

104年公務人員特種考試司法人員、法務部調查局調查人員、國家安全局國家安全情報人員、海岸巡防人員及移民行政人員考試試題

代號：30660 全一頁

考試別：國家安全情報人員

等別：三等考試

類科組：資訊組

科目：網路應用與安全

考試時間：2小時

座號：\_\_\_\_\_

※注意：(一)禁止使用電子計算器。

(二)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。

一、名詞解釋：（每小題5分，共25分）

(一)再傳送攻擊（Replay Attack）

(二)訊息驗證碼（Message Authentication Code, MAC）

(三)憑證註銷表（Certificate Revocation List, CRL）

(四)資訊安全管理系統（Information Security Management System, ISMS）

(五) Triple-Data Encryption Standard（3-DES）

二、人力資源政策（Human Resources Policy）是資訊安全在管理面上一個很重要的政策。

(一)完善之人力資源管理，應注意3個面向，請說明此3面向。（15分）

(二)ISO 17799針對人力資源安全提出了一些執行要點（Code of Practice），請列舉2項執行要點，並說明之。（10分）

三、公開金鑰管理（Public Key Management）：

(一)請說明一個公開金鑰管理系統應該支援的基本功能。（10分）

(二)通常有4種公開金鑰的分配方法，請說明其優缺點。（15分）

四、IP Security（IPSec）：

(一)為什麼需要IPSec？（10分）

(二)除了提供安全性外，IPSec還有那些優點？（10分）

(三)說明兩種IPSec可能的應用情境？（5分）