中央警察大學 110 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 1 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、請說明電腦犯罪在判定犯罪的過程裡數位鑑識與數位證據的相互依存關係。（10 分）
又由於現代科技的資訊通聯裡數位證據無所不在，請說明電腦/手機裡有哪些地方能找到可能蹤跡。（15 分）

二、請說明 Chinese Reminder Theorem 的來由並歸納其規律性。（10 分）
當運用在現代科技的網路環境中，試說明如何達到資料的公開傳遞裡能有隱私性的安全機制。（15 分）

三、資訊安全措施的層級（security measure levels）可分為：實體安全（physical security），應用程式安全（application security），作業系統安全（operating system security），及網路安全（network security）等。試分別說明之。

四、電腦犯罪攻擊的類型可分為：違反機密性（或違反機敏性）（breach of confidentiality），違反誠信（或違反完整性）（breach of integrity），違反可用性（breach of availability），服務盜竊（theft of service），及阻斷服務（denial of service）等。試分別說明之。

中央警察大學 111 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 1 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、請回答下列問題：

（一）何謂勒索軟體（Ransomware）？（10 分）

（二）試說明如何防範勒索軟體的攻擊？（15 分）

二、解釋下列名詞（每小題 5 分，共 25 分）：

（一）深度偽造（又稱深偽技術，deepfake）

（二）進階持續性威脅（Advanced Persistent Threat, APT）

（三）數位簽章（digital signature）

（四）深度防禦（defense in depth）

（五）分散式阻斷服務攻擊（Distributed Denial-of-Service, DDoS）

三、說明 Authentication 與 Forensics 差異與該如何運用於資訊安全與電腦犯罪調查。

四、說明 RSA 的原理與 Diffie-Hellman 公開金鑰的差異，並運用於 Disinformation／Misinformation 的事件處理時，如何以 RSA／Diffie-Hellman 的觀點處理與適度解決相關事件。

中央警察大學 112 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 1 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、說明 Sybil Attack。若 Sybil Attack 運用在科技犯罪裡，將可能有何犯罪方式，至少條列 3 種並說明犯罪模式。

二、當隨身的智慧型手機遺失時，以科技犯罪的觀點說明將造成的可能資安危機與犯罪為何？並以資安的技術觀點說明欲用他人的手機，進行犯罪的各個階段中如何有因應的方式。

三、在偵查過程中，你如何識別某特定 IP 位置是否為跳板或 VPN(Virtual Private Network）主機？（10 分）除了 VPN 跳板之外，以 IP 位址為線索進行犯罪偵查時，還可能遇到哪些挑戰，請列舉 5 項。（15 分）

四、Open System Interconnection Reference Model 簡稱 OSI 模型，是一種制定網路標準的概念性架構，請從資訊安全角度解釋 OSI Layer-7 模型中各層級所對應的資安防護措施。

中央警察大學 113 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、 科技犯罪的手法裡，嫌疑犯利用知識與技術的修習進行訊息的處理，對於網路傳輸文字與金額進行加密，藉以混淆訊息的真實性。案件調查裡，在嫌疑犯的家中查到 1 本筆記，內頁中有 Hill cipher 的記載，記錄有相關的數據如下：

$K = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix}$,$K^{-1} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$,

$C=E_K\ (M)=K * M \bmod n$, $D_K(C)= K^{-1} * C \bmod n = M$, n=26,

並看到可疑文字“DECIDE”。

試對該文字“DECIDE”進行 Hill cipher 的加解密處理，得以協助該案件的偵辦。得藉由正確的解讀方式，進而對嫌疑人於網路所傳輸的文字與金額作後續的正確解密，得到原始的通訊內容，清楚嫌疑人的相關動機，釐清案情？

二、 在資訊安全裡，有一個方法為 CRT，可加速 RSA 的運算，說明何謂 CRT。並在網路的環境，如何運用 CRT 的 privacy 特性得能設計一個安全運作的協定，達到雙方訊息安全通訊的正確傳送？

三、「29 歲陳姓男子上個月 19 日凌晨在捷運忠孝新生站上車，見列車上有名外型亮麗、穿著短裙的女子，便以手機偷拍其裙底風光。身邊的女乘客發現後，立即上前告知該女遭偷拍，於是按鈴通報站務人員及警方到場處理，並在出口處攔下逮捕，全案依妨害秘密罪、性騷擾罪嫌移送偵辦。」

為找出是否有更多受害者，警方持搜索票至陳姓嫌犯住處進行搜索，結果找到 1 個可疑的隨身碟。為慎重起見，於是將隨身碟送交科偵隊進行鑑識。假設你是科偵隊的承辦人員，請詳細說明如何自動找出隨身碟中檔案本體為 JPEG 檔，但附加檔名（file extension）卻不是.JPG 的檔案。

*請注意：以上所使用之情境為虛構，與真實案情無關

四、 根據 OWASP（Open Web Application Security Project）歷年所公布的十大網路應用系統安全弱點（OWASP Top 10）中，注入式攻擊（injection）總是名列前茅。請舉例說明什麼是注入式攻擊？應如何防範？