代號：41460
頁次：1－1

112年公務人員特種考試司法人員、法務部調查局調查人員、海岸巡防人員、移民行政人員考試及112年未具擬任職務任用資格者取得法官遴選資格考試試題

考 試 別：調查人員
等　　別：三等考試
類 科 組：資訊科學組
科　　目：資訊安全實務
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、請條列並說明「數位證據保全標準作業程序」中，進行「電腦設備或儲存媒體蒐集」之作法。（25 分）

二、請條列說明三項 IDPS（Intrusion Detection and Prevention System）偵測技術，並就精準度、已知攻擊、未知攻擊、計算能力與策略調整方式等五個面向做比較。（25 分）

三、請條列說明零信任（Zero Trust）的核心機制與六項組織應考量的零信任原則。（30 分）

四、以下是張三和李四以 Diffie-Hellman key exchange 之技術為基礎欲產生共同密鑰，但未做取模運算（Modulus），所以也沒有選定 Diffie-Hellman key exchange 模數運算的質數，他們所選用的公開基礎參數（底數）g 為 3。請從他們交換的參數破解出張三的秘密參數 X_A、李四的秘密參數 X_B 以及他們產生的共同密鑰 Key。（需有推演計算的過程才給分）（20 分）

張三：選定秘密參數 X_A，後計算出公開參數 $Y_A = 27$ 傳給李四。
李四：選定秘密參數 X_B，後計算出公開參數 $Y_B = 243$ 傳給張三。
張三、李四：各自計算出二人的共同密鑰 Key。