資訊安全課程期末專案

林永松老師

目的：使用非對稱式加解密演算法 (Asymmetric Cryptography Algorithm)及雜湊函數(Hash Function)等機制，實作有關軟體系統升級所需之授權碼(License)上傳驗證及更新檔(Patch)下載安裝的過程，達到機密性(Confidentiality)與完整性(Integrity)之需求。

分組：二個人一組，分別扮演【使用者】及【軟體廠商】。

程式開發語言及執行平台：不限。

非對稱式加解密演算法：自選(例 RSA、ECC 等)。

雜湊函數：自選(例 MD5、SHA-1 等)。

展示環境：請自備。

授權碼及更新檔檔案格式：不限，授權碼檔案內容須為一百個英數字混合的字串(自訂)，更新檔檔案內容須出現 "Update Successfully" 字串(其餘內容自訂，惟此檔案大小須大於 5K Bytes)。

加密檔案格式：分成三個部分，包括 Header、Package、Trail。

1. Header：大小為 1024 bytes

描述區：512 bytes，助教於展示時隨機輸入的文字須放入此區域。

保留區：512 bytes。

2. Package：此區域存放加密過的授權碼或更新檔。

3. Trail：大小係依照所選定之雜湊函數而定(例如 MD5 為 16 bytes)；將Header及 Package 合併後，運用所選定之雜湊函數進行運算，產生雜湊值(Hash Value) 放入此區域。

加密檔案傳送方式：不限，可於展示時透過電子郵件附加檔案方式寄送，或是透過外接式儲存設備交換。

作業展示流程一：

1.使用者：將授權碼使用【軟體廠商】公開金鑰加密後，依照前述之加密檔案格式需求，發送至【軟體廠商】進行驗證。(本項完成者可得20%)

2.軟體廠商：收到【使用者】發送之授權碼後，使用本身的私密金鑰解密；驗證無誤後，再利用【使用者】的公開金鑰對更新檔加密後，依照前述之加密檔案格式需求，發送至【使用者】進行更新。(本項完成者可得30%)

3.使用者：收到【軟體廠商】發送之更新檔後，使用本身的私密金鑰解密，以進行系統升級。(本項完成者可得50%)

作業展示流程二(加分部分，須結合作業流程一)：

透過前述作業展示流程，可確保授權碼或更新檔之機密性與完整性，但無法達成發送方之不可否認性 (Non-Repudiation)，即無法保證授權碼是由使用者所

發送出，或無法保證更新檔是由軟體廠商所發送出。作業展示流程二即是要達成此項保證。(本項完成者可另得30%)

加密方：

1.將加密後之授權碼或更新檔，運用所選定之雜湊函數進行運算，產生雜湊值。

2.將前述的雜湊值，使用本身的私密金鑰加密，以確保授權碼或更新檔的發送來源。

3.將雜湊值加密後的結果，放入 Header 之保留區，隨著加密檔案一起發送至對方。

解密方：

1.將加密檔案 Header 之保留區中的資料獨立取出，並使用對方的公開金鑰解密，得到一個雜湊值。

2.將加密檔案之 Package 部分，運用所選定之雜湊函數進行運算，產生雜湊值。

3.前二步驟中所得之雜湊值相同，方得進行後續解密動作(加密檔案之Package部分)；若二者不相同，則捨棄所得之檔案並顯示警告訊息。