAC 計算。

㈡SSL(Secure Socket Layer)

是由網景(Netscape)公司所提出之網際網路通訊安全標準，提供 WWW 上一個可信賴的通訊服務、保密服務與身分的識別等，用以保障在 Internet 上資料傳輸之安全，利用資料加密(Encryption)技術，可確保資料在網路上之傳輸過程中不會被截取。目前一般通用之規格為 40 bit 之安全標準，被廣泛地用於 Web 瀏覽器與伺服器之間的身份認證和加密資料傳輸。

㈢TLS 建立在 SSL 3.0 協定規範之上，是 SSL 3.0 的後續版本。在 TLS 與 SSL3.0 之間存在著顯著的差別，主要是它們所支援的加密演算法不同。SSL 3.0 和 1.0 有輕微差別，但兩種規範其實大致相同。TLS 的主要目標是使 SSL 更安全，並使協定的規範更精確和完善。TLS 在 SSL v3.0 的基礎上，提供了更安全的 MAC 演算法、更嚴密的警報、灰色區域”規範的更明確的定義等增強。可以預防竊聽、干擾（Tampering）、和偽造訊息。

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。

【擬答】：

㈠Fast retransmit

當傳送端收到 3 個 Duplicate ACK-TCP 會進行 Fast retransmit 操作，此時傳送端會將封包視為遺失，不待 Timeout 便立即重送。接著將門檻的值設為 cwnd 的二分之一並將 cwnd 的值重設為 1。

㈡Fast recovery 階段

用在 TCP Reno 協定中，在使用 Fast retransmit 重送遺失封包後，會將門檻以及 cwnd 的值都設為偵測到封包遺失時 cwnd 值得二分之一並進入 Fast recovery 階段，由於每收到一個 Duplicate ACK 也意味著有一個封包已經離開網路被接收端接收到了，因此如果允許的話，TCP Reno 還是可以使用 self-clocking 的機制繼續送出新的封包以提高 link 的使用率。如果封包遺失情形能夠在不需使用 Timeout retransmit 的情況下就將之回復，那麼 TCP Reno 在收到重送封包的 ACK 後就會直接進入 Congestion avoidance 階段。

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？

【擬答】：

㈠公開金鑰也稱為非對稱金鑰，其加密與解密所用的金鑰不同，公開金鑰對外公開，私密金鑰由個人秘密保存；用其中一把金鑰加密，就只能用另一把金鑰解密。本題的電子投標因為需要秘密投標，不能讓廠商的投標內容被其他業者取得，僅可在開標時獲取。因此該機關可將公開金鑰公開對外發佈，所以想給私密金鑰持有者(該機關)發送資訊的人都可以取得公開金鑰，用公開金鑰加密後，發送給私密金鑰持有者，即使被攔截或竊取，沒有私密金鑰的攻擊者也無法獲得加密後的資訊，可以保證資訊的安全傳輸。

㈡此一方法僅有保證資料傳輸的機密性，無法保證所傳資料的完整性、收送雙方的身分認證與不可否認性，因此仍有弱點存在，應該搭配數位簽章(Digital signature)確保資料的完整性、收送雙方的身分認證與不可否認性。

五、下列為無線網路中常見之術語，請寫出它們的英文全名。

㈠OFDM

㈡MIMO

㈢WiMAX

㈣VANET

㈤3GPP

【擬答】：

㈠OFDM(orthogonal frequency division multiplexing)

正交劃頻多工。是多載波傳輸方案的實現方式之一，將通道分成若干正交子通道，將高速資料信號轉換成並行的低速子資料流程，調變到在每個子通道上進行傳輸。正交信號可以通過在接收端採用相關技術來分開，這樣可以減少子通道之間的相互干擾(ISI）。

㈡MIMO(Multiple Input Multiple Output)

多入多出技術，指在發射端和接收端分別使用多個發射天線和接收天線，使信號通過發射端與接收端的多個天線傳送和接收，從而改善通信品質。

㈢WiMAX(Worldwide Interoperability for Microwave Access)

全球微波互聯接入，是一項新興的寬頻無線接入技術，能提供面向網際網路的高速連接，資料傳輸距離最遠可達 50km。WiMAX 還具有 QoS 保障、傳輸速率高、業務豐富多樣等優點。

㈣VANET(Vehicular ad-hoc network)

車載隨意移動網路，是傳統的行動自組織網路(MANET)在交通道路上的應用，是一種特殊的移動自組織網路。

㈤3GPP(3rd Generation Partnership Project)

第三代合作夥伴計目標，是實現由 2G 網路到 3G 網路的平滑過渡，保證未來技術的後向相容性，支援輕鬆建網及系統間的漫遊和相容性的計畫。主要是制訂以 GSM 核心網為基礎，UTRA(FDD 為 W-CDMA 技術，TDD 為 TD-CDMA 技術)為無線介面的第三代技術規範。

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。

【擬答】：

㈠搜尋選擇可用的 SSID（Service Set Identifier）：

SSID 技術可以將一個無線區域網路分為幾個需要不同身份驗證的子網路，每一個子網路都需要獨立的身份驗證，只有通過身份驗證的用戶才可以進入相應的子網路，防止未被授權的使用者進入本網路。SSID 通常由 AP 廣播出來，通過作業系統的掃描功能可以查看當前區域內的 SSID。出於安全考慮可以不廣播 SSID，此時用戶就要手工設置 SSID 才能進入相應的網路。

㈡AP 上的 WLAN 控制器自動調節射頻功率，建立與無線主機間通道，而後進行身份驗證和安全性驗證(如採用 WEP、WPA 等協定)通過後，讓無線主機連上本無線區域網路。

㈢利用 PPP 協定連上 Internet

無線主機透過數據機或其他連接裝置呼叫 ISP 的路由器，在路由器的連接裝置回覆後，建立一個實體連結。無線主機透過一或多的 PPP 的資料訊框，送給路由器一連串 LCP 分封，並根據其回覆選定所要使用的 PPP 參數。雙方同意設定後，路由器會將一系列的 NCP 分封傳來組織網路層，包括 IP 地址的分配，通常這些 IP 地址是採用動態分配的。