代號：35460
頁次：2−1

113年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員及移民行政人員考試試題

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
考試時間：2 小時　　座號：＿＿＿＿＿＿

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

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

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）

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）

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（Authentication Header）及 ESP（Encapsulation Security Payload）外，還有 IKE（Internet Key Exchange）協定。請說明 IKE 功用為何？（5 分）

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 Event Management）及 SOC（Security Operation Center）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）