探討神奇密碼學

李芳俞

摘要

數學的重要性在軍事中不言而喻，從早期的地道挖掘、弩箭發射到現代戰爭的建模分析、精確打擊……無不有數學參與其中。而從古至今在政治、經濟、軍事及科技方面都有防止重要機密洩漏的安全管制，在當今資訊爆炸的時代，各式各樣的訊息在網路中傳遞，若沒有經過任何保密措施，這些資訊就等同於直接提供給所有人，因此如何保護重要資訊成為了重要的課題。

壹、前言

密碼學是研究如何隱密地傳遞訊息的學門。在現代特別指對資訊以及其傳輸的數學性研究，常被認為是數學和電腦科學的分支，和資訊理論也密切相關。著名的密碼學者 Ron Rivest 解釋道：「密碼學是關於如何在敵人存在的環境中通訊」，自工程學的角度，這相當於密碼學與純數學的異同。密碼學是資訊安全等相關議題，如認證、存取控制的核心。密碼學也促進了電腦科學，特別是在於電腦與網路安全所使用的技術，如存取控制與資訊的機密性。密碼學已被應用在日常生活：包括自動櫃員機的晶片卡、電腦使用者存取密碼、電子商務等等。

貳、正文

一、經典密碼學

在近代以前，密碼學只考慮到訊息的機密性：如何將可理解的訊息轉換成難以理解的訊息，並且使得有秘密訊息的人能夠逆向回復，但缺乏秘密訊息的攔截者或竊聽者則無法解讀。近數十年來，這個領域已經擴展到涵蓋身分認證、訊息完整性檢查、數位簽章、互動證明、安全多方計算等各類技術。

自然數，特別是質數的性質，與祕密通訊關聯很深刻。將通訊內容經過特定的規則轉換成其他記號稱為「加密」；而將加密過後的數據還原成原本可以讀的狀態則稱為「解密」。

由於古時多數人並不識字，最早的秘密書寫的形式只用到紙筆或等同物品，隨著

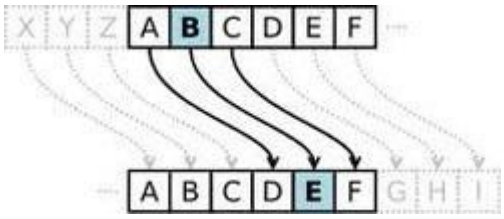
識字率提高，就開始需要真正的密碼學了。最古典的兩個加密技巧是：

(一)置換（Transposition cipher）：將字母順序重新排列，如『help me』變成『ehpl em』

(二)替代（substitution cipher）：有系統地將一組字母換成其他字母或符號，例如『fly at once』變成『gmz bu podf』（每個字母用下一個字母取代）。

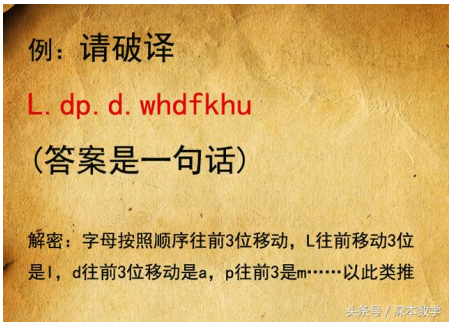
這兩種單純的方式都不足以提供足夠的機密性。世界上最為古老的體制密碼凱撒密碼，所使用的就是有序的代替密碼。即將原有的字母以特定的關係映射到另一個字母，其映射關係可以是線性的，也可以是乘法關係。由來是軍事指揮官尤里烏斯・凱撒設計了一種對重要的軍事信息進行加密的方法，即使這些信息被截獲，敵方不一定能看懂。

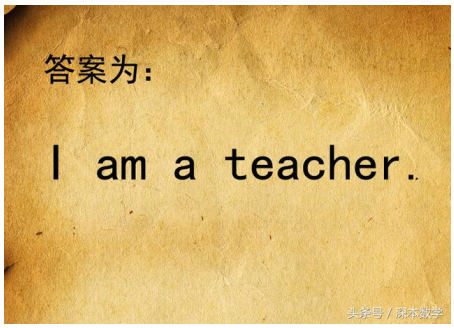
在這種密碼中，從 A 到 W 的每個字母在加密時用字母表中位於後三位的那個字母代替，字母 XYZ 分別被替換成 ABC。凱撒在這裡是將字母向右移動了三位（如下圖）。比如，在三個移位的情況下，信息 DOG（這種需要加密的信息統稱「明文」）就變換成 GRJ（這種經加密後產生的的信息統稱「密文」）；密文 FDW 對應的明文則是 CAT。可以看到，加密、解密過程都是以字母移位的位數為參照的。這種在加密和解密的算法中依賴的參數則被稱為——密鑰。



當然，移位的選擇並不僅僅限制在三位，從 1 到 25 任何數的移位都能產生類似效果。只要通信雙方事先約定好，這個選擇就很任意。很明顯的是，移位方法最多也只有 25 種，這成為凱撒密碼的致命弱點。

我們可以通過試著破解一題凱撒密碼來理解。



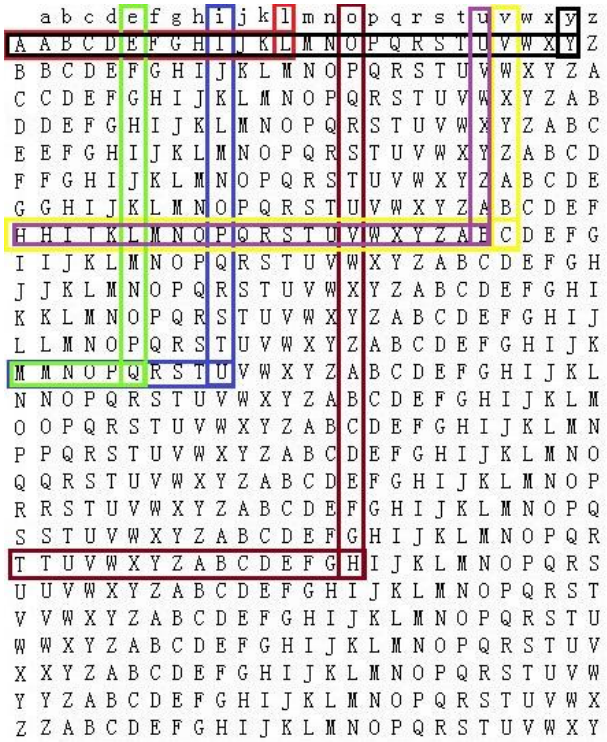


由此我們可以看出凱撒密碼就是一個簡單的線性代替算法，其破譯方法也比較簡單，只要有較多的譯文就可以使用字母頻度分析將其破譯。

古中國周朝兵書《六韜．龍韜》也記載了密碼學的運用，其中的《陰符》和《陰書》便記載了周武王問姜子牙關於征戰時與主將通訊的方式；陰符是以八等長度的符來表達不同的消息和指令，可算是密碼學中的替代法（substitution），把資訊轉變成敵人看不懂的符號。至於陰書則運用了移位法，把書一分為三，分三人傳遞，要把三份書從新拼合才能獲得還原的資訊。

二、中世紀至第二次世界大戰

本質上所有的密碼仍然受到上述的破密法的危害，直到阿伯提（Leon Battista Alberti）約在 1467 年發明了多字元加密法（polyalphabetic cipher），阿伯提的創新在於對訊息的不同部分使用不同的代碼。多字元加密法最典型的例子是維瓊內爾加密法（Vigenere cipher）：首先選擇一個無重複字母的密鑰詞（比如 MATH ），重複密鑰詞直至它成為一個和明文信息一樣長的字母序列，再利用下面這種方陣加密這條信息。信息 ILOVEYOU 密鑰 MATHMATH 密文 ULHCQYHB



這無疑是一種高明的加密手段，維瓊內爾密碼用嚴格的輪換方式重複使用一串簡單的代換密碼，很好的偽裝了基礎語言中的字母頻率。它還有很多變化，比如有一種可以允許密鑰詞中出現重複字母。每種變化都會產生一些新的特徵，從而引發破譯方式的變化，一直到十九世紀中期才被查爾斯・巴貝奇破譯，他用了一種精巧的方法：在密文中搜索重複的字符串，它意味著兩個重複模式之間的距離可能等於周期的整數倍！

蘇格蘭的瑪麗女王

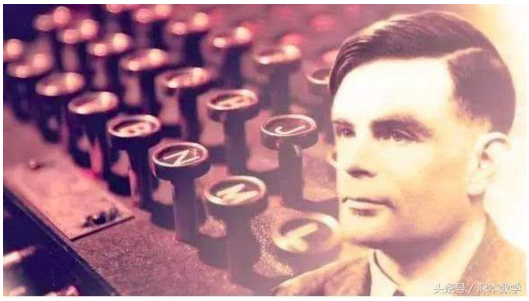
西元 1578 年，瑪麗女王被伊莉莎白女王軟禁。在 1586 年 1 月 6 日瑪麗收到一批秘密信件，得悉了安東尼.貝平頓（Anthony Babington）和幾個同黨在密謀營救瑪麗，並計劃行刺伊莉莎白女王。他們的信件被轉成密碼，並藏在啤酒桶的木塞以掩人耳目。但卻被英格蘭大臣華興翰（Walsingham）的從中截獲、複製、還信入塞，並由菲力普·馬尼斯（Philip van Marnix）破解信件。信件破解後，華興翰使菲力普摹擬瑪麗的筆跡引誘安東尼行動，把叛逆者一網成擒，審判並處死瑪麗女王。

三、第一次世界大戰

1914 年 8 月 25 日德國的馬格德堡巡洋艦（Magdeburg）在芬蘭灣（Gulf of Finland）擱淺，俄國搜出多份德國的文件及兩本電碼本，被送往英國的「40 號房間」（Room40）進行密碼分析。同時，無線電的發明亦使得截獲密信易如反掌。德國借用了美國的海底電纜發電報到華盛頓，但電纜經過了英國，1917 年 1 月 17 日齊默爾曼電報被「40 號房間」截獲。密電內容指德國將在 1917 年 2 月 1 日開始『無限制海戰』，用潛艇攻擊戰時包括中立國在內的海上商運船。為了阻止美國因此參戰，德國建議墨西哥入侵美國，並承諾幫助墨西哥從美國手中奪回得克薩斯、新墨西哥和亞利桑那三州。德國還要墨西哥說服日本共同進攻美國，德國將提供軍事和資金援助。密電內容揭開後，美國在 4 月 16 日向德國宣戰。

四、第二次世界大戰

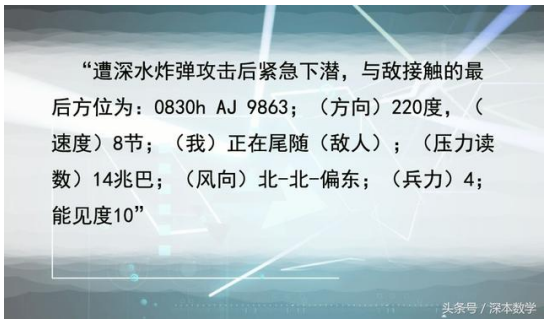
而到了二戰時期，數學原理被廣泛應用到軍事密碼的編制中，比如在太平洋戰爭爆發之前，日本軍方發明的名為「紫密」的密碼，運用這種密碼，日本在二戰中極為瘋狂。直到在中途島海戰中，由於美國成功破譯日本電報密碼，致使日本 4 艘航空母艦，1 艘巡洋艦被炸沉，330 架飛機被擊落；幾百名經驗豐富的飛行員和機務人員陣亡。才使得日本喪失了在太平洋戰場上的制空權和制海權。



同樣在二戰中，德國汲取了第一次大戰的教訓，發展出以機械代替人手的加密方法。雪畢伍斯（Arthur Scherbius）發明了「謎」（ENIGMA）-恩尼格碼密碼機，用於軍事和商業上。「謎」主要由鍵盤、編碼器和燈板組成。三組編碼器合、加上接線器和其他配件，共提供了一億種編碼的可能性，其密碼的複雜程度可以說是無人可以破解。但是，數學家圖靈通過數學的思想和方法設計了一架破譯機「Ultra」（超越）專門對付「Enigma」，破譯了大批德軍密碼。

許多物理裝置被用來輔助加密，例如古希臘斯巴達的密碼棒（scytale），這是一個協助置換法的圓柱體，可將資訊內字母的次序調動，利用了字條纏繞木棒的方式，把字母進行位移，收信人要使用相同直徑的木棒才能得到還原的資訊。在歐洲中世紀時期，密碼欄（cipher grille）用在某類隱寫術上。多字元加密法出現後，更多樣的輔助工具出現，如阿伯提發明的密碼盤、特裡特米烏斯發明的表格法、以及美國總統湯瑪士傑佛遜（Thomas Jefferson）發明的多圓柱（約在 1900 年再次獨立發明改進）。廿世紀早期，多項加解密機械被發明且被註冊專利，包括最有名的轉輪機，第二次世界大戰德軍所用，別名『謎』，謎式密碼機是利用複雜的齒輪結構變換字母順序，而且每次使用時，字母變換的規則都不相同，被認為是不可能破解的密碼。

我們來看看這自二戰以來一直遺留至今的恩尼格碼密文。

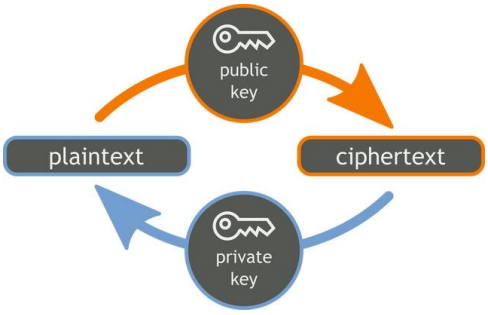


是不是感覺很神奇呢！其實，設置密碼大多藉助數學的知識，而破解的關鍵就是利用數學的思維來思考分析。

五、網際網路時代的密碼學

進入數碼時代，密碼學的目標沒有變：防止溝通雙方交換的信息被第三個人知道。各位可能會覺得，只要加密規則被發現的話，就有可能依照同樣的規則破解密碼，這似乎是將文件加密時無法避免的問題。但是，這個問題是可解決的。想到答案的是美國的惠特菲爾德・迪菲（Whitfield Diffie）及馬丁・赫爾曼（Martin Hellman）。這是 1976 年左右的事，為了說明他們的發想，先來說說南京鎖（鑰匙鎖）吧。一旦南京鎖被鎖上了，只有持有鑰匙的人，或是有特殊開鎖技巧的人才能將鎖打開。雖然知道上鎖的方法，卻無法得知開鎖的方法。就南京鎖而言，上鎖的知識對於開鎖沒有任何幫助。迪菲及赫爾曼他們想著，難道不能有像南京鎖這樣，即使知道加密規則也無法輕易解密的方法嗎？

如果知道規則也無法解密的話，那加密的規則也就不需要保密，於是就能夠將加密的規則公開，不管是誰都可以將通訊內容加密了。雖然公開了加密的規則，只要解密的規則沒有公開的話，就可以守護通訊祕密了。這就是迪菲及赫爾曼的想法。實現了這個公開金鑰密碼概念的，就是現在網路交易時使用的 RSA 密碼



麥可·卡爾德班克（Michael Calderbank）介紹了目前廣泛使用的公鑰加密技術，稱為 RSA 加密。這種加密法利用了質數的數學性質：將兩個質數（大於 1 的自然數中，只能被 1 和自己整除的數）相乘毫不費力，但給定一個數字，反推出它是由哪兩個素數相乘的結果，就不那麼容易了。如果這個數字夠大，那麼即使是地球上最快的計算機，也可能需要數百年才能完成計算過程。

歐拉定理

當 m 為兩個質數 p 與 q 的乘積，也就是 m＝pxq。在這個時候，因為 φ(pxq)＝(p－1)x(q－1)，因此自然數 n 不被質數 p 及 q 整除的話，下面的關係式就能成立。$n^{(p-1)\times(q-1)}$＝1＋（pxq 的　倍數）例如，假設有兩個質數 p＝3、q＝5 而 m＝pxq＝15，φ(3x5)＝(3-1)x(5-1)＝8，n 與 15 互相為質數的話，則應該是 n^{8}＝1＋（15 的倍數）請各位用 n＝7 代入試試看。

使用歐拉定理的話，就可以發現數字的有趣性質。例如，歐拉定理可以證明 9、99、999 這些 9 排成的數，利用質因數分解的話，會出現除了 2 跟 5 之外的質數。

根據歐拉定理，如果自然數 n 無法被質數 p 及 q 整除，那麼就存在下列的關係式：

$n^{(p-1)\times(q-1)}$＝1＋（pxq 的倍數）

如果乘上 s 次方，因為 1^{s}＝ 1，就成為：

$n^{s\times(p-1)\times(q-1)}$＝1＋（pxq 的倍數）

再乘一次 n，就成為：

$n^{1\ +\ s\times(p-1)\times(q-1)}$＝n＋（pxq 的倍數）

也就是說，不管 n 是怎樣的數，只要 n 無法被質數 p 及 q 整除，$n^{1\ +\ s\times(p-1)\times(q-1)}$除以 pxq 的餘數，就會還原成 n。那麼，就來應用在公開金鑰密碼上吧。

計算機打開加密信息的速度，能夠反推出這個素數密鑰的範圍。為了尋找更加先進的加密技術，量子物理學登場了。

六、邁出一大步的密碼學

為了尋找一種牢不可破的密碼，今天的密碼學家們正在研究量子物理學。傳統密鑰是以字節為單位編碼，量子加密則可以對粒子屬性編碼，這種粒子通常是光子。偷窺者必須通過測量光子來竊取密鑰，但根據量子力學，任何偷窺粒子的觀察行為，都會改變它的狀態。當偷窺者行動時，就會發現交流存在安全漏洞。

20 世紀 90 年代，牛津大學的阿圖爾·埃克特（Artur Ekert）提出了一種新的量子加密技術，這種技術基於「量子糾纏」現象，允許兩個光子在很遠的距離上進行實時通信。「量子擁有這種神奇的屬性，如果你將它們分開，甚至超過數百千米，它們還會彼此感受到，」埃克特說，「這種特性允許愛麗絲和鮑勃製作共享密鑰，並交流信息。如果竊聽者試圖攔截密鑰，則粒子就會有反應，並且測量值會發生變化。溝通雙方發現竊聽者，立刻放棄交流，換另一種方法。又因為量子通信是實時的，當發現竊聽者後，放棄信息傳輸，並不會泄露任何內容。」

實際上，雖然還沒有實現，但是已經知道如果能做出使用量子力學的「量子電腦」的話，N 位數自然數的質因數分解，應該只需要 N 次方時間就能完成。1994 年，麻省理工學院的數學家彼得．秀爾（Peter Shor）發現了一種計算質因數分解的演算法，只需要 N 位數自然數的 N^3計算次數就能完成。只是，「量子電腦」目前仍然處於理論的階段，實際上依然無法做到。

另一方面，如果利用量子力學的原理，也有可能做出跟 RSA 相異的通訊密碼。「量子密碼」的方法是，如果密碼被中途攔截並且解密的話，不論藏得多隱密，都一定會被發現。只要量子力學是正確的， 就不可能竊取通訊訊息。不管是「量子電腦」或「量子密碼」被開發出來，應該都會對通訊安全造成很大的改變。

叁、結語

其實，自從文字被發明後，關於信息加密的需求就出現了，不管是經濟、軍事、政治上的大事，還是情侶之間的柔情蜜語，人們都不希望被無關的人打聽到有用的信息，所以為了實現信息的安全傳遞，人們不斷更新加密技術，從密碼棒、換位密碼，到恩尼格碼機，再到量子加密技術。因為信息越來越重要，加密法就得越來越高級，雖然為了保住秘密，人們被折磨得疲憊不堪，焦頭爛額，但我們還在密碼遊戲中玩得樂此不疲，這也許就是密碼學的魅力所在。

肆、引註資料

一、維基百科 Wikipedia。
二、莎拉 • 夫蘭納里、大衛 • 夫蘭納里（2001）。數學小魔女。
三、三谷政昭、佐藤伸一（2009）。世界第一簡單密碼學。世茂出版。
四、Simon Singh（2000 年）。碼書：編碼語解碼的戰爭。Fourth Estate 出版。