Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-6, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

An Approach for Enhancing the Security of Playfair Cipher

Sarita Singh [1] & Abhishek Dixit[2]
[1]M.Tech Research Scholar, [2]Assistant professor
[1,2] Dept. of Computer Science
Shri Ram Murti Smarak College of Engg. &Tech.,Aktu Lucknow, India

Abstract— *A new approch present secure transmission of message by modified version of Playfair cipher with Random number generator methods combining with Vigenere cipher. To develop this method of encryption technique, one of the simplest methods of random number generator methods called linear congruential generator has been used. Playfair cipher method based on polyalphabetic cipher. It is relatively easy to break because it still leaves much of the structure and a few hundred of letters of ciphertext are sufficient. In this we used double encryption and decryption technique. For the encryption, first encrypt the plaintext by vigenere cipher, and then result encrypt by playfair cipher. And result is called ciphertext. After that we are mapping random numbers to ciphertext and corresponding numbers will be transmitted to the recipient instead of alphabetical letter. This method rapidly increases security of the transmission over an unsecured channel.*

Keywords—,*Random number generator method, vigenere cipher,playfair cipher*

I INTRODUCTION

Encryption as provided in **[4]** is a process of converting messages, information, or data into a form unreadable by anyone except the intended recipient.

Encrypted data must be deciphered, or decrypted, before it can be read by the recipient. The root of the word encryption—crypt—comes from the Greek word kryptos, meaning hidden or secret. In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures, this dissertation work highlights in chronology the history of Cryptography throughout centuries. For different reason, humans have been interested in protecting their messages.

Threats to computer and network security increase with each passing day and come from a growing number of sources. No computer or network is immune from attack. A recent concern is the susceptibility of the power grid and other national infrastructure to a systematic, organized attack on the United States from other nations or terrorist organizations.

Encryption, or the ability to store and transmit information in a form that is unreadable to anyone other than intended persons, is a critical element of our defense to these attacks. Indeed, man has spent thousands of years in the quest for strong encryption algorithms.

ENHANCING SECURITY USING PLAYFAIR CIPHER.

There are various algorithms that are used so far for encryption of different file format like text file, audio file, images and videos. While various algorithms are available for encryption. Some of the algorithms that are used for encryption are RSA (Rivest, Shamir, Aldeman), DES (Data Encryption Standard), Playfair cipher and Vignere cipher.The algorithm used in this dissertation work for encryption and decryption of text file is Playfair cipher and vigenere cipher which is more efficient in terms of time and security.

This leads to efficient encryption, which is more refined than the existing techniques. We use Vigenere cipher, Playfair cipher and Linear congruential generator method to enhance the security of classical playfair cipher. First encrypt the plaintext by vigenere cipher with keyword and then result encrypt by playfair cipher with another keyword. We get the cipher text. Linear congruential generator method generate unpredictable sequence of number. This sequence of number depends on the multiplier and increment. We mapping the sequence number to cipher text and find corresponding sequence of

number. We transmit sequence of number to the receiver instead of alphabets.

At the receiver side, receiver receive the sequence of number, and find the cipher text corresponds to sequence of these numbers. First decrypt the cipher text by playfair cipher with same encryption keyword and then result decrypt by vigenere cipher with same encryption keyword. Then we get the original plaintext. This technique increases the security of playfair cipher.

Difficulties with Classical Approach

Difficulties with the classical playfair cipher are given below..

- The traditional playfair cipher uses only 25 uppercase alphabets only.
- One letter has to be omiited and can not be reconstructed after decryption.
- There are only 26 character use this 26*26=676 diagrams will be produced so it was

  very difficult to identify the particular structure.
- It can be easily cracked if there is enough text
- Calculating the key stream can be very easy if plain text and cipher text are known

I. USES OF NEW APPROCH FOR PLAYFAIR CIPHER SECURITY

Data Encryption helps to you protect the privacy of your email messages, documents and sensitive files. Encryption works with both text information and files. We just have to select what we want to encrypt, and encryption and decryption helps us keep documents, private information and files in a confidential way.

Encryption is also used to ensure the confidentiality of the file and documents from the adversary so that the files and documents are remained in a secure way.

Data encryption is also used to provide the security and safety of the files and other important documents from the opponent so that while sending the files or documents nobody else other than the recipient can see it. This work has the similar mechanism to provide the security and safety of the files by using a classical Playfair cipher and Vignere cipher.

Today_s the prominence of internet day to day increased a lot and the transfers of files and confidential information over the internet demands the security and safety of the files and this can be accomplished by using encryption and decryption. In current scenario, encryption and decryption are most widely used in every field like defence, banking and transaction.

II. LITERATURE REVIEW

- For the security purpose to propose a introduce double myszkowski transposition on a modified 6*6 playfair matrix includes the all the alphabets along with the single digit numbers. And comparison with the classical playfair cipher proves the enhanced security of the proposed algorithm.[1]
- For the security purpose present a new approach for secure transmission of message by modified version of play fair cipher combining with random number generator method. To develop this method of encryption technique , one of the simplest methods of random number generator methods called linear feedback shift register(LFSR) has been used.[2]
- A new algorithm to present a new technique for secure transmission of message by modified version of playfair cipher combining with random number generator and transpose of matrix concept provide to generate random number sequences and placing it into 6*6 matrix.then finding the transpose of it and mapping it to secret key of playfair cipher method.Corresponding number s will be transmitted to the receiver instead of alphabetic numeric key. This method increases security of the transmitted key over unsecured transmission media**.[**3]
- A new algorithm implemented a new technique which includes a rectangular matrix having 10 columns and 9 rows and six iteration steps for encryption as well as decryption purpose, this 10*9 rectangular matrix includes all alphanumeric characters and some special characters.[4]
- A new proposed algorithm is an enhancement to the existing algorithm that uses 16*16 matrix to pick cipher characters. It makes use of alphabets both

lower and uppercase characters, number and special characters for constructing the contents of the matrix.[5]

- A new approach to provide diagrams or groups of 2 letters in the plain text is converted to cipher text diagrams during encryption using a key. similarly during decryption cipher text diagrams are converted to plain text diagrams using the same key.[6]
- A new algorithm with modification of playfair cipher. The original 5*5 matrix playfair cipher is modified to 7*4 matrix playfair cipher in which two symbol * and # are included. And also this method can be extended to encrypt and decrypt the message of any languages by taking a proper size matrix.[7]
- A new algorithm proposed a 6*6 playfair cipher and then coupled it with linear feedback shift register based unique random number generator,6*6 playfair cipher supports all 26 alphabets(A-Z)and 10 digits(0-9) which eliminate the limitation of 5*5 playfair in which "i" and "j"both character could not appear at the same time[8].

A new approach for secure transmi Literature review

- For the security purpose to propose a introduce double myszkowski transposition on a modified 6*6 playfair matrix includes the all the alphabets along with the single digit numbers. And comparison with the classical playfair cipher proves the enhanced security of the proposed algorithm.[1]
- For the security purpose present a new approach for secure transmission of message by modified version of play fair cipher combining with random number generator method. To develop this method of encryption technique , one of the simplest methods of random number generator methods called linear feedback shift register(LFSR) has been used.[2]
- A new algorithm to present a new technique for secure transmission of message by modified version of playfair cipher combining with random number generator and transpose of matrix concept provide to generate random number sequences and placing it into 6*6 matrix.then finding the transpose of it and mapping it to secret key of playfair cipher method.Corresponding number s will be transmitted to the receiver instead of alphabetic numeric key. This method increases security of the transmitted key over unsecured transmission media.[3]
- A new algorithm implemented a new technique which includes a rectangular matrix having 10 columns and 9 rows and six iteration steps for encryption as well as decryption purpose, this 10*9 rectangular matrix includes all alphanumeric characters and some special characters.[4
- A new proposed algorithm is an enhancement to the existing algorithm that uses 16*16 matrix to pick cipher characters. It makes use of alphabets both lower and uppercase characters, number and special characters for constructing the contents of the matrix.[5]
- A new approach to provide diagrams or groups of 2 letters in the plain text is converted to cipher text diagrams during encryption using a key. similarly during decryption cipher text diagrams are converted to plain text diagrams using the same key.[6]
- A new algorithm with modification of playfair cipher. The original 5*5 matrix playfair cipher is modified to 7*4 matrix playfair cipher in which two symbol * and # are included. And also this method can be extended to encrypt and decrypt the message of any languages by taking a proper size matrix.[7]
- A new algorithm proposed a 6*6 playfair cipher and then coupled it with linear feedback shift register based unique random number generator,6*6 playfair cipher supports all 26 alphabets(A-Z)and 10 digits(0-9) which eliminate the limitation of 5*5 playfair in which "i" and "j"both character could not appear at the same time[8].
- A new approach for secure transmission of message by modified version of playfair cipher combining with random number generator methods. Here we are mapping random numbers to secret key of playfair cipher method and corresponding numbers will be transmitted to the recipient instead of alphabetical letter [9].

V. Proposed Algorithm

. This technique enhance the security of Playfair cipher to use the double encryption at the sender side and double decryption technique at the receiver side. At the sender side, First encrypt the

message using vigenere cipher with key k1 and then result encrypt using playfair cipher with key k2, then result is called ciphertext . At the receiver side, this ciphertext is decrypt using the double decryption, first using the Playfair cipher with the key k2, and then using the vigenere cipher with key k1, and get the original message.

Steps for Encryption

1. The alphabets and numbers are arranged in 6x6 Playfair key matrix based on keyword.
2. Generate 6x6 unique random number matrix using the linear congruential generator methods.
3. Map the Playfair key matrix with the random number matrix.
4. Encrypt the plain text P using Vigenere cipher with key k1 and get immediate result X
5. Then this result encrypt using Playfair cipher with keyword k2 and get ciphertext C
6. Find the corresponding number to ciphertext C, the sequence of these number is transmit to receiver.
7.

Steps for Decryption

1. Receiver receive the sequence of numbers.
2. Find the ciphertext C corresponding to sequence of number.
3. Decrypt the ciphertext C using the Playfair cipher with keyword k2 and get intermediate result X.
4. **4.** And then X is decrypted by vigenere cipher with key k1 and get plaintext P.

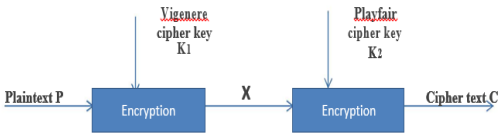

Figure 1 Encryption using vigenere cipher and playfair cipher

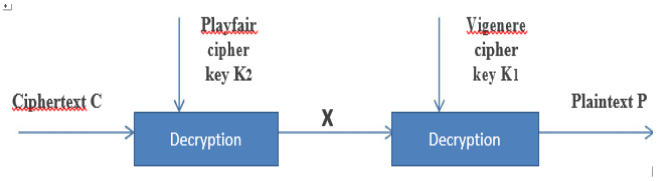

Figure 2 Decryption using Vigenere cipher and Playfair cipher

VI. Analysis of proposed method

The classical Playfair cipher is not secure because it produces only 676 structures. This proposed methodology rapidly increases the security of the ciphertext because we use double encryption and double decryption. And also the inner structure of this method is very simple. Currently many algorithms are available for encryption but it requires many complex rounds like DES, AES etc. AES and DES use two concepts for security, confusion and Diffusion. Confusion means relationship between plaintext and ciphertext as complex as possible. Diffusion means mask the statistical properties of data in the ciphertext. Our approach allows confusion and diffusion can be easily incorporated to Vigenere cipher and Playfair Cipher. The linear congruential generator method can be used to generate random number sequences. Unpredictable different random sequences can be produced from linear congruential generator method by varying multiplier and increment. Increasing modulus value can increase the cycle length. It can be easily implemented with advent of new computer. The implementation of linear congruential generator method in hardware and Software is very easy. The cost is very less and also speed is considerably very high compare to other methods. This method of encryption does not increase size of the ciphertext. For areas with low bandwidth or very less memory storage this method can be used. The classical Playfair cipher is relatively easy to break because it still leaves much of the structure of the plaintext language. This method of incorporating random sequences can also be applied to other ciphers.

VII. CONCLUSION

To implement modified Playfair cipher using random number generation. We use linear congruential generator method, that can be used to generate unpredictable different random sequences by varying increment and multiplier.

The classical Playfair cipher is not secure because it produces only 676 structures.We use vignere cipher and Playfair cipher for encryption and decryption. We are mapping random number sequence to ciphertext and corresponding number will be transmitted to the recipient instead of alphabetical letter. This method increases security of the transmission over unsecured channel. Because we use 6x6 matrix that produces 1296 structures and also use vigenere cipher that produces 456976.The total structures produces will be 1296*456966 = 592240896. The future work shall consider, to increases the size of matrix to include the special character.

REFERENCES

[1]Bhowmick, Anirban, Anand Vardhan Lal, and Nitish Ranjan. "Enhanced 6x6 Playfair Cipher using Double Myszkowski Transposition." *International Journal of Engineering Research and Technology*. Vol. 4. No. 07, July-2015. IJERT, 2015.

[2] Negi, Ashish, et al. "Cryptography Playfair Cipher using Linear Feedback Shift Register." *IOSR Journal of Engineering* 2.5 (2012): 1212-1216.

[3] Kumar, Vinod, et al. "Modified Version of Playfair Cipher Using Linear Feedback Shift Register and Transpose Matrix Concept'." *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* 3 (2013).

[4] Behrouz A. Forouzan. Cryptography and Network Security, Special Indian Edition 2007, The McGraw- Hill companies, New Delhi.

[5] Bhattacharyya, Subhajit, Nisarga Chand, and Subham Chakraborty. "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps."

[7] Dhenakaran, S. S., and M. Ilayaraja. "Extension of Playfair Cipher using 16X16 Matrix." *International Journal of Computer Applications* 48.7 (2012).

[8] Basu, Sanjay, and Utpal Kumar Ray. "Modified Playfair Cipher using Rectangular Matrix." *IJCA (0975-8887) Volume* (2012)

[9]. Alam, A. Aftab, B. Shah Khalid, and C. Muhammad Salam. "A Modified Version of Playfair Cipher Using 7? 4 Matrix." *International Journal of Computer Theory and Engineering* 5.4 (2013): 626.

[10] Kaur, Amandeep, Harsh Kumar Verma, and Ravindra Kumar Singh. "6 X 6 Playfair Cipher using LFSR based Unique Random Number Generator." *International Journal of Computer Applications* 51.2 (2012).

[11] Murali, Packirisamy, and Gandhidoss Senthilkumar. "Modified version of playfair cipher using linear feedback shift register." *Information Management and Engineering, 2009. ICIME'09. International Conference on*. IEEE, 2009.
6/7/2017