《資通安全概論》

一、資訊科技發展快速且應用廣泛，企業面臨的資安挑戰也越來越多，使得企業必須實施有效的資安措施來保護企業的資訊資產。防火牆作為維護資安的重要設備之一，請詳述防火牆對企業網路與資訊安全有那些重要性？（25分）

試題評析	此題為傳統考點，重點於防火牆對於資訊安全的重要性與應用。由於此題已出現多次，因此必須將2025新的防火牆架構帶到，方能在眾多考生中與眾不同。此題是考重要性，因此不要過多注重於防火牆類型，而是提及最新型的防火牆架構即可。
考點命中	《高點・高上資通安全概論講義》第二回，金乃傑編撰，頁48~50防火牆。

答：

(一)防火牆：可由軟體或是硬體來實作的一種安全機制，用來隔離兩個不同的網路或是接觸不明的網路，利用既有的過濾規則，控制與檢閱內部與外部的封包，達到有效的攻擊風險管理。

對於企業的重要性：

1.服務控制：決定哪些服務可以存取，例如：禁止使用ftp提供外部下載，則禁止FTP port 20和21。

2.流向控制：應用階層閘道防火牆進行封包篩選和深度封包檢查，決定流入、流出方向的封包通過防火牆時，檢視連線狀態、篩選惡意IP與過濾服務類型等等，因此也可以限制內部惡意者上傳檔案，防止內部資料外流。

3.使用者控制：根據使用者的存取權限，來控制使用者可以存取的網路服務，但是企業內部必須有使用者的帳號控管與身分認證，例如：只有主管帳號可以看youtube或是FB、X等社群。

4.代理伺服器：內部網路與外部網路不直接交換聯絡，而是透過防火牆進行封包交換，除了可以達到NAT與VPN功能，惡意攻擊者真的要攻擊，損害的範圍也只有代理伺服器受損，不及於公司內部組織。

(二)下一代混合式網狀架構防火牆(Next Generation Firewall，NGFW)：

下一代混合式網狀架構防火牆是軟體、硬體的結合，由於工作組織的龐大，因關稅而導致跨國大廠設廠加速，組織員工與據點大幅增加下，企業組織加速數位轉型與扁平化，因此員工比以往更加分散，網路從中央延伸至邊界，可彈性、快速與整合的部署為下一代防火牆特色，被稱為雲端防火牆或防火牆即服務(FWaaS)。

特色：

1.AI強化的IDS與IPS偵測與即時阻斷。

2.雲端即時更新與部署。

3.零信任領域。

4.AI智能沙盒的預判領域DNS安全性。

5.可部署至IoT裝置，不造成微設備過多工作負荷。

6.資料外洩防治(DLP)。

7.勒索病毒隔離。

8.VPN感知，提高使用深度封包檢查(DPI)高於封包過濾。

二、企業常用STRIDE威脅模型來讓資安分析者可以理解威脅系統的方式，並設法找出威脅。請詳述STRIDE模型代表那六種威脅種類及其對應的安特性。（25分）

試題評析	STRIDE威脅模型原本是一種用在系統分析與設計的方法，讓使用者與設計者了解有預期目標系統那些威脅項目，是開發系統需要投資更多成本的部分，若是臨時忘記STRIDE縮寫，可用CIA與課堂上商務網站的資訊安全需求範例，高點學員還是可以取得不錯成績。
考點命中	《高點・高上資通安全概論講義》第一回，金乃傑編撰，頁.9~11資訊安全要素。

答：

(一)STRIDE包含六種威脅類型與特性：

1.Spoofing 偽造：冒用身分，例如：偽造身分、偽造IP。

2.Tampering 篡改：完整性部分，例如：篡改個人資料、信用卡卡號、購買紀錄。

3.Repudiation 否認性：否認曾經發生行為 ，例如：交易下單賴帳。

4.Information Disclosure 資訊外洩：資訊外流，可用機密性，例如：個人資料外洩、交易紀錄外流。

5.Denial of Service 服務阻斷：耗盡系統資源，例如：系統無法正常連線使用。

6.Elevation of Privilege 權限向上提升：提升自己的權限，往root管理者提權，例如：存取控制修改資料庫、取得統計紀錄。

(二)以電子商務購物網站為例，接續帶入各個攻擊類型例子與防禦手段：

1.偽造：防禦方式可以使用憑證。

2.篡改：防禦方式可以使用MAC(訊息鑑別碼)，雜湊函數MD5或SHA-2。

3.否認性：使用數位簽章。
4.資訊外洩：機密性使用加密，秘密金鑰的結合對稱式與非對稱式。
5.服務阻斷：利用IPv6 Anycast隨播分散攻擊力道、黑洞路由、與封鎖攻擊IP。
6.權限向上提升：SQL injection、緩衝區溢位攻擊。

三、密碼學是一種產生密文的科學與藝術活動，目前是依據柯克霍夫原則（Kerckhoff’s Principle）來發展密碼系統。
(一)請說明柯克霍夫原則？（5分）
(二)另從分析密碼系統角度而言，請詳述有那幾種破密分析（Cryptanalysis）方法？（20分）

試題評析	柯克霍夫原則意思是說密碼系統縱然被人所知，只要金鑰沒有外漏，整個加密系統都是安全的，換句話說，從類似PKI（公開金鑰基礎建設）去構想，高點學員應該沒有太大問題。
考點命中	《高點・高上資通安全概論講義》第一回，金乃傑編撰，頁67古典密碼學。

答：
(一)加密系統需要有的原則：
1.假定攻擊者破解加密方法：就算知道加密方法，也無法破解通訊。
2.加密的密鑰必須容易保存和使用，而且可以改變調整。
3.網路通訊過程中可以有效率運作。
4.加密演算法已知狀態下，只要金鑰沒有外洩，確保密文仍是安全。
5.個人即可獨立完成設定，無須客服或專業人員協助。
(二)密碼分析：
破密分析一門涉及破解、評估和如何騙取密碼的學科，由於要破解一個演算法用到的數學與程式語言難度很高，可能高於政治釋憲程度，不可能於國考短短時間內完成，因此反推考點應該是說，就算密碼完善，可以如何無關數學與程式技術的破密分析。
1.暴力破解法：破解嘗試可能的密碼如電話、生日等，是一種反覆試驗的方法，用來猜測可能密碼。
2.字典攻擊與彩虹攻擊：變相的暴力攻擊，字典攻擊運用常見密碼組合來破解密碼；後者將預先計算好的，用於逆運算加密雜湊函式的表，常用於破解加密過的雜湊（例如：常用於固定長度的信用卡攻擊）。
3.社會工程：假裝好友騙取密碼。
4.假網站釣魚：以假亂真的網站騙取使用者輸入個資；帶有惡意廣告、新聞、影音點擊播放後，進行XSS攻擊。
5.網路監聽：Sniffer透過混亂模式監聽封包，未加密的密碼進行傳遞時，將被監聽軟體竊取密碼。
6.側通道攻擊：硬體安全中最具威脅的攻擊，針對系統密碼啟動時的物理特性（如：電流功率、電磁輻射）反推系統內部的動作是在進行那些功能操作或是傳送的資料內容，進一步直接獲取資料內容。

四、因應量子電腦的發展潮流，量子密碼學及後量子密碼學等兩大新興的密碼科學類型已被提出。
(一)請說明何謂量子密碼學及後量子密碼學，試比較之。（15分）
(二)請詳述量子密碼基於那些特性來確保其安全性。（10分）

試題評析	下一代密碼學-量子密碼，題目很少見過，但是量子密碼學於實驗室的研究時長已經超過20年之久，只是一直無法商業化，隨著人工智慧的輔助，下一代密碼學或許在很快時間可以問世於家用系統，但是其目的應該也是為了對抗人工智慧生成網路日新月異的計算能力，密碼學也被迫加速前進，於未來考題趨勢值得注意。
考點命中	《高點・高上資通安全概論講義》第一回，金乃傑編撰，頁96~97非對稱加密。

答：
(一)

1.量子密碼學：因量子位元的疊加與糾纏特性，可以同時為0和1狀態，大幅度提升運算能力，實現平行運算，運算次數平均只需所有排列組合的平方根。例如：破解4位元的二進位密碼，2^4=16可能性，傳統運算的二進位模式，嘗試2^4=16，最多嘗試16次，量子運算只需4次運算。
因此，量子密碼學是利用量子原理，著名的量子密鑰分發（BB84協議）即是透過量子量測不確定性與不可複製性這兩個量子物理特性發展，實現安全通信的技術，理論上可以達到「無條件安全」。
2.後量子密碼學（Post-quantum Cryptography, PQC），基於既有密碼學基礎，但是金鑰大於現行2048 bit的百倍以上，其目的要能抵抗因人工智慧與量子電腦的日益增強的計算能力，與量子密碼學最大不同的是：「不需要量子力學的介入」，PQC可以在傳統電腦上執行，目前chrome從SSL機制中，已支援ML-KEM PQC演算法。

比較：

	量子密碼學	後量子密碼學

技術基礎	量子力學物理原理（如量子疊加、量子糾纏）	晶格密碼學、編碼密碼學、多變數密碼學、雜湊密碼學、超奇異橢圓曲線密碼學
演算法	Shor演算法	ML-KEM、ML-DSA量子後演算法
硬體需求	量子電腦	相容傳統電腦
限制	實現技術難度大，基礎設施成本高，於近於零度的低溫下操作且易受外在環境影響，干擾電磁場運作	一般傳統個人PC即可，沒有使用量子力學
現狀	實驗室運作階段	Google與微軟已漸採用PQC演算法機制，如實作於chrome瀏覽器
對抗量子能力	使用量子電腦對抗量子計算，成本高	基於傳統電腦，打造可應對量子計算的演算法

(二)量子密碼基於以下特性，確保安全：

1.疊加性：每一個量子位元有兩種狀態，順時針或是逆時針，於1984年的Bennett與Brassard則是用偏震方向來代表0或1，有直線與斜線兩套，直線方案的「|」為1、「-」為0，斜線方案「＼」代表1、「／」代表0，因此有許多種可能出現的情況，也就是同時處於多個狀態的疊加，稱為疊加性。

2.無法測量性：若使用某個濾光片對量子極化產生一量子位元，那麼使用該濾光片對該量子位元進行量測，便能得到確定的量子資訊，若有其他中間人竊聽時，使用其它濾光片進行量測，干擾系統運作，則其量測結果對照原本的結果是不確定的。

3.不可複製性：量子於疊加狀態，不可能複製出兩個一樣光子，因此未知的情況下，是無法對量子狀態進行完整複製，白話說有人偷看過答案，疊加性就消失了。

4.糾纏性：無法任意分解兩個量子態的乘積，因光子無法分割性與極化相反狀態。

高點・高上公職

考取學長姊大推的優秀師資

資料結構

王致強(蕭立人)

- 獨創「程式碼記憶法」，大幅縮短記憶　和答題的時間！
- 教學採考題導向，範圍由淺入深，即使是底子不好，也能茅塞頓開！

廖○成(高大資管畢)

應屆考取　113高考資訊處理

資料結構要掌握這門科目對我來說非常不容易，**不過王致強老師教得非常好**，教學中有時候連比國考難的研究所考題都會提點，也讓大家能夠掌握國考所需再更以上的資料結構實力，我覺得非常不錯！

資通安全

金乃傑(魏取向)

- 以「學習地圖」概念展現資訊管理多構面的知識，並引入自創圖示標記知識所在位置及相連概念；輔以口訣背誦關鍵名詞、要點。

蔡○諺(中興應數畢)

跨域考取

113高考資訊處理【狀元】

題庫班專注於實戰演練，通過不斷作題，能更快適應考試題型，並且針對薄弱環節進行強化。**金乃傑老師在今年考試中預測的範圍非常準確**，特別是在加密演算法與資料保護法規的部分，考題幾乎全中。

資訊管理

蕭維文

- 具有產業與學術經驗，從不同角度提供最客觀的科技觀點。
- 時事與理論精準結合科技產業，透過精闢分析讓同學理解資訊界。

李○翌(北市大資科畢)

應屆考取

113高考資訊處理、普考資訊處理

資訊管理這科廣到沒有範圍，如果有寫考古題就會發現講義是由各種考古題的解答堆疊出來的，因此**蕭維文老師的魚骨解答法就顯得非常重要**，只需把改卷教授想要的關鍵字搭配以上的方法就可以把答案湊出來。

更多命中實證

更多上榜經驗分享

考點命中實證

《資料結構》

一、某一公司有下圖所示的8個優先順序分別為高或低的待執行工作，且將依順序自A至H每間隔一天的時間放入對應的高優先執行佇列（Qucue）或低優先執行佇列（Qucue），例如A（低）表示A工作排於第一天放入低優先執行佇列，而C（高）表示C工作排於第三天放入高優先執行佇列。此外，執行每個工作所需完成的時間均於工行名稱下顯示，例如執行A工作需要2天時間完成，而執行B工作需要1天時間完成。最後，各個工作的執行規則為，當高優先執行佇列內有工作待完成時，須優先執行該佇列內的工作（由第一個開始執行），直到高優先執行佇列內沒有任何待完成工作時，才可執行低優先執行佇列內的工作（由第一個開始執行）。

自A至H每間隔一天的時間放入對應的高優先佇列或低優先佇列

H（低）	G（高）	F（高）	E（低）	D（高）	C（高）	B（低）	A（低）
1	2	1	1	2	2	1	2

（一）試計算執行此8個工作需要多少天方可完成。（10分）

（二）試計算此8個工作自放入佇列至開始執行的平均等待時間。（15分）

試題評析　佇列相關的基本應用問題，題目本身十分平易。在題意確實掌握的狀況下，正常操作佇列，計算正確時間，取分不難。

考點命中　《資料結構》，高點文化出版，王致強編著，頁4-16～4-17。

答：

（一）總共需要12天可以完成8個工作，如下圖：（灰底為執行中工作，括號為工作剩餘天數）

天數	12	11	10	9	8	7	6	5	4	3	2	1
到達工作					H（低）	G（高）	F（高）	E（低）	D（高）	C（高）	B（低）	A（低）
所需天數					1	2	1	1	2	2	1	2
高優先佇列				G(1)	G(2)	G(2)E(1)	F(1)D(1)	D(2)	D(2)C(1)	C(2)		-
低優先佇列	H(1)	H(1)E(1)	H(1)E(1)B(1)	H(1)E(1)B(1)	H(1)E(1)B(1)	E(1)B(1)	E(1)B(1)	E(1)B(1)	B(1)	B(1)	B(1)A(1)	A(2)

（二）各項工作等待時間如下表：

工作	H	G	F	E	D	C	B	A
等待時間	4天	1天	1天	6天	1天	0天	8天	0天

《資通網路與安全》

五、防火牆（Firewall）是當今企業常見的安全防護設備，請問：

（一）企業常用防火牆隔離出一個網段，稱為DMZ（Demilitarized Zone），請詳細說明其用意為何。（5分）

（二）WAF（Web Applicatiou Firewall）和傳統的封包過濾式防火牆（Packet filtered Firewall）有何不同？請詳細說明。（10分）

（三）防火牆常根據從外部收到的IOC（Indicator of Compromise）來做規則調整，請問IOC的意義為何？（5分）

試題評析　本題為資訊安全之防火牆種類及安全網路架構之題型。

考點命中　《高點・高上資通安全講義》第二回，金乃傑編撰，頁14～28，第三章防護架構，二、防火牆（Firewall）與相關技術。

答：

（一）DMZ（Demilitarized zone）是介於內外路由器間的區域，用於放置組織對外重要的伺服器。DMZ 照字面直翻是指非軍事區域，而電腦網路中 DMZ 可以解析為一個既不屬於內部網域同時也不屬於外部網域的一個特殊區域，其目的就是了為防止外來人侵者直接存取內部機密資料，針對不同資源而提供不同安全級別的保護區域。一般企業將網路伺服器放在 DMZ 供網際網路使用者查詢使用，這些伺服器無法連接到內部資料，因此如果不幸被外來人侵者侵入，重要的資料仍不至於外洩。

（二）WAF（Web Application Firewall）提供應用層的訊息過濾與轉送處理，主要依據應用層的資訊來決定是否放行封包流量，與傳統的封包過濾式防火牆相較，WAF 可過濾傳送的資料內容與命令，確保應用層協定的安全；亦可過濾封包內容與命令，阻斷針對應用協定的攻擊。

（三）IOC 為電腦鑑識中的工具器物(Artifact)，其可從網路或作業系統中觀察，與電腦入侵高度相關。傳統的 IOC 包含病毒特徵、IP 位址、惡意檔案的 MD5 雜湊值，或是殭屍網路(Botnet)命令與控制伺服器的網址或網域名稱。通過事件回應與電腦鑑識的處理過程識別 IOC 後，其可用於入侵檢測系統(Intrusion Detection System, IDS)與防病毒軟體，對未來的攻擊嘗試進行早期檢測。