Combination of Transposition and Alpha-Numeric Vigenere Table for Secure Communication

Akhil verma
NIT Kurukshetra, India.

Om Prakash Baghel
NIT Kurukshetra, India.

Dr. Sarika Jain
NIT Kurukshetra, India.

Abstract – Transposition and poly-alphabetic are two very good techniques for encryption. In this paper we enhance the capacity of Vigenere table for providing more secure communication. First transposition technique will be used in which plain text is divide into two equal parts, reverse both the parts separately, then shift each character forward by one; and as second step use alpha-numeric Vigenere table with a random key. By using this technique, the characters as well as numerical data or information can be encrypted. It combines the encryption process of Vigenere and some type of reasoning concept for getting the cipher text from given plain text and random key.

Index Terms – Cryptography, Transposition, Substitution, Poly-Alphabetic Cipher, Alpha-Numeric Vigenere Table, Encryption, Security, Cryptanalysis.

1. INTRODUCTION

The term Cryptography is the combination of two words crypto and graphy. The crypto word comes from Greek word Krypto, which is used for hiding or secret, and graphy for Graphein which mean writing. Now it becomes crucial to protect the data from outsiders. And in this case the role of cryptography comes in to the light. Cryptography allows us to exchange the data between sender and true receiver and not reformed by external elements. The process of cryptography involves an algorithm or technique and a key value convert the content of data in a different format so that no one other can read the information other than sender and the receiver. This encrypted data will be done with the help of well defined algorithm and key value. In this process, the algorithm will be same every time to encrypt the information because it is difficult to generate the different algorithm every time when the information is sent. The accomplishment of the cryptography technique is built upon the fact that the encrypted data should be tough to broken or cracked by cryptanalysis. Here the vigenere table is modified to make the cryptanalysis process more difficult.

In the previous used methods there are some drawbacks. In some paper, only the rearrangement is done which is not good idea to encrypt the data. In some paper the concept of prime number is used where the same prime number is used to encrypt the next information. Index value concept is also used to encrypt the data. Therefore to overcome this entire drawback a better method should be used to secure the confidentiality of the information. And for the betterment of the security we can apply complex method.

2. RELATED WORK

The previous existing paper used Transposition and Vigenere techniques to encrypt the information. Some persons worked on Transposition in many form like convert plain text in equal size blocks and rearrange them in predefined order which becomes the cipher text [2]. To create an extension of Vigenere Table many authors attempted like, Khalid (2012) proposed in alpha qwerty cipher by which he redesigns the vigenere table consist of 92 (including special symbols) characters instead of 26 alphabets. Kester (2013) proposed a hybrid crypto system based on vigenere cipher and columnar transposition cipher. In a paper of 2013 Transposition technique is used, first he calculate the index value of each alphabet and then add a fixed prime number in each index value then he take mod by 26. Then the resulting value is converted to corresponding alphabet [1]. Rahul Joharia et. al [3] first take a prime number and perform arithmetic operation with index of character in plain text then take binary of the result and convert it into decimal then into ASCII that will be cipher text.

3. PORPOSED MODELLING

We proposed a well secured encryption technique which is as followed. First we divide plain text in two equal parts and reverse them separately. Every character of resultant text is forwarded by one character. If there is Z then forward to A. After this, in poly-alphabetic, we use the alphabets and numeric value in vigenere table along with a random key. There are total 36 characters in alpha-numeric vigenere table, 26 alphabets and 10 digits (0-9). In the alpha-numeric vigenere table, the intersection point of row and column will be selected. Where

row represents the Key and column represents the intermediate cipher text. So we will get the Cipher text.

1. There is no facility in the table to represent the numerical value.

2 .To represent the numerical value we have to write them in alphabetic form e.g. 9 will be written as NINE. By this the length of the plain text will be increase and the length of key will also increase.

3. There is no way to represent special symbol in the table.

To remove these disadvantages we propose a new table in which digits will also be represented along with alphabets. Now, digits are appended after the alphabets. Here, the ranges of the alphabets (A-Z) are from (0-25) and the range of digits is from (0-9).

In this table, row represents key value and column value represents plain text value. Then the intersection of the key value and plain text value is the cipher text value.

In our method, we combine the Transposition and Vigenere technique for securing the information and convert the plain text into cipher text. Suppose our plain text is REPUBLIC. Then

Encryption Process:

Encryption is a process of hiding the data or information in encrypted form. In the process the plain text (information) that we want to send is encrypted which becomes the cipher text. And this encryption process can be done in multiple encryption level.

Step A. Transposition (Input: Plain Text, Output: Intermediate Cipher Text)

1. Partition: The given plain text will be divided into two half parts

   Ex. RUPUBLIC ------→ REPU BLIC

2. Reverse: Reverse the first one and then second one

   Ex. REPU BLIC------→ UPER CILB

3. Shifting: Each alphabet will be shifted by one by adding one to their corresponding values.

   Ex. UPERCILB----→ VQFSDJMC

Step B. Vigenere Table (Input: Intermediate Cipher Text Output: Cipher Text)

Generate Random Key: A random key will be generated using any predefined method which helps to encrypt the data. The length of the key will be 8. So the key will be repeated to encrypt the next plain text of length 8.

Ex. Suppose we are taking random key is ASPONXWO.

Encryption: Vigenere table will be used to encrypt the data. The encryption process is depicted in fig. 1.

Decryption Process:

Decryption is a process of getting the original information which is written in encrypted form. This is the reverse process of encryption. In this process the cipher text is decrypted to obtain the cipher (original text).

Step A. Vigenere Table (Input: Cipher Text, Output: Key)

In this process the Vigenere table and the key is used. In this, the row of the table represents the key value and column represents the cipher text. The intersection point of row and column corresponding to key value and cipher text is selected. This becomes the intermediate cipher text.

Step B. Transposition (Input: Intermediate Cipher Text, Output: Plain text)

In this, each alphabet of the intermediate cipher text is shifted backward by one. Then this cipher text is divided into two parts. After this, first part will be reverse and then second part will be reverse. Then we will be getting the original plain text. The Decryption process is depicted in fig.2.

4. RESULTS AND DISCUSSIONS

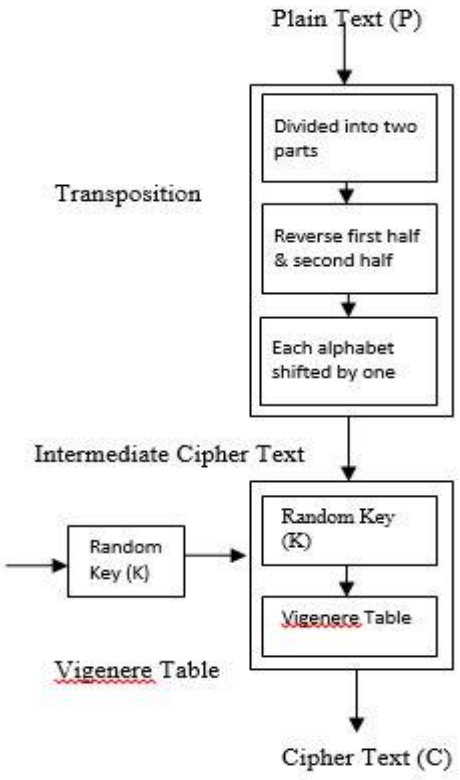

Fig.1.Encryption Process

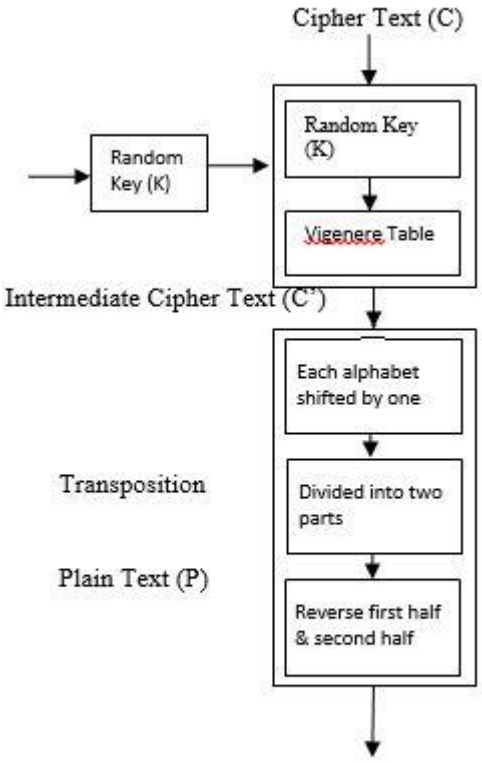

Fig.2. Decryption Process

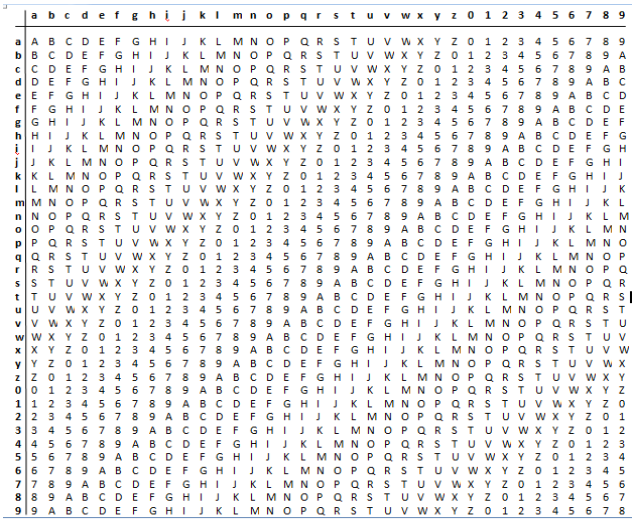

Fig.3. Modified Vigenere Table

5. CONCLUSION

This paper covers various available cipher techniques to encrypt the information. The extensive focus of this paper is on vigenere table. In this paper the vigenere table is enhanced by including the numeric value along with alphabets. By doing this, the alphabet and numeric value can also be decrypt and the process of decryption is also become difficult. In future, the table can also increase by including special symbol. So the process of decryption will be more complex. In future we will try to resolve the complexity of decryption process.

REFERENCES

[1] Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Ceasar and Vigenere cipher." Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on. IEEE, 2013.

[2] Toemeh, R., and S. Arumugam. "Breaking Transposition Cipher with Genetic Algorithm." Elektronika ir Elektrotechnika 79.7 (2015): 75-78.

[3] Johari, Rahul, et al. "Triplicative Cipher Technique." Procedia Computer Science 78 (2016): 217-223.

[4] Nacira, G-Z., and Araar Abdelaziz. "The/spl theta/vigenere cipher extended to numerical data." Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on. IEEE, 2004.

[5] Blair, Alan. "Learning the Caesar and Vigenere Cipher by hierarchical evolutionary re-combination." Evolutionary Computation (CEC), 2013 IEEE Congress on. IEEE, 2013.

[6] Pal, Jayanta Kumar, J. K. Mandal, and SomsubhraGupta. "Composite transposition substitution chaining based cipher technique." Advanced Computing and Communications, 2008. ADCOM 2008. 16th International Conference on. IEEE, 2008.