International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195151

An Extension to Traditional Qwerty Cryptographic Method

V. Vennila*[1], S. Umamaheswari[2]

*[1]Assistant Professor, Department of Information Technology, Bon Secours College for Women, Thanjavur, Tamil Nadu, India

[2]Assistant Professor, Department of Information Technology, Bon Secours College for Women, Thanjavur, Tamil Nadu, India

ABSTRACT

Cryptography comes from the Greek word kryptos which means hidden. The aim of our research is to provide secrecy for the data during transmission. In this we discuss about the qwerty cipher algorithm, its merits and demerits. The existing qwerty algorithm is based on the use of a keyboard which is not much secured. We have proposed an enhancement to the existing algorithm by using a diagonalized qwerty algorithm which is more secure and highly difficult for the intruder to understand or decrypt the cipher text, even if it is decrypted the result would be gibberish.

Keywords : *Transmission, Intruder, Decrypt, Cipher, Gibberish.*

I. INTRODUCTION

Cryptography is the strongest tool used for secret writing which is controlling against the security threats [6]. The study of encoding and decoding is called as cryptography [1]. In cryptography, a cipher is an algorithm consists of well-defined steps for performing encryption or decryption. In encryption process, the original plain text is coded into the cipher text and in the decryption process; the plain text is restored from the cipher text [2]. We need a strong encryption algorithm in order to encrypt the plain text into cipher text [7]. The sender and receiver must have obtained the secret key in a secure fashion and must keep the key secure. The process of encryption and decryption are shown below

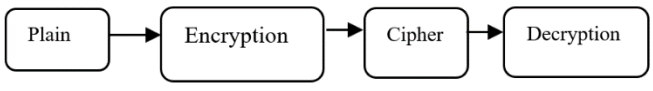

Fig 1. Encryption and Decryption process

Traditional ciphers consist of substitution or transposition techniques [2] [3]. In Substitution ciphers, replace letters in the plain text with other letters or symbols keeping the order as same. It maps plain text elements into cipher text elements [4].

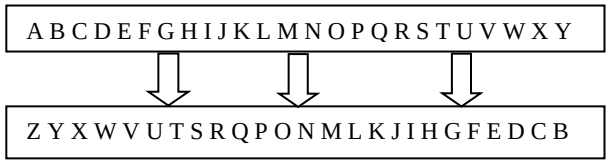

Fig 2. Substitution Cipher

In Transposition ciphers, keep all of the original letters intact, but mix up their order [5]. It transposes systematically the position of plain text elements. Transposition cipher hides the message by rearranging the order. Transposition cipher, just reorder the letters [8]. A character in the first position of plaintext may appear at 12th position in

cipher text, and a character at 6th position in the plaintext may appear at 18th position in cipher text.

Example of the transposition cipher is given bellow,

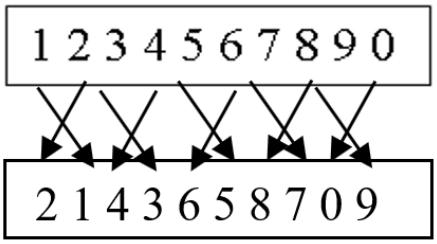

Fig 3. Transposition Cipher

II. EXISTING QWERTY CIPHER

QWERTY is the most common modern day keyboard layout. The name comes from the first six keys appearing on the top left row of the keyboard and read from left to right: Q-W-E-R-T-Y. In the existing qwerty cipher the top line is the keys on a keyboard from top left to bottom right, and the bottom line is the alphabet. It uses a seemingly random letters. The model of qwerty cipher is given bellow in which the plain text uses the qwerty keyboard to cipher the plain text. This cipher is easy to crack.

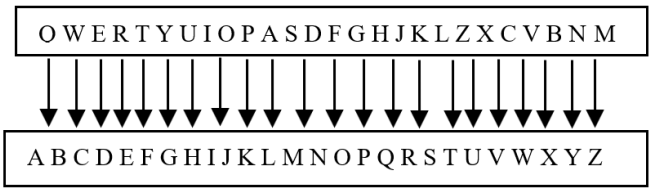

Fig 4. Top box represent keyboard keys and the bottom represent alphabets.

III. EXAMPLE FOR QWERTY CIPHER

Encryption Technique:

Plain text: SUN RISES IN THE EAST
Key: QWERTY
Cipher text: MGY DHMCM HY EPC CLME

Decryption Technique:

Cipher text: MGY DHMCM HY EPC CLME
Key: QWERTY
Plain text: SUN RISES IN THE EAST

IV. PROPOSED DIAGONALIZED QWERTY CIPHER

The proposed diagonalized qwerty cipher is the improvement of the qwerty cipher for making the communication more secure and it is difficulty for the hackers to hack the plain text. Diagonalized qwerty cipher is much secured when compared to the qwerty cipher.

Step 1. The model of a qwerty keyboard is taken.

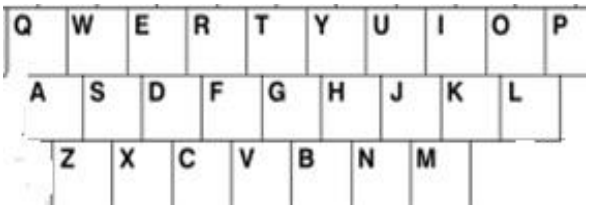

Fig 5. Model of a QWERTY keyboard

Step2. The model of diagonalized qwerty keyboard is framed.

In the qwerty cipher the keys in the keyboard are taken in an diagonal manner for framing an diagonalized qwerty keyboard. Which is more secured form of communication while transmitting message from a source to an destination. The mapping of diagonals is shown below.

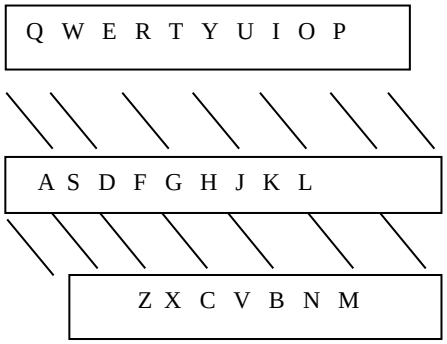

Fig 6. Mapping of qwerty keyboard.

The diagonalized qwerty keyboard is represented as 13 keys in each row for the purpose of encrypting/decrypting a plain text in a secured way.

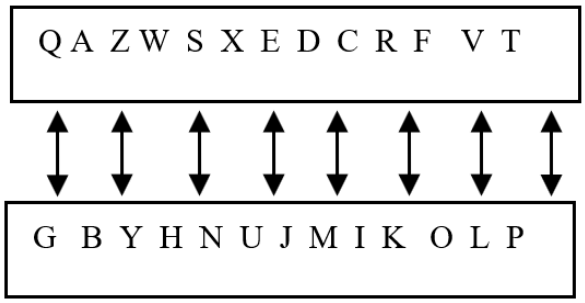

Fig 7. Representation of qwerty keyboard

V. EXAMPLE FOR DIAGONALIZED QWERTY CIPHER

Encryption Algorithm:

Plain text: CRYPTOGRAPHY IS MY FAVOURITE SUBJECT

Key: DIAGONALIZED QWERTY

Cipher text: IKZTPFQKBTWZ CN DZ OBLFXKCPJ NXAEJIP

Decryption Algorithm:

Cipher text: IKZTPFQKBTWZ CN DZ OBLFXKCPJ NXAEJIP

Key: DIAGONALIZED QWERTY

Plain text: CRYPTOGRAPHY IS MY FAVOURITE SUBJECT

VI. ADVANTAGES

This diagonalized qwerty cipher has various advantages over simple cipher. It is more difficult to cryptanalyze. The result cannot be easily reconstructed. Brute force attack cannot crack the code. Overcome all the limitations of the qwerty cipher.

VII. CONCLUSION

Finally through this paper we have pointed the traditional qwerty cipher merits and demerits. In order to overcome the demerits, we have proposed an extension to traditional qwerty cipher which can be used more efficiently while encrypting the plain text. However the used diagonalized qwerty algorithm can be improved for encrypting large amount of data.

VI. REFERENCES

[1]. ”Transformation of plain Text with two ciphers”,(Rajani Bala,Swapnika saxena,Sonal beniwal), Volume 3, Issue 5, May 2013.

[2]. “Implementation of Ceasar Cipher with Rail Fence for Enhancing Data Security”,(Ajit Singh, Aarti Nandal, Swati Malik), Volume 2, Issue 12 , December 2012.

[3]. “An Extension to Traditional Playfair Cryptographic Method”(Ravindra Babu, Uday Kumar, Vinay Babu, Aditya, Komuraiah), Volume 17, No.5, March 2011.

[4]. “An Improved Ceasar Cipher Algorithm”,(Ochoche Abraham, GaniyO.Shefiu), Volume 2, Issue-5,1198-1202.

[5]. "Alpha-Qwerty Cipher: An Extended Vigenere Cipher”(Khalid Imam Rahmani,Neeta Wadhwa, Vaibhv Malhotra), Volume 3, No.3, May, 2012.

[6]. William Stalling “Network Security Essentials (Applications and Standards)”, Pearson Education, 2004 .

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

[8]. William Stallings, Cryptography and Network Security, 5th impression, 2008.

Cite this Article : V. Vennila, S. Umamaheswari, "An Extension to Traditional Qwerty Cryptographic Method", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 340-342, January-February 2019. Available at doi : https://doi.org/10.32628/CSEIT195151 Journal URL : http://ijsrcseit.com/CSEIT195151