International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Cryptographic Techniques in Information Security

Ravi Kumar Choubey, Ahtisham Hashmi
School of Computing Science and Engineering, Galgotias University, Greater Noida, India

ABSTRACT

This paper focuses on the role of cryptography in the information security system and discussed some of the techniques which are used in cryptography. Earlier, Cryptography mainly is used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the uses are limited. In the modern days, the Cryptography be expanded a lot in the area of communication, securing e-commerce etc. Cryptography is used to transmit the message confidentially where no any trouble can happen between transmission.

Keywords: Cryptography, security, cryptanalysis, cryptosystem, cipher.

I. INTRODUCTION

Cryptography is a science by which we can design strong encryption by applying complex mathematics. Attaining strong encryption means data hiding by which we can hide the secret data which can't be permitted by any third person for decryption. So, The art of cryptography also considered as an art of writing where the transfer of secret data can be safely reached to the recipient.

This Four Terms which gives the security service by Cryptography are - Confidentiality, Data Integrity, Authentication, and Non-repudiation.

- ✓ **Confidentiality** - security service keeps the information from an unauthorized person which gives privacy and secrecy.
- ✓ **Data Integrity** - security service that deals with identifying any alteration of data.The data gets modified by an unauthorized person intentionally or accidentally.
- ✓ **Authentication** - security service for data confirms at the receiver which are send by an identified or verified sender.
- ✓ **Non-repudiation** - security service that ensures that an entity cannot refuse ownership for a previous commitment or an action. For example- The order is placed electronically , user can't be denied the purchase order if Non-repudiation was enabled [1].

As early days (5000 yrs ago) when the wars being the opportunity to becomes supremacy between different royals, So Cryptography evolved between them by sending the secret information to the recipient for winning battles.

The first cryptography technique is applied "hieroglyph" in some 4000 yrs ago where an Egyptians sent the message for communication by written in hieroglyph. This Secret code can be reached to transcriber which decrypt this message and transmit to the kings. One such hieroglyph is shown below :

Figure 1. Hieroglyph (First techniques of Cryptography).

After some 500-600 BC when cryptography becomes popular So, we use three method for encrypt information: Substitution, Transposition and Codes. The Different technique which we used to encrypt information know as Traditional Ciphers.

II. TECHNIQUES USED IN CRYPTOGRAPHY

Mono-Alphabetic Cipher

One of the earliest encryption methods is shift cipher. A cipher is a step method or algorithm, that converts plaintext to ciphertext (encryption) or ciphertext to plaintext (decryption). Caesar's shift cipher is known as mono-alphabetic substitution shift cipher as shown in the figure [2].

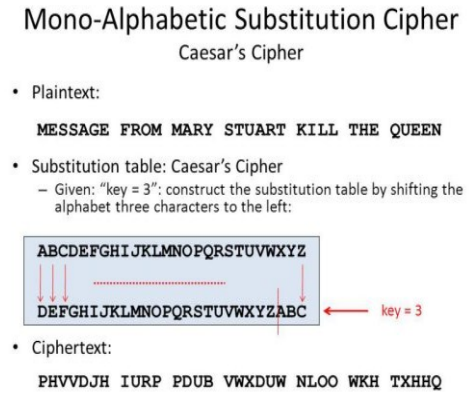


Figure 2. Mono-Alphabetic Substitution Cipher.

Key means replacing alphabet to other alphabet for some secret rule. This rule becomes called a **key.** The name cipher is terrorized, but it is simple to understand.

Mono-alphabetic means One cipher alphabet. Traditionally Each character in ciphertext decrypted in uppercase- is substitution in one character in plaintext which was written in lowercase. Shift cipher is named because we shifted start character in cipher alphabet for some number of letters into the plaintext(without spaces), after shifted it becomes the ciphertext.This type of technique is easy to use and easy to break. The breaking of encrypted information known to be the Cryptanalysis. Also, Cryptography and Cryptanalysis are the part of Cryptology (The study of Cryptosystem).

Cryptography concern about the design of Cryptosystem while Cryptanalysis study for the Breaking of Cryptosystem [3].

Poly Alphabetic Cipher

In mono-alphabetic , for a given key the plain alphabet is fixed through out the encryption or decryption process means if 'A' is substituted by 'D', So All the Occurrence of A's in plain alphabet is substituted by D but In Poly-alphabetic, substituted alphabet in plaintext may be different in different places during encryption or decryption process.

There are Two Examples of Poly-Alphabetic Cipher Playfair and Vigenere Cipher

Playfair Cipher

In this type of Ploy-Alphabetic, pairs of Alphabet are encrypted as an alternatively a single alphabet is encrypted in Mono-alphabetic substitution cipher.

In Playfair, initially, A key table is created where it has 5*5 grid alphabet is put in a sequential manner. Also at the starting, a key alphabet is kept for encrypted plaintext instead of this all alphabet is put in sequentially. But there is 25 alphabet (instead of

26) kept in grid So, usually, **J** is omitted in that table. If the plaintext contains **J**, then it is replaced by **I.**
Here, The Example to explain Playfair Cipher,

Suppose The key which sender can be used is 'HACKER' instead of this all alphabet is put in a sequential manner as it explained in above.

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

Steps to Encrypt:
1. The message which we used to encrypt, divides in pairs . If it is ODD pair So, Z can be added in the last alphabet.

Ex- message is"**RAVIHASHMIADILRIS**".
It will be written as:-

Ra Vi Ha Sh Mi Ad Il Ri Sz

2. The rules of encryption are:
A. if the pairs are present in same column take the alphabet below each one(goes top to bottom).

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

'VI' are in the same column So, alphabet take below is 'HP', as it is all can be followed.
B. if the pairs are present in same rows take the alphabet right of them to replace.

H	**A**	**C**	**K**	**E**

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

As we highlighted shown in table above-
The pairs are 'HA' can be replaced by 'AC', as it is all can be performed.

C. If neither of the preceding rules is true So, the last rule must be true is if the pairs can be present at the opposite corner, the pairs are replaced by next opposite corner on the same row [4].

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

The pairs are 'SH' So, it is replaced by 'PC', same followed to all of them.
Finally, the result of encrypted message is -

Bh Hpac Pc Il Bc Lm Ip Xu
For Decrypted message at the receiver end, this process can be performed in reverse order by taking the Key is "HACKER".
This Playfair gives more security than Mono-alphabetic method because, In Mono-alphabetic, Cryptanalysis used 26 alphabets to decode the encrypted plaintext but in Playfair, It is 25*25= 625 possibilities can be performed by Cryptanalysis to decode which is usually a difficult process.

Vignere Cipher
In this Type of Poly-alphabetic, Caesar shift is modified of their shifting in Vigenere Cipher. Also Key makes the important task for encrypted plaintext in all Cryptography So, Obviously Here is too it applied.

As we know the Plaintext can be written in Lowercase and the Ciphertext can be written in Uppercase So, As it, we can create 27*27 grid alphabet where rows of Lowercase alphabet and columns of the Uppercase Alphabet. Each subsequent row represents a cipher alphabet. For each alphabet, the first character is shifted one position farther than the previous one. In some table, the letter replaced by numbers corresponds letter's position in the standard alphabet [5]. For Example- 'A' is replaced with "1" , 'C' is replaced with "3", etc.

	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

As this above Vigenere table shows different rows,columns and shifting process also.

Let the Key by which the Sender sends a message which is going to Receiver in encrypted form are "HACKER" and the message are "attack on mumbai". So, the key and the message represents are:

KEY	H	A	C	K	E	R	H	A	C	K	E	R	H	A
MESSAGE	a	t	t	a	c	k	o	n	m	u	m	b	a	i

As it we can match that representation on the table by first see the first character of a message(Plaintext) is **'a'** which are of Key **'H'** So, represent in a column and **'H'** row of the letter are **'I'.** Hence by this, the encrypted message which is reached on receiver end are:

"Iuwlhcwopfrtij".

The Repeated alphabet of plaintext also is encrypted by different alphabet. So, It is more difficult to break by Cryptanalysis of shifting make it difficulty critically Harder.

Like as: **"IUWLHCWOPFRTIJ"**

Types of Vignere Cipher

1. Vernam Cipher- The key can be the same length as a message . It is more secure than the typically Vigenere cipher.
2. One-Time Pad- Vigenere cipher becomes a Cryptosystem with perfect secrecy.

1. The key can be the same length as a message.
2. The key can be a randomly generated string.
3. The key is used only once [6].

Security of One-Time Pad

It is more secure than shift cipher because in shift cipher the Cryptanalysis used the possible keys to break encrypted message is only 1to 26 alphabet but in One-Time Pad, if the key is 'HACKER' So, it's length is "6" that is 26^6 = 308915776 keys can be possible to check that are impossible to break.

III. TRANSPOSITION CIPHER

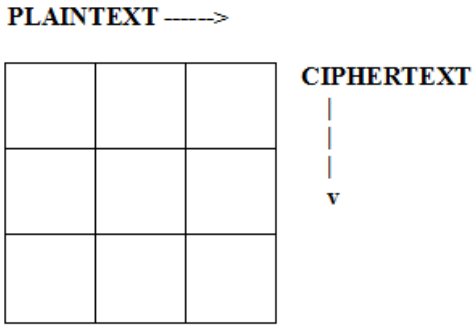
It is another type of technique for encryption is Transposition where rearrangement or reordering of Plaintext message can happen to obtain more difficult to break and provide better security as an above form.

It has mainly Two Important Types of Transposition Cipher are-

1. Simple Columnar Transposition
2. Rail Fence Transposition

1. Simple Columnar Transposition

In this Type of Transposition have some format of written where Plaintext are written Horizontally and Ciphertext are read Vertically as we mention below:-



As we given an Example:

Let us Suppose The Plaintext which the Sender wants to send is:-

"Attack To Taj Mahal On Five Dec Eighteen"

Now we follow the written format of Plaintext :-

A	T	T	A	C
K	T	O	T	A
J	M	A	H	A
L	O	N	F	I
V	E	D	E	C
E	I	G	H	T
E	E	N		

Here, The **KEY** which we used for security is **"KOHLI".**

The **Ciphertext** for this **Plaintext** is read from the first column to till last and goes from left to right [7].

Finally the Ciphertext for this message is:-

"AKJLVEETTMOEIETOANDGNATHFEHCAAICT"

To decrypt, the receiver prepares similar table. The number of columns is equal to key number. The number of rows is obtained by **dividing** the number of total ciphertext alphabets by key value and rounding of the quotient to next integer value.

The receiver then writes the received ciphertext vertically down and from left to right column. To obtain the text, he reads horizontally left to right and from top to bottom row.**[6]**

The Other Type of Transposition are:

2. Rail Fence Transposition

In this type of Transposition, The Plaintext is written with every other letter on a second line.To create the Ciphertext, the letter on the first line is written first and then the letters on the second.

For Example:-

The Plaintext are:- **"attack to taj mahal on five dec eighteen "**

But for this Type, we will be written like that:-

a t c t t j a a o f v d c i h e n

t a k o a m h l n i e e e g t e

The Sender sends the Plaintext by written in that style to perform strong encryption…

So, The Resultant Ciphertext for this message is:-

"atcttjaaofvdcihentakoamhlnieeegte"

For decrypt, This Reachable Ciphertext is divided by 2 and rounding of the quotient to next integer value, This value means that value the second line will start. After this, Perform same above process in reverse order by written the Ciphertext in Plaintext style to obtain the encrypted message.

Using more rows helped, but Complexity increased beyond that which was reasonable and appropriate [8].

IV. CODEBOOKS

This is a special method of encryption where it gives more security of message transmission and also gives more difficulty to break the code by Cryptanalyst.

Here, It uses the "Code" replaces a word or phrase with a character, which includes some special symbols used in encrypting. These codes are used by Contemporary Cryptography.

Using Code, It was a good way to obfuscate meaning if the message are small and the Codebooks were safe. However, using Codebook to allow safe communication of long or Complex messages between multiple locations was difficult [9].

The main task of the encoder is to replace words with some appropriate code. Once code has replaced, encoder created a codebook after a lengthy process has been completed. And this code and codebook were reached to the decoder for decode and perform the given task. But Here are the main task of keeping the codebook safely drop to the hand of the decoder because Once the codebook theft, more difficult to break the reached code to the decoder.

Here, we are giving the easy example of codebook to see how the process is going on:-

Plaintext:- attack to taj on five dec eighteen

plaintext	attack	to	taj	on	five	dec	eighteen
symbol	&	%	@	!	<	#	?

Here, the used symbols were unique for each word in Plaintext. So, the ciphertext or code which are sent to the receiver are:- **&%@!<#?**

But the frequently occuring words in Plaintext are easily identified by the third party [10].

So, this codebook method is also breaking by cryptanalyst but some difficulty been given by it.

V. CONCLUSION

This history of Cryptography is filled with back and forth between Cryptographers creating 'unbreakable' and Cryptanalysts breaking the unbreakable. Here, we have discussed the different types of cryptography and its different application in many different tasks. We have also discussed how it's hard to break by Cryptanalysts or the third party(hackers), so a message should be safely reached to the right organization. Cryptography is truly given a highly secure method for message transmission by the chosen different security of data. Many organization uses cryptography to secure the important information about its current working project by which no any third party can affect its data.

VI. REFERENCES

[1]. Mr. Vinod Saroha, Suman Mor, Anurag Dagar "Enhancing Security of Caesar Cipher by Double Columnar Transposition Method" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 10, 2012.

[2]. M. S. Hwang and C. Y. Liu, "Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.

[3]. Bobby Jasuja and Abhishek Pandya-Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding"

[4]. H. Kruse and A. Mukherjee. - "Data Compression Using Text Encryption", Proc. Data Compression Conference, IEEE Computer Society Press, 1997.

[5]. Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed and Ahmed M Mahfouz -"Hybrid Compression Encryption Technique for Securing SMS", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue(6)

[6]. Dr.Mukesh Sharma and Smiley Gandhi-"Compression and Encryption: An Integrated Approach" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July – 2012.

[7]. V. Kavitha and K. S Easwarakumar,"Enhancing Privacy in Arithmetic Coding" ICGSTAIML journal, Volume 8, Issue I,2008

[8]. Dr. V. K. Govindan and B. S. Shajeemohan -"An intelligent text data encryption and compression for high speed and secure data transmission over internet"

[9]. Akash Kumar Mandal, Chandra Parakash, Department of Electronics & Telecommunication CSIT, Durg, Chhattisgarh, India.Mrs. Archana Tiwari Department of Electronics & Instrumentation CSIT, Durg, Chhattisgarh, India,"Performance Evaluation of Cryptographic Algorithms: DES and AES", 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[10]. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications (Kindle ed.). Indianapolis, IN: Wiley Publishing.