《資通安全》

試題評析	第一題：本題為訂定資訊安全政策，其主要架構即為ISO 27001，若同學能掌握其中的作業規範14個要項，應不難作答。 第二題：本題為基本的SSL數位信封考題，要求同學解釋其流程與特性，屬於基本分，應能完全掌握。 第三題：本題為SET流程，是沉寂一陣子沒出現的考古題，同學需掌握其協定流程，亦不難拿分。 第四題：本題考IPSec的流程及兩種模式，為基本的網路安全題目，同學若能敘寫詳細，即可拿到高分。
考點命中	第一題：高點《資訊管理與資通安全》第四回，金乃傑編撰，頁 121～124。 第二題：高點《資訊管理與資通安全》第四回，金乃傑編撰，頁 34～35。 第三題：高點《資訊管理與資通安全》第四回，金乃傑編撰，頁 36～37。 第四題：高點《資訊管理與資通安全》第四回，金乃傑編撰，頁 38～39。

一、請試述政府行政機關在制訂資訊安全政策時，其內容至少必須包含那些事項。(25 分)

【擬答】

政府機關在制定資訊安全政策時通常會參照經濟部標準檢驗局的 CNS27001、CNS27002 的國家標準，及 ISO 27001 的資訊安全管理系統(ISMS, Information Security Management System)，另外也常依循行政院之《行政院所屬各機關資訊安全管理要點》、《個人資料保護法》、《著作權法》、《電子簽章法(會使用到金流的機關)》等，最後依照機關實際業務需求進行設計。

根據《行政院所屬各機關資訊安全管理要點》之要求，內容必須包含以下事項：

(一)資訊安全之「定義」、「目標」、「原則」與「標準」，對資訊安全政策之解釋及說明。

(二)資訊安全之「範圍(或影響的單位)」，此項中常參考 ISO27001 的作業規範來界定：

1.人力資源安全：確保使用者意識資安問題，降低人為風險；考量資安人員聘僱與解雇。

2.資產管理：對不同重要性資產分類並盤點，以保護及確保可用性。

3.存取控制：訂定存取控制規則，管理使用者、資料、網路與應用程式的存取控制，偵測未授權的活動。

4.密碼學：訂定密碼學控制原則，並使用加密保護資訊的機密性、真實性與完整性。

5.實體與環境安全：避免未授權存取、破壞與影響實體設備，實行安全保護與使用管理。

6.作業安全：確保資訊設備正確且安全的運作且不受惡意程式攻擊；進行系統備份、紀錄並稽核操作行為。

7.通訊安全：維持資訊處理與通訊的完整性及可用性，並確保資訊在網路上的安全。

8.系統開發與維護：確保系統發展生命週期流程的安全、訂定開發安全政策、進行安全測試。

9.供應商關係：保護組織被供應商存取的資訊；監控並檢視供應商的服務、管理供應商服務變革。

(三)員工應遵守之規定，包括：

1.政府法令及契約對機關資訊安全之要求及規定。

2.資訊安全教育及訓練之要求。

3.電腦病毒防範之要求。

4.業務永續運作計畫。

(四)推行資訊安全工作之組織、權責及分工。

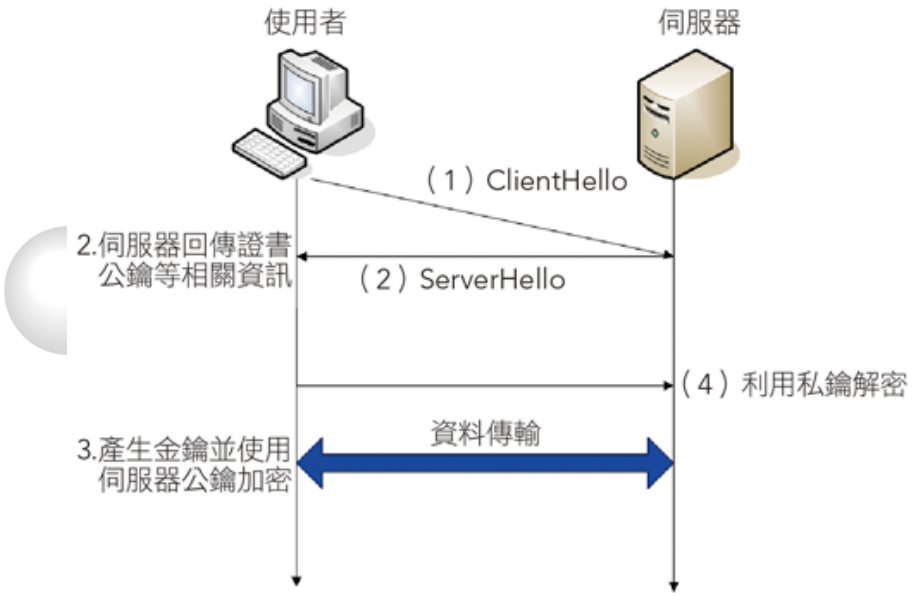
(五)員工應負的一般性及特定的資訊安全責任。

(六)發生資訊安全事件之緊急通報程序、處理流程、相關規定及說明。

二、請說明如何整合對稱式密碼系統（Symmetric Cryptosystem）與非對稱式密碼系統（Asymmetric Cryptosystem）而成一套數位信封（Digital Envelope）機制，並詳述其特色。(25 分)

【擬答】

(一)數位信封(Digital Envelope)是一種電子資料交換的安全機制，將用來加解密檔案的「對稱金鑰」包在「非對稱金鑰」中傳遞給資料交換對象，讓兩方可以使用約定好的對稱金鑰加解密。以下繪製數位信封的資料交換流程：



(來源：http://www.netadmin.com.tw/article_content.aspx?sn=1106140008)

過程步驟說明如下：

1.使用者瀏覽器發出 ClientHello 給 SSL 網站伺服器：告知伺服器瀏覽器可以使用 SSL 加密及演算法版本序號。

2.SSL 伺服器回應 ServerHello：裡面包含伺服器的數位憑證(存放伺服器公鑰及其他伺服器身分認證的資訊)、這次要使用的演算法。

3.使用者瀏覽器傳送加密後的對稱金鑰給伺服器：瀏覽器依照演算法產生一把對稱金鑰(稱為 session key，僅使用於本次加密)，並使用伺服器的公鑰將該金鑰加密(因只有伺服器有解密的私密金鑰，故對稱金鑰不會被傳輸過程中破解)。

4.伺服器解開金鑰取出對稱金鑰進行往後互傳資訊的加解密操作。

在此操作流程中，非對稱金鑰與對稱金鑰扮演的角色如下：

- 非對稱金鑰(Asymmetric Cryptosystem)：保護對稱金鑰的傳輸。
- 對稱金鑰(Symmetric Cryptosystem)：實際對要傳輸的資料加解密。

(二)數位信封的特色如下：

1.執行速度快：使用對稱金鑰演算法的優勢，加解密計算較簡單，執行速度快。此外，也由於使用對稱金鑰，密文的長度不會太長，減少網路傳輸的流量與加快傳輸速度。

2.對稱金鑰交換安全：使用非對稱金鑰保護對稱金鑰的傳送，確保對稱金鑰傳輸時不會暴露於網路上受到擷取。

3.資料機密性：透過加密，確保資料只有特定的對象能存取，避免未授權的存取。

4.資料完整性：經過加密演算法的保護，當資料遭受竄改時便無法完成解密，確保收到的資料都是未經竄改的原始資料。

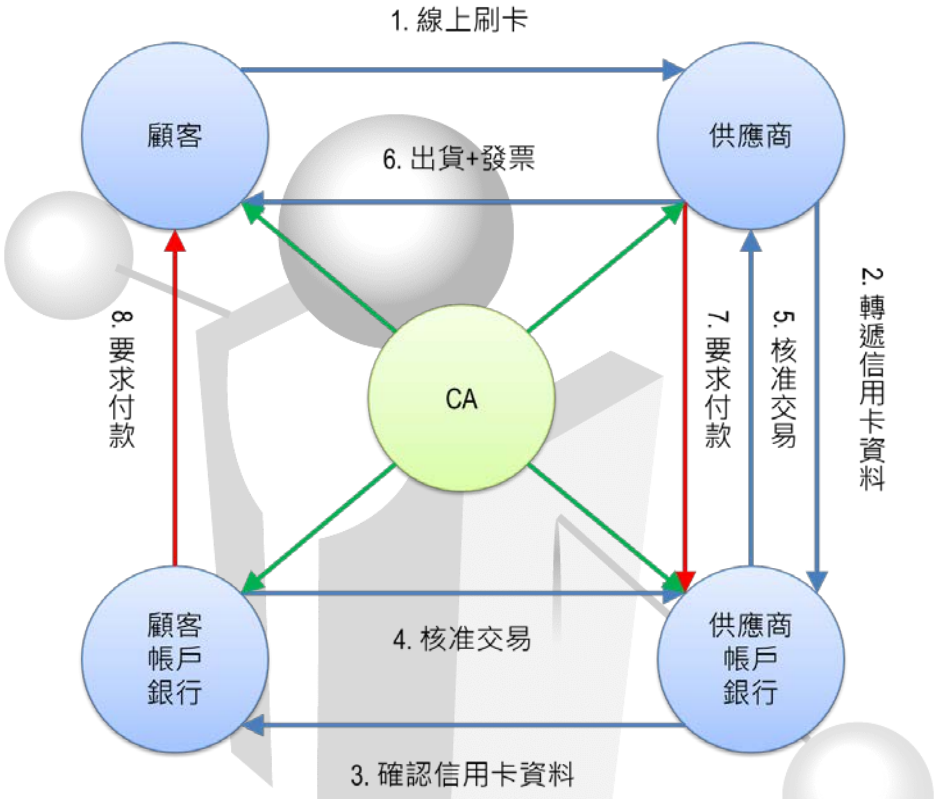
5.片面身分認證性：伺服器提供憑證讓使用者瀏覽器驗證，可以確保資料交換的伺服器確實為其所聲稱的身分；但使用者端瀏覽器沒有提供憑證，因此身分認證僅為片面的。

三、安全電子交易（Secure Electronic Transactions, SET）協定是一套消費者、商家與銀行間的安全交易協定。請詳述其如何運作及如何保障交易的安全性及消費者的隱私。（25 分）

【擬答】

(一)安全電子交易協定(Secure Electronic Transaction Protocol, SET)：在 1996 年由 VISA 與 MasterCard 兩大信用卡組織所共同提出，並與 IBM 合作研發製訂的安全電子交易標準，其所採用的規格是 RSA 在 1024 bits 之下的非對稱式演算法。SET 是一種運用 PKI 並結合 DES 對稱式加密技術的網路安全電子付款協定，用以確保買賣

雙方資料傳遞的機密性、完整性、身分認證與不可否認性。其運作流程如下：



(來源：改繪自《資訊管理：e 化企業的核心競爭能力》，林東清著)

說明：

1.顧客在網路購物時透過 SET 軟體進行線上刷卡。

2.產品供應商將應收金額傳遞給供應商簽約之銀行，並使 SET 軟體直接將信用卡資料傳遞給供應商的簽約銀行。

3.供應商的簽約銀行與顧客的發卡銀行確認顧客信用卡資料。

4.顧客發卡銀行核准交易，將款項轉給供應商合作銀行。

5.供應商合作銀行收到款項，通知供應商核准交易。

6.供應商出貨，將產品寄送給顧客。

7.每月供應商向供應商合作銀行請款。

8.顧客發卡銀行亦每月要求顧客繳交卡費。

(二)對於交易的安全性與保障消費者隱私說明如下：

1.機密性：資訊先以 DES 加密，再透過 RSA 建立數位信封傳遞。

2.完整性：透過數位簽章確保交易資訊未經竄改。

3.身分認證性、不可否認性：SET 使用持卡者、商店的憑證及數位簽章進行不可否認的驗證，確認消費者、商家之身份的正確性。

4.隱私性：採雙重簽署機制(Dual Signature)。顧客對供應商提供訂購清單，對供應商帳戶銀行提供付款資訊。供應商無法得知顧客的付款資訊，但可向供應商帳戶銀行確認是否付款；供應商帳戶銀行無法得知顧客購買商品，但可向供應商取得購買商品總額。

四、IPSec（IP Security）是實現 VPN（Virtual Private Network）的一種方式。請詳述在 IPSec 中，傳送資料前必須先執行的步驟，並說明傳送資料時的兩種模式：傳輸模式（Transport Mode）與通道模式（Tunnel Mode）。（25 分）

【擬答】

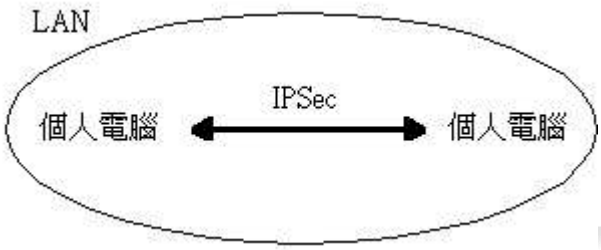
(一)IPSec(IP Security)由 IETF 所提出的 IP 層通訊安全保密架構，是 IPv6 的一部份，應用在網路層，與上層執行的應用程式或路由器無關。透過金鑰等機制提供機密性、完整性與身分認證性等服務，包括存取控制、非連線模式完確保證、資料封包來源鑑別、資料封包複製攻擊保護、資料內容機密性、部份的流量資料機密性等，提供 IPv4 和 IPv6 高品質的封包傳輸。在 IPSec 中傳送資料前必須先執行的步驟如下：

1.初始化：因為 IPSec 是一種連接導向(Connection-Oriented)的協定，因此在傳輸前必須先建立安全連結(Security Associations, SA)，使用 ISAKMP(Internet Security Association and Key Management Protocol)協定來決定傳輸時使用的對稱金鑰(Secret key)，另外也會在此階段決定要使用 AH 或 ESP 的加密協定。由於 SA 是單向的，因此必須建立傳送端到接收端及接收端到傳送端兩條連結。

2.金鑰交換：利用非對稱加密法，讓雙方各自擁有相同的對稱金鑰。

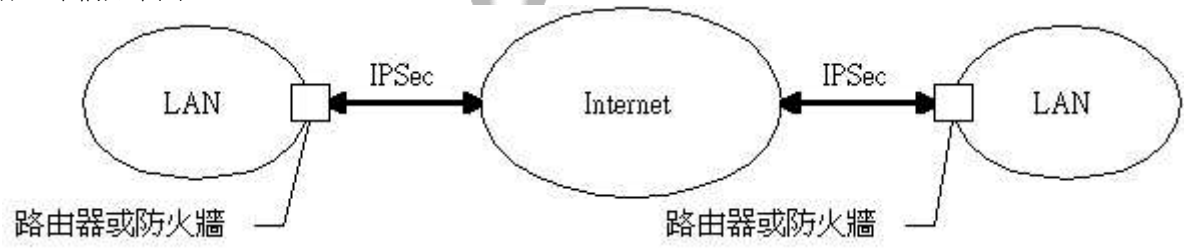
(二)IPSec 的傳輸模式與通道模式說明如下：

1.傳輸模式(Transport mode)：提供主機之間的點對點通訊，因此傳輸模式中傳送、接收資料的雙方裝置都必須能使用 IPSec 協定。在傳輸模式中是提供對上層協定(如 IP 協定)的保護，ESP 在傳輸模式中會加密 IP 承載資料，也會選擇性的進行認證，但並不會處理或更動 IP 標頭的內容。傳輸模式其主要目的為建立區域網路內部的安全通訊，避免在區網內透過 Sniffer 等軟體監聽。架構如下圖所示：



(來源：https://www.microsoft.com/taiwan/technet/columns/profwin/13-IPSec-1.mspx)

2.通道模式(Tunnel mode)：提供區域網路間透過網際網路安全地傳輸資料(即 VPN)，讓區域網路間不必再架設昂貴的專線，而是透過網際網路來連線，確保有安全傳輸的特性。此模式僅需要區域網路對外的路由器(或防火牆)具備 IPSec 的能力，而區域網路中的裝置則不需要額外的設定，因此具備通透性。通道模式常用於提供位於外地的分公司透過網際網路與總公司的區域網路建立安全的通訊管道，以存取總公司的內部伺服器。架構如下圖：



(來源：https://www.microsoft.com/taiwan/technet/columns/profwin/13-IPSec-1.mspx)