A Novel Approach for Encryption of Text Messages, Analysis and Implementation of Simple Columnar Transposition Cipher with Ceasar Cipher and Rail Fence Cipher in C/C++

Jawad Ahmad Dar, Amit Verma

1Research Scholar, Computer Science and Engineering, Kurukshetra University Kurukshetra, Haryana, India
2HOD CSE, NNSS Samalkha Group of Institution, Kurukshetra University Kurukshetra, Haryana, India

Abstract: This paper is a step toward developing an encryption system which can encrypt any text message securely. An ad-hoc network generally consists of nodes, on which sensors are embedded to provide security measures. The main challenge of these sensors is to provide security of data and also to work effectively within a limitation of power and memory. In every important sector these networks are used to collect information or transfer them with a high level of security. For this reason here we require a strong encryption Technique. Cryptography is an art and science of converting original message into unreadable 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 weaknesses and produce a cipher text that is hard to crack. Finally I have implemented this concept with the help of TURBO C++.

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 its own.

2. 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.
3. Block diagram for Encryption Algorithm

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.

4. Block diagram for decryption algorithm

4.1 Analysis

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

6. Result Analysis 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 \(2\times\text{simple columnar} + 2\times\text{substitution rail fence} + \text{stack operation}\).

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 \(T=n \times x\).
3. For Proposed New Algorithm \(T=2 \times x + 2 \times y + z + s\).

\(S=\) 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 \(T=2 \times 1 = 2\) for 2 rounds.
3. For Proposed New Algorithm \(T=2 \times 1 + 2 \times 1 + 1 + 1 = 5\) 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 \(T=2 \times 2 = 4\), for 2 rounds.
3. For Proposed New Algorithm \(T=2 \times 2 + 2 \times 2 + 2 + 2 = 10\).

7. 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.

8. Disadvantages of Proposed Algorithm

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

9. Graphical Analysis
10. Implementation in TURBO C++

A. Encryption

Enter plain text: KURUKSHETRA UNIVERSITY

Enter key (k1): 2654321

Cipher text by single Columnar Transposition (CT): hi y s n t k u i u e r r r u t e k e v

Enter key (k1) again: 

**Frequency Analysis of Standard English Letters**

![Frequency Analysis of Standard English Letters](image1)

**Frequency Analysis of Plain Text “KURUKSHETRA UNIVERSITY” for New Algorithm**

![Frequency Analysis of Plain Text](image2)

**Frequency Analysis of Cipher Text obtained From “simple columnar transposition”**

![Frequency Analysis of Cipher Text](image3)
B. Decryption

Enter the key value (k2): 3

Your cipher text after performing Single Substitution is (CT): nuywhqowadhow hldbo a

Your cipher text after performing Double substitution is (CT): qbozsktyqykeazo emm

Cipher text after applying rail fence (CT5): qbozskyyqemzozoykeazo

length of cipher Text(CT5) is: 21

Divide CT5 into two words, Enter the Words below

Enter first word:

Cipher text after applying rail fence (CT5): qbozskyyqemzozoykeazo

length of cipher Text(CT5) is: 21

Divide CT5 into two words, Enter the Words below

Enter first word: qbozskyy
enter the second word: yqemzozoykeazo

stack operation on word1 zmoozqytshq:
stack operation on word2 yqemzozoykeazo:

Final cipher Text (CT6) is: zmoozqytshqyqemzozoykeazo

Cipher Text Decrypted (Plaintext) is: Marathchetram University
### New Algorithm for Decryption of Text Messages

#### String Length of Cipher Text is: 21

Enter the first word: xnoozcqytdbqanoooklyjxz

Stack operation on first word: qybcypggzcom
Stack operation on second word: xhozyg鞍山
Cipher Text (CT1) is: qybcypggzcomoklyjxz

Cipher Text (CT1) after Performing Rail Fence Decryption: qybcypggzcomoklyjxz

Enter Cipher Text (CT1) for Double Substitution Decryption:

---

### Double Substitution Decryption

#### String Length of CT2 is: 21

Enter the key value (K2) same as used in Encryption: 3
Cipher Text (CT2) after Performing Single Substitution decryption is: moyxwhqwothhbaslldxoxa

Cipher text (CT2) after Performing Double Substitution Decryption is: krvtrensksa ngnttuhr

---

### Reverse Double Columnar Transposition

Enter CT2 below to Perform Reverse Double Columnar Transposition:
Enter the key K2:

7654321

Enter the message for encryption: hiysntkuieasrrutkev
hiysntkuieasrrutkev
hiysntkuieasrrutkev
hiysntkuieasrrutkev
hiysntkuieasrrutkev

Enter the message for Decryption:
11. Conclusion

In this 3rd paper, I have presented how to improve security of Simple columnar Cipher to make it more secure and strong, and finally implement this concept in C/C++. Moreover, the proposed algorithm has lots of advantages in achieving secure communication than Simple One. Simple columnar transposition cipher is the simplest Transposition method. It is also the weak cipher. Its 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.

12. Future Work

Implementation in MATLAB, in future we try to implement it in MATLAB using MEX Function.

13. Acknowledgment

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

References

[8] jawad ahmad dar, Enhancing the data security of simple columnar transposition cipher by Caesar cipher and Rail fence cipher technique. International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 5 No. 11 Nov 2014

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