

等 級：佐級晉員級

類科(別)：技術類（選試資訊管理與資通安全概要）—公路

科 目：資訊管理與資通安全概要

考試時間：1 小時 30 分

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、請說明在網際網路(Internet)封包(packet)傳輸的端點到端點延遲(end-to-end delay)是由傳輸路徑長短，也就是所經過的路由器站數(hops)，以及在每一站路由器及其輸出傳輸線(outgoing transmission link)上的四個主要時間延遲影響。並請指出那一個時間延遲是最大也是最不確定的影響因素。(25 分)

二、請說明網際網路(Internet)之檔案下載服務：

(一)在主從(client-server)架構下的傳輸方式。(5 分)

(二)在對等(peer-to-peer)架構下的傳輸方式。(10 分)

(三)以上兩個不同的網路服務架構對檔案接受端(file receiver)而言，最大的差異為何，試舉出三點。(10 分)

三、網際網路(Internet)主從(client-server)架構下的資訊系統，當遠端 client 要與 server 通訊時，通常需要執行雙方進行相互的身分認證(mutual authentication)，也就是說 client 要確認 server 身分，同時 server 也要確認 client 身分。假設 client A 要傳一個訊息給 server B，在使用公開金鑰基礎建設(Public Key Infrastructure, PKI)的架構下：

(一)請說明這個訊息應該如何在 client 端被加密以認證(1)該訊息真的來自 client A，(2)認證該訊息真的是只要送給 server B，以及(3)確保該訊息在傳輸過程中的私密性(secretcy)。(15 分)

(二)請說明 server B 在收到這個訊息後應該如何解密。(10 分)

四、有關資訊系統，請說明以下名詞：

(一)容錯管理(Fault tolerance)。(12 分)

(二)在軟體開發上，必須要注意所謂的「安全容錯」(Fail-safety)，試述其意義。(13 分)