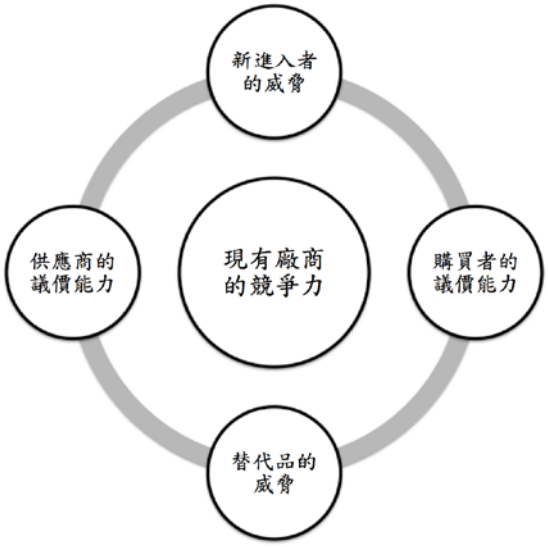
《資訊管理與資通安全》

一、依據波特（Michael Porter）提出的競爭力模式（Competitive Forces Model），請詳述運用資訊科技或資訊系統可以強化企業競爭力的策略為何？（25分）

試題評析	波特的五力分析一直是亙古以來經典的題型，此題又屬於中規中矩的題目，同學在答題上只要有記熟五力分析的基本概念即可，並且針對每一種競爭力分析其影響力即可。 透過波特的競爭力模型可以分析出企業該採取的策略，在舉例上只需要針對幾種影響力來分析企業該採取的行動與邏輯便是很完整的答題架構。
考點命中	《高點・高上資訊管理與資通安全講義》第二回，蕭維文撰，頁88-92。

答：

由Michael Porter於80年代所提出，透過五種力量的不同組合來分析企業的競爭力與制定戰略。



(一)新進入者的威脅

市場的新進入者帶來了新生產力與資源的同時，也讓原有的企業做出抵抗此競爭力的行為，導致不必要的浪費而降低利潤。

1.進入障礙：產品差異、資本、銷售渠道、政府相關政策、地理位置、自然資源……等，有許多是無法透過簡單的複製就可以取得的資源，也是新進入者的挑戰。

2.預期現有企業之反應：企業的財力、資產規模、規模增加速度……等，都有可以影響現有企業所採取的反新進入者之行為。

(二)供應商的議價能力

供應商若具有較高之供給資源優勢，就會對買主產生威脅，對企業的獲利能力有負面的影響，而供方的能力會因為以下因素而較強大：

1.供應商所提供的產品市場非常穩固，且較不受市場劇烈競爭影響，此時任何買方都不可能成為此供應商的主要客戶。

2.供應商的產品具有一定的客製化或特色，買主難以找到其他可替代商品或轉換成本過高。

(三)購買者的議價能力

購買方通常會透過希望壓價並提高服務質量，此行為會影響企業的獲利能力。而通常具有以下幾點的購買方具有較大的威脅：

1.購買者少但購買量皆大

2.賣方市場的組合皆是規模小且數量多

3.購買者個產品無特殊差異性

(四)替代品的威脅

市場上替代品的出現會讓現有企業必須提高質量或壓低售價來與之競爭，而替代品的競爭強度可以透過考察其銷售增加率、替代品廠商的生產力與營利情況來分析。

(五)現有廠商的競爭力

企業競爭加劇的原因：

1.市場進入障礙低

2.競爭者範圍廣泛

3.市場成熟，成長趨緩

4.產品或服務相似，轉換成本低

根據以上觀點，企業可以採取的策略為：

1.成本領導：若商品的同質性高，售價為唯一的考量時，市佔率高的廠商可以利用經濟規模來壓低成本，出售同質但是價位較低的商品。

2.差異化：若成本不是此商品的唯一考量時，企業可以集中資源在某項具重要顧客利益的產品。

3.集中化：致力於一個或多個較窄的市場區隔。

二、何謂智慧合約（Smart Contract）？它與一般的應用程式有何不同？（25分）

試題評析	近年來由於比特幣的狂漲，讓此類的金融科技變成顯學，在準備上除了要嘗試理解目前市面上常見的代幣差異外，最重要的是搞懂其背後運作的基本原理。 在區塊鏈上其實應用非常廣泛，並且可以結合的理論與實用都非常多，像本題的智慧合約即為一例，答題上需要詳細說明其應用結合的優勢與概念。
考點命中	《高點・高上資訊管理與資通安全講義》第二回，蕭維文撰，頁55-56與上課補充。

答：

(一)智慧合約(Smart contract)是由法律學者Nick Szabo在1995年提出來的，其定義為：一個智慧合約是一套以數字形式定義的承諾，包括合約參與方可以在上面執行這些承諾的協議。最常與區塊鏈結合的一種防偽機制，用程式碼撰寫合約內容，並且交由機器或是電腦執行合約內容。其好處是合約不會因為被有心人士干預而被竄改、中斷；約定的行為也不用透過其他人或第三方，而是透過電腦自動執行，可以避免各種因人為因素而起的糾紛，相較於人來執行合約內容更有效率。

(二)智慧合約與一般的應用程式的差異如下：

1.較容易與金流整合

一般的應用程式要整合金流要經過許多程序甚至是政府監管，造成金流服務不能非常普及，但是智能合約和金流概念可以緊密結合，並使用以太幣或是其他新建立的代幣系統。

以以太鏈為例，代幣的概念是以太鏈中可用於智慧合約或區塊鏈事務的東西，有如遊樂場的代幣，智慧合約可以結合代幣，若再搭配其他相關程式，可以非常容易做到分散行的應用程式，像是可以把一般人閒置的電腦計算能力租用給有需要的組織，一般人只要安裝具有租用功能的程式，此程式便可以讓租用人以某種定義好的代幣來支付費用。

2.部署與維護成本較低

一般的應用程式若擺在網路上供人使用，需要提供網址給人下載或服務，也需要大量的人力與資源來維持伺服器的運作，因此在前期部署和後期維護上都需要大量的成本。

智慧合約只需要在部署時提供一筆費用給參與交易驗證的人（通常我們稱這種人所做的事情為「挖礦」），合約在部署後，會變成區塊鏈中不可更動的一部分並分散儲存在全球各地的節點上，換句話說即是部署後就個人就不太需要維運的成本，也不用定期更新，查詢時也不用額外的費用。

3.資料儲存成本較高

一般應用程式的資料是儲存在本機或是伺服器上，當有讀取資料的需求時再跟本機或是伺服器拿取，而智慧合約是將資料儲存在區塊鏈上，節點較多，故一開始的存入成本會較高，而且也需要付一部分費用給挖礦的人，故成本會較高。

4.觸發後無法更改

一般的應用程式可以透過更新或改版來達成新程式的部署，但是智慧合約一旦部署到區塊鏈上，就無法更改，除非加入額外的智慧合約，才可能透過規避或是繞過智慧合約部署後無法再更改的限制。

三、請詳述「虛擬桌面」（Virtual Desktop）的定義及採行虛擬桌面的優點。（25分）

試題評析	虛擬桌面為組織為了管理方便與節省資源的有效方法之一。 此題為非常中規中矩的考題，只需要依照題目要求說明其定義與優缺點即可，答題上只要能把定義與優缺點緊密的結合，在此題上就可以拿到不錯的分數。
考點命中	《高點・高上資訊管理與資通安全講義》第三回，蕭維文撰，頁40-41。

答：

(一)為虛擬化技術的一種，使用上讓伺服器的計算能力搭配精簡的客戶端應用模式來改變傳統電腦的分散式計算模式，讓使用者可以在一般電腦或是桌面上使用伺服器的硬體，亦可在不影響實體環境的情況下，提供異質平臺與軟體測試的能力，除了可以提升應用的靈活度外，並可將分散在各使用者電腦上的作業系統和應用程式，統一收納至後端伺服器，提升管理性和安全性。

(二)虛擬桌面可以分為個人與企業應用二種類型：

1.個人端的虛擬桌面

為一種安裝在原電腦作業系統上的應用程式，使用上會建立相對應的虛擬磁碟檔案與虛擬機器（VM），並在其上安裝虛擬作業系統，在執行時會利用程式來模擬電腦硬體，像是處理器、硬碟、顯示卡……等。也因為此特性，使用者在虛擬環境中所做的任何更動都不會影響到原始的作業系統，是開發人員在測試環境時常用的方法。

2.企業級虛擬桌面

(1)集中型虛擬桌面

利用網路將存放在遠端伺服器上的虛擬機企劃面傳送到使用者的桌面，也可以透過複製映像檔的方式，將相同的環境給不同的使用者來使用，由於這種機制僅會傳送電腦畫面，以及個人端電腦的鍵盤、滑鼠等操作指令，因此需要的頻寬較少，對前端平台的硬體等級要求較低。實際應用上，一台伺服器可以提供給多個使用者使用，且可以重複利用相同的檔案，初期建置成本較低。

(2)分散運算虛擬桌面架構

使用者所使用的桌面平台具有儲存能力，在使用伺服器派送虛擬機器給使用者操作時，須同時保有原作業系統。在此架構下，會使用到較多的個人電腦運算資源，故對於個人電腦的規格要求較高，初期建置時，需要將映像檔逐一傳送到使用者電腦，故前期部署的時候需要較大的頻寬。

四、請詳述內建加解密或數位簽章模組之IC卡或晶片卡可能面臨的安全威脅及攻擊，並說明造成這些安全威脅或攻擊成功的原因。（25分）

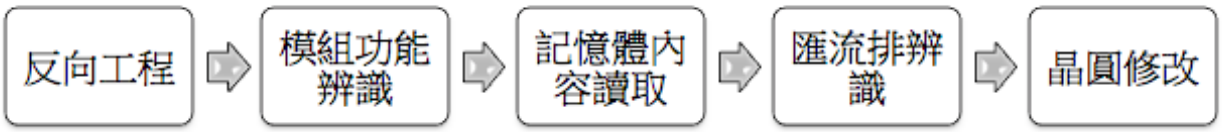
試題評析	此題為較少見的題型，IC晶片卡為目前生活中常見的卡片形式，使用非常廣泛，若對於攻擊的基本概念不熟悉，則不容易拿到高分。此題的心法為掌握IC晶片卡的基本概念與要點，並且針對每種要點分析可能的攻擊模式，順便帶入每種攻擊模式的優缺點與潛在的風險，即可獲得不錯的分數。

答：

(一)侵入式攻擊(Invasion Attack)

利用微探針(Microprobing)直接掃描晶片並取得相關的資訊之技術，此種攻擊模式是利用晶片在製造時必須透過此種探針來量測晶片所達成。在攻擊上不需要知道太多晶片相關的資訊即可做到。

最有效的防禦方法為在晶片硬體製造時就置入反侵入偵測的設計。



(二)軟體攻擊（Software Attack）

利用晶片卡之應用軟體、IC卡與讀卡機之相關通訊協定、密碼演算法、COS等軟體程式之弱點，而取得密碼模組之內部秘密參數等相關資訊。例如：猜測PIN碼、未授權之檔案存取、惡意程式碼、SIM卡之暴力攻擊。

(三)側通道攻擊（Side Channel Attack）

經由非正常通道，即所謂的側通道，監測密碼模組在執行過程中，因運算動作與運算元之不同，造成密碼模組在某些物理特性上之變動，而側錄此變動波形，再經由分析此洩漏之訊息，解讀出密碼模組之內部秘密參數。例如：測量與觀察密碼模組的功率消耗(SPA/DPA)攻擊、執行時間(Timing)攻擊……等。

(四)故障攻擊（Fault Attack）

利用外力造成密碼模組在執行時發生錯誤，並利用錯誤的輸出與密碼模組的相關資訊來推算或找出機密資料。此種外力所造成密碼模組運算錯誤，可能是暫時性的，在攻擊事後，該密碼模組可經由程序回復正常工作稱為暫態故障；也可能該外力造成密碼模組嚴重毀損，而無法回復，此種現象稱為永久故障。