Enhancing Information Security through Cryptography

Pratik Dabhi
Student, MCA Programme,
Institute of Technology
Nirma University of Science & Technology,
Ahmedabad, Gujarat, India.
Email : pratik04dabhi@yahoo.co.in

Dr. Kuntalkumar P. Patel
Lecturer, MCA Programme,
Institute of Technology,
Nirma University of Science & Technology,
Ahmedabad, Gujarat, India.
Email: kuntal_78@yahoo.com

Abstract

The success of today's business in competitive world depends on how successfully and effectively they are using networked based information system. Also, use of the Internet becomes more central among many of the networked based information system in governmental agencies, corporate businesses and among individuals. Also, due to the rapid growth of digital communication and electronic data exchange, data and information security becomes a essential issue in businesses and administration. In this paper we had tried to explain how some of the cryptographic techniques can be useful to enhance the information security in networked based information system.

Keywords: Cryptography, Encryption, Symmetric key, Asymmetric key.

1. Introduction

The requirement of information security within an organization is important today as many of the organizations are using computer based information system. Such computerized systems are networked based. The need of information security is even more sensitive for system that can be accessed over public telephone network, data network, or the Internet.

Also the information security becomes crucial with the introduction of distributed system and the use of network and communication facilities for carrying data between end user and computer, between computer and computer. Network security measures are needed to protect data during their transmission.

To provide security on the information being transferred over the network we can use various cryptographic techniques or algorithms. "Cryptography is the study of mathematical techniques related to aspects of information security, such as confidentially or privacy, data integrity and entity authentication."[1] Cryptography is not only means of providing information security, but rather one set of techniques.

There are several aspects of related to information security. They are security service, security mechanism, and security attack. Security service means a service that enhances the security of the data processing system and information transfers of an organization. A security mechanism mean that is designed to detect, prevent, or recover from a security attacks. Security attack means any action that compromises the security of information owned by an organization.[2]

Encryption means the process of converting from plaintext to cipher text. A key is a piece of information, usually a number that allows a receiver to decode messages sent to him or her. The major categories of cryptographic techniques are: classical techniques, modern techniques, and public-key encryption.[3] In Classical techniques there are substitution techniques and transposition techniques. Caesar cipher, Monoalphabetic cipher and Polyalphabetic ciphers are the examples of classical techniques. In Modern techniques there are block cipher, stream cipher and DES algorithm. RSA algorithm is the widely used Public Key technology.

2. Categories of cryptographic systems

Cryptographic systems are characterized along three independent dimensions:

I. The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged.

II. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

III. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

The two basic building blocks of all encryption techniques are substitution and transposition. We examine these in the next two sections. Finally, we discuss a system that combines both substitution and transposition.

3. Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

W A R F A R E

W+1 A+1 R+1 F+1 A+1 R+1 E+1

X B S G B S F

F(X)=X+1

3.1 Caesar Cipher

Caesar Cipher is one of the earliest known substitution ciphers. It was developed by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example

Plaintext:the quick brown fox jumps over the lazy dog

Ciphertext:WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

Note that the alphabet is wrapped around, so that the latter following Z is A. We can define the transformation by listing all possibilities, as follow:

Plain: a b c d e f g h I j k l m n o p q r s t u v w x y z

Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

If we assign a numeric equivalent to each letter, then encryption of a letter x by a shift n can be described mathematically as,

E(X) = (X+n) mod 26

Decryption is performed similarly,

D(X) = (X-n) mod 26

Value of n *should* be between 1 and 25

Advantages of Caesar Cipher

Easy to understand and implement. Easy to program to implement encryption and decryption algorithms.

Disadvantages of Caesar Cipher

Encryption and decryption algorithms are known. Brute Force cryptanalysis is easily performed by simply trying out all possible 25 key combinations. Thus Caesar cipher is not a secure algorithm. Because of disadvantages in Caesar cipher Monoalphabetic ciphers are used.

3.2 Monoalphabetic Ciphers

With only 25 keys Caesar cipher is easy to break and thus not secure. Monoalphabetic ciphers increases the key space by following arbitrary substitution. From Caesar cipher we have.

Plain: a b c d e f g h I j k l m n o p q r s t u v w x y z

Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Here the cipher line can be any permutation of 26 alphabetic characters. It is called monoalphabetic substitution cipher because a single cipher alphabet is used per message.

Advantage of Monoalphabetic Ciphers

Comparatively more secure then Caesar cipher. It also has 26! Number of keys far more than Caesar ciphers.

3.3 PlayFair

The Playfair cipher was developed by Charles Wheatstone, but his good friend Lord Lyon Playfair, first Baron of Playfair, was the one to promote it for use, and hence it gained his name. This cipher is more complicated then the above, and it gives a much higher level of security than simple substitution ciphers. Instead of having a key relating each letter to another letter as in substitution ciphers, the Playfair cipher uses a table that encrypts pairs of letters at a time. These pairs of letters are called digraphs. For this cipher, one first constructs the key table. A very easy example would be

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

with the letters listed in order. Note that I left out J this is necessary as there are 26 letters but only 25 spaces are available thus I or J can be used at the place I/J.

Now in order to encipher a message, we use the following rules. First take the first two letters of your message and look at the table.

- If your two letters both appear in the same row, then use the letters immediately to their right. AB becomes BC, GI becomes HK, MP bcomes NL. Note that if there is no letter to the right, use the first letter in that row.
- If your two letters both appear in the same column, then use the letters immediately below them. BM bcomes GR, OY becomes TD, and so on. Again, if there is no letter below, use the first letter in that column.
- If your two letters do not appear either in the same row or the same column, then you treat your two letters as the cornders of a smaller square and replace them with the letters in the other two corners. For example, if your letters were GT, you would have a sub-square that is

  G H I
  M N O
  R S T

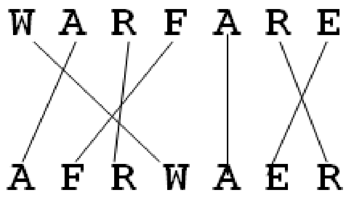
  The letters GT would be replace with IR, the other two corners of the square. Note well, it is important that the first letter in the encrypted digraph be the letter in the same ROW as the first letter in the plain text. So while the letters GT encode to IR, the letters TG encode to RI.
- If you have a double letter, such as LL, replace the second letter with an X and then encode as normal. It does not have to be an X, but whatever letter you choose to replace doubles, make sure both you and whomever you're sending the message to agree on it. So, LL would become LX and then encode to NV in this example.
- To decode, simply use these rules in reverse. Rule 3 works backward just the same as it does forward. In rule one, to decode just use the two letters to the left of the two you're decoding if they appear in the same row, and likewise use the two above if they appear in the same column.

Advantages of Playfair

Playfair enciphers two letters at a time; therefore it is not possible for one letter statistical analysis to break it. Furthermore, the relative frequencies of individual letters exhibit a much greater range than that of digrams, making frequency analysis much more difficult.

4. Transposition Techniques

The techniques presented so far involve the substitution of a ciphertext symbol for a plaintext symbol. The other kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is known as a transposition cipher.



F(X) = RAND(X)

4.1. Rail Fence

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, if we have 2 "rails" and a message of 'HELLO FRIENDS’, then write plain text as

```
H   L   O   R   E   D
  E   L   F   I   N   S
```

The encrypted message is

HLOREDELFINS

This sort of thing would be more difficult to interpret by the attacker.

Disadvantage of Rail Fence

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. If the attacker knows that the message is encrypted using the rail fence cipher then it can be deciphered by brute force because the letters break into rows according to certain fixed patterns based on the number of rows in the key. Thus rail fence is not a secure cipher. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily interpreted.

5. Conclusion

Cryptography has evolved as an important area of research to enhance the information security over communications lines. It provides us the simple substitution ciphers based algorithms as cheaper and faster solutions. On other hand it also provides complex cryptographic algorithms for very critical information. It is now upto the designer of the information system, that which algorithm he wants to implement. According to the criticalness of the information, cryptographic algorithms can be used for enhancing our network based applications. At the same time we have to take care that only cryptographic techniques cannot provide complete security to our information. It should be used along with other tools which can guard us against other attacks - like network intrusion, viruses spy-ware and other malicious codes.

5. References

[1] http://dasan.sejong.ac.kr/~chlim/pub/ Lect1-intro.pdf

[2] William Stallings, “Cryptography and Network Security Principles and Practices” Prentice hall of India, New Delhi.

[3] James Stanger, Ph.D., Patrick Lane, Tim Crothers “CIW™ Security Professional Study Guide” Sybex.