

國營臺灣鐵路股份有限公司

113年第2次從業人員甄試試題

應試類科：第8階-助理管理師-資訊

測驗節次：第二節

測驗科目：網路通訊與資通安全

—作答注意事項—

- ①應考人須按編定座位入座，作答前應先檢查答案卡，入場證號碼、桌角號碼、應試科目是否相符，如有不同應立即請監試人員處理。使用非本人答案卡作答者，不予計分。
- ②測驗期間，嚴禁隨身攜帶及使用行動電話或其他具可傳輸、掃描、交換或儲存資料功能之電子通訊器材或穿戴式裝置(包括但不限於：微型耳機、智慧型手錶、智慧型手環、智慧型眼鏡、電子字典、個人數位助理機、呼叫器等)，並不得置於座位四周或放置於作答區，違者該節以零分計。
- ③答案卡須保持清潔完整，請勿折疊、破壞或塗改入場證號碼及條碼，亦不得書寫與答案無關之任何文字或符號。
- ④本試題本為雙面，共100分，答案卡每人一張，不得要求增補。未依規定劃記答案卡，致讀卡機器無法正確判讀時，由應考人自行負責，不得提出異議。
- ⑤試題若有選擇題，限用2B鉛筆作答。請按試題之題號，依序在答案卡上同題號之劃記答案處作答，單選題在ABCD四個選項中選擇一個正確的答案，若有複選題在ABCDE五個選項中選擇所有正確的答案。未劃記者，不予計分。欲更改答案時，請用橡皮擦擦拭乾淨，再行作答，切不可留有黑色殘跡，或將答案卡汙損，也切勿使用修正帶或其他修正液。
- ⑥試題若有手寫題及作文，限用筆尖較粗之黑色或深藍色原子筆或墨水筆，不得使用鉛筆。在答案卡上規定的區域紅色框線內書寫，不得超出框線。修正時只可使用修正帶，不可使用修正液。若因字跡潦草、超出框線、寫到別的題號位置、或修正不清等原因，致評閱人員無法清楚辨識者，應考人責任自負。
- ⑦測驗結束前不得離場，擅自離場者以零分計。考試結束，試題本及答案卡務必繳回，未繳回者以零分計。

禁止翻面

讀完本頁說明，鐘響時才可以開始作答；翻面以違規記。

非選擇題【共4題，每題25分，共100分】

請以最簡潔完整的字數，將答案清晰填寫於答案卡(非試題本)上的相對題號的紅色框格內。用黑色或深藍色原子筆或墨水筆(非鉛筆)填寫。作答於錯誤區，不予評閱計分。超出紅框、模糊或無法辨識，致評閱人員無法清楚辨識者，應考人責任自負。

第一題 請依照下列題目敘述回答：

1. 請說明 TLS(Transport Layer Security)的工作原理？(12 分)
2. 請舉例一個可以使用 TLS(Transport Layer Security)的鐵路系統，並說明使用 TLS 後可以預防哪些網路攻擊？(13 分)

第二題 以下的三個攻擊方式能夠取得機密資訊嗎？如果能夠取得，請說明哪些資訊遭到這個攻擊方式能夠取得的。

1. SQL Injection (9 分)
2. DDOS (8 分)
3. CSRF (Cross-Site Request Forgery) (8 分)

第三題 網路協定與加密基礎

1. 請說明對稱式加密(Symmetric Encryption)與非對稱式加密(Asymmetric Encryption)的差異，並各舉一個實際應用的例子。(8 分)
2. 解釋 SSL/TLS Handshake 的主要步驟，並說明為何需要同時使用對稱與非對稱加密。(9 分)
3. 畫出 TCP 三向交握(Three-way Handshake)的流程圖，並說明每個步驟的目的。(8 分)

第四題 1. 說明數位簽章(Digital Signature)的運作原理，並解釋它如何同時確保資料的完整性與不可否認性。(8 分)

2. 在以下情境中，請說明對稱式金鑰交換可能面臨的中間人攻擊(Man-in-the-Middle Attack)問題，並解釋 PKI(Public Key Infrastructure)如何解決此問題：(8 分)

- (1) Alice 要與 Bob 建立安全通道
- (2) Carol 可以監聽並修改所有傳輸內容

3. 解釋下列安全相關名詞，並各自說明其應用場景：(9 分)

- (1) Perfect Forward Secrecy (PFS)
- (2) Hash-based Message Authentication Code (HMAC)
- (3) Certificate Revocation List (CRL)

