ISSN:2320-0790

compusoft
An International Journal of Advanced Computer Technology

A GENERALIZED VERSION OF PLAY FAIR CIPHER

Jitendra Choudhary,
Computer Science Department,
SSSIST, Sehore, INDIA
jitendrachoudhary11@gmail.com

Prof. Ravindra Kumar Gupta,
Computer Science Department,
SSSIST, Sehore, INDIA,
ravindrap84@rediffmail.com

Dr. Shailendra Singh,
Computer Science Department,
NITTTR, Bhopal, INDIA,
ssingh@nitttrbpl.ac.in

Abstract: In this paper, we have generalized and modified the play fair cipher. We have introduced confusion and diffusion. The cryptanalysis carried out in this analysis has shown that the proposed play fair cipher is a strong one.
The role of cryptography in today's world is increasing day by day. Information is flowing from are place to another on the network. One most common cryptography technique is substitution cipher. Play fair is most common substitution cipher. In this paper, we present a generalized version of play fair ciphers. Encryption/decryption is a very popular task. We also explain the fundamentals of sequential cryptography.

Keywords: generalized playfair cipher, encoding Decoding, security, cryptanalysis.

I. INTRODUCTION

In this age of universal electronic connectivity, of viruses and hackers, of electronic fraud, there is indeed no time at which security does not matter. The explosive growth in computer systems and their interconnection via network has increased the dependence of both organizations and individuals on the information stored and communicated using these systems which intern has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Also the disciplines of cryptography and network security have matured, leading to the development of practical, readily availablenapplications to enforce network security. Cryptography is the design of certain techniques for ensuring the secrecy and/or authenticity of information. Earlier the requirement of information security within an organization was primarily provided by physical and administrative means [1]. But the concept of network security became quite evident with the introduction of computers and later with introduction of distributed systems. The need of cryptographic algorithm is to avoid threat to integrity confidentiality and availability.

Symmetric Cipher Technique is also known as Conventional, Single key, Secret Key, One – key and classical encryption techniques.

II. Related Work:

In the variation proposed by Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya , P. Komuraiah [8] the 5 x 5 matrix has been replaced by 6 x 6 matrix. In this system all the uppercase alphabets as well as numbers can be handled. However lowercase letters, white space and other printable characters cannot be handled.

In the variation proposed by Shiv Shakti Srivastava, Nitin Gupta [9] the 5 x 5 matrix has been replaced by 8 x 8 matrix. After converting plain text to cipher text using the 8 x 8 matrix, the characters are converted to the corresponding ASCII values in decimal and then to corresponding binary values of 7 bits. Linear Feedback Shift Register is then applied to get the final cipher text.

In the variation proposed by Gaurav Agrawal, Saurabh Singh, Manu Agarwal [10] the frequency of each alphabet in the text to be encrypted is calculated. The 2 letters with the least frequency are combined instead of combining I and J. The 5 x 5 matrix is formed by inserting the keyword without duplication of letters, the combined letters and lastly the other letters.

In the variation proposed by Packirisamy Murali and Gandhidoss Senthilkumar [11] random numbers are mapped to secret key of Playfair cipher method 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.

In the variation proposed by Harinandan Tunga, Soumen Mukherjee [12] multiple array of structure has been used to store the information about the spaces and the other to store the information about whether an „X" has appeared in the alphabet matrix. Secondly the key table has been extended from 5 X 5 matrix to 16 X 16 matrix form. Finally, the 16 X 16 algorithm has been modified so that it can incorporate shifting of rows and columns of the 16 X 16 matrix to ensure that the encrypted text contains any ASCII ranging between 0 – 255.

In the variation proposed by V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani [13] it is assumed that the characters of the plain text belong to the set of ASCII characters denoted by the codes 0 to 127. A substitution table is constructed in an appropriate manner and the rules 1 to 3 are modified suitably for encryption and decryption. Further, interweaving is introduced and iteration which will lead to a lot of confusion and diffusion.

III. Existing Playfair Algorithm using 5x5 Matrix

The existing playfair cipher working on 5x5 matrix is constructed with a keyword “CRYPTO”. The Table 1 below shows the construction of 5x5 matrix using the keyword “CRYPTO” plus the uppercase alphabets satisfying the rules of preparing the table. The matrix is first filled by the keyword from left to right and the remaining cells are filled by the uppercase alphabets ignoring the letters of keyword.

Table 1. Playfair 5x5 Matrix

C	R	Y	P	T
O	A	B	D	E
F	G	H	I/J	K
L	M	N	Q	S
U	V	W	X	Z

In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies an pair of plaintext characters. So, it needs always even number of characters in plaintext message. In case, the message counts odd number of characters a spare letter X is added at the end of the plaintext message.

Further repeating plaintext letters in the same pair are separated with a filler letter, such as X, so that the words COMMUNICATE would be treated as CO MX MU NI CA TE.

Rules

a. Plaintext letters that fall in the same row of the matrix are replaced / substituted by the letter to the right, with the first element of the row circularly following the last. For example pt is encrypted as TC.

b. Plain text letters that fall in the same column are replaced by the letter beneath, with the top element of the row circularly following in the last. For example, cu is encrypted as OC.

c. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, oh becomes BF, and fd becomes IO (or JO, as the enciphered wishes) [2].

Limitations of 5x5 Matrix

- It considers the letters I and J as one character.
- 26 letters alone can take as keyword without duplicates.
- Space between two words in the plaintext is not considered as one character.
- It cannot use special characters and numbers.
- It only uppercases alphabets.
- A spare letter X is added when the plaintext word consists of odd number of character. In the decryption process this X is ignored. X is a valid character and creates confusion because it could be a part of plaintext, so we cannot simply remove X in decryption process.
- X is used a filler letter while repeating letter falls in the same pair are separated.

IV. Proposed System:

We analyzed the current systems and found that they have some limitations. These limitations are as follows.

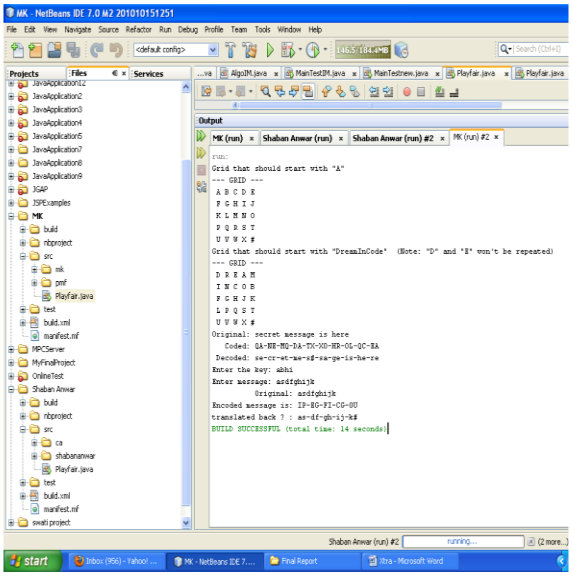
- It does not suit for all the applications having odd number of characters

- The plaintext which is needed to be encrypted should contain even number of characters otherwise the play fair cipher will not be able to divide the given plain text into the pair of characters.
- Also the numbers of characters are fix in all previous versions. In 5 X 5, these are 25, in 6 X 6 these are 36 and soon.

Algorithm of Generalized Play Fair:

1. First of all identify the number of characters in the language.
2. Identify the size of the generalized matrix . it will be computed as follows:
   SIZE = No of Characters + 2
   Here # and * are two additional characters. The # symbol is used for odd pair and the * symbol is used for repeating characters.
3. Create Diagraphs
4. Build mapping of the characters with the Unicode
5. Fill all the cells of the generalized matrix with the characters
6. Select a key and perform the encryption
7. Perform decryption. Ignore # symbol in the result.

V. Calculated result by applying generalized Playfair :



```
run:
Grid that should start with "A"
--- GRID ---
 A B C D E
 F G H I J
 K L M N O
 P Q R S T
 U V W X #
Grid that should start with "DreamInCode"  (Note: "D" and "E" won't be repeated)
--- GRID ---
 D R E A M
 I N C O B
 F G H J K
 L P Q S T
 U V W X #
Original: secret message is here
   Coded: QA-NE-MQ-DA-TX-XO-HR-OL-QC-EA
 Decoded: se-cr-et-me-s#-sa-ge-is-he-re
Enter the key: abhi
Enter message: asdfghijk
          Original: asdfghijk
Encoded message is: IP-EG-FI-CG-OU
translated back ? : as-df-gh-ij-k#
BUILD SUCCESSFUL (total time: 14 seconds)
```

Result: Grid that should start with "A"

--- GRID ---

A B C D E

F G H I J

K L M N O

P Q R S T

U V W X #

Grid that should start with "DreamInCode" (Note: "D" and "E" won't be repeated)

--- GRID ---

D R E A M

I N C O B

F G H J K

L P Q S T

U V W X #

Original: secret message is here

Coded: QA-NE-MQ-DA-TX-XO-HR-OL-QC-EA

Decoded: se-cr-et-me-s#-sa-ge-is-he-re

Enter the key: abhi

Enter message: asdfghijk

Original: asdfghijk

Encoded message is: IP-EG-FI-CG-OU

translated back ? : as-df-gh-ij-k#

BUILD SUCCESSFUL (total time: 14 seconds)

Advantages of the proposed System

- It is a generalized and modified play fair cipher, which will suit any language
- The proposed cipher will also suit for all the applications having odd number of characters
- Unlike all previous versions, the proposed play fair can also contain any number of characters.
- It will be able to divide any given plain text (even or odd) into the pair of characters.
- It will be more secure. It contains confusion and diffusion. It is proved the forthcoming cryptanalysis section.

Cryptanalysis:

In the science of cryptology, the different types of cryptanalytic attacks are (1) Cipher text only (Brute force) attack, (2) Known plaintext attack and (3) Chosen plaintext/cipher text attack.

1. Brute force attack the size of the key domain is (M X N)! (factorial M X N). Thus brute force attack will be very difficult for the modified Playfair cipher when the value of M X N is large.
2. Known plaintext attack: We know the plaintext at the beginning of the iterative procedure, and the ciphertext at the end of the iteration. And in between, as we have transpositions in form of confusion and diffusion (# and *). It makes finding key or plaintext more difficult.
3. Chosen plaintext/ciphertext attack: Obtaining the key is relatively straightforward if both plaintext and ciphertext are known.

VI. Conclusion

In this paper, we have analyzed the current play fair cipher. We have also discussed the limitations of the present play fair systems. We have proposed a generalized play fair cipher; it will be able to encrypt plain text of any natural language.

References:

[1] Andrew S. Tanenbaum, Networks Computer, 5th edition, Pearson Education, ISBN-10: 0132553171.

[2] William Stallings, “Cryptography and Network Security: Principles and Practice”, 4th Edition, Prentice Hall, 2006.

[3] Aftab Alam, Sehat Ullah, Ishtiaq Wahid, & Shah Khalid, “Universal Playfair Cipher Using MXN Matrix”. International Jourmal of Advanced Computer Science, Vol.1, No.3, Pp.113-117, Sep.2011.

[4] Ravindra Babu K, S.Uday Kumar, A. Vinay Babu, I.V.N.S. Aditya, P.Komuraiah, “An Extension to Traditional Playfair Cryptographic Method”. International Journal of Computer Applications (0975 – 8887), Volume 17- No.5, March 2011.

[5] Dhenakaran, Ilyaraja, “Extension of play fair cipher” IJCA, pg no 37-41, June 2012.

[6] http://en.wikipedia.org/wiki

[7] http://unicode.org/standard/WhatIsUnicode.html

[8] Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya , P. Komuraiah “An Extension to Traditional Playfair Cryptographic Method”, International Journal of Computer Applications (0975 – 8887) Volume 17– No.5, March 2011.

[9] Shiv Shakti Srivastava, Nitin Gupta “A Novel Approach to Security using Extended Playfair Cipher”, International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.

[10] Gaurav Agrawal, Saurabh Singh, Manu Agarwal “An Enhanced and Secure Playfair Cipher by Introducing the Frequency of Letters in any Plain text”, Journal of Current Computer Science and Technology Vol. 1 Issue 3 [2011]10-16

[11] Packirisamy Murali and Gandhidoss Senthilkumar “Modified Version of Playfair Cipher using Linear Feedback Shift Register”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008

[12] Harinandan Tunga, Soumen Mukherjee “A New Modified Playfair Algorithm Based On Frequency Analysis”, International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 2, Issue 1, January 2012)

[13] V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani “A Modified Playfair Cipher Involving Interweaving and Iteration”, International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009 1793-8201