Novelty Approach of “Odd-Even Transposition Technique”

Mr.Bobba Veera Mallu[1],Mr.Tammineedi Venkata Satya Vivek[2], Mr.K.Srinivasulu Achari[3]

Computer Science and Engineering, Koneru Lakshmaiah University
Vaddeswaram, Vijayawada

Abstract

Cryptography is the science of writing message in secret code and is an ancient art. There are many techniques to encrypt “plain text” and convert it to the “cipher text”. In this paper we made an attempt to enhance “Odd-Even Transposition Technique”[1] and make out the technique more advanced. One of the most important point is that we applied the “Rail-Fence Technique” to the cipher text to improve the complexity to the intruders. Any cryptographic scheme is safe if and only if it is unbreakable in reasonable time using feasible resources in spite of the intruder’s being aware of the encryption and decryption algorithm and size of the key.

Keywords— Cipher text, Network cryptography, Network security, Plain text, Transposition.

I. INTRODUCTION

Cryptography is the study of mathematical techniques related to the aspects of the information security such as confidentiality, data integrity, authentication and data origin authentication [2]. Cryptography is not only the means of providing information security, but rather one set of techniques. Security is often viewed as the need to protect one or more aspects of network’s operation and permitted use. Security requirements may be local or global in their scope depending upon the networks or internetwork’s purpose of design and deployment. Cryptography can exist with or without networks but network cryptography specifically address the needs of networks and is thus a subset of general cryptography.

The encrypted form of a message in the cryptographic term is called a “cipher text”. The sender encrypts the plain text and sends it to the destination end. The algorithm that is used to encrypt the message is called “cipher”. The word “Privacy” can be defined as “Preventing third party from snooping”. Two kinds of Authentication takes place:- 1.Gaurantee that no third party has modified the data. 2. Receiver can prove that only the sender originated the data. In the cryptographic privacy two components takes place:1.Key, 2.Algorithm. For military systems the algorithm must be kept secret. The key distribution must be secure between them.

“Transposition ciphers” attempt to exploit the power of permutation on the plaintext symbols/letters. In real life these ciphers “complement” the substitution ciphers. Example of transposition cipher include “Rail Fence” cipher, here letters of plaintext or organised as a sequence of diagonal elements of depth ‘k’ while writing, and the cipher text gets generated when these elements are read out as the resultant rows. However it is easy to break unless the encoding scheme is used with any other scheme for final effect. Cannot withstand frequency analysis in its purest form.

All encryption algorithms are based on the two general principles: Substitution, in which each element in the plaintext is mapped into another element; and Transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information is lost in the transposition. Thus the cipher text contains the same letters as in the plaintext, but the order of text is changed.

II. PROCEDURE

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. 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.
The below are the steps of our technique:
Step1: Give numbering to each word in the plaintext in sequence. For each word the sequence will start from 1,2,3..n

Step2: Now start our technique with odd numbers; first write the odd number characters from the top of the table, after it write even number characters. For each and every word repeat the same procedure.

Step3: Now starting from the first column, write down the words vertically downwards until the last column reaches.

Step4: Now for every column of words, reverse the text for all columns.

Step5: write whole text eliminating spaces between them.

Step6: Now assign the numbers for all the words starting from the number 'one' to 'n'.

Step7: Now first write all the odd number characters, and next after to it write the even number characters.

Step8: Reverse the whole text from the last word.

Step9: For the above step apply "Rail-Fence Technique". A strong 'Cipher' will occur.

Let us discuss the above steps with an example.

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

Step9: on applying "Rail-Fence Technique" to the above step we get cipher text as:

enhasreirvgiif
monnartvrasecl

III. CONCLUSION

Transposition is often combined with other techniques. In this we enhance the [1] and make our technique more advanced than the older one. In this we have changed the format of [1] and placed another formula. When different types of transposition techniques are combined, a strong cipher which is more secure is obtained. This technique improves the complexity to the intruders.

REFERENCES

[1] "Odd-Even Transposition Technique*"-"The IUP Journal of Computer Sciences", vol.v.No.4,2011*

[2] *"Handbook of Applied Cryptography"*-by "A.Menezes,P.Van Oorschot and S.Vanstone.

[3] *"Cryptography and Network Security"*-by "William Stallings".

[4] *"Mathematical Cryptology for ComputerScientists and Mathematicians"*-by "Wayne".

[5] *"A Course in Number Theory and Cryptography"*-by "Neal Koblitz".

[6] *"Foundations of Cryptography"*-by "Oded Goldreihch".

[7] *"Cryptography and Network Security"*-by "Kahate", 2nd Edition.

[8] *"Practical Cryptography"*-by "Fergulson, Niels and Schneier".

[9] *"Cryptography Decrypted"*-by "Mel, Baker, Doris".

[10] *"Understanding Cryptography"*-by "ChristofPaar and Jan Pelzl".

[11] *"Cryptanalysis"*-by "Gainer, Helen fouche".

[12] *"Course and Cryptography"*-by "Dominic Welsh".

[13] "Bansal Sathish (2011). "Transposition Based Cryptography", *in the 2nd International Conference*.

[14] "Ajay Mahimkar, R.K. Shyamsundar*" "S-MECRA A Secure Energy-Efficient Routing Protocol for Wireless Ad Hoc Networks" IEEE 2004.*

[15] "Bissias, G.D., Liberatore, M., Jensen, D., Levine, B.N., *"Privacy vulnerabilities in encrypted HTTP streams" In Proc. Privacy Enhancing Technologies Workshop (PET 2005).*

[16] "Adrian Perrig Ran Canetti J.D Tygar Dawn Song" *"The TESLA Broadcast Authentication Protocol", UC Berkeley and IBM Research.*