A Novel Approach for Encryption of Text Messages, Enhancing the Security of Simple Coloumnar Transposition Cipher with Ceasar Cipher and Rail Fence Cipher, Under 15 Parameters

Jawad Ahmad Dar[1], Amit Verma[2]

[1]Research Scholar, Computer Science and Engineering, Kurukshetra University Kurukshetra, Haryana, India

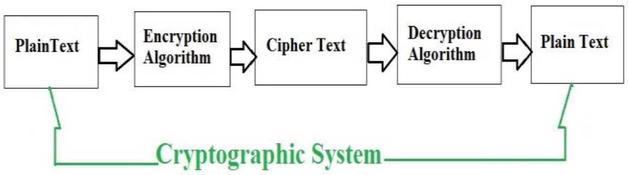
[2]HOD CSE, NNSS Samalkha Group of Institution, Kurukshetra University Kurukshetra

Abstract: ***Cryptography is an art and science of converting original message into no readable form. There are two techniques for converting data into no readable form. Transposition technique, Substitution technique. In recent years there is drastic progress in Internet world. Sensitive information can be shared through internet but this information sharing is susceptible to certain attacks. Cryptography was introduced to solve this problem. Cryptography is art for achieving security by encoding the plain text message to cipher text. Substitution and transposition are techniques for encoding. When Caesar cipher substitution, Rail fence cipher and Columnar Transposition Cipher techniques are used individually, cipher text obtained is easy to crack. This talk will present a perspective on combination of techniques substitution and transposition. Combining Caesar cipher and rail fence with Columnar Transposition Cipher can eliminate their fundamental weakness and produce a cipher text that is hard to crack. In this 2 paper I am going to compare The performance analysis of already designed new algorithm according to 15 Parameter's with simple columnar transposition cipher.***

Keywords: Cryptography, Cipher text, Substitution, Transposition, Caesar Cipher, Columnar Transposition Cipher, cryptanalysis, key.

1. Introduction

This modern era is dominated by paperless offices-mail messages-cash transactions and virtual departmental stores. Due to this there is a great need of interchanging of data through internet. The dramatic rise of internet has opened the possibilities that no one had imagined. We can connect to any person, any organization or any computer, no matters how far we are from them. Internet cannot be used only for browsing purpose. Sensitive information like banking transactions, credit card information and confidential data can be shared through internet. But still we are left with a difficult job of protecting network from variety of attacks. With the lots of efforts, network support staff came up with solution to our problem named "Cryptography". Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable gibberish called cipher text. You use Encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption.



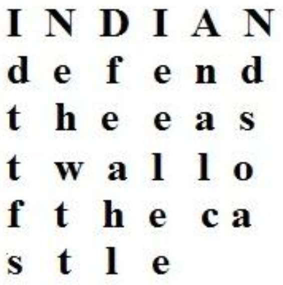
There are two primary ways in which plaintext can b codified to corresponding Cipher text: Substitution and Transposition. A Substitution technique is one in which the letters of Plain text are replaced by other letters or by numbers(Caesar Cipher, Hill Cipher, Monoalphabetic cipher etc).A Transposition technique is one in which the letters of the message are rearranged or permuted. (Rail Fence method, Columnar method etc.). The columnar transposition cipher is a fairly simple, easy to implement cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher text. Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on it's own.

2. Columnar Transposition Cipher

The columnar transposition cipher is a fairly simple, easy to implement cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the ciphertext. Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on its own.

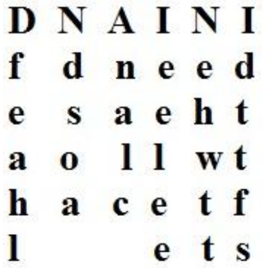
A. Example

The key for the columnar transposition cipher is a keyword e.g. INDIAN. The row length that is used is the same as the length of the keyword. To encrypt a piece of text, e.g. defend the east wall of the castle, we write it out in a special way in a number of rows (the keyword here is INDIAN):



I	N	D	I	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e		

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

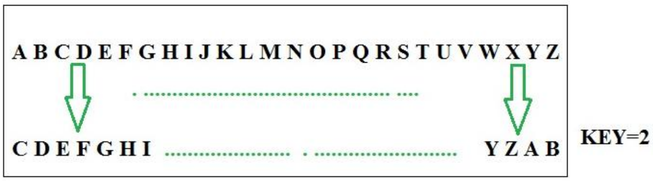


D	N	A	I	N	I
f	d	n	e	e	d
e	s	a	e	h	t
a	o	l	l	w	t
h	a	c	e	t	f
l			e	t	s

The ciphertext is read off along the columns: dttfsehwttfeahleeleenalcdsoa

3. Ceasar Cipher

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages C = E (k, p) = (p + k) mod26



Example
"**KURUKSHETRAUNIVERSITY KURUKSHETRA**" is encoded as (Key=2)

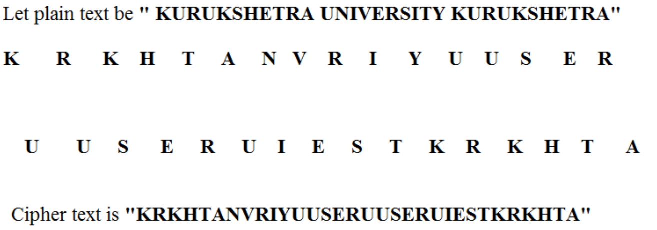
"**MWTWMUJGVTCWPKXGTUKVAMWTWMUJGVTC**"

4. Analyzing Caesar Cipher

Cryptanalysis means breaking codes and ciphers. The decryption algorithm of Caesar cipher is simple. P= D(C) = (C - k) mod 26 If it is known that given cipher text is a Caesar cipher, then a brute-force cryptanalysis can be easily performed. Simply by trying all possible 25 keys a cryptanalyst just has to find the shift that causes the cipher text frequencies to match up closely with the natural English frequencies and then decrypt the text using that shift. This method can be used to easily break Caesar ciphers by hand

5. Rail Fence Cipher

Similarly Rail Fence cipher is also a very weak cipher to Cryptanalyze. A code breaker simply has to try several depths until the correct one is found. It is very easy to find depth if you know some of the plain text. Letters break into rows according to certain fixed patterns based on the number of rows in the key. For example, if there are two rows, then letters 1, 3, 5, … of the message are in row one and letters 2, 4, 6,... are in row two.



Let plain text be "**KURUKSHETRA UNIVERSITY KURUKSHETRA**"

K R K H T A N V R I Y U U S E R

U U S E R U I E S T K R K H T A

Cipher text is "**KRKHTANVRIYUUSERUUSERUIESTKRKHTA**"

RAIL FENCE CIPHER

6. Proposed Work

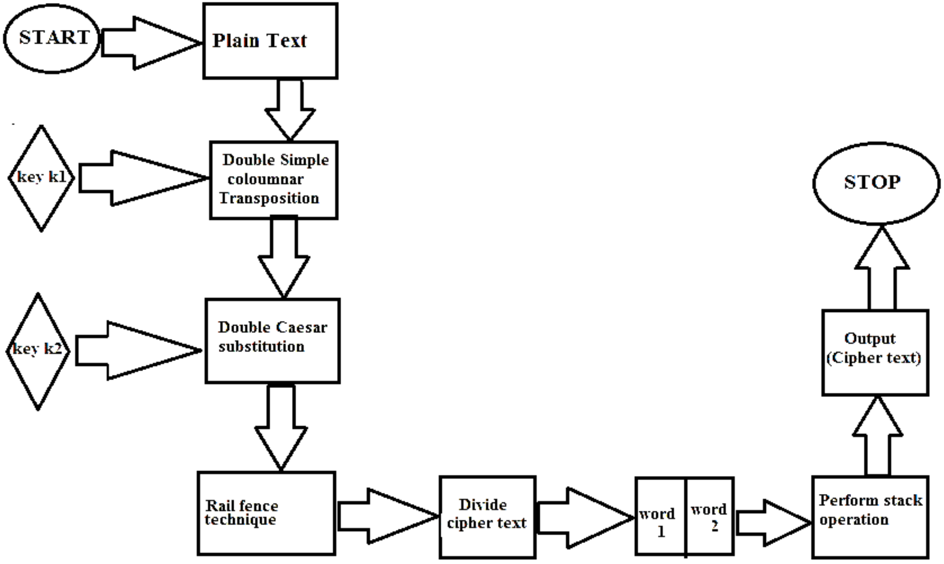
A. Encryption Algorithm

1) First take the plain text to be encrypted from sender.
2) write the plain text in rectangular format across rows, order is determined by key k1.(Columnar transposition technique).
3) Read off the message column by column in order using Key K1,we get cipher text CT1.
4) Repeat step2 and 3,we get CT2
5) Perform substitution on CT2,using key k2,we get CT3
6) Repeat step5,we get CT4.
7) Perform Rail fence technique on CT4 we get,CT5
8) Now divide the cipher text(CT5),into two halves, as Word 1,andWord 2.
9) To add more complexity put these different words, on different stacks using PUSH operations, now POP the Values from stack, we get two words. Let it be CT6.
10) Finally CT6 is our required Cipher Text.

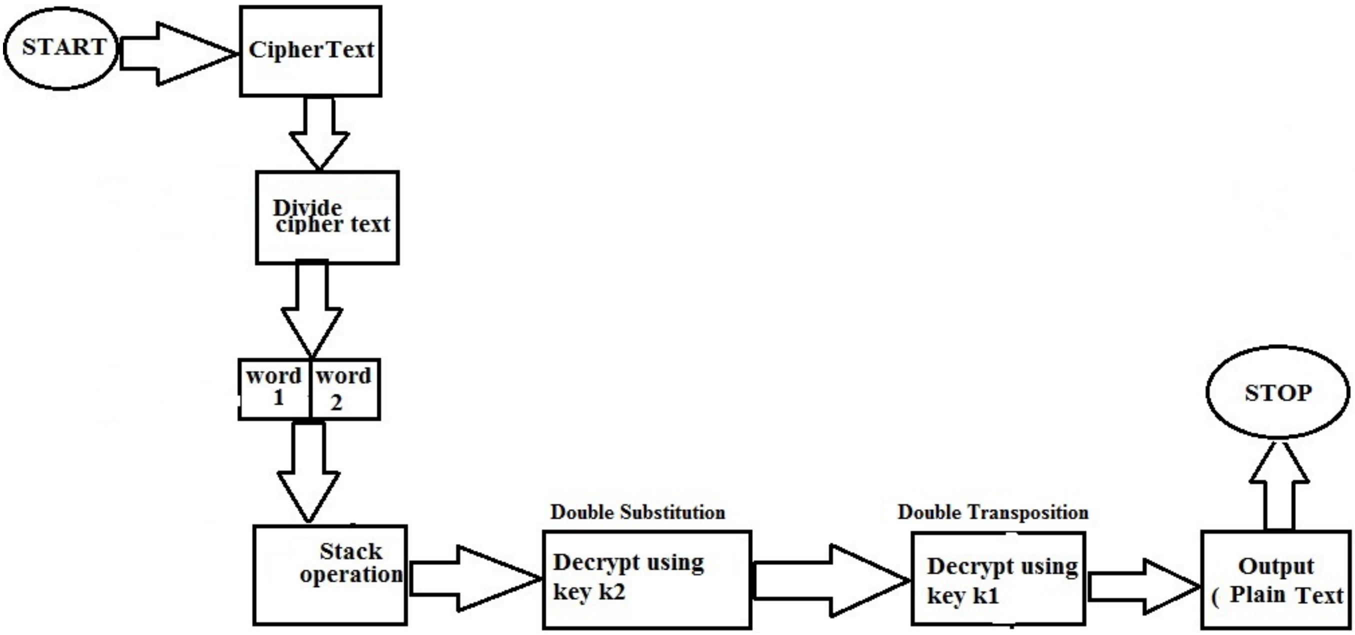
B. Decryption Algorithm

1) Write the cipher text to be converted into plain text,(CT6)
2) Divide cipher text as two separate words Word 1,and Word 2.
3) PUSH two words on to stacks, using different stacks
4) POP one element from stack one and second element from stack second(CT5).
5) Using Key K2 to decrypt CT5,we get CT4.
6) Repeat step 5,we get CT3
7) Arrange cipher text obtained in step 5(CT3),into rectangular format, as column by column using Key K1 and read of as rows. Let it be CT2
8) Repeat step 7,we get CT1
9) Read of row by row we get our plain text
10) Output of step 9 is our required plain text.

7. Block diagram for Encryption Algorithm



8. Block Diagram for Decryption Algorithm



9. Example

A.Encryption

1.let the plain text to be Encrypted is**" KURUKSHETRA UNIVERSITY KURUKSHETRA".**

2.Arrange the plaintext across rows in a rectangular format,using **key K1= 4 3 2 1**(Columnar Transposition),as shown in figure

Key K1=4	3	2	1
K	U	R	U
K	S	H	E
T	R	A	U
N	I	V	E
R	S	I	T
Y	K	U	R
U	K	S	H
E	T	R	A

3.Now read columns in order, we get cipher text(CT1)."**UEUETRHARHAVIUSRUSRISKKTKKTNRYUE**"

4.Repeat Step 2 on CT1,as shown we get CT2=**"EAVRITNEUHASRKTUERHUSKKYUTRIUSKR"**

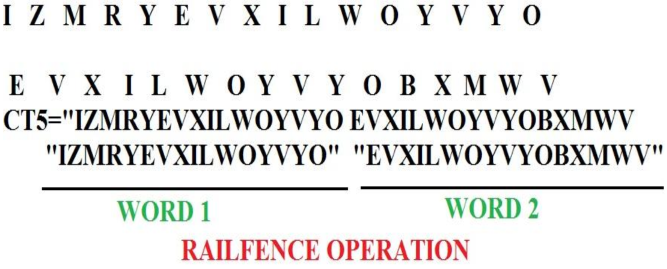
4	3	2	1
U	E	U	E
T	R	H	A
R	H	A	V
I	U	S	R
U	S	R	I
S	K	K	T
K	K	T	N
R	Y	U	E

CT2="EAVRITNEUHASRKTUERHUSKKYUTRIUSKR"

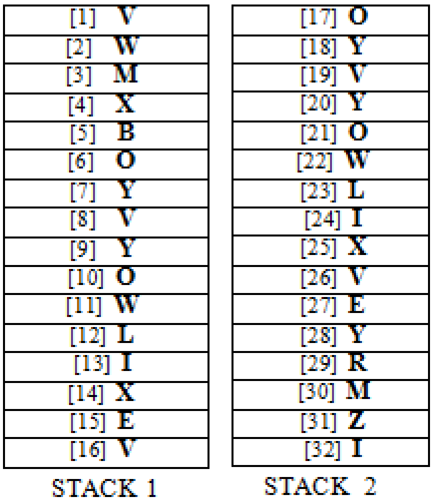
5..Using Caesar cipher(Substitution Technique),shift the characters of CT3 by **K2=2** positions, we get New cipher text, let it be labeled as

CT2=”**GCXTKVPGWJCUTMVWGTJWUMMZWVTK WUMT**”.

6.Repeat
Step5onCT3,weget
CT4=”**IEZVMXRIYLEWVOXYIVLYWOOBYXVMYW OV”**
5.Now perform rail fence technique on **CT2,**as shown in figure, we get again New cipher text, labeled as **CT4**
6.Now divide cipher text CT3,into two equal Halves, as Word1 and Word 2,as shown above


I Z M R Y E V X I L W O Y V Y O
E V X I L W O Y V Y O B X M W V
CT5="IZMRYEVXILWOYVYO EVXILWOYVYOBXMWV
"IZMRYEVXILWOYVYO" "EVXILWOYVYOBXMWV"
WORD 1
WORD 2
RAILFENCE OPERATION

7.To add more complexity, put these different words in different stacks, by using PUSH Operations.



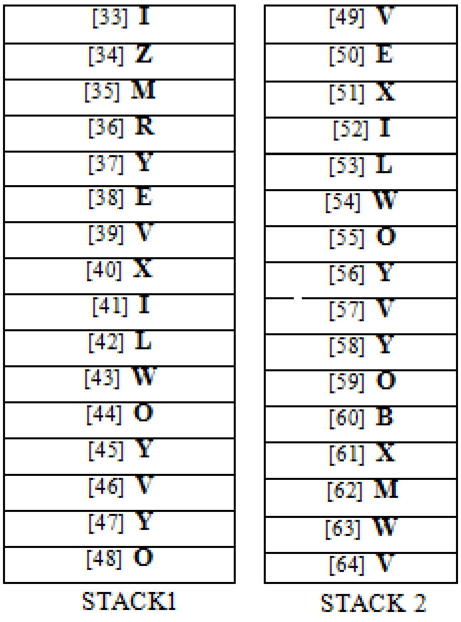
[1] V	[17] O
[2] W	[18] Y
[3] M	[19] V
[4] X	[20] Y
[5] B	[21] O
[6] O	[22] W
[7] Y	[23] L
[8] V	[24] I
[9] Y	[25] X
[10] O	[26] V
[11] W	[27] E
[12] L	[28] Y
[13] I	[29] R
[14] X	[30] M
[15] E	[31] Z
[16] V	[32] I
STACK 1	STACK 2

8. Now **POP** elements from both stacks
Stack1:**OYVYOWLIXVEYRMZI**
Stack2:**VWMXBOYVYOWLIXEV,**let this be CT6.

9.Final cipher text is Stack1+Stack2,that is
CT7=
“OYVYOWLIXVEYRMZIVWMXBOYVYOWLIXEV”

A. Decryption

1.Write cipher text **CT7=**
“OYVYOWLIXVEYRMZIVWMXBOYVYOWLIXEV”
2.Separate it into two halves as
=”**OYVYOWLIXVEYRMZI**”and“**VWMXBOYVYOWLI XEV,”**
3Push these two words on different stacks, as shown in figure



[33] I	[49] V
[34] Z	[50] E
[35] M	[51] X
[36] R	[52] I
[37] Y	[53] L
[38] E	[54] W
[39] V	[55] O
[40] X	[56] Y
[41] I	[57] V
[42] L	[58] Y
[43] W	[59] O
[44] O	[60] B
[45] Y	[61] X
[46] V	[62] M
[47] Y	[63] W
[48] O	[64] V
STACK1	STACK 2

4.POP one element from Stack 1 and Second element from Stack 2,we get pair of two words,example first pair **IE,ZV,MX,RI,YL,EW,VO,XY,IV,LY,WO,OB,YX,VM,Y W,OV**
CT6=“
IEZVMXRIYLEWVOXYIVLYWOOBYXVMYWOV”

5.Using **Key K2= -2** decrypt CT6,We get CT5
CT5=”
GCXTKVPGWJCUTMVWGTJWUMMZWVTKWUM T”

6.Repeat step 5,on
CT4=”
EAVRITNEUHASRKTUERHUSKKYUTRIUSKR”

7.Now using Key **K1=4 3 2 1,**arrange CT4 in rectangular format columns, and read as rows,we get CT3 as
UEUETRHARHAVIUSRUSRISKKTKKTNRYUE

4	3	2	1
U	E	U	E
T	R	H	A
R	H	A	V
I	U	S	R
U	S	R	I
S	K	K	T
K	K	T	N
R	Y	U	E

8.Repeat Step 7,We get Plaintext as shown

Key K1=4	3	2	1
K	U	R	U
K	S	H	E
T	R	A	U
N	I	V	E
R	S	I	T
Y	K	U	R
U	K	S	H
E	T	R	A

8. Now Read as row by row we get original plain text.

PT=KURUKSHETRA UNIVERSITY KURUKSHETRA

10. Objectives

1. Overcomes limitations of simple columnar transposition cipher
2. Results cannot be easily reconstructed.
3. To understand the algorithm is not very difficult.
4. It is more difficult to crypt analyze.
5. It provides moderate complexity to encrypted messages
6. Simple to perform double substitution
7. Double transposition method is applied which provides much less structured permutation.

11. Comparison

Comparative study between New Proposed Algorithm and Simple columnar Transposition Cipher.

Parameters	*Simple columnar Transposition*	*Simple columnar Transposition with 2 rounds*	*New Algorithm*
Security	Less	Less	More
Keys	One	One Or Two	Two
Diversified Cipher Text	No	No	Yes
Complexity	Less	Less	Less
Cryptanalysis	Easy	Easy	Difficult
Brute Force Attack	Possible	Possible	Not Possible
Double Substitution	No	No	Yes
Rounds	One	2	5
Implementation	Easy	Easy	Easy
Can Result Be Easily Reconstruct-Ed	YES	YES	NO
Time To Break Cipher Text	Time Required By Simple Coloumnar	Time Required By Simple Coloumnar* Number Of Rounds	2*Simple Coloumnar+2*Substitution +Railfence+Stack Operation
Double Transposition	No	Yes	Yes
Use Of Stack	No	No	Yes
Confusion	No	No	Yes
Diffusion	Yes	Yes	Yes

12. Result Analysis of of New Algorithm

During comparative study or during graphical analysis of simple columnar transposition cipher with the proposed algorithm, we can notice that simple columnar is weak cipher, easily gets cryptanalyze when key length small (2, 3, 4, 5, 6).On other hand the Proposed algorithm can work successfully with small and large keys.

1) Time required to break the simple columnar transposition cipher can be analyzed as if key length is 2, then we need 2 permutations, if key length is 3 then we need 6 permutations and so on.
2) Time Required to break the simple columnar transposition cipher with multiple rounds can be analyzed as if key length is 2,the we need 2 permutation multiplied by number of rounds, if key length is 3,then we need 6 permutation multiplied by number of rounds and so on.
3) Time required to break the New Algorithm can be analyzed as, New Algorithm is a combination of simple columnar transposition, substitution, followed by rail fence and time require for performing stack operation. Therefore time required can be calculated as

2*simple coloumnar+2*substitution rail fence + stack operation.

Let ' x' be the time required to break the cipher text of simple columnar transposition cipher, 'y' be the time required to break cipher text in Caesar cipher and ' z ' be the time required to break cipher text of rail fence cipher. Then

1. For simple Columnar Transposition T=x.
2. For simple Columnar Transposition with multiple rounds T=n * x
3. For Proposed New Algorithm T=2 * x + 2 * y + z + s
S= Time Required for Performing Stack Operation

For a particular Example if x=1,y=1,z=1 (x,y,z can be in sec,Min,Hours etc)
1.Then for simple columnar Transposition T=1.
2. For simple Columnar Transposition with multiple rounds T=2 * 1=2 for 2 rounds
3. For Proposed New Algorithm T=2 * x + 2 * y + z + s=2 * 1+ 2 * 1 + 1=5+

if x=2,y=2,z=2 (x,y,z can be in sec,Min,Hours etc)
1.Then for simple columnar Transposition T=2.
2. For simple Columnar Transposition with multiple rounds T=2 * 2=4, for 2 rounds
3. For Proposed New Algorithm T=2 * x + 2 * y + z + s=2 * 2+ 2 * 2 + 2=10+.

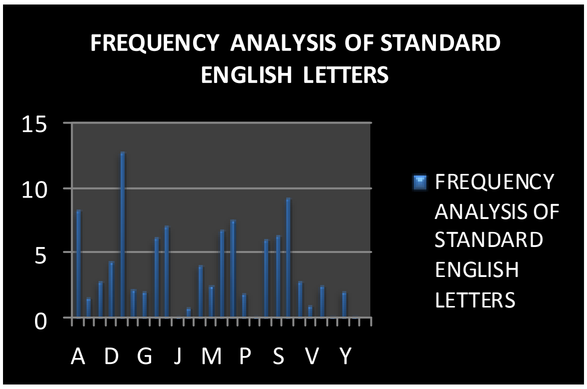
13. Advantages of Proposed Algorithm

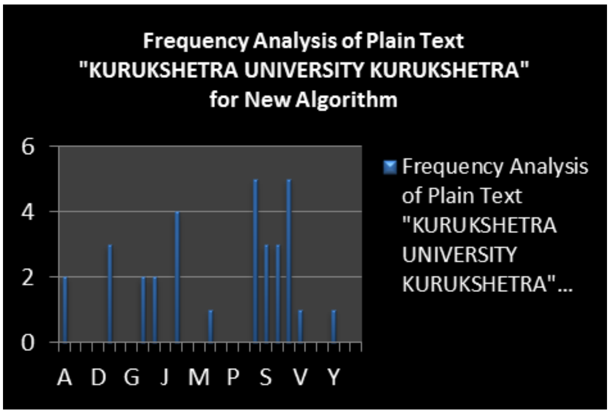
1) If we scrutinize at the Algorithm we can notice at every Stage we are getting diverse cipher text, thus more trouble to cryptanalyst.
2) It is more difficult to crypt-analyze.
3) Brute force attack is not possible.
4) It is simple to perform substitution.

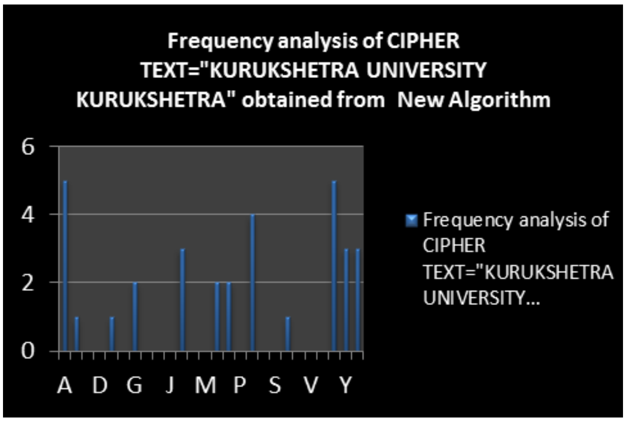
14. Disadvantages of Proposed Algorithm

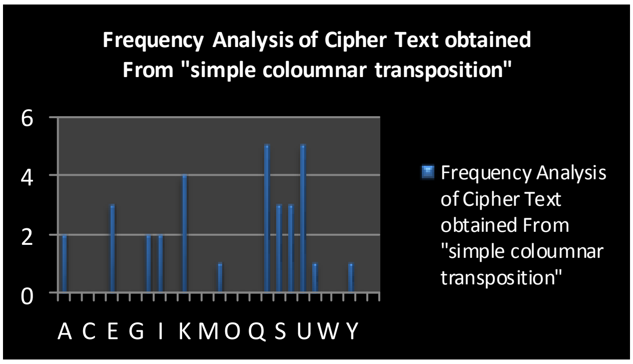
1. It makes use of two keys.
2. Also difficult to implement.

15. Graphical Analysis









16. Conclusion

In this paper I have presented how to improve security of Simple columnar Cipher to make it more secure and strong, and compare its performance according to 15 parameters. Moreover the proposed algorithm has lot of advantages in achieving secure communication than Simple One. Simple columnar transposition cipher is the simplest Transposition method. It is also the weak cipher. It's only advantage lies in the fact that it is not complex and can be understood easily. This advantage leads to the problem of easy detection. For overcoming this problem Caesar cipher and rail fence cipher is combined with transposition techniques. Transposition technique used here is simple columnar cipher. For adding further complexity stacks are used which makes the detection of both the techniques (Caesar cipher and rail fencing) difficult.

17. Acknowledgment

Author would like to give sincere gratitude especially to Mr.Amit Verma, for his guidance and support to pursue this work.

References

[1] Jawad ahmad dar,*"Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques,International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 3 Issue 9, September 2014*

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

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

[4] http://www.cs.trincoll.edu/~crypto/historical/railfence.html

[5] practicalcryptography.com/ciphers/rail-fence-cipher/

[6] Charles P.Pfleeger "Security in Computing", 4th edition, Pearson Education.

Author Profile

Jawad Ahmad Dar is currently in final year **M TECH** Computer science and Engineering from **Kurukshetra University, Kurukshetra**. He did **B.TECH** in Computer Science and Engineering from **Islamic University of Science and Technology Kashmir in 2013(2009 BATCH)**. He has already published more than 5 papers at international and national journals. His interested areas of research are Neural Networks, Mobile computing, Network security, and Algorithms.