Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study of Cryptography and its Techniques

Ajit singh, Madhu Pahal, Annu Malik
School Of Engineering And Sciences,
Bhagat Phool Singh Mahila Vishwavidyalaya
Sonipat (Haryana) India

Abstract – In this paper, we have given an overview about cryptography and its various techniques which are used for converting a readable text into non readable text and thus makes data more secure. To increase security we use such type of techniques and study of this is called cryptography.

Keywords – Cryptography, substitution technique, transposition technique, cipher text, Plain Text, Caesar cipher

1. Introduction

Cryptography is the art and science of encoding messages from readable format to non readable format. In terms of data and telecommunications, cryptography plays an important role when we communicate over any untrusted medium like internet. While communicating over the network some specific security requirements are needed such as:

- Authentication : it proves the identity of the person to whom we are communicating or we can say that it provides the host to host authentication over the internet.
- Confidentiality : it ensures that no one can read the message other than sender.
- Integrity : it assures that message has not altered in any way from the original during arrival from sender to receiver.
- Non repudiation : it is a mechanism which proves that sender really sent this message.

So we can now say that cryptograhy not only protects data from theft but it can also be used for authentication of user. In all cases, initial data is plain text and data after encryption is known as cipher text which in turn converted back to plain text for reading the plain text.

1. cryptography

- Cryptography is the art and science of achieving security by converting readable message into non readable format.
- Cryptanalysis is the technique of converting non readable form without knowing how they were converted from readable to non readable form.

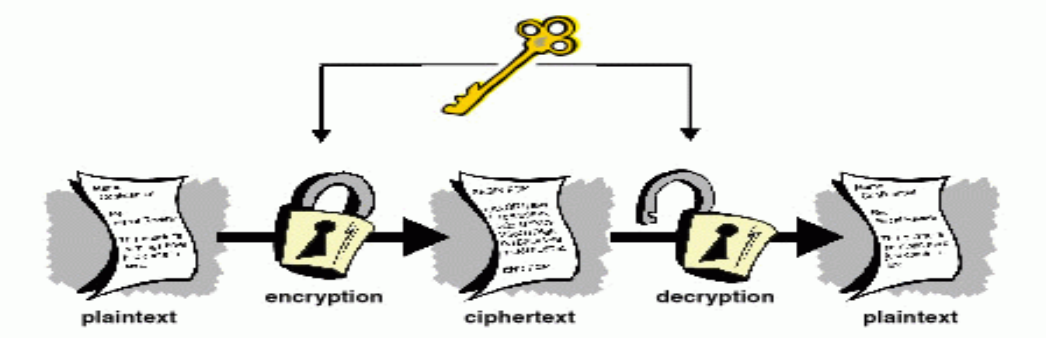


Fig. process of cryptography and cryptanalysis

- Cryptology is the combination of cryptography and cryptanalysis.

In early days, we perform cryptography manually that is if we have to make any make any message secure then we have to perform all task manually it takes lot of time but now computer perform these cryptographic functions and it is more secure and performs very fast.

Basic terms used in network security are:

- **Plain text :** any human language in which we communicate is plain text. A message in plain text is understood by everybody if they know that language. For example, when we don't want to hide anything from the persons available near us we use plain text to exchange information. Suppose that I say hello to my friend and anybody who is listening to our conversation he can easily come to know that I am greeting my friend because I am not talking something important. If someone know that language that I am using he can get the message with out problem.

We also use plain text during electronic communication. For example, suppose some one is sending an email to his friend and message in the mail is not that much important then he can use plain text in English language or in any other language.

Example of plain text

Hi annu
Hope you are doing fine. We are planning for get together this weekend. Please let me know if it is ok with you.
Regards
Madhu

Plain text is a message that can be understood by the sender, the recipient and also by anyone else who is able to read the message.

- ***Cipher text:*** But if we want that nobody other than sender and receiver gets an access to that message we convert the format of message into non readable format using any scheme available to us.

Example, suppose given plain text is CIPHER and we have to encrypt it.
Plain Text : CIPHER
Cipher text: FLSKHU
This is the conversion of plain text into cipher text using alphabet replacement scheme.
When a plain text message is converted into non readable form using any scheme available to us, the resulting message is called as cipher text.

2. *Techniques*

Primary ways with the help of which a plain text messages converted into cipher text are as follows:

a) Substitution
b) Transposition

Substitution technique : in substitution technique we replace the alphabet of plain text with any other alphabet that is we substitute the character of plain text with other characters.

Some of the schemes available in substitution technique are :

i) ***Caesar cipher*** : this scheme was first proposed by Julius caesar that is why it is known as caesar cipher. It was the first example of substitution cipher. In this plain text messages are replaced by other characters.
For example, replace each alphabet with the alphabet four alphabet up the order.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
YZABCDEFGHIJKLMNOPQRSTUVWX

Example : plain text : CAESAR
Cipher text: ZBXPBO

Mathematically, it can be represented as ,
For encryption C= E(2,p)=(p-2)mod26
For decryption P =D(2,c)=(p+2)mod26

It is not that much secure because cryptanalyst can break the cipher code if he know any point from following :

- There are only 25 possibilities to try.
- Language of plain text was English.
- Substitution technique was used to derive cipher text from plain text.

3. Limitation

the main limitation of caesar cipher is predictability. If once we come to know about single replacement in plain text that weather it is m possibilities up or down . in this cryptanalyst has to try maximum 25 possible attacks and he can get success for sure.

SOLUTION*:* to overcome the problem of caesar cipher we use mono alphabetic technique or some other.
ii) mono alphabetic : In mono alphabetic we do n use a uniform scheme for all plain text instead we use different scheme for each alphabet we use random substitution . In this we can replace each A with any other alphabet B to Z except A, each B with A, C to z and so on. We can say that there is no relationship between replacement of A and replacement of B. for cryptanalyst, mono alphabetic ciphers is a difficult problem because it is very difficult to crack large number of possible permutations and combinations.

iii) Homophonic substitution cipher : As in mono alphabetic cipher we replace each alphabet independently without any relationship with previous replacement. It is also similar to mono alphabetic up to some extent . The main difference between two techniques is that in this we choose a set which consists of few alphabets for each alphabet in plain text. For

example, suppose set choosen for A is { C,F,I,X} then according to user's choice A can be replaced by any of these four alphabet where as in homophonic we replace A with B to Z.

example : plain text : text
cipher text : kofa
t = {k,l,m,a}
e={b,m,o,p}
x={p,d,y,f}

iv) Polygram substitution cipher : rather than replacing one alphabet from plain text with one cipher text alphabet at a time, we replace a block of alphabets in plygram substitution at one time.
Example, PLAIN TEXT CIPHER TEXT

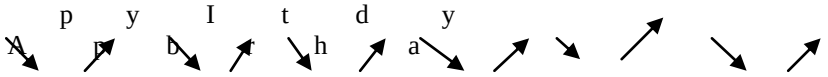
YOU QUP
YOUR DFKN

In this example first three alphabet of both blocks are same but we encrypt block by block that is why result of both plain text is different because we encrypt by taking one block at a time.
It does not work character by character.

Transposition technique : as we have seen in substitution technique we replace each plain text with new alphabets in cipher text but in transposition, we don't not replace one alphabet with another alphabet. We just rearrange the positions of plain text and get the cipher text.
Techniques used in transposition :

i) ***Rail fence technique:*** it is a type of transposition technique which rotates the position of plain text message.

Example, suppose that we have a plain text message HAPPY BIRTHDAY we can convert this text in cipher text using rail fence as



Cipher text : HPYITDYAPBRHA
Algorithm :

- Arrange the plain text message in sequence of diagonals as shown above .
- Read the text row by row and write it in sequence and thus we will get the cipher text.

ii) ***Simple columnar transposition technique*** : it rotates the position of alphabets in plain text and then find out the cipher text.

Algorithm :

a) write the plain text message in a rectangle of pre defined size.
b) Read the message column by column in random order of columns.
c) The message obtained by doing so is the cipher text.

Example,

suppose plain text that we have to encrypt is HAPPY BIRTHDAY.

We can encrypt this as follows:

a) Consider a rectangle with four columns and write the plain text row by row.

Col1	col2	col3	col4
H	a	p	p
Y	b	I	r
T	h	d	a
y			

b) Now decide the order of columns as random order. Suppose order decided is 3,1,4,2 and read the text in this order.
c) Resulting text is the cipher text that is in this example cipher text is PIDHYTYPRAABH

iii) ***Simple columnar transposition technique with multiple rounds :*** to improve the simple columnar transposition technique, we increase the complexity of this technique by implementing the same steps twice or thrice or depending upon the security of message.

Algorithm :

a) write the message row by row in a rectangle of pre defined size.

b) Read the message column by column in random order of columns.
c) The message thus obtained is cipher text.
d) Repeat steps a to c as many times as needed.

Example, consider the same PLAIN TEXT as above HAPPY BIRTHDAY.

a) Consider a rectangle with four columns and write the plain text row by row.

Col1	col2	col3	col4
h	a	p	p
y	b	i	r
t	h	d	a
y			

b) Now decide the order of columns as random order. Suppose order decided is 3,1,4,2 and read the text in this order.
c) Resulting text is the cipher text that is in this example cipher text is PIDHYTYPRAABH
d)Perform step a to c once more.

Col1	col2	col3	col4
p	i	d	h
y	t	y	p
r	a	a	b
h			

d) Assume the order of column and read in that order. Suppose order is 3,1,4,2
e) Resulting text by doing so is DYAPYRHHPBITA
f) If you want iterations for more security and complexity then continue with the same steps as many times as needed.

4. Conclusion

Security in the internet is improving day by day as use of internet is increasing for every purpose. So to protect information many technologies are now available so that other than sender and receiver can not get access to the information. Cryptography is one among those technology . other technologies are also available like use of symmetric and asymmetric key pair. But user leaves key lying around, choose easily remembered keys and don't change the keys for years. The disadvantage of this is that if some how attacker achieve key then he can easily get access to the data but use of cryptography is better as comparison to the use of key for security. The complexity of cryptography effectively puts it outside the understanding of most people and make it more secure.

Refernces

[1] http://www.garykessler.net/library/crypto.html
[2] www.cl.cam.ac.uk/~jac22/books/mm/book/node352.html
[3] http://www.google.co.in/imgres
[4] http://books.google.co.in

