《資訊安全實務》

一、試說明資料傳輸之對稱式（Symmetric）加密法與非對稱式（Asymmetric）加密法以及二者之間的差異性。並說明 TCP/IP 網路上傳輸層（Transport Layer）和網際網路層（Internet Layer）所提供的資訊安全機制之通訊協定與其功能。（25 分）

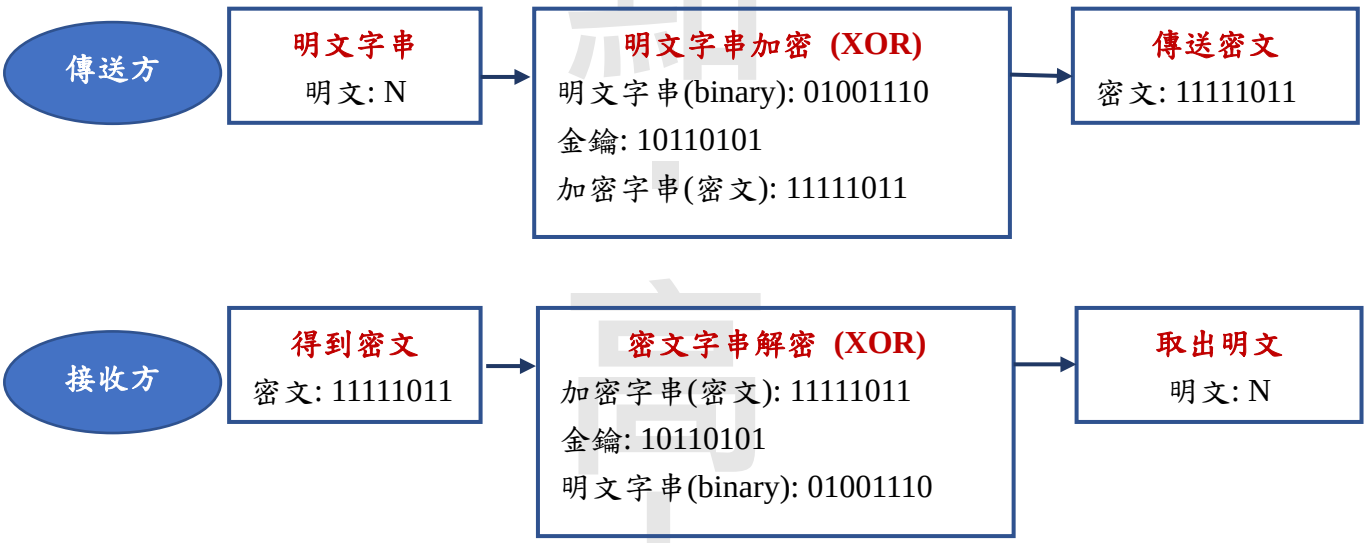
答題關鍵	對稱和非對稱主要是加解密金鑰是否相同，而傳輸層和網路層是 TCP/IP 的網路模型架構，此為功能比較題型，作答時應透過圖示或表格明確寫出兩者差異性。

【擬答】

(一)對稱式加密

1.定義

傳送方與接收方對明文的加解密都是使用同一把金鑰並進行 XOR 運算，舉例如下。



2.常見的對稱式加密方法

(1)DES 加密

一種區塊式加密方法(Block Cipher)，基於 56bit 的金鑰，將明文進行使用 16 輪的運算進行加密。其衍生加密法為 3DES，但容易被暴力破解法破解。

(2)AES 加密

另一種區塊式加密方法，用於取代原先的 DES，AES 一個區塊的長度為 128bit，金鑰長度則是可以為 128bit、192bit 或 256bit，目前被廣泛運用。

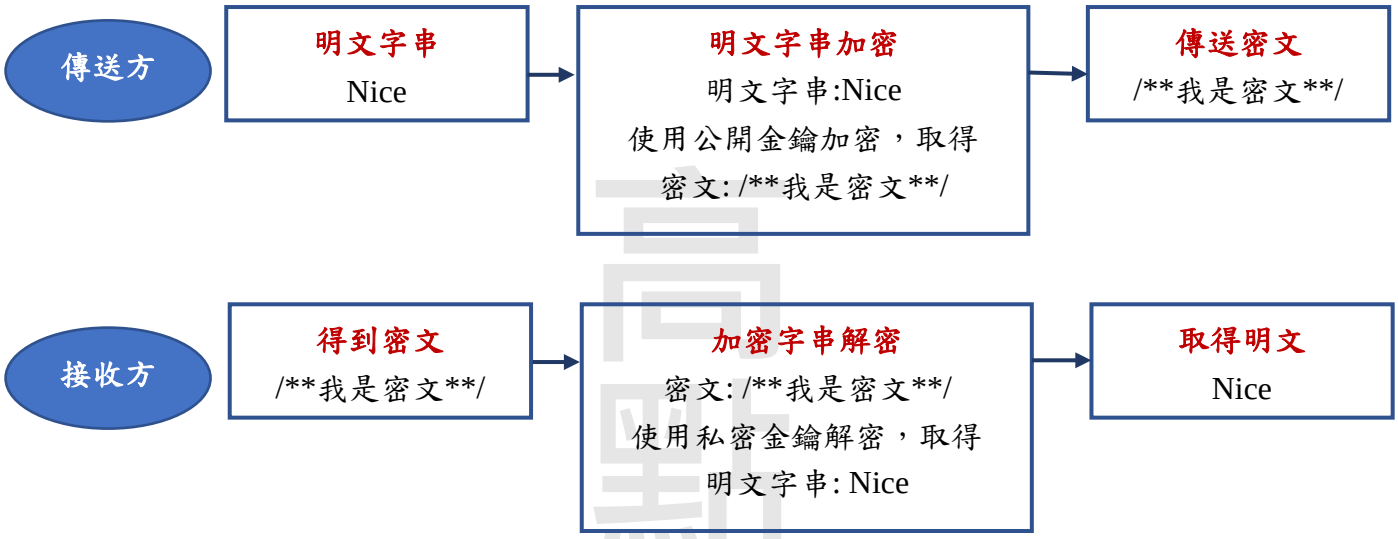
(3)RC4 加密

一種串流加密法(Stream cipher)，密鑰的長度是可變化的，可為 40~256bit，常見的長度則為 40bit、64bit 或 128bit，但目前已被破解。

(二)非對稱式加密

1.定義

傳送方與接收方對明文的加解密使用不同的金鑰，傳送方使用的是「加密公鑰」(public key)，而接收方則是「解密私鑰」(private key)，因加密公鑰是公開的，因此每個人都可以依照加密規則將資料進行加密，但若要解開該加密的資訊，僅有解密私鑰可以將加密的資料解開。



2.常見的非對稱式加密方法

(1)RSA 加密

一種對「極大整數做因數分解」的方式，其因數分解的難度決定了 RSA 的可靠性，因為當數值越大，做因數分解越困難，截至目前為止還沒有可靠破解 RSA 的方式。

3.兩者之間的差異(以比較圖為例)

	對稱式加密	非對稱式加密
產生的金鑰數目	1 把	2 把
金鑰種類與用途	1 把秘密金鑰 傳送方與接收方共同保護	1 把公開金鑰，1 把秘密金鑰 傳送方持有公開的加密金鑰，接收方持有機密的解密金鑰。
金鑰管理的困難程度	較困難 雙方都需確保該把金鑰的機密性、完整性、不可否認性。	較簡單 但是需要數位簽章或公正的第三方來驗證公鑰的真實性，避免公鑰配發過程遭受竄改。
處理速度	較快	較慢
舉例	DES、3DES、AES、RC4	RSA

(三)TCP/IP 架構傳輸層與網路層之資安機制協定與其功能

1.傳輸層所提供的資安通訊協定及功能

(1)傳輸層主要功能

主要提供端對端的連線通訊，處理其流量控制(如：TCP Sliding Window)、壅塞控制(如：TCP Tahoe)、錯誤控制(如：TCP Error Control)，強化網路層所提供的服務品質(QoS)，並接收上層資料，決定所提供的服務型態(TCP、UDP 等)。

(2)傳輸層資安通訊協定其功能

A.SSL(Secure Socket Layer)

負責於傳輸層建立端對端之間的安全連線，防止在兩個設備之間發送的所有資料被駭客讀取及修改任何傳輸中的資訊，並與應用層的協定互相獨立，提供兩端安全機密通訊，Client 與 Server 端的互相認證等功能。而最新版本的 SSL3.0 已於 2015 年正式棄用，轉使用 TLS 協定。

B.TLS (Transport Layer Security)

以 SSL3.0 為基礎，將 SSL 標準化後所發布。TLS 提供端對端之間身分驗證與通訊保密，並且與上層協定是獨立無關聯的。而最常見的運用則是於使用者瀏覽網站保障其安全，當 Web 的 HTTP 於 SSL/TLS

上運作時，即為 HTTPS。目前最新使用的版本為 TLS1.2，目前 TLS1.0 已被發現弱點，駭客可以發送錯誤提示，使得安全連線等級強制降級至 SSL3.0，故使用時務必注意關閉 SSL3.0 與 TLS1.0。

C.SSH(Secure Shell)

建立於應用層與傳輸層基礎之上的加密傳輸協定，可以在不安全的網路環境下建立一個安全的傳輸環境。最常見的應用是遠端登入系統，最常利用 SSH 下指令或遠端執行命令等等。SSH 取代了明文傳輸資料的協定，如：FTP、POP、Telnet 等等，並可防止 DNS 欺騙(DNS Spoofing)與 IP 欺騙(IP Spoofing)，但目前已開發出可以竊取 SSH 對談的工具。

2.網路層所提供的資安通訊協定及功能

(1)網路層主要功能

提供網路之間路徑的選擇，提供網路的服務品質(QoS)、流量控制、壅塞控制，設備可以透過 IP 協定找到對方的位址並互相連線；透過 ARP 協定以 IP 位址詢問其 MAC address；ICMP 可以查詢網路狀況。

(2)IPSec (IP Security)

是一種網路層資安通訊協定套件，透過對 IP 協定的封包進行加密和認證來保護 IP 協定的網路傳輸協定，避免網路封包傳遞過程中被竊取或進行中間人攻擊。IPsec 主要由以下兩個安全協定組成。

A.認證標頭(AH)：主要認證封包標頭是否有遭受竄改或偽裝，提供完整性檢查、訊息認證及反重播攻擊，不提供機密性保護，有『傳輸模式』與『通道模式』兩種封包模式。

B.封裝安全負載(ESP)：透過加密，重新封裝原 IP 為另一個 IP 封包，進而提供機密性、資料來源認證、完整性檢查和傳輸機密性保護，同樣也有『傳輸模式』與『通道模式』兩種封包模式。

二、試寫出下列無線區域網路（Wireless LAN）相關的名詞之定義與其功能：

(一)什麼是 AP？此外，並寫出其功能。(10 分)

(二)什麼是 WPA2？此外，並寫出其功能。(15 分)

答題關鍵	本題屬於無線網路相關考題中算是較為基本的名詞解釋題型，作答時應完整敘述相關名詞及功能，避免僅回答題目要求之單一名詞。

【擬答】

(一)Access Point 解釋及其功能

IEEE 公佈之 802.11 無線區域網路標準(Wireless Local Area Network, WLAN)，通稱 Wi-Fi，並不斷的更新其標準。以下為 WLAN 相關名詞解釋。

1.Access Point(AP)：提供無線網路資源的設備，是無線網路與有線網路的中介裝置，無線網路透過無線電發出訊號，而有線網路則是接上實體網路之設備，如：router 等。提供了身分驗證、加解密、DHCP 等功能。

2.Basic Service Set(BSS)：指一個 AP 所涵蓋的區域稱之。

3.Distribution System(DS)：指一個 AP 彼此相互串連的區域網路組成一個 DS。

4.Extended Service Set(ESS)：相同一個區網(區域)內可能安裝了多台 AP，由多個 AP 所組成的 BSS 與 DS 組合而成，稱之一個 ESS。

5.Service Set IDentifer(SSID)

(1)BSSID：AP 之 MAC Address 稱之。

(2)ESSID：無線網路顯示出的名稱稱之。

(二)WPA2 的定義與功能

1.WPA2 定義

是一種保護無線網路存取安全的技術標準，因前一代的 WEP 產生許多漏洞，因此 WPA 是在 802.11i 完備之前替代 WEP 的過渡方案。WPA2 一定要啟動並且被選來代替 WEP 才能生效，但是在某些舊裝置的安裝指引或預設組態中，WEP 標準是預設選項。

在 2017 年揭露了 WPA2 的漏洞，使得全球的 Wi-Fi 加密連線都面臨高風險危機，隔年(2018)Wi-Fi 聯盟就公布了 WPA3 加密協定，並表示它能提供更安全可靠的加密方式，保護用戶的網路連線裝置，避免封包資料被竊聽與偽造，以取代 WPA2 和其他較不安全的加密協定。

2.WPA2 功能與驗證方式

在 WPA 的設計中，要用到一個 802.1X 認證伺服器來分發不同的金鑰給各個終端使用者；不過它也可以用在較不保險的「預共享金鑰模式」(Pre-Shared Key, PSK)，讓同一 AP 底下的每個使用者都使用同一把金鑰。

Wi-Fi 聯盟把這個使用 Pre-Shared Key 的版本稱「WPA-個人版」或「WPA2-個人版」(WPA-Personal or WPA2-Personal)，用 802.1X 認證的版本稱「WPA-企業版」或「WPA2-企業版」(WPA-Enterprise or WPA2-Enterprise)，而使用 802.1X 認證伺服器的驗證方式如下：

(1)Client 端發送「要求存取」的訊息給 AP，AP 再回傳要求 Client 端身分。

(2)Client 端以其身分封包回傳給驗證伺服器。

(3)驗證伺服器再傳送許可封包給 AP。

(4)AP 最後將 Client 端的連接埠放在授權狀態，正式允許資料傳輸。

而 WPA2 提供 2 項新的資料鏈結層加密協定，TKIP(使用 RC4 加密演算法)以及 CCMP(Counter Mode with CBC-MAC Protocol, 採取 AES 演算法)。

三、試寫出下列雲端運算（Cloud Computing）相關的名詞之定義與其資訊安全問題：

(一)什麼是 VM？此外，並寫出其功能。(10 分)

(二)於雲端運算平台上，目前常見的網際安全攻擊（Cyber Security Attacks）有那些並說明其特性？請列舉三項？(15 分)

答題關鍵	虛擬化平台常被用於雲端服務中，且因其具有減少甚至避免惡意程式直接影響到實體主機的特性，而被用來作為動態分析(Dynamic Analysis)惡意程式的沙箱(Sandbox)。雲端平台上常見的資安攻擊大多針對阻斷雲端服務或利用遠距傳輸需求，夾帶或植入惡意程式。

【擬答】

雲端運算為使用者透過雲端業者所提供的伺服器來做運算的過程。業者現能夠利用雲端服務來傳遞各式各樣不同的資訊，其中包括數據、伺服器、分析等，所有的東西都能夠在雲端上運作、儲存、以及存取。

(一)VM 為虛擬機(Virtual Machine)，是一種受到隔離保護且內含作業系統和應用程式的軟體容器。每個虛擬機都功能完備且完全獨立，而一部主機內可同時存在多個虛擬機。使用者可透過虛擬機的彈性部署及有效分配系統資源種種特性，充分利用既有的硬體資源。

(二)於雲端運算平台上目前常見的網際安全攻擊（Cyber Security Attacks）有：

1.DDoS 攻擊：利用大量的互聯網流量使目標伺服器或其周圍的基礎設施不堪重負，從而阻斷目標伺服器、服務或網路的正常流量。

2.網路釣魚攻擊：會嘗試透過電子郵件、網站、文字訊息或其他形式的電子通訊來竊取敏感資訊。

3.惡意軟體：當雲端運算平台被植入惡意軟體，如：間諜軟體、勒索軟體、病毒和蠕蟲等，使用這些服務的資訊主機將遭到感染，造成損失。

四、什麼是 SOC？於 SOC 風險管理中，執行其風險評估以衡量威脅(Threats)與弱點(Vulnerabilities)的發生機率（Likelihood）時，可能會衍生那兩項主要的問題？此外，請提出策略以解決此問題。（25 分）

答題關鍵	SOC 在許多組織中被視為發現資安事件的第一道防線，然而，SOC 發出告警的機制可能會因為風險評估機制的種種因素，造成誤判和漏判兩個主要問題。

【擬答】

資訊安全監控中心（Security Operation Center, SOC）又稱為資安維運中心或資安營運中心，為集中式即時掌控組織資訊安全狀態的單位。成立目的為整合並管理組織各種情況下的資安訊息，對資安事件依管控機制緊急應變，並整合及分析安全事件，以確保組織資訊安全。於 SOC 風險管理中，執行其風險評估以衡量威脅與弱點的發生機率時，可能會衍生下列兩項主要的問題。

(一)第一個面臨的問題會是誤判（False Positives，FP），意即把正常行為判定為異常行為，其結果可能是導致使用者所需要的服務被封鎖，這樣的原因通常來自黑名單、例外管理以及處置方式，或是 SOC 判斷的依據不夠全面。當一個正常的使用行為經過 SOC 的風險評估，認為類似某些黑名單中的惡意行為特徵時，隨即警報或直接採取措施。雖然資安人員會根據這些警示進行審查並捕捉任何可疑行為，不過，如果資安人員每天收到數以千計的低真實性警示，這些告警將失去意義。

解決：一個 SOC 系統，若未經良好的調整與設定，可能會產生大量的無用警報，以至於淹沒了實際上真正的惡意行為，而分析師往往只能花更長的時間來確認這些警報，甚至使分析人員不再信任警報。在 SOC 中沒有任何一種方案可將誤報完全消除，唯有不斷的調整設定並與時俱進才能有效解決。

1.盤點目前所蒐集的設備紀錄，確保這些紀錄並沒有重疊的部分。

2.對關鍵資產做出分類及風險評鑑，以利區分優先級別。

3.負責資安、開發、及管理等相關人員，定期招開會議審視警報精準度。

4.避免只用一種判定標準，例如：當多個判定條件都針對同一事件認定為異常事件時，才發出告警，如此可使警報精準度提升。

(二)第二問題則是漏判（False Negative，FN），意即將真正的惡意行為視為正常，而導致疏漏，此問題較誤判嚴重，因有可能會對資訊系統造成損失而不自覺。這樣的原因通常因為威脅情資不足、無法即時更新或過於僵化的判斷模式。過於僵化的例子是僅透過雜湊值判斷是否為惡意程式，若 SOC 採用的判斷模型過於單一，且無法透過正規化及關聯比對所蒐集的資料取得較為全面的資安事件特徵，很可能會造成漏判。

解決：未知或能避開 SOC 偵測的惡意行為可透過下列方式減少漏判：

1.部署蜜罐(Honey Pot)系統或誘捕技術將狀況回報至 SOC 中，以提高警報的精準度。

2.進行滲透測試，由紅隊的駭客思維中，實際從攻擊面學習經驗，調整警報精準度。

3.使用機器學習的技術，允許識別模式，藉此進行學習和改進，判斷警報的前後時間的訊息，提高精準度。

4.平時不斷執行威脅獵捕(Threat Hunting)以及針對組織資訊系統之零日弱點(Zero-day Vulnerability)進行挖掘，並對互聯網、暗網或資安相關論壇所公開且與組織相關之資安資訊持續關注。