行政院國家科學委員會專題研究計畫　成果報告

設計一種具有學習能力的基因演算法做為新的密碼分析途徑之研究(I)

計畫類別：個別型計畫
計畫編號：NSC91-2213-E-034-002-
執行期間：91 年 08 月 01 日至 92 年 07 月 31 日
執行單位：中國文化大學應用數學系

計畫主持人：林豐澤

報告類型：精簡報告

處理方式：本計畫涉及專利或其他智慧財產權，2 年後可公開查詢

中　華　民　國 92 年 10 月 24 日

設計一種具有學習能力的基因演算法做為新的密碼分析途徑之研究 (I)

計劃編號：NSC 91-2113-E-034-002
執行期限：91 年 8 月 1 日 至 92 年 7 月 31 日
主持人：林豐澤　　中國文化大學 應用數學系

摘要

密碼分析是一門不知金匙參數而可破解任何密碼系統的藝術或科學。因此，密碼分析是將一篇密文復原為原來明文以及得到它所使用金匙參數的複雜分析過程。學習密碼分析是件十分困難的工作，因為到目前為止沒有任何標準的教科書可用。已知的密碼分析方法有：字母頻率分析、兩字母一音分析、卡西斯基測試、相似索引、差分密碼分析、與線性密碼分析等等。多年來密碼分析師一直不斷在尋求可以自動攻擊密碼的新方法，通常的做法是先將新方法破解簡單的密碼系統，經過仔細評估後，才去破解更複雜或性質不同的其他密碼系統。

三年前，我們開始嘗試應用基因演算法破解密碼系統。為了研究計劃的順利進行，我們先縮小研究的範圍，將目標訂在 Vigenère 密碼上，同時提出一些合理的假設，簡化研究的困難度，期許這個研究能夠延伸到更複雜的密碼系統上。我們的研究動機是要設計有效率且有制度的方法來協助破解各種密碼系統，找出設計上的漏洞。這是因為唯有不能被破解的密碼系統，方才能確保資訊通訊的安全性，也可確保數位簽章的可靠性。這個研究得到下列的結論：基因演算法可以破解具有固定長度的金匙參數的串流式密碼系統。我們已將這個研究成果發表在第五屆人工智慧與應用的研討會上。現在，我們想進一步研究如何應用基因演算法破解更複雜的密碼系統，因此，我們提出一個為期兩年的研究計劃，期許將來能夠將基因演算法視為是密碼分析的一種新途徑。我們的構想是：第一年的研究計劃，研究如何應用基因演算法來破解較複雜的區塊式密碼系統，例如：DES, LUCIFER, FEAL, IDEA, SKIPJACK 等等。第二年的研究計劃，則打算應用分類元系統做為基因演算法的學習工具，藉由學習之威力，能夠使基因演算法有效的破解更複雜的非對稱式密碼系統，例如：迷袋密碼系統。

關鍵詞：密碼分析、密碼學、區塊密碼、迷袋密碼系統、學習、基因演算法、分類元系統、非對稱密碼系統。

Abstract

Cryptanalysis is the art or science of deciphering encrypted communications without knowing the proper keys. Therefore, cryptanalysis is the complex process of recovering the plaintext and key from a cipher. Studying cryptanalysis is a difficult task because there is no standard textbook to use. The well-known cryptanalysis methods in the literature are Letter Frequencies, Digraph Analysis, Kasiski Tests, Coincidence Index, Differential Analysis, Linear Analysis, etc. Over the past years, cryptanalysts are continually seeking new methods for automating attacks on ciphers. Traditionally, the new technique is applied to a simple cipher in the first instance, following which it is scrutinized for possible use against more complex or different kind of cryptosystems.

We proposed a project and started to study cryptanalysis by applying genetic algorithms to break ciphers three years ago. To simplify this study, we limited our work on Vigenère cipher and made some reasonable assumptions on cryptanalysis. We expected this study could be extended to the more complex cryptosystems. The motivation of our study is that we plan to design a systematic and efficient approach to attack various cryptosystems for finding the weakness of their design. This is because an unbreakable cryptosystem ensures the security of data communications and the reliability of digital signatures over the network. The conclusion of our work is that genetic algorithms can be used for breaking stream ciphers, which have fixed-length key parameters. We presented this result at the Fifth Conference on Artificial Intelligence and Applications and received an honorary excellent paper award.

Now, we would like to continue the previous work for breaking more complex cryptosystems using genetic algorithms. Therefore, we propose a two-year NSC project in an attempt to use genetic algorithms as a new approach for cryptanalysis. Our proposal is that in the first year we plan to study how to apply genetic algorithms to break block ciphers, including DES, LUCIFER, FEAL, IDEA, SKIPJACK, which are more complex than stream ciphers. In the second year, we plan to include classifier systems as a genetic algorithm's learning tool. With the learning power, we hope that the proposed genetic algorithm approach can attack asymmetric cryptosystems, e.g., knapsack algorithm, effectively.

Keywords: Cryptanalysis, Cryptography, Block Ciphers, Knapsack Cryptosystem, Learning, Genetic Algorithms, Classifier Systems, Asymmetric Cryptosystems

一、 前言與研究目的

密碼術 (Cryptology) 包含了研究如何秘密通訊與研究如何破解密碼系統兩個領域，研究製造密碼的領域稱為密碼學 (Cryptography) 而研究破解密碼的稱為密碼分析 (Cryptanalysis)。早期的密碼學主要使用於軍事與外交的通信系統，然而近年來電子商務的熱潮，使得資訊界、商業界、與工業界對於資訊安全的需求與日俱增。這是因為在開放式的網際網路裏，所流通的資訊隨時可能被有心人士獲知，他們可能利用特殊軟體直接從網路上攔截封包，或者利用電表、或電磁感應器來量測訊號而獲得資訊。因此，電子商務急需使用各種密碼技術，來隱藏雙方的商業通訊訊息，避免被第三者獲悉，以確保網路資訊的通訊安全與數位簽章的正確性。

評估一個密碼系統的優劣程度，安全性是最重要的指標，因為再好的密碼系統如果容易被攻擊而破解，則絲毫沒有使用的價值。但是，我們很難使用理論方式去證明密碼系統的絕對安全性。由此可見，製造密碼與分析密碼其實是相輔相成的，因為唯有不斷地接受被破解的挑戰，設計者方才能構思更精良的密碼技術。密碼術就是成長於這種反覆挑戰與改進的環境中，它的歷史其實就是幾世紀來編碼者與解碼者之間的戰爭史。然而密碼學的發展，從傳統到現代密碼系統，從週期性到非週期性的金匙參數，從串流密碼 (Stream Ciphers) 到區塊密碼 (Block Ciphers)，從對稱金匙 (Symmetric Keys) 到非對稱金匙 (Asymmetric Keys) 的密碼系統，結構愈來愈複雜。而且近代密碼學又大量運用數論 (Number Theory)、組合論、機率、線性代數等數學基礎，這使得破解密碼系統愈來愈困難，但也因此相對的提昇了資訊通訊的安全性。

密碼分析是一門沒有金匙參數而可破解密碼系統的藝術或科學。可是，學習與研究密碼分析是件十分困難的工作，因為目前沒有標準的教科書可用。密碼分析的攻擊方式，依其攻擊威力由弱而強的層次關係是：密文攻擊 (Ciphertext-only Attack)、已知明文攻擊 (Known Plaintext Attack)、選擇明文攻擊 (Chosen Plaintext Attack)、以及選擇密文攻擊 (Chosen Ciphertext Attack)。其中密文攻擊是最弱的攻擊方式，而選擇密文攻擊是最強的方式。近幾年也有學者提出中途攻擊 (Meet-in-the-Middle Attack) 的新做法。一般而言，破解密碼系統最直接的方式就是使用 “嘗試錯誤” (Try-and- Error)。此法對於簡單的密碼系統是沒有問題的，但是對於複雜的系統，往往需要耗費甚鉅的成本與時間，成效當然不彰。從過去以來，已知的密碼分析途徑有：字母頻率分析 (Alphabetic Frequency)、兩字母一音分析 (Digraph Analysis)、卡西斯基測試 (Kaisiski Test)、相似索引 (Coincidence Index)、差分密碼分析 (Differential Cryptanalysis)、線性密碼分析 (Linear Cryptanalysis) 等等。然而在現有的這些途徑中，我們無法明確的歸納出那一種途徑最適合於破解什麼性質的密碼，而且每一種方法適用的攻擊層次及其效力亦有所不同。這代表著密碼分析仍在起步階段，值得我們繼續研究與發展新的途徑，嘗試其他不同的分析方法。

多年來密碼分析師一直不斷在尋求可以自動破解密碼的新途徑，通常的做法是新方法先破解簡單的密碼系統，經過仔細評估後，再去破解更複雜或性質不相同的密碼系統。四年前，我們開始嘗試應用基因演算法來破解密碼系統。為了研究計劃的順利進行，我們先縮小研究的範圍，將目標訂在 Vigenère 密碼系統，同時也提出一些合理的假設，來簡化研究的困難度，期許這個研究將來能夠延伸到更複雜的密碼系統上。這個研究計劃所得到的初步結論是：基因演算法可以快速破解具有一定長度金匙參數的串流式密碼系統。因此，這個研究計畫的目的就是想延續前一個研究計劃的工作，嘗試去攻擊與破解較複雜的區塊式密碼系統。進一步來說，想要在基因演算法加入學習的功能，希望能夠自動建立一些樣板規則。有了樣板規則則可加速猜中金匙參數的速度與機率，可將基因演算法做為密碼分析的一種新途徑。

二、 相關研究文獻探討

通常密碼系統為了維持它的最高安全性，均會假設破密者擁有強大的知識，是屬於智慧型的犯罪者。因此 Kerckhoff 對密碼系統的安全性做了以下的定義：密碼系統的安全性，必須僅依賴解密金匙。也就是說，一個密碼系統中除了解密金匙外，其餘的加密方法與解密方法等，均假設破密者全然知道。因為只有在這個假設下，任何人無法破解密碼系統時，這個密碼系統才能被稱為是安全的。所以，當一個密碼系統被找到對映的解密金匙參數時，我們稱此密碼系統被破解了。一般而言，破解密碼系統最直接的方式就是使用"嘗試錯誤" (Try-and- Error)。此法對於簡單的密碼系統是沒有問題的，但是對於複雜的系統，往往需要耗費甚鉅的成本與時間，成效當然不彰。過去有人利用分析密文中某一字串出現的頻率以及出現的位置，求出這些數據的最大公因數當做金匙參數的長度，經過仔細的比對分析後，再去猜出金匙參數來破解密碼，這就是卡西斯基測試 (Kasiski Test) 與相符索引 (Index of Coincidence) 等方法。然而，計算字串出現的頻率或者分析字串出現的位置或者使用兩字母一音 (Digraph) 或者找出某一相同長度的字串的相符索引，也都需要耗費眾多的人力與時間。尤其當金匙參數很長時，它們破解密碼成功的比率也相對的降低。1990 年 Biham 與 Shamir 提出差分密碼分析 (Differential Cryptanalysis) 的觀念。此法是分析一對明文之間的差值與它們所映射的一對密文之間的差值所產生的影響，來推導出一些可能的金匙參數並附上機率以供選擇。差分攻擊法屬於選擇明文攻擊方式，需要指數的時間複雜度。1991 年他們使用差分密碼分析先破解一些簡單密碼系統，於 1992 年破解 16 回合的 DES 密碼系統，於 1993 年破解 Lucifer 密碼系統。1993 年 Matsui 則介紹線性密碼分析 (Linear Cryptanalysis) 的觀念，這是屬於已知明文攻擊法，需要知道一定數目的明文與所對應的密文配對，其困難度與差分密碼分析相近，但是技術上較差分密碼分析容易。之後，Langford 與 Hellman 結合上述兩種方法而提出差分--線性密碼分析 (Differential-Linear Cryptanalysis)，擷取兩法之優點。1994 年 Matsui 與 Yamagishi 提出 meet-in-the-middle 的方式破解 FEAL 密碼，同年 Matsui 提出破解 16 回合的 DES 的線性分析方法。1995 年 Youssef 與

Trvars 分析比較線性與差分密碼分析方法對 S-Box 的作用效果。1995 年 Jakobsen 提出一種快速方法來破解簡單的替換式密碼 (Substitution Ciphers)，他的方法是藉由兩字母一音在密文的分布情況與在明文中的期望分布情況來破解之，但此法只適合破解單一字母與多字母的替換式密碼系統。

然而在現有的這些方法中，我們無法明確的歸納出那一種途徑適合於破解什麼性質的密碼，而且每一種方法適用的攻擊層次及其效力亦有所不同。事實上，密碼分析仍在起步階段，值得我們繼續研究與發展新的破解途徑。多年來研究者一直不斷在尋求可自動攻擊密碼的新途徑，通常的做法是先嘗試破解簡單的密碼系統，經過仔細評估後，再去破解更複雜或性質不相同的密碼系統。

三、研究方法

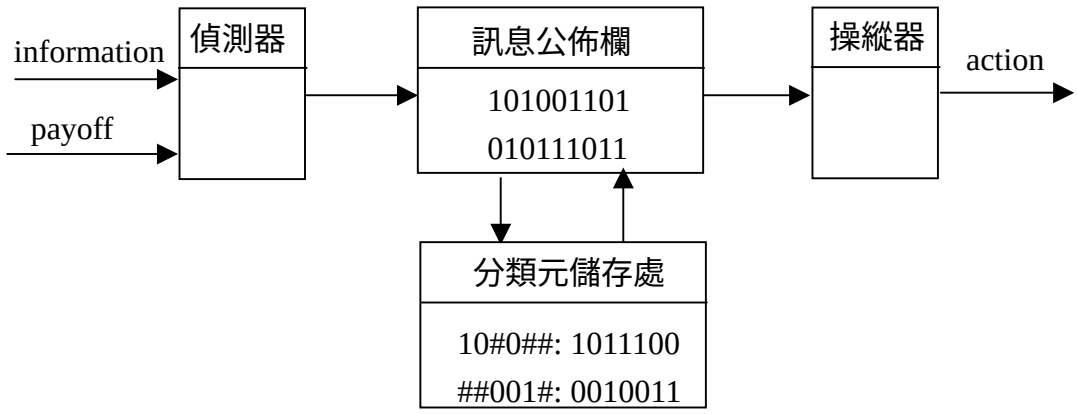
我們的初步研究顯示：基因演算法可以破解具有一定長度金匙參數的串流式密碼系統。但是對於無限長度金匙參數的串流式密碼系統目前沒有這種能力。因為這個問題涉及到密碼術所探討的理論安全 (Theoretical Security) 與實際安全 (Practical Security) 觀念。Shannon 定義的理論安全是：不管破密者截獲多少密文，其結果與沒有截獲密文直接來猜明文是一樣的。因此欲達到理論安全 (或絕對安全) 金匙參數的長度必須要大於或等於明文的長度，此即金匙參數只能使用一次，用完即丟。這種系統稱為一次活頁 (One-Time Pad)。著名的 Vernam Cipher 就是一次活頁的串流式密碼系統。雖然 Vernam Cipher 可達到理論安全，但是對於當明文很長時，很難找到與明文相等長度或更長的金匙參數。因此一次活頁的密碼系統不適合於實際的應用。由此可知一個密碼系統並非一定要滿足理論安全才是安全的系統，這必需要考慮實際安全的觀念。假設 $W(n)$ 是破解某一密碼系統所使用最佳方法需要的最少次數，而 n 是密文之長度。當 n 是無窮大時，$W(n)$ 值也變成無窮大。若某一密碼系統的 $W(n)$ 值大到無法在 ”合理時間” 內破解系統者，則此密碼系統可稱為是實際安全或計算上安全。目前有一種破解密碼的理論說法，假設 $W_h(n)$ 是某一 n 長度之密文，目前所知道最好的攻擊方法 h 來破解密碼系統所需要的計算量。當有人提出一種途徑能夠降低 $W_h(n)$ 值時，則這個密碼系統有可能會被破解。至於 $W_h(n)$ 值要降低到什麼程度，則要看實際之情況。這個理論對於我們這個研究計畫相當的重要。

於這個研究計畫中，我們是做破解區塊式密碼方面的研究。所謂區塊密碼 (Block Ciphers) 是指對一定大小的明文或密文來做加密或解密動作。這就是說使用有限長度的金匙對一文件進行編碼，然後使用這個金匙將加密後的文件給解回來。由於許多區塊式密碼是由不同人使用不同觀念獨立設計的，因此不像串流式密碼有共通之特性，其破解之困難度也稍高。根據我們歸納所知，有四種基本的區塊密碼模式：Electronic Code Book (ECB), Cipher Book Chaining (CBC), Cipher Feedback (CFB), 與 Output Feedback (OFB)。而具代表性的區塊密碼演算法有：Data Encryption Standard (DES), Triple-DES, Rivest Cipher 5 (RC5), International Data Encryption Algorithm (IDEA), Skipjack, 與 CAST 等等。其中 DES 與 IDEA 均可使用於上述的四種模式。依安全性而言，金匙長度過短很容易被攻擊，而過長則影響加密速度。DES 使用 56 位元，DES 使用 56 位

元，Skipjack 使用 80 位元，而 IDEA 使用 128 位元。我們考慮從 DES 著手，但是 DES 使用 S-Box 替換盒，使明文與密文以及金匙間的關係複雜化。而 IDEA 使用三種函數的混合，它們的原理都是利用迷惑 (Confusion) 與擴散 (Diffusion)，來使得密碼分析的工作複雜化。DES 是 56 位元的單密鑰系統，對每 64 位元的明文區塊產生 64 位元的密文區塊輸出，一共有 16 回合的重複運算，每一個運算利用 XOR 函數及 S-Box 做非線性處理。這是我們這個研究首先面臨的第一個課題，其次面臨的是 IDEA 八個回合的重複計算，加上最後一次的變換運算。我們以現有的差分攻擊法或線性攻擊法選取有相同特徵值的明文配對，藉由加密後得到的明文配對，經由特徵值去推導可能的金匙，賦予一個權重，來逐漸破解之。對於這項工作我們使用基因演算法加入了學習機制來增強的搜尋的威力，這個學習機制就是分類元系統。設計中的分類元系統主要由下列三子系統所組成的。

(a) Rule and message subsystem
(b) Reward subsystem
(c) Rule Generation subsystem

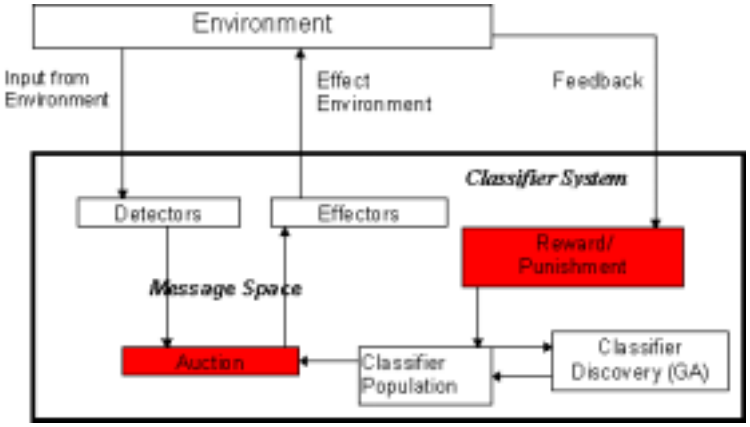
而其主要架構包括有：偵測器 (Detector)、操縱器 (Effector)、訊息公佈欄 (Message list)、與分類元儲存處 (Classifiers store) 或規則庫 (Rule base)。如下圖所示。



分類元的語法結構是：

<classifier> ::= <condition> : <message>
<condition> ::= $\{0, 1, \#\}^n$

condition 就是一般規則的 if-part，message 就是 then-part。 每一個 classifier 是密碼的金匙，開始是隨機產生的。if 部分只是個假設，有一定的可信度，因此被賦予一個數值稱之為強度，強度較強的 classifier 代表是有較高正確率的金匙，如此產生了叫價制度。每一分類元根據自己的強度來叫價，這就是創造了通貨，如同一個自由市場的經濟體系。每一分類元叫價後會削減它的強度，但它也會有機會從市場得到利潤的回饋，而增加它的強度，進而達成學習的效果。



我們扼要的說明分類元系統的學習過程，來得到正確的密碼金匙。首先偵測單元接收基因演算法的輸入資料，依據問題的定義將資料轉換成訊息再傳送給分類元系統的競標模組。競標模組是一個與告示版功能相似的模組，主要用來張貼分類元送出的訊息。張貼訊息後分類元儲存庫的分類元會做比對工作，而比對成功者可做叫價競爭，再由競標模組找出優勝者。最後這個優勝的分類元便能執行動作來影響環境，其接收動作方式是透過影響單元來影響有助於導向目標的答案。當環境受到影響後會對得勝的分類元做回饋的動作，這是透過獎勵與懲罰模組來對分類元做獎勵或懲罰，獎勵是增加分類元的強度，而懲罰是減少強度。同時，系統使用可自動判斷對環境的修正是優或劣的機制，它能長時間紀錄各分類元對環境的影響並回饋至分類元，其回饋方式也是增加或是減少分類元的強度，我們稱這樣的回饋機制為 reinforcement trainer。分類元儲存庫中會有一些很少或是從未被比對成功的分類元，我們稱之為閒置分類元，而報酬分配子系統對於這些閒置分類元有一種特別的處理方式。這是因為在叫價過程中，閒置分類元可能會從叫價得勝者獲得到部分強度。然而事實上這些閒置分類元從未被比對成功，如此可能會造成不真實的強度或造成過多閒置分類元的母代演化出更多閒置的子代，最後分類元儲存庫中會充斥著太多的閒置分類元。為了避免這種情況的發生，於是報酬分配子系統利用生命稅（life tax）來對這些閒置分類元減弱其強度，所以在每個週期沒有被比對成功的分類元其強度會逐漸的降低。值得注意的是，有些分類元可能只是在幾個週期內處於閒置狀態，生命稅不能訂的太高，否則在接連兩次的減弱動作下這些分類元便會被淘汰出局。最後會逐漸得到密碼的金匙。

四、 結果與討論

這個研究我們以基因演算法與機器學習做為主軸，目的是想知道如何讓基因演算法具有學習的能力，期盼分類元系統來協助破解複雜的密碼系統。分類元系統是一種 genetic-based machine learning，它利用一套叫價制度，來迅速找出合適的分類元。當分類元系統搭配基因演算法後，會具有發現新規則的能力，而分類元系統的運作機制是建

立在分類元以大量互相傳遞訊息與交換報酬方式來進行規則的演化。任何一個分類元必須提供報酬才能獲得所需要的訊息，然後藉由本身的反應提供轉化後的新訊息以期獲得更多的報酬。分類元所累積的報酬，就是它在系統演化中的生存適應度。我們得到的初步結果是：設計一套分類元系統的功能、架構與運作模式，利用公開拍賣市場的叫價制度做為分類元系統的學習模式，這是屬於 reinforcement learning 的一環。我們使用一種稱為 BBA 的演算法則，最初系統只有一組完全隨機產生的隨機金匙 (分類元)，然而當環境強化某些行為，經由 BBA 的作用後，這些金匙會自我組織而變成某一種有連貫關係的序列，因而產生近似真實金匙的結構，可破解一定長度的區塊密碼。這只是一個初步的結果，這個研究會再持續下去，以期得到更佳的學習途徑。

參考文獻

1. E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, Berlin, 1993.
2. L. Davis, editor, Genetic Algorithms and Simulated Annealing, Morgan Kaufmann Publishers, Los Altos, CA, 1987.
3. B. Den Boer, “Cryptanalysis of F. E. A. L.”, Advances in Cryptology EUROCRYPT ‘88 Proceedings, Springer-Verlag, 1988, pp. 275-280.
4. D. E. Denning, Cryptography and Data Security, Addison-Wesley Publishing Company, Reading Mass., 1982.
5. W. Diffie and M. E. Hellman, “New directions in Cryptography”, IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.
6. L. J. Fogel, A. J. Owens, and M. J. Walsh, Artificial Intelligence Through Simulated Evolution, Wiley Publishing, New York, 1966.
7. M. Gardner, Codes, Ciphers, and Secret Writing, Dover Publications Inc. 1972.
8. D. E. Goldberg, “Genetic Algorithms and Rule Learning in Dynamic System Control”, Proceedings of the First International Conference on Genetic Algorithms and Their Applications, pp.8-15, 1985.
9. D. E. Goldberg, “Genetic Algorithms and Rule Learning in Dynamic System Control”, Proceedings of the First International Conference on Genetic Algorithms and Their Applications, pp.8-15, 1985.
10. J. H. Holland, “Adaptation in Natural and Artificial Systems”, Ann Arbor: The University of Michigan Press, 1975.
11. J. H. Holland, “Properties of the Bucket Brigade”, Proceedings of the First International Conference on Genetic Algorithms and Their Applications, pp.1- 7, 1985.
12. T. Jakobsen, “A Fast Method for the Cryptanalysis of Substitution Ciphers”, From T.Jakobsen@mat.dtu.dk.
13. D. Kahn, The Codebreakers: The story of Secret Writing, Macmillan Co., New York, 1967.
14. D. Kosiur, Understanding Electronic Commerce, Microsoft Press, Redmond, Washington, 1997.
15. J. Koza, Genetic Programming, The MIT Press, Cambridge, MA, 1992.
16. F. T. Lin, “Genetic Algorithms for Ciphertext-Only Attack in Cryptanalysis”, Proceedings of 1995 IEEE International Conference on Systems, Man, and Cybernetics, Vancouver, Canada, pp. 650-654, 1995.
17. J. L., Massey, “An introduction to Contemporary Cryptology”, Proceedings of the IEEE, vol. 76, no. 5, pp. 533-549, 1988.

18. M. Matsui, “Linear Cryptanalysis Method for DES Cipher”, Proceeding of EUROCRYPT’93, Springer-Verlab, Berlin, pp. 386-397, 1993.
19. M. Matsui, The First Experimental Cryptanalysis of the Data Encryption Standard, Advances in Crytology, CRYPTO’94, pp.1-11, 1994.
20. M. Matsui, The First Experimental Cryptanalysis of the Data Encryption Standard, Advances in Crytology, CRYPTO’94, pp.1-11, 1994.
21. M. Mitchell, An Introduction to Genetic Algorithms, A Bradford Book, The MIT Press, Mass.,1996.
22. K. Nyberg, “Linear Approximation of Block Ciphers, Advances in Cryptology” EUROCRYPT ‘94 Proceedings, Springer-Verlag, 1995, pp. 439-444.
23. P. C. van Oorschot, M. J. Wiener, “A Known-Plaintext Attack on Two-Key Triple Encryption”, Proceedings of EUROCRYPT’90, LNCS 473, pp. 318-325, 1990.
24. T. Ritter, “Differential Cryptanalysis: A Literature Survey”, From http://www.io.com/~ritter/RES/DIFFANA.HTM
25. T. Ritter, “Linear Cryptanalysis: A Literature Survey”, From http://www.io.com/~ritter/RES/LINANA.HTM
26. B. Schneier, Applied Cryptography Second Edition, John Wiley & Sons, New York, NY, 1996.
27. B. Schneier, A Self-Study Course in Block-Cipher Cryptanalysis, Cryptologia, Vol. 24, No. 1, 2000, pp. 18-34.
28. D. R. Stinson, Cryptography Theory and Practice, CRC Press, Boca Raton, FL, 1995.
29. S. Wilson and D. E. Goldberg, “A Critical Review of Classifier Systems”, Proceedings of the Third International Conference on Genetic Algorithms, 1989, pp. 244-255.
30. Advanced Encryption Standard Development Effort, http://csrc.nist.gov/encryption/aes/aes_home.htm.
31. 張真誠，電腦密碼學與資訊安全，松崗電腦圖書公司，1989。
32. 賴溪松，韓亮，張真誠，近代密碼學及其應用，松崗電腦圖書公司，1995。