中央警察大學 114 學年度碩士班入學考試試題

所　別：資訊管理研究所
科　目：電腦犯罪與資訊安全

作答注意事項：

1.本試題共 4 題，每題各占 25 分；共 2 頁。
2.不用抄題，可不按題目次序作答，但應書寫題號。
3.禁用鉛筆作答，違者不予計分。

一、在車聯網的智慧交通管理、自動駕駛、車隊管理、車輛安全與防盜等應用中，須有車輛對基礎設施（V2I）、車輛對車輛（V2V）、車輛對行人（V2P）、車輛對雲端（V2C）、車輛對網路（V2N）等加密連線，請分析使用對稱式加密法或是使用非對稱式加密法於車聯網應用時，各有何優缺點？（15 分） 採用非對稱式加密法進行車聯網應用時，為因應後量子電腦時代，NIST（美國國家標準技術研究所）已經選定了一些 PQC（Post-Quantum Cryptography）演算法作為標準，請說明何謂「後量子密碼學」？（10 分）

二、門羅幣（Monero）挖礦程式事件為駭客透過惡意程式或網站植入挖礦工具，非法利用受害者設備運算資源進行加密貨幣挖礦的資安威脅。著名的事件有：色情網站大規模植入挖礦程式 Coinhive、Chrome 擴充軟體 Archive Poster 遭植入挖礦程式、Ohsoft 軟體預設安裝挖礦程式、Smominru 惡意程式攻擊(又稱為 WannaMine，利用 EternalBlue 漏洞程式），請問如何調查挖礦程式事件（15 分）與防範其發生？（10 分）

三、請解釋何謂 「TCP/IP Fingerprint」？（10 分）在網路巡邏或網路安全防護中，如何利用 TCP/IP Fingerprint 技術來辨識可疑的網站或網路服務？（15 分）

四、區塊鏈技術的三大特性（匿名性、不可竄改性、可追蹤性）對現今的數位犯罪調查造成極大的影響。假設你是一名數位鑑識專家，正依法監控某條網路線路，並擁有該線路完整的封包側錄（Packet sniffing）權限。請論述你是否可從側錄的網路流量中，分析出被側錄對象所使用的加密貨幣錢包地址？無論你認為「可行」或「不可行」，請提供詳細的論證過程。