申論題

一、
(一)FinTECH 是近年相當重視的觀念，請定義何謂 FinTECH？
(二)承上小題，這類的創新推動在各國會進行 Regulatory Sandbox 配套措施，請說明其意義。

擬答：

(一)金融科技（Financial technology，FinTech），是指一群企業運用科技手段使得金融服務變得更有效率，因而形成的一種經濟產業。這些金融科技公司通常在新創立時的目標就是想要瓦解眼前那些不夠科技化的大型金融企業和體系。位於愛爾蘭都柏林的國家數位研究中心把金融科技定義為一種＂金融服務創新＂，同時認可這個名詞也可以用於指稱那些廣泛應用科技的領域，例如：前端的消費性產品、新進入者與現有玩家的競爭、甚至指比特幣這樣的新東西。因此 FinTech 可說是一種新型的解決方案，這種方案對於金融服務業的業務模式、產品、流程、和應用系統的開發來說，具有強烈顛覆性創新的特性。

(二)沙盒或稱沙箱（Sandbox）是指在開發軟體過程中，所建立的一個與外界環境隔絕的測試環境，工程師會在沙盒內放置軟體測試其功能。英國金融業務監理局（Financial Conduct Authority）將這個概念應用在金融科技（Fintech）的創新上，新創公司只要在沙盒內，就可以在一定的範圍內不需要受到國家法律的規範，可以逕行測試自己的創新服務、商業模式，這個模式就被稱為監管沙盒（Regulatory Sandbox）。這是政府為了因應金融科技的快速發展而制定出來的機制，因為很多金融科技公司屬於破壞式創新的公司，這些公司試圖打破業界原有的制度、嘗試建立起新的遊戲規則，而這樣的嘗試通常伴隨著法規上的罰則和限制，或是根本無法可管。因此，英國政府打造了一個安全空間讓新創公司可以在裡面進行實驗，讓新創公司可以在裡面盡情的嘗試新服務、功能，除此之外政府也可以在監管沙盒內與公司一同研擬在創新過程中可能需要面對的法律、商業問題。對新創公司來說進入監管沙盒內除了有法律的豁免好處外，監管沙盒也是一個能夠了解自己的服務對群眾來說是否適用的方法。

二、區塊鏈被視為是金融科技(Fintech)與物聯網(IoT)等產業不可或缺的應用趨勢，請說明區塊鏈技術中如何利用單向雜湊函數(One-way Hash Function)等技術來達到不可竄改及去中心化等特性？

擬答：

(一)**確保資料不被竄改：**比特幣區塊鏈採用 Hashcash 演算法來進行工作量證明，Hashcash 可將任意長度的資料經由 Hash 函數轉換為一組固定長度的代碼，這是一個基於單向雜湊函數(One Way Hash Function)的轉換，容易被驗證，但卻很難推出原本的值。

(二)**經由 Merkle Tree 將大量訊息縮短成一個 Hash 值達成去中心化**：在比特幣區塊鏈中，每筆交易產生後，都已經被 Hash 成一段代碼才廣播給各節點，為節省儲存空間並減少資源耗費，比特幣區塊鏈的設計原理採用 Merkle Tree 機制，讓這些數百到數千筆的交易 Hash 值，經由兩兩一組形成一個新 Hash 值的方式，不斷重複進行，直到最後產生一組最終的 Hash 值，也就是 Merkle Tree Root，這個最終的 Hash 值便會被記錄到 Block Header 中，只有 32 Bytes 的大小。Merkle Tree 機制可大幅減少資料傳輸量與運算資源消耗，驗證時，只需驗證這個 Merkle Tree 的 Root 值即可。接著再**用時間戳伺服器（Timestamp Server）確保區塊序列**，將每個區塊 Hash 後加上一個時間戳（Timestamp）並發布出去，這個時間戳用來證明資料在特定時間的有效性，每一個時間戳章會與前一個戳章一起進行 Hash，這個 Hash 值會在與下一個時間戳章進行 Hash，因此而形成一個用來確保區塊序列的鏈。由此達成去中心化的效果。

三、請詳述機器學習（Machine Learning）的定義及其應用。

擬答：

(一)機器學習是一門人工智慧的科學，該領域的主要研究物件是人工智慧，特別是如何在經驗學習中改善具體演算法的效能，研究能通過經驗自動改進的電腦演算法，用資料或以往的經驗，以此最佳化電腦程式的效能標準。

(二)機器學習應用方式包括下列：

1.背誦式學習(Rote learning)
這是機器學習中最簡單的一種形式，因為它不對輸入資料做任何處理，直接儲存問題的解答，等到以後同樣的問題出現時再取出解決。其知識可經由不同的管道獲得，包括已經預先製作好的學習或以記憶給定之事實和資料。

2.例舉式學習(Learning from Examples)→類神經網路
就是從一些例子中歸納出規則，由電腦推導出一個一般性表示式，必須可以包含所有的正例，並且排除所有的反例。例舉學習可能是漸進式的(Incremental)，即對每一個例子修改其目前已建立的知識基礎，或者是一次式(One Trial)的，即針對所有的資料形成觀念，當新的例子進來時，一次式的演算法必須重新執行。目前主要應用在類神經網路上，用來解決複雜問題。

3.教導式學習(Learning from instruction)→建立 KB
就是將人類所熟習的高階語言，翻譯成程式可用的內在知識結構，且將此知識與現有的知識基底整合在一起，以做有效的應用。可用於發展專家系統中使用的知識庫。

4.類推式學習(Learning by analogy)→CBR
就是將現有的知識類推應用到類似的新問題上，類推式學習要求學習者具有更多的推論能力。可用於案例推理系統(Case-Base Reasoning)，以電子化的方式將組織過去發生過的許多案例的過程、問題、解決方案，儲存在案例庫(Case Base)中，並設計許多屬性(Attribute)來區分其特質(例如系統規模、支援功能、專案預算、客戶特性、所使用的技術、主要發生的問題等)，然而當有新的問題發生時，使用者輸入各種屬性後，系統內的搜尋引擎，便會去找到屬性最相似的過去案例，並提供最佳解決方案。又或者法官可根據各種不同案例的特色，在 CBR 內搜尋到過去相類似判例來參考。

5.觀察與發現式學習(Learning by observation and discovery)
這種學習是針對非監督式學習(Unsupervised learning)，學習內容並不由指導者組織好，通常不是以原始的形態輸入程式，就是由程式自己經由實驗產生。例如 AlphaGo zero 與 Alpha zero 均為此種應用，可以自行學習發展出應用於圍棋與其他棋類的人工智慧程式。

四、請試述下列名詞之意涵：
(一)何謂電子郵件社交工程攻擊？
(二)勒索病毒的攻擊方式為何？
(三)何謂紅隊演練？
(四)何謂應用程式介面(Application Programming Interface, API)？
(五)何謂軟體即服務(Software as a Service)？

擬答：

(一)是指通過電子郵件與他人的交流，來使其心理受到影響，做出某些動作或者是透露一些機密資訊的方式，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破資通安全防護，遂行其非法的存取、破壞行為。

(二)勒索軟體通常透過木馬病毒的形式傳播，將自身為掩蓋為看似無害的檔案，通常會通過假冒成普通的電子郵件等社交工程方法欺騙受害者點擊連結下載，但也有可能與許多其他蠕蟲病毒一樣利用軟體的漏洞在聯網的電腦間.....傳播。入侵後，有一種勒索軟體僅是單純地將受害者的電腦鎖起來，而另一種則系統性地加密受害者硬碟上的檔案。所有的勒索軟體都會要求受害者繳納贖金以取回對電腦的控制權，或是取回受害者根本無從自行取得的解密金鑰以便解密檔案。

(三)紅隊演練(Red Team Assessment) 是在不影響企業營運的前提下，對企業進行模擬入侵攻擊，在有限的時間內以無所不用其極的方式，從各種進入點執行攻擊，嘗試達成企業指定的測試任務。

(四)應用程式介面是一種計算介面，它定義多個軟體中介之間的互動，以及可以進行的呼叫(call)或請求(request)的種類，如何進行呼叫或發出請求，應使用的資料格式，應遵循的慣例等。它還可以提供擴充機制，以便使用者可以通過各種方式對現有功能進行不同程度的擴充。

(五)是一種軟體交付模式。在這種交付模式中，軟體僅需通過網路，不須經過傳統的安裝步驟即可使用，軟體及其相關的資料集中代管於雲端服務。使用者通常使用精簡客戶端，一般即經由網頁瀏覽器來存取、存取軟體即服務。

五、組織資訊安全的重要議題之一為近期內通過的個人資料保護法，請問該法中所指的個人資料包含哪些？試從資訊系統設計的角度，列舉至少四項企業防範觸犯個資法應採取的措施。

擬答:

(一)個人資料保護法的個人資料指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

(二)1.注意工作帶回家可能產生的資料外洩風險：

(1)除非組織規定允許，否則不應將公務資料帶回家。

(2)如果必須將公務資料帶回家處理，應確認家中電腦亦有適當的安全防護，例如啟用防火牆、安裝防毒軟體並更新最新病毒碼、更新系統修補程式等。

(3)若使用家中電腦處理公務資料，應儘量保持為較安全的使用環境，例如不要安裝 P2P 軟體，甚至離線作業。

(4)儲存重要資料的外接式儲存媒體應小心保管。

(5)個人慣用的筆記型電腦常存有個人、公務資料，應特別留意保管，勿讓宵小有機可乘。

2.重視個人帳號的密碼安全：

(1)帳號密碼為身份驗證的基本防護，務必重視密碼保護並設定強度足夠的安全密碼。

(2)在工作場所之外的電腦登入使用系統，須留意是否為安全的使用環境並確認密碼無外洩之虞。

3.保護敏感資料：

(1)適當保護敏感資料，例如將文件加密或設定開啟密碼。

(2)遵守組織的保密規定及遵行各項使用規範。

(3)提供資料供公開查閱，須確認是否有民眾敏感資料(例如身份證字號、醫療資訊、通訊資料等)被不當暴露。

4.遵循組織的電腦使用規定：

(1)工作電腦的使用，應遵循組織的電腦使用規定。

(2)即使工作電腦的使用權限允許安裝軟體，亦必須合乎組織資訊安全規定、軟體使用規範與法令。

5.防範網路詐騙攻擊：

(1)當點擊的網址為原網站的外部連結時，應格外提高警覺。

(2)不要因為好奇心任意點擊情色、聳動等標題的網址連結。

(3)電子郵件夾帶副檔名.exe、.com、.bat 等檔案，幾乎都是惡意程式，不要開啟。

六、

(一)政府部門的資訊系統與網路若是被非法入侵，將影響政府的聲譽。請列出資訊安全三要素並簡要說明。

(二)資訊安全管理系統 / 制度(Information Security Management System–ISMS)以 ISO 27001 與 ISO 17799 規範為參考依據，請列出 ISMS 的四項運作模式。

擬答：

(一)資訊安全三要素一般簡寫為 CIA：

1.機密性要求(Confidentiality)：
維護資訊資源(產)使免受不當之存取、使用、揭露，確保只有被授權的用戶可以依權限存取資料。

2.完整性要求(Integrity)：
確保資料是完整的，沒有被竊取或不當修改。

3.可取用性(Availability)：
確保被授權的用戶，當有需要存取資料時，得以順利獲得。

(二)ISMS 的四項運作模式：

1.規劃(Plan)：訂定 ISMS 環境與風險評鑑。

2.設計(Design)：ISMS 設計與實作。

3.檢查(Check)：監控、審核 ISMS。

4.行動(Act)：改進 ISMS。

七、當資訊人員面臨會引起倫理議題的情境時，該如何分析此一情境呢？一旦分析完成後，有那些倫理準則可幫我們制訂決策？

擬答：

(一)可用資訊時代的五大道德層面(Laudon,2005)進行分析：

1.資訊權(Information rights)：
網際網路時代中的隱私權和自由，其中隱私權(privacy)是個人要求獨處，不受他人或組織甚至政府監督或干擾的一種權利。政府網站必須留意維護民眾的隱私權，避免資料外洩。

2.財產權(Property Rights)：
智慧財產，包括商業機密、著作權和專利權。政府網站必須遵守相關智慧財產法規規範。

3.責任歸屬、賠償責任與控制：
電腦相關的賠償責任問題。政府網站必須遵守相關規範，負起可能的賠償責任。

4.系統品質(System Quality)：
處理資料品質與系統錯誤。政府網站必須儘量減少錯誤，並提高資料品質。

5.生活品質(Quality of Life)：

(1)公平、使用與範圍，考量 IT 帶來的社會負面效果，如電腦犯罪與濫用。

(2)科技與再造使得職位逐漸流失。

(3)資訊公平與使用權：增加種族與社會階級的不協調。

(4)健康的風險：重複受壓傷害(RSI)，電腦視力症候群(CVS)與科技壓力症。政府網站必須遵守相關規範，努力縮減數位落差，儘量減少負面效果。

(二)倫理分析步驟：

1.清楚的辨認與描述事實：
清楚的釐清事實會讓問題\較容易解決。

2.確認衝突或困境，並辨認其中更高層次的價值：
例如資訊安全與個人隱私可能相互衝突。

3.確認利害關係人(stakeholder) ：
找出這些人或團體及其需求，將會使問題解決變的簡單。

4.確認可以合理執行的方案：
因為可能沒有一個方案可以滿足所有的利害關係人。

5.確認執行所選方案後的可能結果：作為以後檢討改進。

(三)倫理準則：

1.Imperative Kant 普遍理論(Immanuel Kant’s Categorical)：
一個原則敘述如果一個行動對每依個人去做都是不對的，那麼它對任何人都是不對。

2.Descartes 改變原則(Descartes’ rule of changes)：
一個原則敘述如果一個行動不能重複執行，則任何時間都不能採取這種行動。

3.功利主義原則(Utilitarian Principle)：一個原則假設人會將價值排序也了解不同行動方式的後果。

4.風險規避原則(Risk Aversion Principle)：
是說人都會採取產生最小傷害或最低成本的行動準則。

5.天下沒有白吃的午餐原則(no free lunch rule)：
假設所有有形的或無形的物件，除非有特別的宣告，否則都是由某些人所擁有，而且該物件的創造者對此物件會要求相對的報酬。

八、我國目前正在評估選舉是不是可以採取網路投票，但很多人都非常擔心網路投票如何確保資料安全。請以網路投票為例，說明何謂 ：
Confidentiality (安全隱密性) (5 分)
Authentication (身分認證性) (5 分)
Integrity (資料的完整性) (5 分)
Authorization (授權性) (5 分)
Non-repudiation (不可否認性) (5 分)

擬答:

(一)安全隱密性(Confidentiality)：
確保資訊的機密，防止機密資訊洩漏給未經授權的使用者，以網路投票來說就是要確保每個人所投的票不能被未經授權者所竊知。

(二)身分認證性(Authentication)：
要能確認資料訊息之傳輸來源，以避免有惡意的傳送者假冒原始傳送者傳送不安全的訊息內容。以網路投票來說就是要確保每個投票人的身分，避免被人假冒身分投票。

(三)資料的完整性(Integrity)：
保證資料內容僅能被合法授權者所更改，不能被未經授權者所篡改或偽造。以網路投票來說就是要確保所投的票不會被人竄改。

(四)授權性(Authorization)：
使用者只能擷取被授權部分的資訊，以網路投票來說就是要確保所有的使用者(包含投票者、開票者等)都只有擷取被授權部分的資訊，例如投票者可以擷取到是否已經投票，而開票者只能擷取到投票者投給誰，但是無法了解誰投給誰。

(五)不可否認性(Non-repudiation)：
對於傳送方或接收方，皆不能否認曾進行資料傳輸或接收，意即傳送方不得否認其曾傳送某筆資料，而接收方亦無法否認其確實未曾接收到某訊息資料。以網路投票來說就是要確保投票者無法否認已經投票，也要開票者無法否認已經收到此一投票訊息。