Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Comparative Survey on Various Encryption Techniques for Information Security

Priyanka Nema
Dept. of IT,UIT BU, Bhopal
India

Prof.Ashish Jain
Dept. of MCA & IT,UIT BU, Bhopal
India

Abstract— There are many security aspects in data communication, while transferring data in a distributed network. Encryption is also a way to provide security in data communication using a key. Several techniques are already introduced for encryption as well as decryption. Some of them do not provide so much security as required, but many techniques are very useful and can be implement to be made more secure our data. Brute force attack is the most common attack, which makes a threat in data communication and cryptanalysis also make easy to break the code. In this paper, we have discussed several substitution and transposition encryption techniques as well as decryption of them also discussed. Substitution techniques are Caesar cipher, monoalphabetic, polyalphabetic, playfair and Transposition techniques are Rail fence with depth 2 and depth 3, columnar, odd-even, plaintext based. We have analyzed these encryption techniques on the basis of cryptanalysis and possibility of attack. This analysis gives some better results about comparison among these encryption techniques to provide more security.

Keywords— Encryption, Decryption, Brute Force Attack, Cryptanalysis, Security, Cipher tex , Plain text , Key.

I. INTRODUCTION

There are several encryption techniques which have a major role to provide the security for data communication encrypted with the help of secret key, encrypted message is called cipher text and it is sent to the receiver. If this cipher text is captured by other one, it will not be able to understand or use by other one. When receiver receive the cipher text, then again key is use to convert it original plain text. So in this process at the communication line only cipher text consist, which is of no use for the other. So the data is secure while communication[1],[2]. This encryption process is good at a time but as the time passes and technology explores hacker became able to steal information. The most common way to steal information is with the help of Brute Force Attack. This attack tries to find out the original plain text. So to be making secure our data, various different algorithms are used. So that this attack can be made more time consuming and the probability of finding the key or original message become much less.

Several types of encryption techniques are available, but the application of them creates difference while using in a cloud network. When data is more sensitive and cannot be lost at any cost then many costly algorithms are used e.g. MD5, AES (Advance Encryption standard) , DES (Data Encryption Standard) [2] and other hardware implementation can also be derived for them. But for normal data we can use medium level algorithm which provide more security and less time to implement. Any encryption algorithm does not have only aim of security. It also has a major concern about the applicability, time consumption for implementation and use. So here we have discussed several encryption techniques using a key, which are commonly used to protect communicating data. These techniques are analyzed for the brute force attack. Every technique is compared with the other in term of security and time consuming for implementing and safety. In this paper, next section describes the algorithm of the encryption techniques as well as decryption process. A way also discussed for the brute force attack and the cryptanalysis can be possible on the plain text.

II. ENCRYPTION TECHNIQUES

There are two techniques of encryption : Substitution Technique and Transposition Technique. In substitution technique, the letters of plain text are replaced by other letters or any number or by symbols. Example Caesar cipher ,hill cipher, monoalphabetic cipher etc[3]. In transposition technique, some sort of permutation is performed on plaintext. Example rail fence method, columnar method etc.

A. Substitution Technique

1.CAESAR CIPHER:

It is one of the simplest encryption technique and invented by Julius Caesar . In this technique we replace each character with the key place further character in english alphabet[6], consider the example given below.

Key: 5
Plain Text: I am the best
Cipher Text: N FR YMJ GJXY

So here each alphabet of Plaintext is replace by five places further down and create Cipher text.
The general Caesar algorithm

For **Encryption** :-
C = E (k, p) = (p + k) mod 26 (1)

For **Decryption** :-
p = D (k, C) = (C- k) mod 26 (2)
where value of k varies from 1 to 25
For brute force attack in Caesar Technique, we have check only 25 possible keys. So cryptanalysis over this technique is very easy as compared to other due to small number of possible keys for brute force attack.

2. MONOALPHABETIC CIPHER:

The previous technique is not far secure only because of there 25 possible keys ie; key space is very small but in this technique the key space is increased because of the random substitution as a result number of possible keys is also increased. In this technique, assign a different alphabetic character for each different plaintext alphabetic character. Key is in the form of a table and the total mechanism of this technique is much different from Caesar technique. Here is the following example which explains the mechanism of monoalphabetic cipher[6].

KEY:-
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: G C H D F T J K V R N X P Q M S I U Z W O Y L B A E
Plaintext :- tommorow we will meet at party
Ciphertext:- WMPPMUML LF LVXX PFFW GW SGUWA

Now for decryption process use the same table as a key and find plain text from cipher text. However this technique eliminates the possibility of brute force because it has 4 x 1026 possible keys which mean brute force cryptanalysis is not possible. But still this technique is not so far secure cryptanalysis is possible if attacker compared the relative frequency of cipher text character with the actual frequency of the letters in English, attacker will able to find the nature and structure of the plaintext without unveil the key.

Table 1: Relative Frequency of Letters in English Text

A	B	C	D	E	F	G	H	I	J
8.16	1.5	2.78	4.25	12.7	2.23	2.015	6.01	9.97	0.15
K	L	M	N	O	P	Q	R	S	T
0.77	4.025	2.41	6.75	7.51	1.93	0.095	5.98	6.33	9.05
U	V	W	X	Y	Z				
2.76	0.97	2.36	0.15	1.97	0.074				

From this table it is very clear that letters like Q and Z are very rarely use and A, E and T are most frequently use, so while attacking attacker will replace the most and least frequent character of cipher text with high and low relative frequency of letters in English respectively and try to find the structure of actual message. The most powerful tool that attacker use to break this technique is "digrams" which always look at the frequency of two letter combination and another tool is "trigrams" look at three letter combination.

3. POLYALPHABETIC CIPHER:

The previous technique is also not good enough to protect the arcane of plaintext but if we different and arbitrary multiple substitution technique at a time over plain text then the conquences are different as comparision to previous one. The general name for this approach is polyalphabetic substitution cipher and VIGNERE CIPHER, in this technique it uses a set of related monoalphabetic substitution rules. Vigenere tableau plays an important role, in this technique this Vigenere tableau [9] is a matrix which is use to encrypt and decrypt the message[6]. This table is known as "Vigenere tableau". The mechanism of this technique is clearly explained in the example given below.
Key= county**, Plaintext**= "enemy troops are discovered"
Key(X) :- countycountycountycounty
Plaintext(Y) :- enemytroopsarediscovered
Ciphertext(V) :- gbyzrwtciclytsxvlbqjyexb

Here in Vigenere Tableau, the characters of plain text is at top ie. coloumn of table, which is arranged horizontally where keys are arranged vertically beside the table ie. row of table and the cipher text alphabet is arranged horizontally in each row .Now during encryption process take the Plain text character(X) from coloumn and Key character(Y) from row , now find where X and Y will intersect in table then we will access a cipher character alphabet from Vigenere tableau Decryption is equally simple as Encryption process. We identify the key letter from row and then the position of the ciphertext letter in that row which determines the column, and the plaintext letter is at the top of that column.
This technique is far better than monoalphabetic technique and but the tools like "digrams" and "trigrams" are useful against this technique because in this case also ciphertext reflect the frequency of occurrence of letter which is determined with the help of these two tools.

Table:2 The Vigenere table used in Poly Alphabetic Cipher

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

4. PLAYFAIR CIPHER:

Another substitution cipher which was popular in World War -I and beyond is named after the Englishman Play fair[3], but it was actually invented by his friend Wheatstone. Some rearrangement of the alphabet is written in a 5 X 5 square, with two letters equated (usually I and J) as shown below

Table 3: a 5X5 Matrix for Play fair cipher

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

In this case the key word is *monarchy*. The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and the filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plain text is encrypted two letters at a time, according to the following rules: Repeating plain text letters that would fall in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

Plain text letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example *ar* is encrypted as RM. Plain text letters that fall in the same column are replaced by the letter beneath, with the top element of the row circularly following the last. For example, *mu* is encrypted as CM. Otherwise, each plain text letter is replaced by the letter that lies in its own row and the column occupied by the other plain text letter. Thus, *hs* becomes BP and ea becomes IM/JM.

From our example:

Plaintext: th es ch em er ea lx ly wo rk sx

Cipher text: pd i/jl hy lc km i/jm su qc vn dt xa

For deciphering, the rules are exact opposite.

B. *Transposition Ciphers:*

Transposition ciphers are block ciphers that change the position (or the sequence) of the characters or bits of the input blocks. To encipher, the plaintext is broken into *n* symbols and a key specifies one of (n!—1) possible permutations. Deciphering is accomplished by using an inverse permutation which restores the original sequence.

Transposition ciphers preserve the frequency distribution of single letters but destroy the diagram and higher-order distributions.

Transposition ciphers are often combined with other ciphers to produce a more secure product cipher.

1. RAIL FENCE WITH DEPTH 2:

The simplest such cipher is the *rail fence technique[6]*, in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows.

For example, to encipher the message ***— meet me after the toga party***‖ with a rail fence of depth 2, we write the following:

m e m a t r h t g p r y
e t e f e t e o a a t

The encrypted message is: MEMATRHTGPRYETEFETEOAAT

2. RAIL FENCE WITH DEPTH 3:

Same example**: meet me after the toga party ,** we write the following:

m t a e h o p t
e m f r e g a y
e e t t t a r

The encrypted message is :MTAEHOPTEMFREGAYEETTTAR.

3. COLUMNAR TRANSPOSITION:

But the technique which has been explained below is much more complex than the rail fence. In this technique we write the message in a rectangle, row by row, but when we read the message we consider column by column, but permute the order of the columns[6]. The order of the columns is the key of the algorithm. For example,

Key: 4 3 1 2 5 6 7
Plaintext: t r o o p s w
i l l a r r i
v e a t t w o
p m
Ciphertext: OLAOATRLEMTIVPPRTSRWWIO

4. ODD-EVEN TRANSPOSITION:

This technique involves giving plaintext a sequence of numbers starting from "one‟ to "n‟ to each and every word. The first word in the plaintext will take "odd number‟ and the "second word‟ as "even number‟. This continues till the plaintext is completed. In the odd set we have to take first the odd values and next the even values, and in the even set we have to take first even values and next odd values[7]. We have to place each and every character in a table. The length of the table will depend on the number of words in the plaintext. The table length must be rounded to the nearest value.

EXAMPLE: The plain text is:"change never informs its arrival"

Step1: change: c=1,h=2,a=3,n=4,g=5,e=6. (O)
Never: n=1,e=2,v=3,e=4,r=5. (E)
Informs: i=1,n=2,f=3,o=4,r=5,m=6,s=7. (O)
Its: i=1,t=2,s=3. (E)
Arrival: a=1,r=2,r=3,i=4,v=5,a=6,l=7. (O)

Step2:

c	a	g	h	n	e
e	e	n	v	r	i
f	r	s	n	o	m
t	i	s	a	r	v
l	r	i	a		

Step3: ceftl aerir gnssi hvnaa nror eimv
Step4: ltfec rirea issng aanvh rorn vmie
Step5: ltfecrireaissngaanvhrornvmie
Step6:l=1,t=2,f=3,e=4,c=5,r=6,i=7,r=8,e=9,a=10,i=11,s=12,s=13,n=14,g=15,a=16,a=17,n=18,v=19,h=20,r=21, O=22,r=23,n=24,v=25,m=26,i=27,e=28
Step7: lfcieisgavrrviterrasnanhonme
Step8: emnohnansarretivrrvagsieicfl

5. PLAINTEXT BASED TRANSPOSITION:

1) First, we take a message (plain text) from user which we have to encrypt.
2) Find the value of P ie. number of character which present maximum number of time in the given plaintext.

3) Find the value of Q ie. number of characters which present minimum number of times in the given plaintext.
4) Calculate, N = P-Q;
5) if (N<9 && N>2)
Perform K = N;
else
Perform K = N%9;
if (K=0 || K=1 || K=2)
Perform K = K+3
6) Replace all characters which present maximum number of times in the plaintext by the character which present minimum number of time.
7) Replace all characters which present minimum number of times in the plaintext by the character which present maximum number of time.
8) Form the group of „K" characters including space, digits, characters and all special characters.
9) Reverse characters of each group.
10) Finally we get secure encrypted message (cipher text)[5].

EXAMPLE

ENCRYPYION:
1) Suppose plaintext is :
To accomplish great things, we must not only act, but also dream.
2) In above plaintext the character "t" present maximum number (7) times,
P = 7;
3) In above plaintext the character „p" present minimum number (1) time,
Q = 1;
4) Calculate :
N = P- Q; N = 7 – 1 = 6;
5) If (N<9 && N>2)
(6<9 && 6>2)
(T && T) = T
a. Perform K = N;
K = 6;
6) Replace all characters "t" by "p" and all characters "p" by "t".
To accomplish great things, we must not only act, but also dream.
Po accomtlish greap phings, we musp nop only acp, bup also dream.
7) K=6, form the group of „6" characters including space, digits, characters and all special characters.
po_acc omtlis h_grea p_phin gs,_we _musp_ nop_on ly_acp ,_bup_ also_d ream.
8) Reverse characters of each group.
cca_op siltmo aerg_h nihp_p ew_,sg _psum_ no_pon pca_yl _pub_, d_osla .maer
9) Finally we get secure encrypted message
cca op siltmo aerg h nihp p ew ,sg psum no pon pca yl pub , d osla .maer

DECRYPTION:
1) Take cipher text :
Cca opsiltmoaerg hnihp pew ,sg psum no ponpca yl pub ,d osla.maer
2) In above plaintext the character „p" present maximum number (7) times,
P = 7;
3) In above plaintext the character „t" present minimum number (1) time,
Q = 1;
4) Calculate :
N = P- Q;
N = 7 – 1 = 6;
5) If (N<9 && N>2)
(6<9 && 6>2)
(T && T) = T
A. Perform K = N;
K = 6;
6) Replace all characters „p" by „t" and all characters „t" by „p".
cca_op siltmo aerg_h nihp_p ew_,sg _psum_ no_pon pca_yl _pub_, d_osla .maer
7) K=6, form the group of „6" characters including space, digits, characters and all special characters.
cca_ot silpmo aerg_h niht_t ew_,sg _tsum_ no_ton tca_yl tub_,d _osla. maer
8) Reverse characters of each group.
to_acc omplis h_grea t_thin gs,_we _must_ not_on ly_act ,_but_ also_d ream.
9) Finally we get decrypted original information.
to accomplish great things, we must not only act, but also dream.

III. CONCLUSION

In our topic we have discussed some important and mostly useful aspects of various substitution and transposition techniques and our analysis carry out some important results that are very useful in case of security of data transmission in a cloud network. Our experimental analysis proves that Caesar cipher is not useful for the security purpose as anyone can break the code through Brute Force Attack within a second. while Transposition techniques is most suitable for security purpose from all discussed techniques. This method takes less than a sec to encrypt our message while there is very much complexity to find out the original message for hackers. Polyalphabetic techniques followed by monoalphabetic also useful and provide good result for the security purpose. These techniques taken very less time in encryption but brute force attack take very much time to break the code. So these are most applicable in the field of security. These techniques provide much security at a level but today's high technology and modern era or great mind made easy to break the message from these encryption techniques. So we always cannot say the most secure algorithm for security. But at a level these techniques can be used. The main applications of these techniques occur where security is required at a level but speed requirement is much more. As the complexity of the encryption techniques increase, security also increases but speed decreases. So these algorithms required maintaining both and data is not so much sensitive.

REFERENCES

[1] Atul Kahate (2009), *Cryptography and Network Security*, second edition, McGraw-Hill.

[2] William Stalling "*Network Security Essentials(Applications and Standards)*",Pearson Education,2004

[3] Kallam Ravindra Babu, Dr.S.Udaya Kumar, Dr.A.Vinaya Babu "A Survey on Cryptography and Steganography Methods for Information Security" International Journal of Computer Applications(0975-8887) volume 12-No.2,Nov2010

[4] Satyanarayana Reddy Beeram, Bandarupalli Renuka Devi, Paleti Lakshmi Kanth, Kiran Kumar M "Secure Data Transfer Based on Conventional Encryption Technique Including Random Number Key Generation" International Journal of Latest Trends in Computing (2045-5364) Vol-2No.3 Sep,2011.

[5] Prof.S.D.Padiya, Prof.D.N.Dakhane "Plaintext Based Transposition Method" International Journal of Advanced Research in Computer Science and Software Engineering(2277 128X) Vol-2, Issue 7, July2012.

[6] Sandeep Mahapatra "A Comparative Evaluation of Various Encryption Techniques Committing Cryptanalysis" Proceedings of the 5th National Comference;INDIACom-2011.

[7] Mr.Bobba Veera Mallu, Mr.Tammineedi Venkata Satya Vivek, Mr.K.Srinivasulu Achari "Novelty Approach of Odd-Even Transposition Technique" International Journal of Engineering Research and Application (2248-9622) Vol-3, Issue1, Jan-Feb 2013,pp.1145-1146.

