International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques

Jawad Ahmad Dar

[1]M.Tech (CSE) Final Year, Department of Computer Science and Engineering,
Kurukshetra University, Kurukshetra, Haryana, India

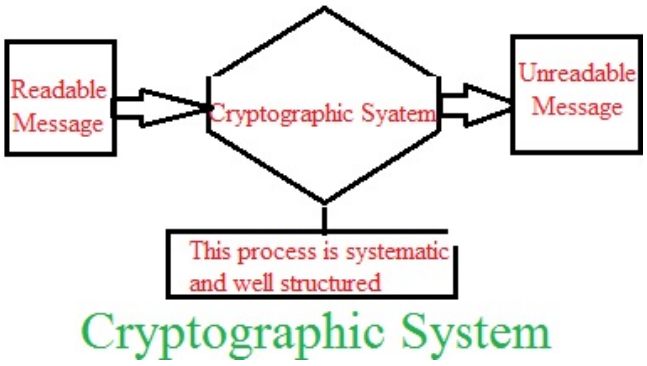
Abstract: ***Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Achieving strong encryption, the hiding of data's meaning, also requires perceptive leaps that allow creative application of known or new methods. So cryptography is also an art. We can say now that Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography, as the most important aspect in the never ending evolving information technology era, is being criticized in its aspect. Information outbreaks make users doubtful on relying on their own information in current cryptosystems. Cryptography is used to maintain the secrecy and integrity of information, whenever it is exposed to potential attacks. Cryptography comes from the Greek words for "secret writing". The plain text is encrypted into the corresponding cipher text, using an algorithm and a key. Substitution and Transposition are two Techniques used for converting data into non-readable form. Rail Fence Cipher is an example of Transposition technique. In this paper we have proposed a cipher that uses basic encryption techniques of substitution and transposition. A double columnar transposition followed by a double substitution is applied on a Rail Fence cipher in order to make it a stronger and a more secure cipher.***

Keywords: Cryptography, Cryptanalysis, Substitution Technique, Transposition Technique, Hill Cipher, Key.

1. Introduction

Computer security presents one of the fastest-evolving segments in the Information Technologies (IT) area. The traditional system security approach is slightly focused on defence but more attention has been drawn to aggressive forms of defence against potential attackers and intruders.

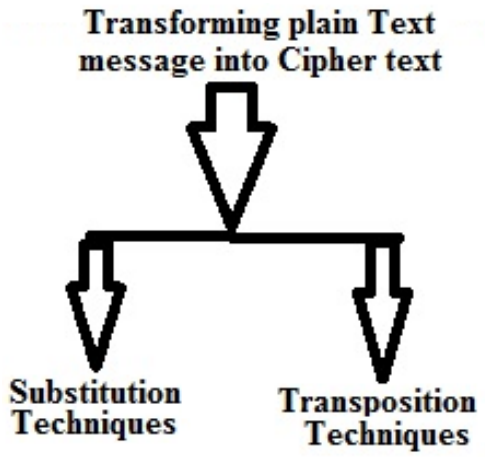
In Cryptography we are encrypting the messages, so that it should not be understood to third party apart from recipient. Encryption is process of encoding a message in such away as to hide its contents. We can use substitution and Transposition Techniques to encrypt the message. The development of internet has put a lot of burden on a cryptanalyst to develop suitable encryption techniques that could secure the data over internet. In this age of information, it is impossible to imagine without internet. A huge amount of data is interchanged over internet, sensitive information like credit card information, confidential data, banking transactions, needs to be protected demanding a highest degree of security. The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key [1]. The cipher text is transmitted to the intended receiver(s) where the reverse of encryption process is done to get the original plaintext. Encryption process can be categorized into: substitution ciphers and transposition ciphers. In a substitution cipher each letter or a group of letters is replaced by another letter or group of letters to disguise it [1].Caesar cipher, Hill cipher, mono-alphabetic cipher are some examples of the substitution cipher. Whereas, in transposition ciphers, letters are reordered in such a way to create confusion to the intruder. Rail fence cipher, Columnar cipher are some examples of the transposition cipher.



Cryptographic System

2. Techniques of Transforming Plain text to cipher Text

Two primary ways in which a plain text message can be codified to obtain the corresponding cipher text message: **Substitution** and **Transposition**



2.1Substitution Cipher

Substitution cipher is a method of encoding by which units of plaintext are replaced with cipher text, according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution. Substitution ciphers can be compared with transposition ciphers. In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the cipher text, but the units themselves are altered. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the cipher text and vice versa.

2.2 Example of Substitution cipher Technique

Caesar Cipher and its Cryptanalysis

The Caesar cipher is of oldest and simplest known cipher. It is one of the types of substitution cipher, in which each letter in the message or plaintext is shifted a certain number of places down the alphabet. For example, with a shift of 2, A would be replace by C, B would be replaced by D, C would be replace by E, and so on. The encryption for the given plaintext with as shift (key) of 2 can be done as:

Plaintext: defend the wall of china
Cipher text: fghgpf vjg ycnn qh ejkpc
Decryption is simply done using an offset of -2 to get the original plaintext.
We translate all the 26 characters to numbers, ‘a’=0, ‘b’=1,’c’=2…’z’=25. The Caesar cipher encryption function, E(x), can be now represented as:
$E(x) = (x + k) \bmod 26$
Where ‘k’ is the key (the shift) applied to each character ‘x’.
The Caesar cipher decryption function, D(x), will be
$D(x) = (x – k) \bmod 26$

2.3 Transposition Cipher

Transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed.

2.4 Rail Fence Cipher Technique

The Rail Fence cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows. Now rail fence technique involves writing plain text as a sequence of diagonals and reading it row –by- row to produce cipher text. For example, using three "rails" and a message of **'SECUTITY IN COMPUTING**, The cipher writes out: The cipher text is: **SCRTICMUIGEUIYNOPTN** as shown

Analyzing Rail Fence Ciphers

The analysis isn't difficult. If you know that a message was encrypted with a Rail Fence Cipher, it can easily be deciphered by brute force because the 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. If there are 3 rows, then letters 1, 5, 9 ... are in row one, letters 2, 4, 6, 8 ... are in row two and letters 3, 7, 11... are in row three. Therefore, the Rail Fence Cipher is not a particularly secure cipher.

3. Limitations of Rail Fence Technique

1. Rail fence Cipher is not very Strong. The number of practical keys is small enough that a cryptanalyst can try them all by hand
2. It simply allows mixing up of characters in plain text to form the cipher text, it offers essentially no communication security and will be shown that it can be easily broken.
3. It cannot be used to encrypt images containing large areas of single color.

3.1 Solution to Limitations

Now although weak on its own, it can be combined with other ciphers such as substitution cipher, combination of which is more difficult to break than either cipher on its own.

4. Proposed Algorithm

The proposed algorithm that is used for encryption and decryption of the data provides a new Hill cipher which is stronger more secure than the original one.

A. Encryption

1) First let us take the plaintext to be encrypted from the sender.
2) Reverse the string (plaintext) ,This is our first cipher text (CT1)
3) Perform Rail fence technique on CT1, this gives CT2.
4) Write theCT2 (cipher text) in a rectangular way, row by row. Order of columns is determined by key K1.

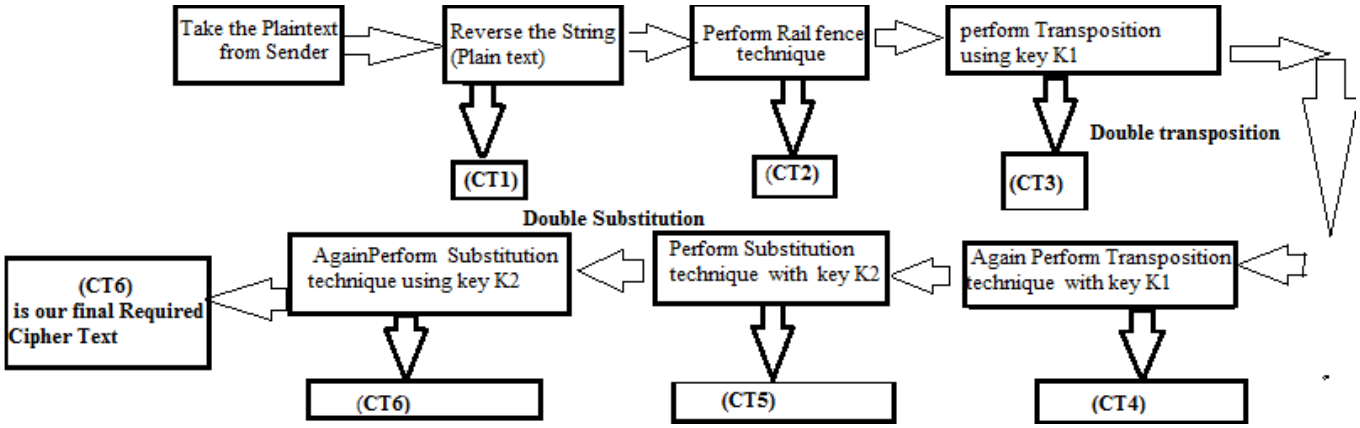
5) Read off the message column by column using Key K1, we get cipher text CT3.
6) Repeat the steps 4-5 on CT3 using key K1,This gives output CT4
7) Use key K2 to shift each of the character of cipher text CT4.we get cipher text CT5.
8) Repeat step 7 for cipher text CT5, this gives us CT6
9) Output of step 8 is our required cipher text Cipher
10) Text(CT6)

B. Decryption

This follows all the steps of encryption process but in the reverse order to get the original plaintext.

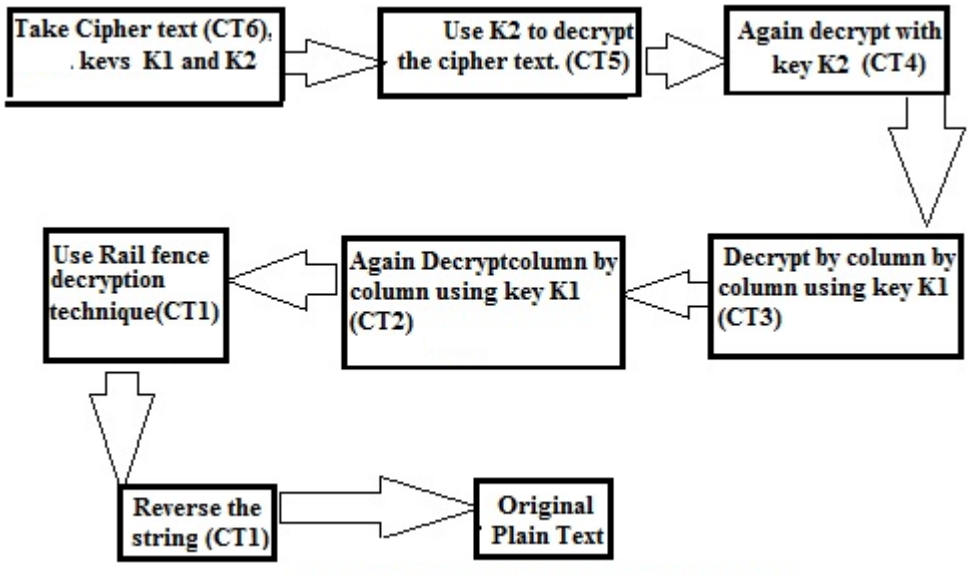
1) It takes cipher text, keys K1 and K2. The number of rows is also known to the receiver.
2) Use key K2 to decrypt the cipher text.
3) The output of step 2 is again decrypted with key K2.
4. Arrange the output of step 3 in a rectangular way, column by column using key K1
5. Read off the message row by row.
6. Again Arrange the output of step 5 in a rectangular way, column by column using key K1
7. Read off the message row by row.
8. Now here we use Rail fence decryption technique to decrypt output of step 7
9. Reverse the string that is output of Step 8
10. Output of step 9 is our required plaintext.

5. Block diagram showing Encryption of proposed Algorithm



Improved form of Rail Fence Cipher/Technique

6. Block diagram showing Decryption of proposed Algorithm



Decryption Technique of Proposed Algorithm

7. Example

7.1 Encryption

1. Let us suppose Our Plain Text is

SIMULATEDANNEALING
2. Reverse the String we get **GNILAENNADETALUMIS**
This is our First Cipher Text (CT1)
3 .Using Rail fence Encryption technique encrypt CT1 as usual we get **GIANAEAUINLENDTLMS** as shown this is (CT2)

G I A N A E A U I

N L E N D T L M S

READ AS ROWS WE GET

GIANAEAUINLENDTLMS

4. Suppose 4 3 2 1 be the key K1. We arrange cipher text (CT2) in rectangular way

Key K1	4	3	2	1
CT2:	G	I	A	N
	A	E	A	U
	I	N	L	E
	N	D	T	L
	M	S		

5. Read off message column by column, we get cipher text CT3. **CT3: NUELAALTIENDSGAINM**

6. Again 4 3 2 1 be the key K1. We arrange cipher text (CT3) in rectangular way

Key K1	4	3	2	1
CT3:	N	U	E	L
	A	A	L	T
	I	E	N	D
	S	G	A	I
	N	M		

7. Read off message column by column, we get cipher text CT4, **CT4: LTDIELNAUAEGMNAISN**

8. Now use key K2 = 2 to shift characters of cipher text CT4,we get CT5, **CT5: NVFKGNPCWCGIOPCKUP**

9. Repeat step 8 for cipher text CT5,We get CT6 **CT6: PXHMIPREYEIKQREMWR**

10. Our final encrypted message will be

CT: **PXHMIPREYEIKQREMWR**

7.2 Decryption

1. Use key K2=2 to decrypt cipher text CT.**: PXHMIPREYEIKQREMWR** we get

NVFKGNPCWCGIOPCKUP

2. Again use key K2=2 to decrypt the output of step 1,we get

LTDIELNAUAEGMNAISN

3Arrange output of step 2 in rectangular format, column by column, using key K1= 4 3 2 1

Key K1:	4	3	2	1
	N	U	E	L
	A	A	L	T
	I	E	N	D
	S	G	A	I
	N	M		

4. Now read off the message row by row, we get

NUELAALTIENDSGAINM

5. Arrange output of step 4 in rectangular format, column by column, using key K1= 4 3 2 1

Key K1:	4	3	2	1
	G	I	A	N
	A	E	A	U
	I	N	L	E
	N	D	T	L
	M	S		

6. Read off the message row by row, we get **GIANAEAUINLENDTLMS**

7. Using Rail Fence decryption Technique decrypt Output of Step 6 we get: **GNILAENNADETALUMIS**

G I A N A E A U I

N L E N D T L M S

READ NOW DIAGONALLY WE GET :**GNILAENNADETALUMIS**

8.Reverse the above string that we get from Step 7,we get original plain Text as shown

GNILAENNADETALUMIS ⇨ SIMULATEDANNEALING

REVERSING THE STRING WE GET ORGINAL PLAIN TEXT

8. Advantages of Proposed Algorithm

The proposed Rail fencer cipher employing a double substitution and Transposition method has following advantages over the simple Rail fence cipher.

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 double substitution.
5. Overcomes the limitations of simple Rail Fence cipher.

9. Disadvantages of Proposed Algorithm

It makes use of two keys as compared to the simple Rail fence cipher.

10. Conclusion and Future Scope

10.1 Conclusion

In this paper I have presented how to improve security of Rail fence Cipher to make it more secure and strong. Moreover the proposed algorithm has lot of advantages in achieving secure communication than Simple One.

10.2Future Scope

There is a need to do more research to boost the security of transposition techniques where we have a less permuted data, with minimum number of keys, so that it can be easily implemented. Substitution techniques also need research to enhance the security like Caesar cipher, Rail fence Cipher etc

References

[1] Andrew S. Tanenbaum, ”Computer Networks”, Fourth Edition, PEARSON.
[2] Atul Kahate (2009)”Cryptography and Network Security”, 2nd edition, McGraw-Hill.
[3] Stallings W(1999)”Cryptography and Network Security”,
[4] Ismail, A. I., Amin, M. and Diab, H., “How to Repair the Hill Cipher”, *J.Zhejiang Univ Sci. A, 7(12): pp. 2022-2030.*
[5] Cherenkov, A. G., “Secure Hill Cipher Modification SHC-M”, *Proc. Of the First International Conference on Security of Information and Networks* (SIN2007) 7-10 May 2007, Gazimagusa (TRNC) North Cyprus,Elci, A., Ors, B., and Preneel, B. (Eds.) Trafford publishing, Canada, 2008: pp. 34-37, 2007.

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 2009**. His interested areas of research are Neural Networks, Mobile computing, Network security, and Algorithms.