Unit 6：電子交易安全

Section 1: 電子銀行常用的密碼學技術

非對稱性系統

所謂非對稱性系統就是加密與解密分別使用不同的金鑰：公開金鑰(Public Key)與私密金鑰(Private Key)，因此亦稱為公開金鑰加解密系統。此系統具有以下特性：

・通訊雙方只需交換公開金鑰，因無隱密之特性，故無須以秘密通道進行交換。
・可經由認證中心(Certificate Authority，簡稱 CA)簡化金鑰之交換作業與信賴關係之建立。
・目前主要應用包括 FEDI、SET、FXML、VISA 3D-Secure 發卡行授權資料之簽章及部分網路銀行業務等。
・常見演算法包括 Diffi-Hellmen(主要用來做秘密金鑰之協商交換)、DSA (NIST 公告之簽章標準
，只適用於數位簽章)及 RSA(可同時做加密與數位簽章)等。
・可應用於確保資料的隱密性、來源性、完整性及不可否認性。

由於 RSA 乃目前國內金融應用最廣的非對稱性加解密技術，以下將說明其在數位簽章與數位信封之應用。

一、數位簽章

數位簽章(Digital Signature)類似資料押碼，主要目的在防止非法第三者冒名傳送或竄改傳輸中的資料，以確保資料之來源辨識性與完整性。不同的是，若配合 CA 做金鑰之認證，數位簽章在法律上已直接賦予其合法性。

雜湊(Hashing)是數位簽章進行資料前置處理不可或缺之技術，它具有以下特性：
1.將任意長度之輸入資料轉換成固定長度之資料。
2.具單向不可逆之特性，故又稱為單向函數(One Way Function)。
3.目前常見之演算法有 MD2、MD5(輸出長度均為 128 bits)、SHA-1(輸出長度為 160 bits)等。
4.單獨使用無法防範惡意之資料竄改，通常搭配數位簽章使用。
5.若加入金鑰運算(如 RFC2104 定義的 HMAC: Keyed-Hashing for Message Authentication)，可確保資料的正確性及來源辨識性。

傳送端產生數位簽章前，先將欲簽章之本文經由雜湊運算取得訊息摘要(Message Digest)，再以私密金鑰對訊息摘要做解密(簽章)運算。(訊息摘要在簽章前可能需做 Padding 處理，細節在此略過。)最後將數位簽章連同本文一併送至接收端。

接收端取得訊息後，先取出本文，以相同雜湊運算取得訊息摘要，然後再以傳送者的公開金鑰對數位簽章做加密(驗章)運算，將結果與訊息摘要比對，即可判斷訊息之正確性。

在此作業下，因私密金鑰只有傳送者才知道，也只有傳送者可產生對應之簽章，故可確保訊息的來源辨識(唯一)性及正確性，另若公開金鑰經 CA 認證，更可確保其不可否認性。

二、數位信封

RSA 公開金鑰系統同樣可運用於資料之加密，然而基於效能考量，通常不以 RSA 演算法直接對本文做加密，而是採用數位信封(Digital Envelop)技術，其特色是以快速的對稱性加解密演算法進行大量資料之加密運算，而以非對稱性加解密演算法解決對稱性金鑰基碼交換之棘手問題。

傳送端首先任意產生用以加密此次本文資料之秘密金鑰(Session Key)，對欲傳送之本文做加密，再以接收端之公開金鑰對此 Session Key 做加密，最後將密文與加密保護後之 Session Key 一併傳送至接收端。

接收端在取得訊息時，先以其私密金鑰解密取得正確的 Session Key，再以此對密文做解密，即可取得完整之明文資料。

在此作業下，只有接收者知道 Session Key 解密所需之私密金鑰，因此可確保傳送資料之隱密性。

結語

密碼學是提供電子銀行交易安全的關鍵技術，根據業務性質、交易對象、安全需求及相關法令規定，選擇適當之安全技術，將可有效降低交易之安全威脅，進而提供便捷且安全之電子銀行交易平台。

作者：蘇偉慶
現任：財金公司安控部高級工程師
學歷：中山大學電機工程研究所碩士
經歷：資策會技術研究處工程師

Section 2: 電子商業交易的安全標準

網路虛擬商店經由安全認證中心審核通過是給線上消費者最基本的安全保障，線上消費者的消費行為是受到 SSL 及 SET 兩主要安全協定系統保護，確保消費者資料隱密性和傳輸過程的完整安全。

1. 什麼是 SSL？

安全通信協定（SSL；Secure Socket Layer）是一種網路安全模式。此一網路資料安全協定是由 Netscape 首先發表。SSL 利用公開金鑰的加密技術(RSA)來做為用戶端與主機端在傳送機密資料時的加密通訊協定。目前，SSL 技術已被大部份的 Web Server 及 Browser 廣泛使用。

2. 什麼是 SET？

安全付款協定（SET；Secure Electronic Transcation）是用來保護消費者在開放型網路持卡付款交易安全的標準。由 VISA、MasterCard、IBM、Microsoft、Netscape、GTE、VeriSign、SAIC、Terisa 等公司聯合制訂，運用 RSA 資料安全的公開鑰匙加密技術，保護交易資料之安全及隱密性。

SET 的架構是由幾個元件所共同組合起來的。分別是電子錢包（Electronic Wallet），電子證書（Digital Certificate)，付款轉接站（Payment Gateway），和 認證中心（Certification Authority）。而運用這四個元件，即可構成於 Internet 上符合 SET 標準的信用卡授權交易。

而電子證書（Digital Certificate）可說是 SET 的核心，用以建立電子交易中各交易主體間之信任。它是由一個公正的單位來擔任「認證中心」角色，簽發電子證書給銀行，持卡人及特約的網路虛擬商店。加密數位碼有了電子證書的輔佐，網路上往來的消費者和商店就能彼此辨識對方確實是真正的商店和有效的持卡人。進行電子交易的時候，持卡人和特約網路虛擬商店兩邊符合 SET 規格的軟體，會先在電子資料交換前確認雙方的身份，也就是檢查由認證中心所發給的電子證書。此外，當我們以自己的數位碼加密某些訊息並發送出去後，由於電子證書已經確認這組用來加密的數位碼確實為發送訊息者所有，所以發送訊息的人將無法否認他曾經發送這筆訊息。因此有了加密數位碼和電子證書的設計，將可以滿足三項重要的網路交易安全需求：

身份確認與隱私權保密：交易雙方的身份可以被辨識。
資料隱密和完整安全：網路上傳遞的資料不會被竊取或竄改。
交易的不可否認性：一旦確定發出交易訊息便無法否認。

SET 1.0 版於 1997/6 正式問世。時至今日，SET 已成為國際上所公認在 Internet 電子商業交易的安全標準。

資料來源：http://www.3cbank.com/profile/shopping_procedure2.jsp