# 112 年公務人員高等考試三級考試試題

類　　科：資訊處理
科　　目：資通網路與安全

一、請回答下列資訊安全三大元素的相關問題：（每小題 15 分，共 30 分）
㈠請說明機密性，並說明如何應用非對稱式密碼學達成。
㈡請說明完整性，並說明其主要演算法暨應注意事項。

**1.《考題難易》：★★**
**2.《解題關鍵》：資訊安全三大元素基本題，掌握機密性、完整性概念，搭配相關演算法即可完美作答。**
**3.《命中特區》：AF24 資通安全講義第三章完全命中**

【擬答】：
㈠機密性是指確保信息不被未經授權的人員、實體或流程訪問或披露。非對稱式密碼學（也稱為公開金鑰加密）是一種加密方法，它需要兩個金鑰：一個公開金鑰用於加密，另一個私有金鑰用於解密。使用公鑰對明文進行加密後所得的密文，只能用相對應的私鑰才能解密並得到原本的明文，最初用來加密的公鑰不能用作解密 1。
㈡完整性是指確保信息和處理方法的準確性和完整性。完整性演算法通常用於檢查數據是否被篡改或損壞。例如，訊息摘要演算法（如 MD5 和 SHA）可以生成數據的數字指紋，用於檢查數據的完整性。在使用這些演算法時，應注意選擇安全且經過充分測試的演算法，並定期更新以確保安全性。
㈢機密性是指確保資訊只能被授權的人或系統訪問和閱讀，防止未經授權的存取、使用或披露。非對稱式密碼學（Asymmetric Cryptography）是一種加密技術，可用於實現機密性。非對稱式密碼學使用一對密鑰：公開金鑰（Public Key）和私密金鑰（Private Key）。公開金鑰可以被任何人使用，用於加密資訊，而私密金鑰則只能由特定的實體保有，用於解密資訊。應用非對稱式密碼學的主要優勢是在於金鑰的分發和管理。由於公開金鑰可以自由分發，可以建立一個開放的金鑰基礎設施（PKI），使得安全的通訊變得更為便捷和可靠。同時，私密金鑰只由接收方保有，不需要在通信過程中傳輸，提供了更高的安全性。以下是使用非對稱式密碼學實現機密性的過程：
1. 金鑰生成：接收方生成一對公私密鑰。私密金鑰保密保存，而公開金鑰可以自由分發。
2. 加密：發送方使用接收方的公開金鑰將資訊加密。加密後的資訊只能使用相應的私密金鑰進行解密。
3. 傳輸：加密後的資訊可以通過不安全的通道（例如網際網路）安全地傳輸給接收方。
4. 解密：接收方使用自己的私密金鑰對接收到的密文進行解密，從而恢復原始的明文資訊。
㈣完整性是指保證資訊在傳輸或儲存過程中不被非法篡改或修改，確保資訊的完整性和可靠性。
1. 主要演算法用於確保完整性的包括數字簽章（Digital Signature）和訊息摘要（Message Digest）。
⑴數位簽章：數位簽章是一種使用私密金鑰來對資訊進行加密的技術。發送方使用私密金鑰對資訊進行加密，生成一個簽章。接收方使用相應的公開金鑰對簽章進行驗證，確認資訊的完整性和來源的真實性。如果簽章驗證通過，則確定資訊在傳輸過程中未被篡改。
⑵訊息摘要：訊息摘要是將任意長度的資訊壓縮成固定長度的摘要，且不可逆的過程。這通常使用雜湊函數（Hash Function）來實現。發送方將資訊進行摘要計算，並將生成的摘要隨同資訊一起發送給接收方。接收方再次計算接收到資訊的摘要，並將其與原始摘要進行比對。如果摘要匹配，則確認資訊的完整性。
2. 需要注意的事項包括：
⑴金鑰管理：在使用非對稱式密碼學確保完整性時，需要適當地管理私密金鑰，確保其保密性，並且確認公開金鑰的真實性。

⑵安全通道：為了保護數字簽章或訊息摘要的完整性，需要確保傳輸通道的安全性，以防止篡改或替換。

⑶雜湊函數的選擇：選擇具有良好安全性和防衝突性的雜湊函數是確保完整性的關鍵。應該使用廣泛接受的標準雜湊函數，例如 SHA-2 系列或 SHA-3 系列。

⑷確保資訊的完整性是保護資訊安全的重要一環，它可以防止未經授權的修改和篡改，確保資訊的真實性和可靠性。

二、請回答下列分散式阻斷服務相關問題：（每小題 10 分，共 20 分）

㈠請說明分散式阻斷服務的原理與難以防守之原因。

㈡請列舉五項分散式阻斷服務的防護策略。

***1.《考題難易》：★★★***
***2.《解題關鍵》：DDoS 概念題，掌握 DDoS 原理與防護策略概念，即可完美作答。***
***3.《命中特區》：AF24 資通安全講義 P3-25~3-27 完全命中***

【擬答】：

㈠分散式阻斷服務（Distributed Denial of Service，DDoS）是一種攻擊方法，惡意攻擊者運用網路上大量被攻陷的電腦作為殭屍（Bot）向特定的目標發動 DoS 攻擊。DDoS 攻擊的目的是使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法訪問。以下是分散式阻斷服務的原理和難以防守之原因：

*1.* 原理：

⑴攻擊者組織了一個由多個受感染的「僵屍」計算機組成的「僵屍網絡」或「肉體網絡」，也稱為「Botnet」。

⑵攻擊者通過命令和控制伺服器（C&C Server）控制僵屍計算機。

⑶攻擊者發送指令，使所有僵屍計算機同時向目標系統或網絡發起大量的請求或流量。

⑷目標系統或網絡被淹沒在大量的請求或流量下，超出其處理能力，導致服務無法正常提供。

*2.* 難以防守之原因：

⑴分散性：攻擊者使用的僵屍計算機來自不同地區，往往分布在全球各處，使得攻擊流量難以從單一來源識別和阻擋。

⑵規模化：攻擊者可以使用大量的僵屍計算機，甚至數十萬台，組成強大的攻擊力量，以淹沒目標系統的帶寬和資源。

⑶偽造 IP 地址：攻擊者可以使用偽造的 IP 地址或攜帶偽造的源 IP 地址的偽造封包，使得追踪和過濾攻擊流量變得困難。

⑷網路容量：攻擊者可以利用公共互聯網中的龐大頻寬，使攻擊流量難以被鏡像和過濾，導致阻斷服務攻擊更加困難。

㈡分散式阻斷服務的防護策略：

*1.* 流量過濾：實施流量過濾是第一線防禦手段。使用防火墻和入侵防禦系統（IDS/IPS）等工具，對進入網絡的流量進行分析和過濾，過濾掉可能的攻擊流量。

*2.* 負載平衡：使用負載平衡器分散流量，將流量分發到多個服務器上。這樣可以減輕單一服務器的負擔，提高系統的容量和韌性。

*3.* 增強帶寬：擴大網絡帶寬能力，使系統能夠承受更大規模的攻擊流量，減輕攻擊對帶寬的耗損。

*4.* CDN 服務：使用內容傳遞網絡（CDN）服務，將網絡資源分發到全球多個節點，使得攻擊流量能夠在不同節點上被分散和處理，減輕對單一服務器的影響。

*5.* 攻擊流量檢測和過濾：使用流量分析和行為分析工具，檢測和過濾掉異常或具有攻擊特徵的流量。可以基於流量的來源 IP 地址、流量的頻率、流量的特徵等進行檢測和過濾。

三、110 年至 113 年的國家資安發展方案為建構主動防禦基礎網路，打造堅韌安全之智慧國家，請回答下列問題：（每小題 10 分，共 20 分）

㈠請舉例說明何謂數位韌性？

㈡請說明主動式防禦知識庫，並對策略之運用機會舉例。 [112 高]安 1

***1.《考題難易》：★★***
***2.《解題關鍵》：我國資安政策概念題，掌握數位韌性與主動式防禦知識庫概念即可作答。***
***3.《命中特區》：AF24 資通安全講義 P1-39~P1-45 運用資安情資分享與資安聯防體系撰寫。***

【擬答】：

㈠數位韌性（Digital Resilience）是指組織或系統在遭受資訊安全事件或其他數位威脅時，能夠快速恢復正常運作並有效地應對威脅的能力。數位韌性關注的是組織的持續運作和業務功能，而非僅僅對單一安全事件做出反應。例如在俄烏戰爭中，烏克蘭因為有低軌衛星網路（Starlink）的支援，而能持續保持通訊暢通不致中斷。因此，數位韌性的目標是減少損害和中斷，並在威脅發生後盡快恢復正常運作。例如一家銀行遭受了一次大規模的網絡攻擊，導致其資訊系統癱瘓和網上銀行服務中斷。這對該銀行的業務和聲譽都造成了重大損失。然而，由於銀行已經建立了強大的數位韌性，它能夠快速回應並恢復運作。銀行立即啟動了備份系統，以確保資訊系統的連續性。同時，他們通過應急通訊系統向員工和客戶提供了即時的通知和指導。銀行的 IT 團隊開始調查攻擊事件，並進行修復工作，同時與相關的法執機構和專家合作。在數小時內，銀行恢復了資訊系統的正常運作並重新開放了網上銀行服務。這種數位韌性的回應使銀行能夠快速恢復業務運作，減少了損失和業務中斷的時間。

㈡主動式防禦知識庫（Active Defense Knowledge Base）是一個組織使用的資料庫，其中包含了關於已知威脅行為、攻擊者技術和攻擊方法的詳細資訊。該知識庫通常由組織的安全團隊或專業的資訊安全供應商維護，以幫助組織更好地理解和應對數位威脅。主動式防禦知識庫不僅僅是一個資訊收集和存儲的工具，更重要的是它的運用機會。以下是一些運用機會的例子：

1. 威脅情報分享：主動式防禦知識庫可以收集和分享有關新興威脅、攻擊者的行為模式和攻擊方法的情報。組織可以利用這些情報來加強其安全防禦措施，預防類似攻擊。
2. 強化安全事件監控：通過了解已知的攻擊模式和技術，組織可以在其安全事件監控系統中設定相應的規則和警報，以偵測和識別潛在的攻擊行為。
3. 威脅建模和仿真：利用主動式防禦知識庫的資訊，組織可以進行威脅建模和仿真，模擬各種攻擊情境，評估自身的防禦能力，並改進相應的安全措施。
4. 攻擊者追蹤和反制：通過收集和分析攻擊者的行為模式和方法，組織可以更好地理解攻擊者的動機和手法。這有助於組織追蹤攻擊者、收集證據並進行反制。

四、請回答下列資訊安全的相關問題：（每小題 15 分，共 30 分）

㈠請說明 ISO 27001 資訊安全管理系統，並列舉出相關內外部風險。

㈡請列舉五項通過 ISO 27001 資訊安全管理系統驗證的效益。

*1.*《考題難易》：★★
*2.*《解題關鍵》：**ISO 27001 基本題，掌握 ISO 27001 概念即可作答。**
*3.*《命中特區》：**AF24 資通安全講義 P1-5~P1-7 完全命中**

【擬答】：

㈠ ISO 27001 是國際標準組織（ISO）制定的一套資訊安全管理系統（Information Security Management System，簡稱 ISMS）的標準。該標準提供了一個結構化的方法，幫助組織建立、實施、維護和持續改進資訊安全管理系統，以確保組織的資訊資產得到適當的保護。目前最新的 2022 版，綜整為 4 個控制主題(Organization, People, Physical 與 Technological)共計 93 項控制措施外，對於每一個控制措施也都會再界定該控制措施的控制屬性(Control Attributes)：Control type (控制型態)。ISO 27001 的主要目標是確保組織在處理資訊時能夠有效地管理相關的風險，以防止資訊資產的損失、破壞、竊取或不當使用。它要求組織進行全面的風險評估，確定可能對資訊資產產生威脅的內外部風險。以下是一些常見的內部和外部風險，可能會對組織的資訊資產產生潛在威脅：

*1.* 內部風險：

⑴員工失職或不當行為：員工可能因為疏忽、無意或有意地泄露敏感資訊，或者違反組織的資訊安全政策。

⑵內部流程和控制不足：組織內部的流程和控制機制可能不足以防止未經授權的訪問、資料洩漏或其他資訊安全事件。

⑶資訊系統漏洞：內部資訊系統的漏洞可能被惡意使用者或駭客利用，以取得未經授權的訪問或進行系統攻擊。

*2.* 外部風險：

⑴駭客攻擊：惡意駭客可能試圖進入組織的資訊系統，竊取敏感資訊、破壞資訊資產或干擾組織的業務運作。

⑵網路威脅：包括病毒、惡意軟件、勒索軟件等網絡威脅可能對組織的資訊系統和資訊資產造成損害。

⑶第三方供應商風險：與第三方供應商合作時，他們的安全措施可能不足以保護組織的資訊資產，可能導致資訊外洩或被盜取。

⑷自然災害：火災、水災、地震等自然災害可能導致資訊系統中斷或資訊資產損壞。

㈡通過 ISO 27001 資訊安全管理系統驗證可以帶來許多效益，例如：

*1.* 確保客戶與公司內部資訊的安全性、完整性及可用性：通過實施 ISO 27001 標準，組織可以確保其資訊安全控制措施得到有效實施，從而確保客戶和公司內部資訊的安全性、完整性和可用性。

*2.* 取得利害關係人和客戶的信任：通過取得 ISO 27001 認證，組織可以向利害關係人和客戶展示其對資訊安全的承諾，使他們相信自己的資料有受到保護。

*3.* 藉由遵循法規之實踐贏得供應商首選的地位：許多行業和國家都有相關法規要求組織必須遵守資訊安全標準。通過取得 ISO 27001 認證，組織可以證明其符合相關法規要求，從而在與供應商競爭時處於有利地位。

*4.* 遵循法規之實踐更符合招標要求：在招標過程中，許多政府和企業都要求投標者必須符合資訊安全標準。通過取得 ISO 27001 認證，組織可以更容易滿足招標要求，增加中標的機會。

*5.* 提升企業形象，增強競爭力：ISO 27001 認證是一個國際公認的資訊安全管理系統標準。通過取得認證，組織可以提升其在市場上的形象，增強其競爭力。