113 年公務人員特種考試國家安全局國家安全情報人員考試試題

考 試 別：國家安全情報人員考試
等　　別：三等考試
類科組別：資訊組 (選試英文)
科　　目：網路應用與安全

一、RSA 公開金鑰系統是目前常用的密碼系統，如今 Alice 想利用 RSA 密碼系統加密訊息“CA”送給 Bob。假設此 RSA 系統參數分別為：

1. 兩大質數分別為 47 及 53。

2. Alice 及 Bob 的公開金鑰分別為 5 及 3。

㈠請問 Alice 的私鑰為何？（10 分）

㈡ 2 當 Alice 利用 RSA 加密 CA 給 Bob 時，其所得的英文密文為何？（15 分）

字母	A	B	C	D	E	F	G	H	I	J	K	L	M
編碼	01	02	03	04	05	06	07	08	09	10	11	12	13

字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
編碼	14	15	16	17	18	19	20	21	22	23	24	25	26

1.《考題難易》：★★★
2.《解題關鍵》：本題為 RSA 實作題，掌握 RSA 計算方式即可解題。
3.《命中特區》：AF24 資通安全講義 P3-7~3-8 頁完全命中。

【擬答】：

㈠計算 Alice 的私鑰

1. 計算 n：由於本題選擇兩大質數分別為 p = 47 及 q = 53，n = 47 * 53 = 2491

2. 計算 **φ(n)**：φ(n) 是 n 的歐拉函數，對於質數 p 和 q，φ(n) = (p-1)(q-1)。所以，φ(2491) = (47-1)(53-1) = 46 * 52 = 2392。

3. **選擇公開金鑰 e**：e 必須是一個與 φ(n) 互質的數，並且 1 < e < φ(n)。在這個例子中，Alice 的公開金鑰 e 是 5。

4. **計算私鑰 d**：d 是 e 在模 φ(n) 下的乘法反元素。也就是說，d 是一個數，使得 (d * e) % φ(n) = 1。在這個例子中，我們可以找到一個數 957，使得 (957 * 5) % 2392 = 1。所以，Alice 的私鑰 d 是 957。

㈡ Alice 利用 RSA 加密訊息 “CA”

1. 將 "CA" 轉換為數值對應：C = 03, A = 01，數值訊息為 03 01。

2. 加密公式為 c=m^e mod n，其中 m 是我們要加密的訊息，e 是公開金鑰，n 是兩個大質數的乘積。若使用 Bob 的公鑰(可以確保只有 Bob 可以解密) 此時 e_B = 3 和 n = 2491 加密每個字母： 對於 C = 03： $C_{加密}$= 03^3 \mod 2491=27 mod 2491 = 27
對於 A = 01： $A_{加密}$= 01^3 \mod 2491=1 mod 2491 = 1
加密後的訊息為 “27 01” 。

二、大多數企業的災難復原計畫皆有賴於異地服務提供廠商。一般有三種不同的備援形式：熱備援（Hot Site）、暖備援（Warm Site）或冷備援（Cold site）。請說明這三種備援機制及其間的差異性。（20 分）

1.《考題難易》：★★

2.《解題關鍵》：災難復原實作題，了解備援形式即可作答。
3.《命中特區》：AF24 資通安全講義 P1-73 頁完全命中。

【擬答】：

㈠熱備援（Hot Site）

熱備援是一種完全運行的備援站點，具備所有必需的硬體、軟體、網絡設備及最新的數據。它可以立即接管主要站點的工作，幾乎沒有中斷。具有下列特點：

*1.*實時同步：數據和應用程序與主要站點實時同步，保證數據的即時可用性。

*2.*立即切換：在主要站點發生災難時，可以幾乎無縫地切換到熱備援站點，確保業務的連續性。

*3.*成本高：由於需要維持一個完全運行的備援站點，其運行和維護成本較高。

㈡暖備援（Warm Site）

暖備援是一種部分配置的備援站點，具備必要的硬體和網絡設備，但數據和應用程序不是實時同步的，需要在災難發生後進行部分配置和數據恢復。具有下列特點：

*1.*延遲恢復：相比熱備援，暖備援需要一定的時間來恢復數據和配置系統，恢復時間通常在數小時到數天之間。

*2.*中等成本：暖備援的成本低於熱備援，但高於冷備援，因為需要維護一些必要的設備和基礎設施。

*3.*定期更新：數據和系統配置需要定期更新，以確保在災難發生時可以盡快恢復。

㈢冷備援（Cold Site）

冷備援是一種未配置的備援站點，僅提供基本的基礎設施，如電力、網絡連接和空間。在災難發生後，需要完整的硬體、軟體安裝和數據恢復。具有下列特點：

*1.*長恢復時間：冷備援需要較長的時間來部署和配置所有必要的系統，恢復時間可能在數天到數週之間。

*2.*成本低：由於冷備援不需要維持運行中的設備，其運行和維護成本最低。

*3.*高風險：因為需要較長時間來恢復，業務中斷的風險和損失較高。

㈣差異性總結

*1.*恢復時間：熱備援最快，幾乎無縫；暖備援需要數小時到數天；冷備援需要數天到數週。

*2.*成本：熱備援成本最高，因為需要保持運行中的備援站點；暖備援成本適中；冷備援成本最低，因為僅提供基本設施。

*3.*業務連續性：熱備援能夠提供最高的業務連續性；暖備援次之；冷備援則業務中斷風險最高。

三、在軟體系統建置過程，都會考慮其系統發展生命週期（SDLC）。隨著時代的演變，如今已將安全相關措施融入其發展生命週期，提出所謂 SSDLC 的概念。請詳細說明在軟體系統建置過程中，於需求階段及測試階段所需考量的資訊安全措施為何？（20 分）

1.《考題難易》：★★★
2.《解題關鍵》：SSDLC 進階題，掌握 SSDLC 個階段安全措施即可作答。
3.《命中特區》：AF24 資通安全講義 P1-101 與 p1-104 類似考古題。

【擬答】：

㈠需求階段的資訊安全措施

在需求階段，主要是識別和記錄系統的功能需求和非功能需求，這其中包括對安全性的需求。以下是該階段需要考量的資訊安全措施：

*1.*安全需求分析：

識別安全需求：確定系統需要滿足的安全需求，這些需求可以來自法律法規、行業標準、企業政策和風險評估。

威脅建模：分析潛在的安全威脅，識別系統可能面臨的攻擊和弱點。建立威脅模型來幫助理解攻擊者可能的行為和方法。

風險評估：評估不同安全風險的影響和可能性，並根據風險評估結果確定優先級。

2.安全需求文檔：

記錄安全需求：將識別出的安全需求詳細記錄在需求文檔中，包括訪問控制、數據保護、審計和監控要求等。

安全標準和規範：列出相關的安全標準和規範，如 ISO 27001、NIST 等，確保系統開發過程中遵循這些標準。

3.利益相關者參與：

利益相關者溝通：與所有利益相關者，包括安全專家、業務人員和開發人員，討論並確定安全需求，確保所有人對安全需求達成共識。

㈡測試階段的資訊安全措施

在測試階段，主要是驗證系統是否按照設計需求正常運行並滿足安全需求。以下是該階段需要考量的資訊安全措施：

1.安全測試計畫：

制定安全測試計畫：制定詳細的安全測試計畫，確保所有安全需求和控制措施都得到測試。計畫應包括測試範圍、測試方法、測試工具和測試時間表。

2.安全測試技術：

靜態分析：使用靜態分析工具檢查代碼中的安全漏洞，如代碼中的弱點和錯誤配置。

動態分析：使用動態分析工具在運行時檢測應用程序的安全漏洞，模擬攻擊者的行為來發現潛在的安全問題。

滲透測試：進行滲透測試，模擬真實攻擊者的行為來檢查系統的防禦能力和安全漏洞。

安全功能測試：測試系統的安全功能，如認證、授權、數據加密、日誌記錄和入侵檢測等，確保這些功能按預期工作。

3.漏洞管理：

漏洞檢測與修復：建立漏洞檢測和修復流程，及時發現和修復測試中發現的安全漏洞。

重新測試：在修復漏洞後，重新測試相關功能和系統，確保漏洞已經完全修復且沒有引入新的問題。

4.合規測試：

合規性檢查：確保系統符合所有相關的法律法規和標準，如 GDPR、HIPAA、SOX 等，進行合規性測試以確認系統的合規性。

5.安全測試報告：

生成測試報告：在測試結束後，生成詳細的安全測試報告，記錄測試過程、發現的問題、修復狀況和最終的測試結果，為後續的維護和審計提供參考。

四、針對虛擬私有網路常使用之 IPSec 協定運作情形，回答下列問題：

㈠請說明 IPSec 有那兩種基本操作作業模式？（10 分）

㈡在 IPSec 的運作協定，除 AH（AuthenticationHeader）及 ESP（EncapsulationSecurity Payload）外，還有 IKE（Internet Key Exchange）協定。請說明 IKE 功用為何？（5 分）

1.《考題難易》：★★
2.《解題關鍵》：安全協定進階應用題，了解 IPSec 作業模式與 IKE 即可作答。
3.《命中特區》：AF24 資通安全講義 P3-15 頁命中 IPSec 兩種基本操作作業模式。

【擬答】：

㈠ IPSec 的兩種基本操作作業模式

IPSec（Internet Protocol Security）是一套用來保護網際網路通訊安全的協定套件。IPSec 有兩種基本操作作業模式：

1.傳輸模式（Transport Mode）：

在傳輸模式中，IPSec 只保護 IP 封包的有效負載部分（Payload），而不包括原始的 IP 標頭（Header）。IPSec 首部被插入到 IP 標頭和傳輸層協定（例如 TCP 或 UDP）首部之間。主要用於端到端的通信保護，比如兩個主機之間的通信。這種模式適合於內部網路內的通信保護。IP 封包的原始標頭保持不變，因此路由功能不受影響，但負載數據被加密或驗證。

2.隧道模式（Tunnel Mode）：

在隧道模式中，IPSec 不僅保護 IP 封包的有效負載部分，還會對整個 IP 封包進行保護。這意味著原始 IP 封包會被整個封裝在一個新的 IPSec 封包中，並加上新的 IP 標頭。主要用於網關之間的通信保護，比如兩個路由器之間或 VPN 客戶端和 VPN 伺服器之間的通信。這種模式適合於跨越公共網絡的通信保護。整個原始 IP 封包被封裝和保護，提供了更高的安全性，但增加了一些通信開銷。

㈡ IKE 協定的功能

IKE（Internet Key Exchange）是 IPSec 的一部分，負責建立安全的通信通道並進行密鑰交換。IKE 的主要功能包括：

1.協商安全聯盟（Security Association, SA）：負責在通信雙方之間協商和建立 IPSec 安全聯盟。安全聯盟定義了 IPSec 通信所需的參數和算法，包括加密算法、哈希算法、鑑別方法等。

2.密鑰交換： IKE 使用 Diffie-Hellman 密鑰交換算法在通信雙方之間安全地交換密鑰。這些密鑰將用於 IPSec 加密和驗證過程中。

3.認證： IKE 協定支持多種認證方式，包括預共享密鑰（Pre-shared Key, PSK）、數位證書（Digital Certificates）和公鑰基礎設施（Public Key Infrastructure, PKI）。這些認證方式用於確認通信雙方的身份，確保只有合法的用戶才能建立 IPSec 通道。

4.建立和管理 SA 的生命週期：IKE 負責建立、維護和更新安全聯盟的生命週期。在安全聯盟到期之前，IKE 將自動重新協商新的安全聯盟，以確保通信的持續安全。

5.協商加密和鑑別算法： IKE 協商並選擇雙方支持的最佳加密和鑑別算法，以確保通信過程中使用的算法是最安全和最兼容的。

五、目前資安事件層出不窮，而企業為防範資安事件發生，會結合 SIEM（Security Information and EventManagement）及 SOC（Security OperationCenter）兩種機制作為網路安全防禦機制。

㈠請解釋 SIEM 及 SOC 所代表的意義。（12 分）

㈡說明 SIEM 和 SOC 之間的關聯性。（8 分）

1.《考題難易》：★★★
2.《解題關鍵》：資安聯防體系概念題，掌握 SIEM 及 SOC 概念即可作答。
3.《命中特區》：AF24 資通安全講義 P1-83 頁命中 SIEM，搭配 P1-45 即可完整作答。

【擬答】：

㈠ SIEM 及 SOC 的意義

1. SIEM（Security Information and Event Management）

SIEM 是一套用於收集、分析和報告安全相關數據的系統。其主要功能包括：

日誌管理（Log Management）：收集和存儲來自不同來源的安全日誌和事件數據，如防火牆、入侵檢測系統、操作系統、應用程式等。

事件管理（Event Management）：對收集到的日誌和事件數據進行分析，識別潛在的安全威脅和異常行為。

實時監控（Real-time Monitoring）：實時監控安全事件和警報，及時發現和響應安全威脅。

合規性報告（Compliance Reporting）：生成合規性報告，滿足企業遵循各種法律法規和行業標準的需求。

事件關聯（Event Correlation）：通過將不同來源的數據進行關聯分析，識別複雜的安全威脅和攻擊模式。

2. SOC（Security Operation Center）

SOC 是一個集中化的安全運營中心，負責企業的整體網絡安全運營和管理。其主要職責包括：

監控與分析：24/7 實時監控企業網絡，識別和分析安全事件。

威脅響應：迅速響應和處理安全事件，減少安全威脅對企業的影響。

威脅情報：收集和分析最新的威脅情報，了解最新的安全威脅和攻擊技術。

事故管理：協調和管理安全事件的處理過程，確保有效和有序地應對和恢復。

風險管理：評估和管理網絡安全風險，制定和實施相應的安全策略和措施。

持續改進：分析過去的安全事件和響應過程，不斷改進安全運營流程和技術。

㈡ SIEM 和 SOC 之間的關聯性

SIEM 和 SOC 在企業的網絡安全防禦中密切相關，互補協作，以提供全面的安全防護。以下是兩者之間的關聯性：

1. 數據收集與分析：

SIEM：負責收集和分析來自不同來源的安全數據和事件，提供實時監控和警報。

SOC：利用 SIEM 提供的數據和分析結果，進行進一步的威脅分析和事件響應。

2. 事件響應：

SIEM：檢測並生成安全警報，幫助識別潛在的安全事件。

SOC：基於 SIEM 的警報和分析，快速響應和處理安全事件，確保安全威脅得到有效控制。

3. 持續監控：

SIEM：提供 24/7 的實時監控和報告功能，確保所有安全事件都能及時被發現。

SOC：依靠 SIEM 的實時監控數據，持續監控企業網絡，保護企業免受安全威脅。

4. 合規性管理：

SIEM：生成合規性報告，確保企業遵循相關的法律法規和行業標準。

SOC：根據 SIEM 的合規性報告，制定和實施安全策略，確保企業的合規性要求得到滿足。

5. 威脅情報：

SIEM：收集和分析來自不同來源的威脅情報，提供對最新威脅的洞察。

SOC：利用 SIEM 的威脅情報，調整和優化安全策略，提升整體防禦能力。

總結來說，SIEM 為 SOC 提供了強大的技術支持和數據分析能力，而 SOC 則利用這些數據和技術進行全面的安全運營和管理。兩者的結合可以有效地提升企業的安全防禦能力，保護企業免受各種安全威脅。