Diagnosis of Some Cipher Systems

Ali Mohammed Kadhim
Al-Salam university College
Computer Science Dept.

المستخلص

في هذا البحث يتم دراسة التشخيص لعدد من الانظمة الشفرية ،حيث تعتبر عملية التشخيص الجزء الاساسي والمهم في عملية تحليل النظام الشفري .من تلك الانظمة هي الانظمة الشفرية الكلاسيكية المصنفة الى الانظمة التعويضية والانظمة الانتقالية البسيطةمنها والمعقدة بالاضافة الى تناول الملاحظات عن بعض الانظمة الحديثة تتطلب الدراسة استخدام عدد من الطرق والمعادلات الاحصائية التي تفيد في تشخيصالنظام الشفري .

Abstract

In this research, we study the diagnosis of some cipher systems which consider Asan important part of cryptanalysis of cipher system .Some of this systems are the classical cryptosystems ,the substitution and the transposition cipher systems ,the simple one and the complex systems, as well as some modern cipher systems .we will use some statistical methods which are useful in the diagnosis of the cipher system.

Introduction:

The science concerned with data communication and storage in secure and usually secret form is cryptology which encompasses both cryptography and cryptanalysis, cryptography is the study of the principles and techniques by which information could be concealed in ciphers. Cryptanalysis is the science of recovering cryptographic secured information without knowledge of the key. The secret information known only to the legitimate users is the key, and the source information is referring to as the plaintext,whereas the transformation of the plain text under control of the key called the cipher text.

In the history of cryptology, the first period used manual classical cryptography, starting with the original of the cryptology in antiquity and continuing through world war I. Ciphers were limited to at a few pages in size. General principles for both cryptography and cryptanalysis were known,and most systems could be cryptanalyzed.

The second period ,(the mechanization of cryptography), began shortly after world war I and continues even today .The applicable technology involved either telephone and telegraph communications or calculating machines .This resulted in machine cipher (such as rotor machines) used in world war II . These machines could realize for more complex operations than were feasible manually and, more importantly, they could encrypt and decrypt faster and with less chance of error. The switch from electromechanical device to electronic ones accelerated this trend. The design of a single silicon chip implementation of the data Encryption standard (DES) and the advanced Encryption standard (AES) illustrate the progress that was made.

The third period, dating only to the last two decades of the 20^{th} century, marked themost radical change of all the dramatic extension of cryptology tothe information age, digital signatures,authentication and the public key cryptography.

Diagnosis of classical ciphers

The diagnosis is the first step process for cryptanalyzing cipher. This process is differ from cipher to another depending on the complicate of the cipher.Classical cipher system can be classified into two main types of cipher system:

- Substitution cipher
  - Monoalphabet substitution cipher (such as caser cipher).
  - Polyalphabet substitution cipher (such as periodic)
  - Polygraphic (digraph) cipher (such as play fair).
- Transposition cipher:
  - Simple transposition cipher.
  -Double transposition cipher.

To analyze the cipher you should know the process of enciphering, deciphering and lastly finding the secret key which is used to get the plain text of the cipher .There are four important processing can be used for diagnosis of classical cipher system:

1. Frequency Distribution :

This process the basic tool for breaking most classical simple ciphers such as (i.e.Caesar cipher, monoalphabet cipher).In any sample of plain text some letters of the alphabet appear more frequently than others, and the most common letter in English alphabet is the letter “E”, and the digraph “TH” is the most pair of letters in English. By comparing the statistical frequency analysis of the ciphertext letters with the known distribution of the letters in the plaintext (as shown in fig.1) can be easily broken the cipher system and get the plaintext .

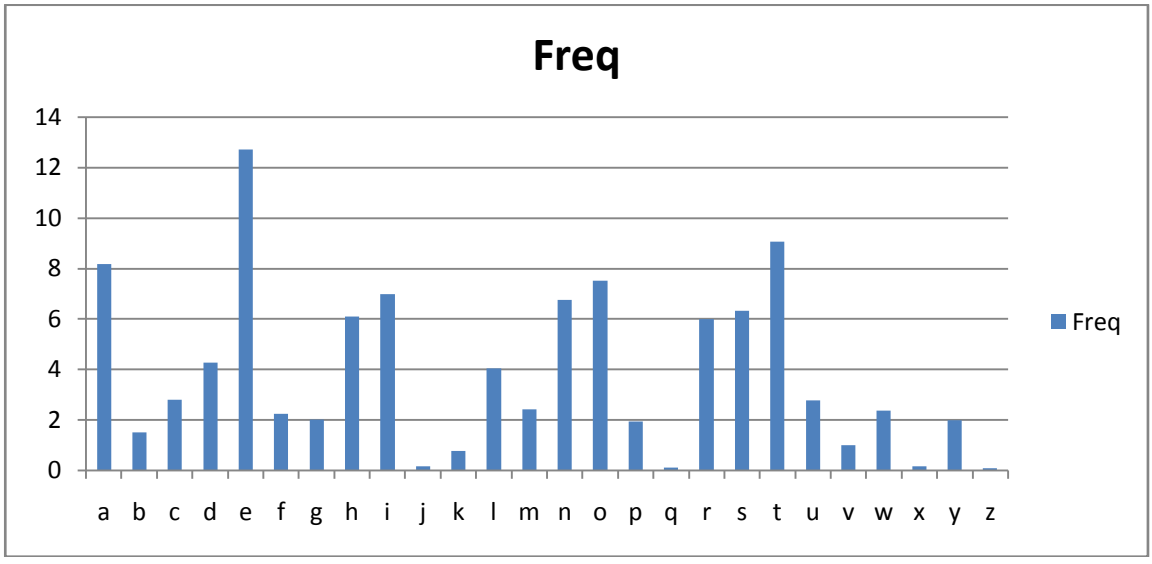

Fig.1
Frequency Distribution of Letters in English Language Text

2. Index of coincidence :

This process in useful in cryptanalysis substation cipher system by coincidence counting can test the cipher is simple substitution (monoalphabet) which the value of (I.C) is the same of plaintext

$$IC = \frac{\sum_{i=1}^{C} n_i(n_i - 1)}{N(N-1)} \quad \dots(1)$$

Where N in the length the text, n_i frequency of alphabet letters in English language(IC=0.067) for plaintext and for random (IC=1/26 =0.0385).IC also (Called Kappa test). This value isdifferent withanotherlanguage. Coincidence Counting can help determine when two texts using the same alphabet (or in the ploy alphabet), such text will be distinctly higher than Coincidence Count for texts using different alphabet:

$$IC = \frac{\sum_{J=1}^{C} f_{a_j} \cdot f_{b_j}}{N_a . N_b} \dots(2)$$

Where N_a, N_b is the length of texts.f_a,f_b is the frequency of text a and b respectively.

3. Repetition (Repeated string):

In the polyalphabet cipher (periodic) often used keyword which represents number of alphabets used to encrypt the cipher.In this method, the advantage of the repeated word in plaintext which can be encrypted using the same key letters leading to repeated string (repetition) in the ciphertext. This repetition easily seen in the ciphertext of polyalphabet cipher. The method of repetition also called Kasiski test will be effective by finding the distances between all repeated groups. All these factors of the distance are possible keyword lengths, by taking the intersection of these sets of distances or by using greatest common divisor (GCD),then the cryptanalysis of the cipher will be much easier.

4. In-Depth

This Process depends on certain case,when two or more messages are sending with the same key then this process is an insecure.These messages are said to be “in-depth” which have the same indicator concerning the key generator initial settings for the message. Knowledge of a key of course allows the cryptanalyst to read other messages encrypted with the same key and also to diagnose the cipher system. Many of ciphers such as a ploy alphabet cipher with long key (a periodic) which used the key length along the message can be cryptanalyzed using in depth process for some messages with the same key.

Diagnosis of modern ciphers

The Diagnosis in classical ciphers depends on the security of the process of encryption/decryption and the secret key,whereas in the modern ciphers depends only on the secret of the key.The most process which used in the Diagnosis of the classical ciphers cannot be useful in the modern ciphers except the in depth process of some systems.

The basic point which is taken in account in modern ciphers that the algorithm of cipher system is known, i.e. enemy knows the systems (Shannon's maxim). So, the most important thing in the Diagnosis of modern ciphers is finding a weakness in the cipher that can be exploited with a complexity less than brute force.

The modern ciphers are classified into symmetric and asymmetric ciphers as shown below:

- **Symmetric ciphers :**

Symmetric ciphers are ciphers that rely on using one secret key for both encryption of plaintext and decryption of ciphertext. Symmetric ciphers can use either stream ciphers or block ciphers.

-Stream cipher: encrypt a message bit by bit at a time.

-Block cipher: take a number of bitsand encrypt them as a single unit (block).And these blocks for example (64 bits) have been commonly used, such as in DES.

An attacks can be classified based on what type of information that been available to the attacker. There are six general types of cryptanalytic attacks. Each of them assumes that the cryptanalyst has complete knowledge of the encryption algorithm used:

1-Ciphertext only attack: The cryptanalyst has the cipher text of several messages, all of which have been encrypted using the same encryption algorithm, to recover the plaintext of many messages.

2-known plaintext attack: The cryptanalyst has access not only to the ciphertext of several messages, but also to the plaintext of those messages, to deduce the key or keys used to encrypt the massages.

3-chosen plaintext attack: The cryptanalyst not only has access to the ciphertext and associated plaintext for several messages, but he also chooses the plaintext that gets encrypted. This is more powerful than a known-plaintext attack, because he can choose specific plaintext blocks to encrypt. The job in to deduce the key or keys used to encrypt the message.

4-Adaptive chosen plaintext attack: This is a special case of a chosen plaintext attack. Not only can the cryptanalyst choose the plaintext that is encrypted, but he can also modify his choice based on the results of pervious encryption. He can choose a smaller block of plaintext and then choose another based on the results of the first, and so forth.

5-Chosen ciphertext attack: the cryptanalyst can choose different ciphertexts to be decrypted and has access to the decrypted plaintext. (This attack is primarily applicable to public key algorithms.)

6-Related key attack: Like a chosen plaintext, except the attacker can obtain ciphertexts encrypted under two different keys. The keys are unknown, but the relationship between them in known, for example, two keys that differ in the one bit.

Many of symmetric ciphers was shown to be breakable using some attacks that cryptanalysis the symmetric ciphers such as Differential cryptanalysis linear cryptanalysis , integral cryptanalysis , sandwich attack , Boomerang attack, slide attack, by using the weakness in the ciphers as well as the brute force attack.

- **Asymmetric ciphers (public key cryptography)**

An asymmetric cipher (or public keys cryptography) is cryptography that relies on using two keys, one private and One public. Thiscipher invariably relies on 'hard' mathematical problems as the basic of their security, so an obvious point of attack is to develop methods for solving problem.

The algorithms (such as RSA) used for public key cryptography are based on mathematical relationships that presumably have no efficient solution .Although it is computationally easy for the intended recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key , but it is extremely difficult for anyone to derive the privet key, based only on their knowledge of the public key. Algorithms also allow the authenticity of a massage to be checked by creating a digital signature' of the message using the privet key, which can be verified by using the public key .

Some asymmetric ciphers can be proven secure on the basis of the presumed difficultly of a mathematical problem, such as factoring the product of two large primes or computing discrete logarithms. In a secure system the privet key should not be deductible from the public key which can be published.

There are many examples of asymmetric key algorithms such as Markel- Hellman knapsack, RSA, Elgamal, paillier, elliptic curve cryptosystem, etc. All public key algorithms are susceptible to a “brute-force attack “.Such attacks are impractical if the amount of computation needed to succeed is out of reach of all potential attackers. But other algorithms may have much lower work factors making resistance to a brute-force attack irrelevant.

These insecurities can be generally avoided by choosing key sizes large enough that the best known attack algorithm would take so long to have reasonable chance at successfully and it is not worth any adversary's time and money to proceed with the attack.

Major weaknesses have been found for several formerly promising asymmetric key algorithms. The “knapsack packing algorithm” was recently found to be insecure after the development of new attack .Recently , some attacks based on careful measurements of the exact amount of time it takes known hardware to encrypt plaintext have been used to simplify the search for likely decryption keys.

So, a great deal of active research is currently under way to both discover and to protect against new attack algorithms.

Conclusion

Most systems of classical cipher can be diagnosed andcryptanalyzed in recent days (except the one time pad cipher). Studies for finding weaknesses of many modern ciphers with symmetric key algorithms are shown to be breakable using different attacks which Stated before. That means ,the security of two key cryptography (public key) cryptography depends on well-defined mathematical equations in a way that single key cryptography (symmetric key algorithm) generally doesnot, conversely, it equates cryptanalysis with mathematical research in a typical way.

References

[1] David, Kahn," the Code breakers”, rev.ed., (Newyork): simon and Schuster, 1996.

[2] Encyclopedia, Britannica, Feb.2013, http://www.britannica.com/EB checked/cryptology.

[3] Goldwasser**,** Shafi & Bellare,Mihir ,"lecture Notes on cryptography", MIT Laboratory of Comp.sci ,Aug 2001.

[4] Junod, Pascal & Canteaut ,Anne ,"Advanced linear cryptanalysis of block and stream ciphers " ,IOS press ,(2011).

[5] Piper ,F.& Beaker ,H ,"Cipher system " , Aegen park press ,1982 .

[6] Schneier, Bruce, "Applied cryptography ", Second Edition, John wiley &Sons, 1996.

[7] Schneier, Bruce, "A self-study Course in Block–cipher cryptanalysis”, cryptologia 24 (1), (Jan 2000), PP.18-34.

[8] Swenson, Christopher, "Modern cryptanalysis: techniques for advanced Code Breaking ", John wiley & Sons, 2008.

[9] Talbot ,John & Welsh , Dominic , " Complexity and cryptography " , Cambridge univ. press ,2006 .

[10] Wikipedia, The free encyclopedia: cryptanalysis, Feb. 2013,Http://en. Wikipedia.org /wiki/ cryptanalysis.