第二章　文獻探討

本章節針對傳統資訊安全及檔案加密之動機與常見的加密方式做探討。第一節為資訊安全的意義和資訊安全可能碰到的問題做說明，第二節是密碼學背景，第三節探討常用的加密技術，第四節則是資料驗證研究，第五節為數位簽章原理，第六節為密碼破解原理。

第一節　資訊安全

一、資訊安全的意義

在資訊時代的現在，資料不再只是一連串原始的紀錄，大部份的資料被整理成人們可以了解或運用的格式，使得資料有意義。資訊(information)是由資料(data)整理成對人有意義的格式。

資料的儲存，關係到後續資料使用的便利性，因此如何適當地、安全地儲存也是重要步驟。適當的資料儲存方式，能讓後續的資料處理速度加快；而安全的資料控管方式，才能保障資料的機密。

而資訊安全就是拿來防止非法存取、竄改、偷竊、和任何一切惡意的行為。周全的資訊安全維護了資料的機密性、完整性、和可用性。而維護資訊安全的三項重要目標說明如下：

(一)機密性(confidentiality)：資訊僅在授權的時間供人物使用。

(二)完整性(integrity)：資訊確保其精確性與完整性。

(三)可用性(availability)：資訊在需要的時候都能使用或存取。

二、資訊安全會遇到的問題

資訊是經過處理之後有意義的資料，是有價值的物件，會牽扯到濫權或是犯罪行為，例如遭到駭客、電腦病毒，或是被組織內部人員竄改、偷竊、等忽略隱私權、所有權的惡意行為。本研究提出一個加密以及驗證的方法來確保資訊安全，來防止新聞資料遭到非法修改或是非法暴露的可能性。

電腦駭客攻擊的行為通常可歸納為以下的類型：

(一)消極性攻擊(passive attack)

1. 竊聽(release of message contents)
2. 通訊分析(traffic analysis)

(二)積極性攻擊 (active attack)

1. 竄改資料內容 (message stream modification)
2. 干擾通訊活動(denial message services)

例如，入侵國防部電腦網路竊取資料並散佈在 Internet 上之破壞行為。

本研究的目的是為了解決竄改資料內容，著重於遭到竄改之後如何第一時間得知，以避免發佈之後的損失。

第二節　密碼學背景

Diffie 和 Hellman 是首先提出公共金鑰概念的兩位學者，他們在 1976 所提出的概念(Diffie and Hellman, 1976)，也深深影響著往後密碼學的發展。此演算法在於密碼金鑰的交換，被用於許多商品的密鑰交換技術。在兩方的通行碼認證金鑰交換協定中，通訊的雙方可以利用事先分享的通行碼來認證彼此的身份並且建立出一把會談金鑰來加密其後的通訊內容。因此，此種通訊協定十分適合應用在主從式的架構之中(Denning, 1982)。因為，伺服器可以

簡單的利用通行碼來認證其所有的使用者並且和他們進行安全的通訊。之後 Rivest, Shamir, and Adleman (1978)也提出公共密鑰加密系統。McEliec (1978)使用代數理論來提出公共金鑰。

Merkle (1990)提出「單向雜湊函數」並使用在數位信號上。Miyaguchi (1990)提出發展快速資料加密演算法 FEAL-8。NIST (National Institute of Standards and Technology, 國家標準和科技機構，1993)提出安全的雜湊標準，並命名為 SHS，以上這些都是加密的方法。Biham and Shamir (1991)提出不同的攻擊方法，且 Matsui (1994)也發表線性密碼分析去攻擊 DES 類型的安全系統。Stallings (2007)提出加解密的模型。Lee and Lee (2007)使用插入、旋轉、調換、位移和一些電腦基本的計算操作來設計加解密演算法，將加密後的明文、相關的資料和表格來整合成密文。資訊系統需要在技術、形式、非形式三層級上的安全，管理資訊系統必須保證更安全，企業使用複雜的技術控制來保護他們在電腦系統中所有的資訊。

第三節　加密技術

所有的加密方法都是由兩種方式而構成，分別是替換(substitution)與排列(transposition)，另外還有一種是兩者方法的混合。

一、替換技術

替換的方法(Kahate, 2007)為將明文中的所有元素，以對應的元素做替換。如已知最早的替換加密法凱薩加密法(Caesar Cipher)，將每個字母以該字母的後三個字母來替換，對照圖如圖 2-1，圖 2-2 是凱薩加密法的替換過程。

明文 (M)	A	B	C	D	E	F	G	H	I	J	K	L	M
⇓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
密文 (C)	G	E	D	C	A	K	M	F	L	N	H	R	I
明文 (M)	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
⇓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
密文 (C)	V	X	J	B	W	Q	R	S	P	T	U	Z	O

圖 2-1　凱薩加密法字母替換表

明文	meet me after the toga party
密文	Iaar ma gkraw rfa rxmg jgwrz

圖 2-2　凱薩加密法(Caesar Cipher)的明文和密文轉換

另一種方法是利用數字替換字母，如 A=0、B=1、…、Z=25，則可將凱薩加密法定義如圖 2-3：

加密：C＝(M+K) mod26

解密：m＝(C-K) mod26

圖 2-3　數字替換法的定義

因為只有 A-Z 的對映方式，所以只有 26 種加密方法，很容易被解密。

除了上述的方法，也可以將字母替換成任意的另一字母，不單只是簡單的位移法，使字母隨機對映到另一個字母，稱

為 Monoalphabetic 加密法(Merkle , 1990)，如圖 2-4。

明文	meet me after the toga party
密文	qaax qa gcxak xsa xtfg bgkxh

圖 2-4　數字替換法轉換過程

此加密方法共有 26 階乘種，雖然看起來很安全，但因為語言的特性，會常常出現某些特定字母組合，如 th、er、on，各字母的頻率出現不一，有些字出現頻率比較高，如圖 2-5 所示，故密碼容易被猜出。

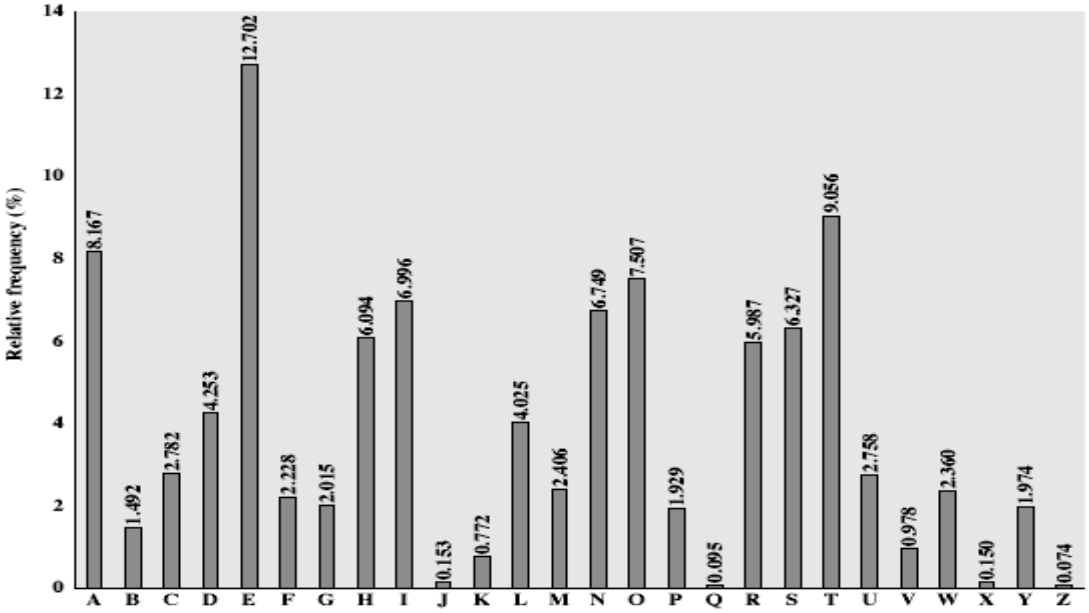


圖 2-5　英文字母出現之頻率

資料來源：W. Stallings (2007). *Cryptography and network security: Principles and practice (3rd ed.)*. New Jersey:Prentice-Hall, 41.

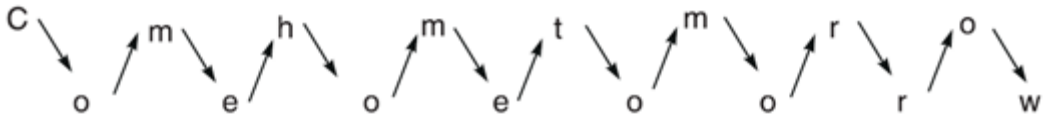
二、排列技術

排列是將原有的字母,重新做不一樣的排列來隱藏訊息，並沒有改變原有的字母，如柵欄加密法。柵欄加密法的方法是將原本的訊息改寫成對角形式，再組合起來，見圖 2-6。

明文	Come home tomorrow
轉換過程	C m h m t m r o o e o e o r w
密文	Cmhmtmrooeoeorw

圖 2-6　柵欄加密法的明文及密文轉換

此種加密法是對明文訊息字母按照對角順序排列之後，他將呈現如圖 2-7 的形狀：



2-7　柵欄加密法

先在大小預定的矩陣中寫出明文訊息，然後逐欄讀取訊息，這樣獲得的訊息就是密文。

三、位元轉移

DES (data encryption standard)演算法是 IBM 公司在 1970 年代發展出的一個加密演算法。 DES 演算法在 1977 年經由美國國家標準與技術協會(National Institute of Standards and Technology, NIST)採用聯邦標準(FIPS PUB 46-2)之後，成為金融界及其他產業應用最為廣泛的加密系統，DES 系統的基本原理(Biham and Shamir, 1991)是混淆(confusion)和散佈

(diffusion)。混淆就是將明文轉換成其他樣子，散佈則是指明文中的任何一個小地方的變更，都會影響到密文的各部份。

DES 加密系統為一對稱型區塊加密系統(Biham and Knudsen, 1998)。其輸入的明文大小為 64 位元，經過 DES 加密系統加密之後，再輸出 64 位元的密文，而 DES 所需的金鑰大小為 56 位元。將 64 位元大小的明文輸入 DES 加密系統後，系統會先將明文初始排列，再將明文經過 16 回合的運算，最後將第 16 回合的運算結果交換，經過終結排列後輸出 64 位元的密文。如圖 2-8。

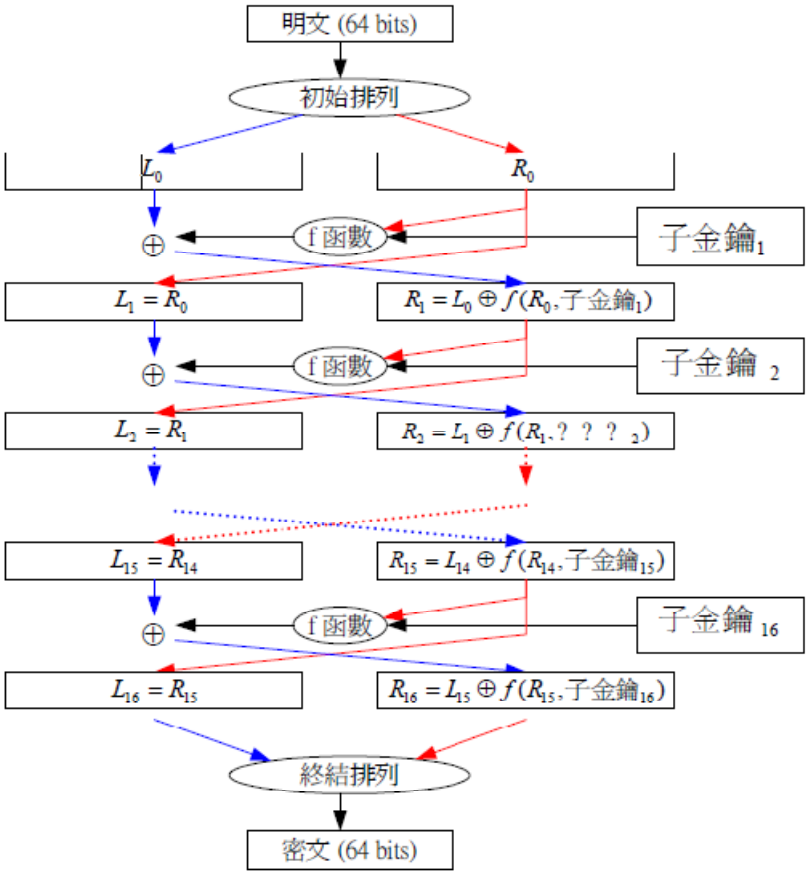


圖 2-8　DES 演算法原理

先在 DES 演算法中，用來進行混淆動作的，就是 S-BOX。

S-BOX 輸出值的方法就是：輸入 6 位元的頭尾兩個位元數的二進位數字(0~3)當作數列，中間 4 個位元的二進位數(0~15)當作行數，找出 S-BOX 中該位置的數字就是輸出。舉例如下：

將 010010 輸入 S-BOX 1

取出頭尾兩個位元：002 = 010

取出中間四個位元：10012= 910

S-BOX 1 中第 0 列，第 9 行的數字是 1010，而 1010 = 10102 因此輸出為 1010。。

由於上述三者單獨使用都有被破解的可能性，因此採取三種加密方法混合使用，讓破解變得更加困難。

第四節　資料驗證

Lee and Lee (2010)提出一種嶄新的資料驗證模組，透過設定不同的加密資料表，使用這些加密資料表來加密新聞資料，每一筆加密的檔案都用不同的加密代碼。當想要解密資料時候，使用者可以從加密的檔案中得到密文、加密資料表以及關鍵代碼，利用關鍵代碼以及檔案長度來驗證資料是否有遭到竄改，說明如圖 2-9。

當提取出來的驗證碼和驗證資料表產生的驗證碼比對符合，代表資料沒有遭到任何竄改。

基於第四節，我們提出加密驗證系統應用於新聞資料儲存及播放的研究。

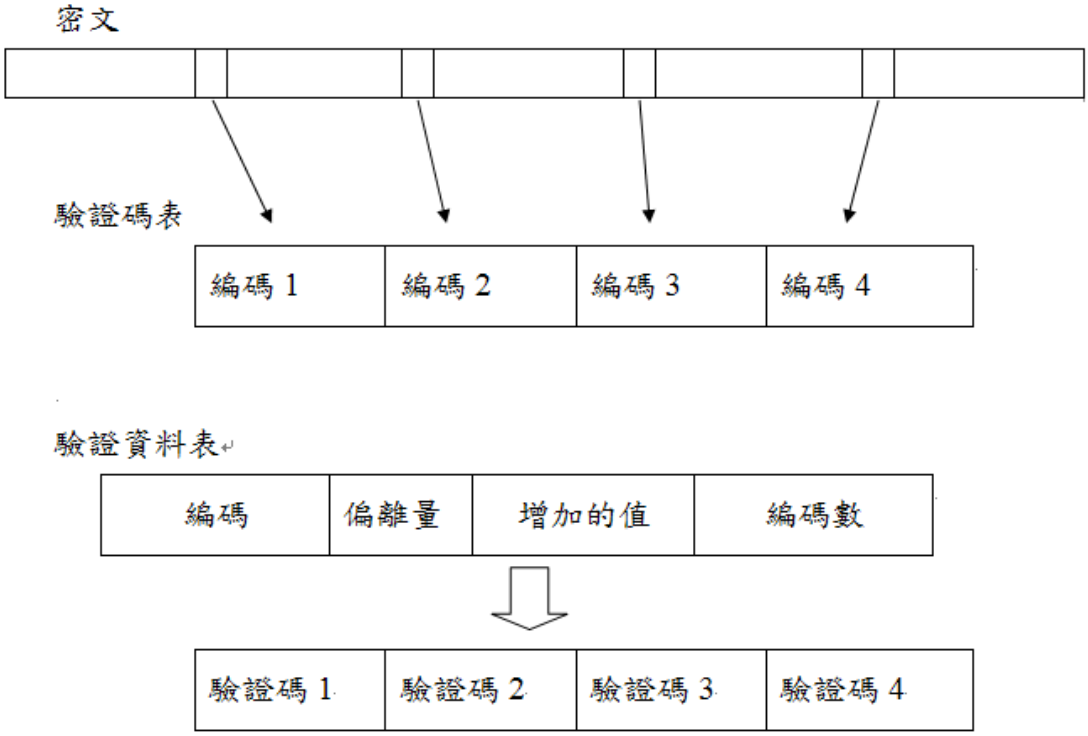


圖 2-9 驗證碼原理

第五節 數位簽章

數位簽章(digital signature)是將交易資料利用雜湊演算法轉換為訊息摘要(Pieprzyk, Hardjono, and Seberry, 2003)，再利用私密金鑰對訊息摘要進行亂碼化運算即可得到此筆交易資料之數位簽章。所使用之雜湊演算法具備「單向不可逆運算」之特性，僅能由交易資料推算出訊息摘要，而無法由訊息摘要反向推算出交易資料之內容，因此交易資料與訊息摘要之內容具有關聯性，且不同之交易資料內容不會運算出相同之訊息摘要。其原理如圖 2-10。

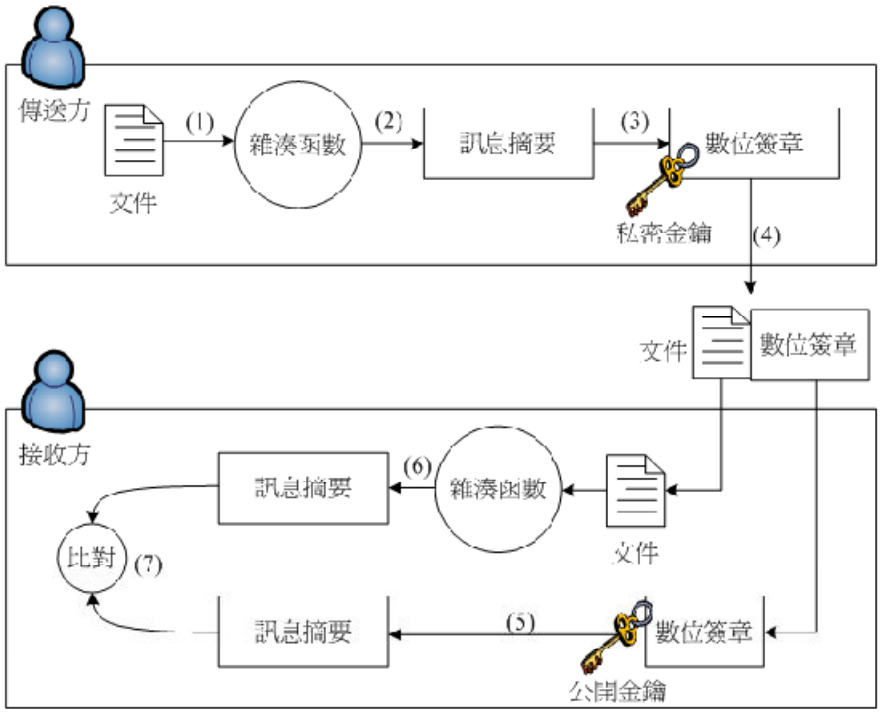


圖 2-10 數位簽章原理

一套數位簽章通常定義兩種互補的算法，一種用於簽名，一種用於驗證。每個人都有一對「鑰匙」(數位身分)，其中一個只有她/他本人知道的密鑰，另一個公開的公鑰。簽名的時候用密鑰，驗證簽名的時候用公鑰。公鑰必須向接受者信任的人(認證機構)註冊。註冊後認證機構給你發一個數位證書。對文件簽名後，把此數位證書連同文件及簽名一起發給接受者，接受者向認證機構求證是否是用你的密鑰簽發的文件。

第六節　密碼破解

對稱式加解密演算法有兩個主要原則(Shannon, 1949)，一個是取代(substitution)，一個是置換(transposition)，想還原明文的行為就稱為密碼破解，一般密碼破解方式有下列幾種：

一、僅知密文：

攻擊者僅能獲得一些加密過的密文。

二、已知明文：

攻擊者手上有一些密文，且知道相對應的明文。

三、自選明文：

攻擊者在開始攻擊之前，可以選擇一些密文並從系統中獲得相對應的明文。

四、自選密文：

攻擊者在開始攻擊之前，可以選擇一些明文並從系統中獲得相對應的密文。

五、自選文字：

與選擇明文(密文)攻擊類似，但是攻擊者可以得到兩個以上不同金鑰所加密(解密)的密文(明文)，攻擊者不知道金鑰的實際值，但是知道兩者之間大部分的關連。

對於密碼分析的結果來說，其有用的程度也各有不同。密碼學家 Knudsen and Martin (1998)將對於分組密碼攻擊，按照獲得的密文的不同分為以下幾類：

一、完全破解：

攻擊者獲得加密金鑰。

二、全局演繹：

攻擊者獲得一個和加解密相關的演算法，儘管他不知道金鑰的值。

三、局部演繹：

攻擊者獲得了一些攻擊前並不知道的密文(明文)。

四、訊息演繹：

攻擊者獲得了一些以前不知道的密文和明文的相關訊息。

五、分辨算法：

攻擊者能夠區分加密演算法和隨機排列。

六、程式解譯：

攻擊者竊取了加密程式，但沒有解密程式，可以拿大量的明文去加密測試藉此尋找出公式。

本研究為了防止攻擊者獲得加密金鑰之後的破解行為，嘗試使用格式碼來控制六種加密表單數值排列順序，即使攻擊者手中握有金鑰，他也要必須嘗試最多 6 階乘種的不同組合才能試出可能的密文破解。