密碼學初步

許介彥
大葉大學　通訊與計算機工程學系

前言

「密碼學」(Cryptography)，這門研究如何將機密資料依特殊的方式書寫使資料不為外人所悉的學問，在世界各國的歷史演進中都扮演著重要的角色。當一個領導者要對遠方的下屬下達重要且具機密性的指示，若是在古代，飛鴿傳書、驛馬快遞是常用的方式，在現代則可透過電話、電報、甚至電腦網路，但這些方式都不能保証可以將指示安全且秘密地送達；一旦重要軍情為敵方截獲並且知悉，一個領導者乃至整個國家的命運可能就此產生重大的變化。

除了政府的情報單位外，密碼學也可以應用在我們的日常生活中。每個人都喜歡保有一些秘密，當我們希望將秘密記錄起來而又不希望因內容被別人看到而曝光時，就可以用密碼學的特殊方式書寫或處理以達到保密的效果，這樣的做法自古有之，許多名人的私人日記都刻意用密碼寫成，後世經過一番解讀始得以一窺全貌。

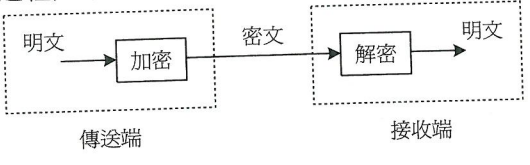
密碼學中保護資料的方法有很多，不同的方法對資料提供的保密程度可能有很大的差異，要選擇什麼方法通常要依被保護的資料的性質而定，或者說是希望要讓被保護的資料「安全」到什麼程度；私人書信、日記等資料主要的考量可能是方法的好用與否，若是涉及國家安全的機密資料就要不惜代價，以能達到希望具備的安全程度為前提。

換位(Transposition)及代換(Substitution)是密碼學中保護資料最基本的兩種運算，本文限於篇幅，將針對前者的基本原理及運作方式做一個概略性的介紹。

基本概念

考慮以下情況：A 有一筆機密資料要傳送給 B ，且資料在傳送過程中有可能被第三者透過管道得知。為了預防機密資料外洩，A 先將資料以某種特殊方式重新書寫一遍再送出，使得即使第三者在傳送過程中探知傳送的內容亦無法看懂；當資料到達B後，B再用一種事先跟 A 協調好的特殊方式將資料還原。

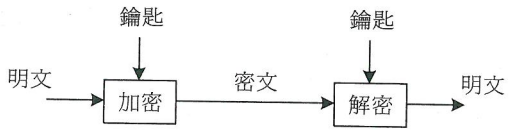
上面的例子中，通常我們將A稱為「傳送端」(sender)，B則稱為「接收端」(receiver)，將原始資料稱為「明文」(plaintext)，將經過A處理後第三者無法解讀的資料稱為「密文」(ciphertext)，A將明文改寫為密文的動作稱為「加密」(encipher 或 encrypt)，B將密文還原為明文的動作稱為「解密」(decipher 或 decrypt)；整個運作過程如下圖所示：



由以上的運作方式不難看出：資料是否安全的關鍵在於所用的加密及解密的方法是否不為外人所悉，因為所用的方法一旦曝光，不但外人有可能將密文破解而得知 A 要傳送的明文，更有甚者，外人也可能將假造的資料經由相同的加密手法加密後傳送給 B，讓 B 誤以為接到的資料是來自 A。不讓傳送及接收兩方以外的第三者有輕易破解密文或假造明文的可能是設計任何安全要求較高的加解密系統最主要的目標。

以現代的眼光來看，上述的運作方式已經不合時宜了。現代的加解密系統希望能夠讓傳送端及接收端都可以是一群人，而非只有一人，且人數可能隨時增加或減少；如果如上所述，系統的安全性是建立在加解密方法的不為人知，那麼當任一方有一人離開，全部的人將被迫重新選擇並適應另一套加密及解密的方法，以免離開的人將原來的加解密方法外傳而讓系統的安全受到威脅；當人數進出頻繁時，經常變換加解密方法對系統中的每個人將造成很大的學習上的負擔及使用上的不便。另一方面，好的加解密方法並不是非常容易取得的，因此加解密方法若需常常變換，會有實際上的困難。另外，如果加解密方法不對外公開，將無法接受系統以外其他人對方法好壞的分析與評估，因此除非系統中有人是密碼學的專家，否則可能所用的加解密方法只是使用者自以為安全，實際上卻是外人非常容易破解的方法。

現代的密碼學解決上述問題的方式是在加密及解密的過程中引進一個「鑰匙」(key，或翻譯成「金鑰」)，也就是在做加密及解密時，須另外有一個鑰匙來配合；鑰匙可能是一個英文單字、一個句子，或是一個數字、好幾個數字等，依不同的加解密方法而定。在運作上，通常假設加密及解密的方法都是公開的，但是將鑰匙當成只有傳送端及接收端才知道的祕密。由於將加密及解密的方法公開，因此可接受世界各地專家的分析與評估，而如果採用一套可以和很多鑰匙搭配的加解密方法，當系統有人離開時，即使有安全顧慮，只需換一個新的鑰匙就夠了，更換鑰匙通常比更換整套加解密方法要省事得多。新的運作方式如下：



如前所述，要選擇什麼樣的鑰匙須視所採用的加密及解密的方法而定，目前受到廣泛採用或討論的加解密方法有非常多的種類，在某些加解密方法中，加密與解密所用的鑰匙是同一個，但某些方法中加密有加密用的鑰匙，解密有解密用的鑰匙；有些方法的鑰匙包含了好幾部份（例如：好幾個數字），而其中甚至有某些部份是可以公開的。

當要保護的文件是英文資料時，為了增加破解的困難，在加密時一個很普遍的做法是將英文句子中所有的字母全部轉換成大寫或是小寫，因為若是照一般的習慣，一個句子只有開頭第一個字母大寫而其餘字母都是小寫的話，將使得句首第一個字母頗為特殊，經過加密後有可能還是非常特殊，以致讓有心人士可以經由分析密文中這種特殊之

處而收集到一些有利於破解的資訊。基於相同的理由，加密時另一個普遍的做法是將英文句子中所有的空格及標點符號拿掉。對絕大部分的英文句子（中文亦然）而言，空格及標點符號的存在固然較方便於閱讀，將它們全部刪除對文意的表達其實並不會造成任何的影響，asthissentenceshows。

所有的加密方法中，「換位」及「代換」可說是兩種最基本的運算，許多複雜的方法其實是由這兩種基本運算組合而成。所謂換位是指透過明文中的字元與字元（或位元與位元）間位置互換來加密的方式，而代換則是將明文中的字元或位元以其他字元、位元、數字、或符號取代的方式（例如：所有出現字母A的地方都以字母B取代）。

接下來，讓我們來看幾種利用換位運算做成的加密法。

柵欄加密法（Rail-Fence Ciphers）

以換位運算做成的加密法常須與特定的幾何圖形配合，運作的過程大致上如下所示：

明文 —寫入→ 圖形 —讀出→ 密文

明文先依特定的方式或路徑被填入一個幾何圖形中，然後再循不同的路徑被讀出而成為密文。所用的幾何圖形及寫入與讀出的路徑共同組成了這類加密法的鑰匙。

柵欄加密法是借助如鋸齒般的幾何形狀將明文加密的方法。要加密時，明文先依序填入鋸齒狀的幾何圖形中，再一列一列由上至下將字母讀出，例如：

明文：SCIENCEEDUCATION

⇓

```
S   N   D   T
 C E C E U A I N
  I   E   C   O
```

⇓

密文：SNDTCECEUAINIECO

柵欄的高度當然是可以變的；上圖中，柵欄的高度為3。要解密時，只要知道加密時所用的柵欄的高度，即可輕易地將密文還原。

柱形加密法(Columnar Transposition)

二維陣列（矩陣）是許多以換位運算做成的加密法常採用的幾何形狀。利用柱形加密法加密時，將明文依由左而右的方式一列一列由上而下填入矩陣，再將矩陣的內容以傳送與接收雙方約定好的特定順序一行一行地讀出；以下以一個4×7矩陣當做例子：

明文：MEETMETOMORROWNIGHTINLIBRARY

⇓

順序：7 5 2 4 1 3 6

M	E	E	T	M	E	T
O	M	O	R	R	O	W
N	I	G	H	T	I	N
L	I	B	R	A	R	Y

⇓

密文：MRTAEOGBEOIRTRHREMIITWNYMONL

這個例子中，加密及解密雙方都須知道7524136這串阿拉伯數字。如果雙方在要決定數字之初覺得數字不容易記住，可先隨便找一個由七個字母組成且每個字母都不同的英文單字（如：MICHAEL），然後將字母間依由A到Z的字母順序排出先後，再將這七個字母由1至7依序編號。以MICHAEL為例，A對應

到1，C對應到2，E對應到3，H對應到4，I對應到5，L對應到6，M對應到7：

7 5 2 4 1 3 6
M I C H A E L

依此類推，SIMPLE對應到624531，COVER對應到13524。對一般人而言，記住鑰匙是那一個單字要比記住是那一串數字來得容易。

以單純的換位運算做成的加密法通常很容易被有心人士破解，因為寫入及讀出的路徑有一定的規律；如果將已經加密的結果利用相同或是不同的換位運算再加密一次，常常可以使破解的工作困難許多。以上面的例子而言，再經過一次相同的運算：

MRTAEOGBEOIRTRHREMIITWNYMONL

⇓

順序：7 5 2 4 1 3 6

M	R	T	A	E	O	G
B	E	O	I	R	T	R
H	R	E	M	I	I	T
W	N	Y	M	O	N	L

⇓

ERIOTOEYOTINAIMMRERNGRTLMBHW

假設我們把原來明文中的28個字母依位置編號：

01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

若只觀察位置的變化，在經過第一次的運算後所得的結果為

05 12 19 26 03 10 17 24 06 13 20 27 04 11
18 25 02 09 16 23 07 14 21 28 01 08 15 22

不難看出上面這些數字有一定的模式（例如：最前面四個數字各差7）；如果再經過一次相同的運算，結果為

03 27 16 08 19 13 02 28 10 04 23 15 26 20
09 01 12 06 25 21 17 11 07 22 05 24 18 14

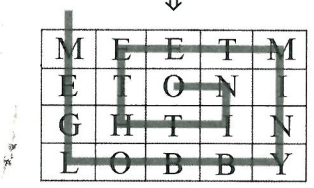
數字間的模式已經很不明顯，大大地增加了破解的困難。

曲徑加密法（Twisted-Path Ciphers）

將資料寫入或讀出矩陣的路徑當然不一定要以整列或整行為單位；曲徑加密法用的還是長方形的陣列，但在寫入或讀出的時候使用了較不規則的路徑。下面的例子中，明文還是很有規律地一列一列被填入矩陣，但是在讀出時，用的是一條螺旋狀的路徑：

明文：MEETMETONIGHTINLOBBY

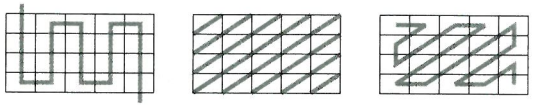
⇓



⇓

密文：MEGLOBBYNIMTEETHTINO

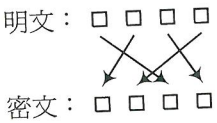
路徑的形狀除了螺旋形外，當然還有許多的可能。再多舉三個例子：



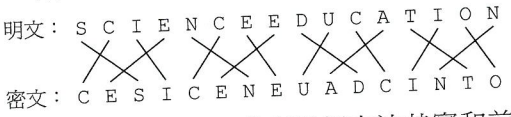
週期性排列加密法（Periodic Permutation Ciphers）

週期性排列加密法是將相同的換位運算週期性地應用在明文中的加密法。以週期等於四為例，明文以每四個字母為單位進行加

密，假設明文與密文中每四個字母的關係為



則



讀者也許已經注意到這個方法其實和前面提過的柱形加密法非常類似；柱形加密法是將明文一列一列寫入矩陣再一行一行讀出，而這個方法可以看成是將明文一列一列寫入但還是一列一列讀出；或者，上面這個例子也可以看做是將柱形加密法以1×4矩陣連續應用到明文中。

結語

隨著電腦軟硬體的發展及網路技術的成熟，世界上每天有越來越多的資料經由電腦處理及傳送；為了對電腦所處理的資料做適當的保護，「密碼學」這門歷史悠久的學問在近年來受到了廣泛的重視與討論。藉由電腦快速而準確的計算能力，一些原本非常複雜以致幾乎無法純粹由人力完成的加密法有了實現的可能；另一方面，一些原本被視為安全的加密法也受到了嚴峻的考驗。

西方國家的文字是由總數不多的字母（如英文的26個字母）組成，且句子都是由左而右由字母如磚頭般一個一個依序堆砌而成（忽略空白與標點符號的話），因此與中文相比，西方的文字特別適合做字母間位置對調、將某個字母以另一個字母或符號取代等動作，因為處理後的結果還是一連串由左而右由字母或符號組成的資料，只要知道加密的方法，就可以將密文中的字母或符號一個一個還原回去。當加密及解密是由電腦來做時，由於電腦內的資料都可以看成是由一個一個的位元排列而成，因此可以將上面提到的方法應用到任何格式的資料或檔案中（圖檔、執行檔、中文資料等）。

純粹以換位運算做成的加密法很適合做為認識密碼學的起點，但以現代密碼學的眼光看來是太簡單了，若有電腦的幫助，對專業人士而言通常不難破解，而且有許多純粹以換位運算做成的加密法在使用上需要不小的記憶體，或是對明文的長度有特殊的限制，因而造成使用上的不便；代換運算其實才是研究人員設計加密法時較常使用的運算，有機會筆者將另文介紹。

參考資料

1. Dorothy E. R. Denning, Cryptography and Data Security, Addison-Wesley, 1982.
2. Martin Gardner, Codes, Ciphers, and Secret Writing, Dover, 1972.
3. William Stallings, Cryptography and Network Security, 2nd edition, Prentice Hall, 1999.