《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。（20分）

試題評析	本題屬於基本的錯誤檢查碼原理，答題須注意使用模數爲2的計算，以說明傳輸與接收兩方的處理方法。
考點命中	《高點資通網路講義》第二回，王致強編撰，頁14。

答：

(一)檢查碼計算如下面公式

$R = (D \times 2^n) \bmod G$

(1)將資料D乘上2^n，相當於尾巴補上n個0。

(2)再用module－2的除法，除以G取餘數。

(二)傳輸端將資料以(一)公式計算出檢驗碼，將資料D尾巴加上R，公式爲$M = D \times 2^n - R$(module-2)，然後將M傳送出去。

(三)接收端檢驗方法，將收到的訊息M除以同一個生成多項式，如果餘等於0，則資料正確，計算方法爲$D=(M+R)/2^n$ ；如果餘式不爲0，表示有錯誤，必須重傳。

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）

試題評析	本題測驗SSL與TLS基本概念，只要有基本了解，而且英文全名能夠寫出，即可取得分數。
考點命中	本題屬於網路安全問題。

答：

(一)TSL全名爲Transport Layer Security；SSL全名爲Secure Sockets Layer。

(二)SSL原先是Netscape設計的一種安全協定，後來IETF將其標準化，更名爲TLS。

(三)主要是在TCP與Application Layer之間，加上加密/解密的機制，主要用於Web的安全傳輸協定，而且獲得了廣泛的應用。

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）

試題評析	這是常考的TCP滑動窗口的運作方法，上課仔細了解，當可拿分。
考點命中	《高點資通網路講義》第四回，王致強編撰，頁55~57。

答：

(一)Fast Retransmit：是爲了可以快速傳送遺失的區段。其方式爲TCP若收到3個重覆序號的ACK時（即4個相同序號的ACK），不用等到計時器逾時，就會立刻重傳區段。

(二)Fast Recovery：是爲了避免經常窗口會被減半，造成傳輸緩慢，方法爲(一)Fast Retransmit的區段，如果ACK沒有逾時，就立刻回到Congestion Avoidance，窗口大小不變；如果逾時，則將windows減半，並且回到Slow Start狀態。

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）

試題評析	RSA與數位簽章的基本觀念題。
考點命中	本題屬於網路安全問題。

答：

(一)RSA加密法，是由資料接收方產生一組金鑰（一個發送訊息時加密用的公鑰，與一個接收訊息用以解密的私鑰），然後將公鑰傳送給發送訊息者。

(二)發送訊息時，以公鑰將訊息加密；接收端則以對應的私鑰解密。

(三)最容易出現的問題是匿名信的問題，因爲公鑰通常不需要保密，容易讓取得公鑰者可以冒他人之名傳送僞造的訊息給接收者。

(四)要認證發送訊息者的身分，解決的方法就是使用數位簽章，數位簽章就是反用RSA，發送端以自己的私鑰將訊息加密，以產生數位簽章傳送給對方；接收端則用對方的公鑰來進行解密，以確認發送者的身分。

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

試題評析	考記憶綜合名詞英文全名。
考點命中	《高點資通網路講義》第五回，王致強編撰。

答：

(一)OFDM：Orthogonal Frequency Division Multiplexing。

(二)MIMO：Multiple-Input-Multiple-Output。

(三)WiMAX：Worldwide Interoperability for Microwave Access。

(四)VANET：Vehicular Ad Hoc Networks。

(五)3GPP：3rd Generation Partnership Project。

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）

試題評析	本題考無線基地台連線的基本方法，屬於常識性質的問題。
考點命中	《高點資通網路講義》第五回，王致強編撰，頁7。

答：

(一)公開的SSID：無線AP每100ms將SSID（Service Set Identifier）經由beacons（信號台）封包廣播一次，beacons封包的傳輸速率是1Mbit/s，並且長度相當的短，所以這個廣播動作對網路效能的影響不大。因爲Wi-Fi規定的最低傳輸速率是1Mbit/s，所以確保所有的Wi-Fi client端都能收到這個SSID廣播封包，client可以藉此決定是否要和這一個SSID的AP連線。

(二)隱藏的SSID：無線AP將其SSID隱而不宣，此時client的使用者必須提供正確的SSID，同時選擇與AP同的加密法，並給予正確的密碼，才能與AP連線。