《資訊管理與資通安全》

試題評析	今年考題算是較有挑戰性的，除了要具有對基本概念的理解外，也要知道應用的場域並融會貫通相關的概念才可以在分數上脫穎而出。從第一題便知道如果只準備基本概念而沒有深入了解他的演算方式會在答題上過於單調。第二、三題則是大量的考驗同學融會貫通的技能，智慧城市雖然是主要在問「城市」的智慧化，但是對於智慧化有概念的同學，不管是什麼樣的智慧化都可以完整的解答並獲得高分。最後則是考了同學對於整體PKI與數位憑證架構的了解，知道政府在依照一個技術制定相關管理規定與法律時要考量的重點。本次考題需要同學平時不斷的複習與一直補充相關技術性的知識才可以在分數上有明顯地差異。

一、支援向量機（Support Vector Machine, SVM）是常見的資料分類演算法，請詳述支援向量機的運作原理，並舉出兩個採用支援向量機進行資料分類的應用實例。（25分）

試題評析	此題為非常專業的考題，多數同學在答題時要掌握SVM的基本概念與領域是拿到基本分數的必要條件。如果要更近一步拿到更多分數，則需要將其演算法做稍微的描述，但是這對於許多非理工科系的同學會較為吃力。總結來說「基本概念」、「應用場域」和「特性」是必要寫出的部分，對同學來說不會太困難，「演算法內容」、「關係定義」和「相對接近度的拿捏」是較為困難的也是本題拿高分的關鍵。

答：

(一) SVM是一種分類(Classification)演算法，由學者Vapnik等根據統計學習理論提出的一種新的機器學習方法。其在解決小樣本、非線性及高維模式識別問題中表現出許多特有的優勢，從有限訓練樣本得到的決策規則對獨立的測試集仍能夠得到較小的誤差。其概念是建構一個超平面(hyperplane)，讓資料在空間中能夠被區分成兩類，所以又被稱為二元分類器(binary classifier)。直觀來說，分類邊界距離最近的訓練資料點越遠越好，因為這樣可以縮小分類器的泛化誤差。儘管原始問題可能是在有限維空間中陳述的，但用於區分的集合在該空間中往往線性不可分。為此，有人提出將原有限維空間對映到維數高的多的空間中，在該空間中進行分離可能會更容易。為了保持計算負荷合理，人們選擇適合該問題的核函式 $k(x, y)$ 來定義SVM方案使用的對映，以確保用原始空間中的變數可以很容易計算點積。高維空間中的超平面定義為與該空間中的某向量的點積是常數的點的集合。定義超平面的向量可以選擇在資料基中出現的特徵向量 x_i 的圖像的參數 α_i 的線性組合。通過選擇超平面，被對映到超平面上的特徵空間中的點集 x由以下關係定義： $\sum_i \alpha_i k(x_i, x) = \text{constant}$ 注意，如果隨著 y 逐漸遠離 x ， $k(x, y)$ 變小，則求和中的每一項都是在衡量測試點x與對應的資料基點 x_i的接近程度。這樣，上述核心的總和可以用於衡量每個測試點相對於待分離的集合中的資料點的相對接近度。

(二)常用的分類如下：

1.目前常用於手寫辨識系統，能夠透過上述演算法分辨出使用者的字跡。

2.用於圖像分類。實驗結果顯示：在經過三到四輪相關回饋之後，比起傳統的查詢最佳化方案，支援向量機能夠取得明顯更高的搜尋準確度。這同樣也適用於圖像分割系統，比如使用Vapnik所建議的使用特權方法的修改版本SVM的那些圖像分割系統。

二、智慧城市(Smart City）是現代化城市的創新建構。請說明智慧城市的定義，並舉出兩個智慧城市的應用實例及其搭配採用的相關資訊科技。（25分）

試題評析	本題看似陌生，但其實在考同學對於基本概念的融會貫通，只要能夠理解「智慧ＸＸ」的概念，並套用在不同的領域上，本題即可迎刃而解。唯獨較有挑戰性的是使用的範例，這部分需要理解在都是規劃上所需要的建設，並輔以上課補充，即可連結都市建設和各種新興系統產生的綜效，並達到智慧城市的訴求。
考點命中	《高點・高上資訊管理與資通安全講義》第一回，蕭老師編撰，頁18-21

答：

(一)智慧城市基本特徵的界定是：全面聯網、充分整合、激勵創新、協同運作等四方面。即智慧型傳感裝置將都市公共設施物形成物聯網，物聯網與網際網路系統完全對接融合，政府、企業在智慧基礎設施之上進行科技和業務的創新應用，都市的各個關鍵系統和參與者進行和諧高效地共同作業。智慧城市不僅強調物聯網、雲端運算等新一代資訊科技應用，更強調以人為本、協同、開放、用戶參與的創新2.0，將智慧城市定義為新一代資訊科技支撐、知識社會下一代創新（創新2.0）環境下的都市形態。智慧城市基於全面透徹的感知、寬頻泛在的互聯以及智慧型融合的應用，構建有利於創新湧現的制度環境與生態，實現以用戶創新、開放創新、大眾創新、協同創新為特徵的以人為本可持續創新，塑造都市公共價值並為生活其間的每一位市民創造獨特價值，實現都市與區域永續發展。因此，智慧城市的四大特徵被總結為：全面透徹的感知、寬頻泛在的互聯、智慧型融合的應用以及以人為本的可持續創新。

(二)常見的應用範例如：

1.公共運輸管理和監測及電子道路收費系統，均能應用於交通繁忙的地區，有助改善和紓緩道路擠塞的問題，實踐「智慧流動」。公共運輸管理和監測能向車主提供實際資料，避免車主將車輛駛入擠塞的路段，提升都市運輸效率。電子道路收費系統則是以用者自付原則減低非必要的交通需求，從而改善地區性交通擠塞及空氣品質。

2.在都市計畫上，透過網路和遙距監控技術，政府可充分掌握及分析都市的天氣狀況、資源運用的程度和道路交通狀況等資料，因而調節及善用社群的資源，實現節能減排，減低「環境足跡」，提升環境的可持續性。

三、依據行政院所屬各機關資訊業務委外服務作業參考原則，除相關法令另有規定或屬政府核心資訊業務者外，基於提升營運效率的考量，請詳述政府機關有那些類型的資訊業務可委託民間資訊服務業者辦理？（25分）

試題評析	此題非常需要融會貫通的能力，在答題上除了要先講述基本的委外原則跟考量因素外，接下來要套用在政府的思維上。老師在這邊列出完整可委外的項目，同學在答題上未必能夠完整的記得全部的細項，但這不影響獲得高分關鍵，同學只要掌握可以委外項目之特性，並抓緊每個特性思考資訊系統在開發的過程中的每個階段，哪些符合講述的特性即可。

答：

若資訊系統具有「競爭優勢的核心能力」、「高專屬性與獨特性」、「高策略機密性」和「高交易成本與不確定性」時是不適合做委外的，相反的，大部分政府委外的項目皆具有以下特性：

1.低競爭優勢
2.低策略性
3.低不確定性
4.低獨特性
5.高成熟
6.高標準化
7.高安全性
8.高開發穩定性

綜合以上考量，並根據中華民國資訊軟體協會，政府在委外時，可以考量的項目如下所列：

委外內容	工作說明
整體規劃	對組織未來資訊系統應用方式，提供一個整體性的藍圖，以確定使用資訊系統(電腦)的目的，分析所需之各項資源(設備、人力、經費、時程等)及具體的實施步驟。
顧問諮詢	顧問諮詢係為了因應資訊系統開發、使用過程中，可尋求專業機構提供管理技術、專業知識及建議。
資料登錄	將原始文件委外以人工作業方式輸入成電腦可處理之媒體。
資料處理	委外單位將需要以電腦處理之工作，全部或一部份委由業者以其自有設備，代為規劃、設計、處理或委由業者派員前來操作委外單位之設備，按一定之程式處理產出媒體者。
軟體開發	指應用軟體系統製作及相關之服務。其作業範圍包括新系統開發設計、舊系統汰舊換新、

	舊系統架構更改、系統移轉訓練、系統保固等工作。
軟體維護	指應用軟體之維護服務，包括版本更新、錯誤偵測與排除、更正性服務等。
系統管理	將全部或部份資訊系統之整體運作，包含人員、環境設備、機器設施，作業程序及管理制度，以及其它相關或延伸之作業委外管理：系統管理服務之方式可以是委託單位自備設備，服務單位提供管理服務；或者由服務單位提供資訊或環境設備及管理服務，委託單位擁有使用權等不同之方式。工作內容包含整體資訊管理制度之規劃及建置，擬定資訊系統之運作方式及執行，訂定服務水準指標以作為執行之要求及改善之依據等工作。
網路服務	從最基本的兩部工作站的串接、區域網路建置，伺服器建置、主機銜接進而廣域網路連結，國內、外長距離傳輸等等，不僅含蓋硬體、軟體系統之建置，更涉及資料庫之使用，各地(國)之電信線路(機具)租用。
機房設施管理	電腦設備、機房及相關管理業務委外處理，運用外界之專業技術，協助執行設施管理任務。包括管理制度之規劃、執行，提供運作環境及軟硬體設備之規劃或管理等。
備援服務	備援中心之規劃、建置或提供備援中心服務以及資料處理中心有著實體上的脆弱性，發展災變發生時及時恢復重要資訊系統之運作及利用計畫。
訓練推廣	資訊教育訓練之規劃與執行委外單位在業務資訊化過程中，有關各階層人員常態性資訊教育訓練之規劃與執行。其訓練範圍可包括電腦軟硬體技術、資訊管理技術、行政管理技術及領域專業技術等。
硬體維護	對於購買的硬體設(如：系統主機、終端機、工作站、個人電腦、印表機、繪圖機、連線設備等)於保固期限內由原供應業者依購買時、約定提供各項售後服務。在保固期滿後，為維持原硬體之功能及正常運作，所提供的定期維護合約工作統稱為硬體維護。
系統整合	針對特定業主特定專案需求，以重新開發之軟體、搭配硬體、網路及週邊設備等所組成的整體資訊系統。這類系統通常只針對極少數客戶的大型專案計畫(金額以千萬元新台幣計者)整合不同廠牌電腦硬體、軟體及週邊產品，並且結合行業專業知識(Domain knowledge)包括網路、需購置或開發的硬體設及軟體。
系統稽核	確保電腦中心內部作業安全控制能有效的建立並長期維持一定品質。協助評估並稽核電腦中心安全作業管制標準。

四、公開金鑰基礎建設（Public Key Infrastructure，簡稱PKI）涵蓋技術、管理、法令等三大議題。以發行數位憑證（Digital Certificate）為例，請詳述這三大議題的主要具體內容。（25分）

試題評析	此題算是本次考試中較為挑戰性的一題，需要整體面地回答數位憑證的流程、發行和使用。在技術面要專注於回答如何發行的流程與技術架構，管理上需要回答較為概念性的架構與管理方法，最後是法令要站在政府的角度出發要怎麼樣設計法律上的管理機制，如此即可以達到較高的分數。
考點命中	《高點・高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁64-65

答：

數位憑證(certificate)利用公開金鑰密碼技術來提供身份識別的能力，以保護網路上資料傳輸的正確性、保密性等，不僅可以代表使用者，也可以代表機器、組織機構甚至是程式的身份。它是由憑證管理機構應用數位簽章技術所簽發的一組資訊，內容包含個體的公開金鑰、一組資訊內容，包含個體的公開金鑰憑證擁有者、簽發單位以及其他一些訊息。

(一)技術

在發行時需要數位憑證密鑰：對當與其他個人或企業通過網路環境進行通信時，需要建立一個安全的交換資訊通道來保證不會有第三方非法用戶截獲和讀取資訊，現在最先進的加密資料的方法是通過使用密鑰對方式。密鑰對包含一個公鑰和一個私鑰。我們可把開鎖的鑰匙比作密鑰，不同的是密鑰是一對鑰匙，一把用來保證安全，即加密；而另一把用來解密。

當申請一個數位憑證時，以瀏覽器為例，瀏覽器產生一個私鑰和一個公鑰。私鑰只被憑證申請者使用，而

公鑰會成為數位憑證的一部分。

收到並安裝數位憑證後，把數位憑證發給任何需要發送資訊給你的人。在數位憑證中包含了用於加密資訊的公鑰。別人給你發送資訊時會使用你的公鑰對資訊進行加密。因為只有你有與之相同的私鑰，能夠解密用你的公鑰加密的資訊。

同樣的，當你想要向別人發送加密的資訊，你必須首先獲得他們的公鑰。你可以在目錄中伺服器中（一般，CA（Certificate Authority）系統在簽發憑證的同時會將該憑證發佈到公開的目錄伺服器中供其他客戶查詢、下載用）查找他們的數位憑證。如果你只有經過簽名處理的電子郵件，你的電子郵件應用軟體一般會自動的保存發送方的數位憑證。

(二)管理

在發行上，需要一個可以信任的第三方當作CA，「憑證管理中心」是如同「護照簽發機關」或「認證會計師」一樣可信任的第三方機構。憑證管理中心負責數位憑證的發行、廢止、續約，並提供數位憑證目錄。憑證管理中心在發行憑證時，必須遵循嚴格的程序來驗證申請個人及組織。所有數位憑證皆以「憑證管理中心」的私密金鑰加以簽章，以確保其真實性。憑證管理中心的「公共金鑰」則會廣泛發行。

(三)法令

在我國憑證市場發展的初期，為避免政府因對於起步中的電子認證產業限制過多而侷限其應用，並鼓勵電子認證產業的多元發展，因此在電子簽章法中，對於憑證機構之管理規範，乃採尊重市場機制自由發展的模式，對於認證業務之經營並不太過限制。然而憑證機構既扮演公正第三人的角色簽發憑證，若政府完全放任其經營而不適度介入規範，恐難保障使用憑證之消費者或信賴憑證之第三人的權益。為兼顧扶植產業發展及保障消費者權益，電子簽章法乃採規範憑證實務作業基準應載明事項之管理方式，賦予主管機關適當程度介入監督相關憑證服務契約的權力，來維護保障消費大眾之權益。