

114年公務人員高等考試三級考試試題

類 科：資通安全
科 目：資通安全概論
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。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、資訊科技發展快速且應用廣泛，企業面臨的資安挑戰也越來越多，使得企業必須實施有效的資安措施來保護企業的資訊資產。防火牆作為維護資安的重要設備之一，請詳述防火牆對企業網路與資訊安全有那些重要性？（25 分）
- 二、企業常用 STRIDE 威脅模型來讓資安分析者可以理解威脅系統的方式，並設法找出威脅。請詳述 STRIDE 模型代表那六種威脅種類及其對應的資安特性。（25 分）
- 三、密碼學是一種產生密文的科學與藝術活動，目前是依據柯克霍夫原則（Kerckhoff's Principle）來發展密碼系統。
 - (一)請說明柯克霍夫原則？（5 分）
 - (二)另從分析密碼系統角度而言，請詳述有那幾種破密分析（Cryptanalysis）方法？（20 分）
- 四、因應量子電腦的發展潮流，量子密碼學及後量子密碼學等兩大新興的密碼科學類型已被提出。
 - (一)請說明何謂量子密碼學及後量子密碼學，試比較之。（15 分）
 - (二)請詳述量子密碼基於那些特性來確保其安全性。（10 分）