# 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？