I. Extended Vigenère using double Transposition Cipher with One Time Pad Cipher

Anuja Priyam
Assistant Professor
Rama University, Kanpur India
anujapriyam@gmail.com

***Abstract* - Cryptography is a technique which converts any intelligible message into unintelligible message; it is used for secure communication between any two parties in any insecure channel like internet. The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. Vigenère is a simple form of polyalphabetic substitution and One Time Pad Cipher is the only existing mathematically unbreakable encryption [2].**

Research paper "EXTENDED VEGENERE CIPHER WITH TRANSPOSITION CIPHER", 2014 written by Anuja Priyam [1], proposed an extended Vigenère cipher in which encryption and decryption applied using 128 ASCII and 128 extended ASCII character with two keys. After message is encrypted by first key, transposition cipher is applied under certain order then adds some logical bits, now use second key for encryption and again apply transposition cipher, which gives more secure cipher text and vice-versa process applied in decryption part. This paper provides security in text field only but latest research said that there is an attack possible in key field also. To avoid this attack a secure approach is important in key field also.

To avoid this problem a new approach is using i.e One Time Pad cipher. In proposed cipher, key is secured by one time pad cipher. In encryption part, message is encrypted by using One Time Pad Cipher, in which a random key is generated, this key is XOR with the message and the key length is equal to the message length. After message is encrypted by first key, transposition cipher is applied under certain order then adds some logical bits, now use second key by One Time Pad Cipher for encryption and again apply transposition cipher, which gives more secure cipher text and vice-versa process applied in decryption part.

Index Terms – One Time Pad Cipher, Vigenère Cipher, Polyalphabetic Cipher, Encryption, Decryption, XOR Operation, Ceaser Cipher, Transposition Cipher .

I. INTRODUCTION

A good cryptographic system must always be considered so that they are as complicated to break as possible. It is feasible to build systems that cannot be broken in practice. This does not extensively increase system implementation effort; yet, some care and expertise is essential. Here, no excuse for a system designer to leave the system breakable. Any mechanisms that can be used to evade security must be made explicit, acknowledged, and carried into the attention of the end users. Theoretically, trying all probable keys in sequence can break any cryptographic technique. If applying brute force to try all keys is the only choice, the essential computing control increases exponentially with the length of the key. The areas of cryptography and cryptanalysis together are called cryptology [9, 10].

There are basically 4 objectives of cryptography described in [11].

A. Authentication: The process of proving the identity of host. (The most important forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are infamously weak.)

B. Confidentiality: This is the process by which no one can read the message apart from the intended receiver.

Integrity: Ensuring the receiver that the received message has not been altered in any way from the original message.

C. Non-repudiation: A method to prove that the sender actually sent this message.

II. RELATED WORK

One Time Pad Cipher

One-time pad (OTP), also known as the Vernam-cipher or the perfect cipher, it is a crypto algorithm where message is combined with a random key. It is the only existing mathematically unbreakable encryption [2].

Vigènere cipher

In the cryptography, it contains different methods among them the cryptography with the Vigenère matrix. Cipher was proposed by **BLAISE** DE VIGENÈRE in 1583 and has reigned about **03** centuries. The encoding by the Vigenère matrix is the type by substitution. It consists to employ a key composed by a word or by an expression. It utilizes a square composed by the alphabet 25 times in such way it signifies a square matrix where each cell contains a letter of the alphabet (it exists several variants of the matrix).Message is divided in blocks.

Length's block is equal length's key K. Maximal Length of key **is** 208 bits (26*8=208). Key length then could be 128,192,256 ... for one matrix.

Extended Vigenère Cipher with Transposition Cipher

This research paper is published by Anuja priyam[1]. In this paper a new, difficult to break methodology proposed. Vigenère cipher is extended to use 128 ASCII and 128 extended ASCII characters in the place of 26 alphabetic characters. This expansion makes Vigenère cipher further secure because if there is 26 characters in the algorithm and key size is one then possibility of making bruite-force attack is 26 and if there is 2 characters in key then possibility of making bruite-force attack becomes 26^2 similarly for n character key the possibility of making bruite-force attack becomes 26^n .

In extended Vigenère cipher number of character are 256 then if the key size is 1 then possibility of making bruite-force attack is 256 and if there is 2 characters in key then possibility of making bruite-force attack becomes 256^2 similarly for n character key the possibility of making bruite-force attack becomes 256^n , which is very hard to attack.

Transposition cipher is applied after encryption in the encrypted part both times, which makes extended Vigenère cipher more complex.

This paper makes text at two levels secure so it is difficult to achieve the original plain text, but there is an attack possible at key level because Vigenère has a drawback of key repetition.

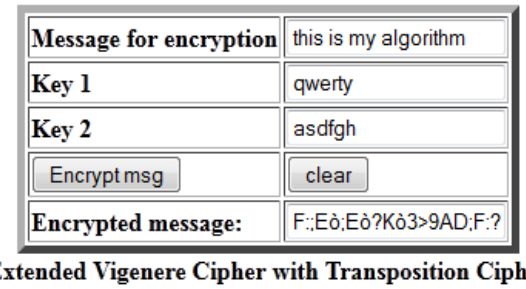

Figure 1: Encryption

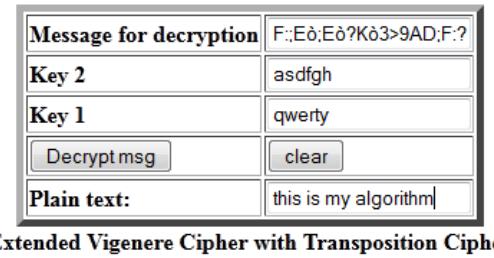

Figure 2: Decryption

Cipher for Secure Data Communication [3]

In this paper, a modified hybrid of Caesar Cipher and Vigenere Cipher with diffusion and confusion is proposed. The caesar Cipher and Vigenere Cipher have been modified and extended so as to contain alphabets, numbers and symbols and at the same time introduce a complete confusion and diffusion into the modified cipher developed. Classical ciphers can be made efficient and used for providing security by adding the properties possessed by the modern ciphers. In this paper, the characteristics of modern cipher were included to classical cipher

Hybrid Cryptosystem Based On Vigenère Cipher And Columnar Transposition Cipher [4]

This process employs use of both Vigenère cipher and columnar transposition cipher in its encryption process. The cipher text will first be operated on using columnar transposition cipher encryption. A selected key out of random will initiate the transposition process. At the end of this method, the resulting cipher text then becomes a key for the Vigenère process. By the encryption process, a table of Vigenère cipher was produced. The key is then used to manage on the message which is the plaintext to produce the last cipher text. This technique will end up making the final cipher text more difficult to be broken using existing cryptanalysis processes.

FPGA implementation of improved version of the Vigenère cipher [5]

In this cipher proposed algorithm want to disperse random bits between the bits of the plaintext and after that encrypt it by the Vigenère cipher. This makes the cipher text length twice. There is a function F(x) to find that how to disperse the random bits between the bits of plaintext. One way function, F(x), consisting of a prime number, p, a initiator less than p, g, and a positive constant less than eight, c. Prime number p should be more than the length of the plain text to prevent the possible detection of cycles. The eq. (1) shows F(x) where x represents the (n-1)th character of plain text that is started from 0. To reduce the size of the pad to a reasonable number, F(x) is reduced by performing F(x) mod 8. This allows the F(x) vary from 0 to 7.

$$F(x)=(g^x+c) \bmod p \qquad (1)$$

Alpha-Qwerty Cipher: An Extended Vigenère Cipher[6]

The alpha-qwerty cipher intends to extend the original 26 character Vigenère cipher to a 92 characters case sensitive cipher including digits and some other symbols commonly used in the English language and can be written from a computer keyboard. The alpha-qwerty cipher also changes the mapping sequence used in the Vigenère cipher. The mapping takes from a extended alphabet sequence to extended qwerty keyboard series. To decrypt the code repeal mapping takes place (compliment of encryption) that is from extended QWERTY keyboard to extended alphabet progression. Shortly this proposed version extends and rearranges the original Vigenère table, so making it much more complex than the existing one.

The greater character set allows more type of messages to be encrypted like passwords. This also enhances the key domain and hence provides more security.

Generalization of Vigenère Cipher [7]

A generalized way of Vigenère cipher is planned. In the place of using a Vigenère square for encryption and decryption, any two reversible four-sided figure matrices whose rows or columns are unique are used for encryption and decryption use. One matrix can be simply obtained from the other and hence any one of them can be used for encryption while the other can be derived from the other for decryption. This method avoids the necessity of using two separate reversible matrices for encryption and decryption process. Also, a new algorithm for generation of key-stream with or without using a random symbol sequence is proposed. The key streams are generated from small key words. The key streams are different for any slight difference of keywords either in content or length. Furthermore, a key stream would be effectively random and could be made as long as we please.

A Simple, Fast and Secure Cipher [8]

Vigenère cipher is a poly-alphabetic cipher once thought to be secure. The cipher is easy to understand and implement. However the weak point is that the cipher uses a key stream formed by a periodic repetition of a chosen keyword. This outcome in the replication of some character sequence at the multiple intervals of the length of the keyword used. By suspicious study and analysis of the repeated character sequences, the key length can be deduced. Once the correct length is known, the cipher text can be decrypted or deciphered. To conquer this awkwardness, a random key stream generation method is suggested. The cipher text produces using a random key is found be effective and detection of key length is approximately impossible. As well as, to provide more security, use of a random series of alphabet is also proposed for enciphering and decryption purposes. Experimental results show that the use of random tables and random key streams makes the Vigenère cipher stronger and resistant to cipher text only attack.

III. PROPOSED METHOD

In this paper, security of key with text is main concern. Vigenère cipher is extended to use 128 ASCII and 128 extended ASCII characters in the place of 26 alphabetic characters in research paper of Anuja Priyam[1], This paper provides security in text field only but latest research said that there is an attack possible in key field also. To avoid this attack a secure approach is important in key field also.

To avoid this problem a new approach is using i.e One Time Pad cipher. In proposed cipher, key is secured by one time pad cipher. In encryption part, message is encrypted by using One Time Pad Cipher, in which a random key is generated, this key is XOR with the message and the key length is equal to the message length. After message is encrypted by first key, transposition cipher is applied under certain order then adds some logical bits, now use second key by One Time Pad Cipher for encryption and again apply transposition cipher, which gives more secure cipher text and vice-versa process applied in decryption part.

.

Algorithm:

ENCRYPTION

1. Input the Message M.
2. Use One Time Pad Cipher to generate a key K_1.
3. XOR the key with message.
$$P=M \oplus K_1$$
4. Apply Extended Vigenère Cipher on above result
$$C_1= (P+K_1) \bmod 255$$
5. Apply transposition cipher and add some logical bits on C_1 to get C_2.
6. Generate a key K_2 by One Time Pad Cipher.
7. Again, apply Extended Vigenère Cipher on above result to generate unintelligible message
$$C_3= (C_2+K_2) \bmod 255$$
8. Now apply transposition cipher and replace bits with other bits under certain order to get cipher text C.

DECRYPTION

1. Input the cipher text C.
2. Use transposition cipher and replace bits with other bits under certain order to get C_3.
3. Apply second key into cipher text C_3 by using Extended Vigenère Cipher to get C_2.
$$C_2 = (C_3- K_2) \bmod 255$$
4. Apply transposition cipher and remove extra added logical bits on C_2 to get C_1.
5. XOR the K_1 with Cipher Text C_1
$$C' = C_1 \oplus K_1$$
6. Now apply extended Vigenère Cipher on C' to get plain text P.
$$P = (C'-K1) \bmod 255.$$

Here

P= PlainText

K_1= First Encryption key

K_2= Second Encryption Key

C= CipherText

IV. CONCLUSION

In this proposed algorithm, security of key with text is main concern. To secure text extended Vigenère cipher is used in which 128 ASCII and 128 extended ASCII characters in the

place of 26 alphabetic characters [1] are used. To secure key One Time Pad Cipher is used, in which a random key is generated; this key is XOR with the message to provide a secure result. One Time Pad Cipher is the only existing mathematically unbreakable encryption [2]

REFERENCES

[1]. Anuja Priyam "EXTENDED VIGENERE WITH TRANSPOSITION CIPHER" 2014 International Conference on "Computing for Sustainable Global Development", 5th – 7th March, 2014

[2]. http://users.telenet.be/d.rijmenants/en/onetimepad.htm#top

[3]. O.E. Omolara, A.I. Oludare and S.E. Abdulahi "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication", Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222-2863 Vol.5, No.5, 2014

[4]. Aphetsi Kester, "A HYBRID CRYPTOSYSTEM BASED ON VIGENÈRE CIPHER AND COLUMNAR TRANSPOSITION CIPHER"IJATER January 2013

[5]. Massoud Sokouti, Babak Sokouti, Saeid Pashazadeh and Leili Mohammad Khanli "FPGA implementation of improved version of the Vigenère cipher" Indian Journal of Science and Technology April 2010

[6]. Md. Khalid Imam Rahmani1, Neeta Wadhwa1 and Vaibhav Malhotra "ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER" Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012

[7]. Yumnam Kirani Singh, "GENERALIZATION OF VIGENÈRE CIPHER", ARPN Journal of Engineering and Applied Sciences VOL. 7, NO. 1, JANUARY 2012

[8]. Yumnam Kirani Singh, "A SIMPLE, FAST AND SECURE CIPHER", ARPN Journal of Engineering and Applied Sciences VOL. 6, NO. 10, OCTOBER 2011

[9]. William Stallings: "Cryptography and Network Security: Principles and Practices" 4th Edition, Prentice Hall".

[10]. Dara Kirschenbaum: "Advances in Cryptography History of Mathematics".

[11]. http://www.garykessler.net/library/crypto.html.