International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 5, Issue 3, 2019 Special Edition: *Science, Applied Science, Teaching and Education*

Modification of Playfair Chiper to Strengthen Playfair Chiper Algorith with 2 Key Layer Matrix (KLM) Method

Edi Winarko[1]

Study Program of Mathematics, Departement of Mathematics, Airlangga University, Surabaya, Indonesia

Email: edi_winarko@fst.unair.ac.id

Abstract

Playfair ciphers are one of the popular classic encryption methods that are difficult to manipulate manually, but this method has many drawbacks because they only use uppercase or lowercase letters. This makes the combination easier to be guessed, even though it takes time. This study attempts to modify the playfaircryptographic algorithm key matrix with the Key Layer Matrix (KLM) method, by changing the 5x5 key matrix in 2 layers, so that the key combination becomes 25 x 25 consisting of upper and lower case letters. To perfect this modification, the key used is two, the key for layer 1 and the key for layer 2. The results of the calculations, with this method, make the complexity of the process slower, but makes it harder to hack.

Keywords: *Playfair, cryptanalysis, encryption, decryption, cryptography*

Introduction

One of the most popular classical methods in cryptography is the Playfair Cipher Algorithm. This method is a simple encryption method but has a large combination of possibilities and is very difficult for manual analysis. Although it is quite difficult to solve, Playfair can still be solved by looking for information on the frequency of occurrence of the character pairs (bigram). Therefore, Playfair is a symmetric encryption technique that is included

in the digraph substitution system. In the playfair algorithm the main components needed, in the process of encryption and decryption, are cipher tables and default tables in the form of matrices with 5x5 orders whose elements are in capital letters from A-Z but negating the letter J.

Playfair is a classic algorithm that is relatively easy to solve just by knowing the ciphertex. Without knowing the cipher table, one can guess the bigram based on the frequency of the occurrence of letter pairs (Alam, Khalid, & Salam, 2013; Choudhary, Kumar, & Singh, 2013) Further, the Playfair default table does not accommodate lowercase letters (az), numbers (0-9), or special characters in plaintext (Babu, Kumar, & Babu, 2011; Kumar, kr Upadhyay, Mishra, & Singh, 2013; Shrivastava, Chouhan, & Dhawan, 2013). However, this algorithm is still interesting to study by modifying both the order size of the default table matrix and adding the required characters.

The development of Playfair Cipher shows a large improvement over monoalphabetic ciphers. An Identifying diagrams is more difficult than individual letters. In a monoalphabetic password, the attacker searches in only 26 letters. But by using Playfair Cipher, the attackers must look at 26 * 26 = 676 diagrams. (Srivastava, 2011; Murali, 2009)

One of the papers discussing the power of encryption belongs to Haridanan (2014), according to Haridanan, increasing the size of the playfair matrix can complicate the hacking processes. (Harinandan et al, 2014).

A lot of research has been done to strengthen the Playfair Algorithm by modifying the default matrix size. There are those who have changed the size of the matrix to 6x6 (Choudhary et al., 2013), change it to a matrix measuring 7x4 (Alam et al., 2013), and changed the size of the matrix to 16x16 (Eweoya, Daramola, & Omoregbe, 2013).

In development of the model, a 7 x 7 matrix is considered for extended character

support and additional features. Primarily, the matrix supports 49 characters but, the model uses 47 of them for general purpose and 2 for special purpose. The character set includes 26 lower-case letters, 10 numerals, 10 most frequently used punctuation marks and a whitespace character. The two remaining characters serve exclusively as a filler character and a padding character. These two particular characters are not eligible to participate in plaintext or keyword. During decryption they are omitted. They eliminate the existing ambiguity. (Shakil, Islam, 2014).

The Playfair Cipher was first used by Britain in World War I. (Basu & Umar, 2012)

All modifications are intended to meet the needs of letters and special characters, while making it stronger and more difficult to break. Calculating the key stream can be very easy if the plaintext and cipher text are known [Menezes, 1997]. In today's computer era, this method can be broken in just a few seconds.

Literature Review

Some studies have been done by modifying the default order matrix table, namely: Bhowmick, et al (2015) who modified the matrix size to 6x6, where entering an alphabet letter (A-Z) includes J and numbers 0-9. Chipertext obtained, after replacing playfair with multiple Myszkowski transpositions, will increase the algebraic power against cryptanalytic attacks.

Aftab, 2013 (Alam et al., 2013) modified the size of the matrix to 7x4 by entering all alphabetic letters (A-Z) including J and special characters '*' and '#'. This study will eliminate the ambiguous nature that arises when using the default 5x5 matrix, because all letters have been accommodated while making it difficult for the cryptanalysis process to solve the ciphertext.

The method proposed by Ashish Negi, using an 8x8 matrix uses 64 grids. The proposed system will encrypt letters, numbers and special characters. (Negi, et al, 2012). This development

can accommodate more characters, so that it can eliminate the ambiguity of characters that appear.

Harinandan, 2012 proposed modification of the playfair method on a frequency basis which succeeded in providing several advantages, namely the entry of spaces and the use of arrays that can store information on the appearance of character X. (Harinandan, 2012)

Siddiqui, 2017 has combined playfair encoding techniques with several genetic operators to improve cipher security. Even though only 62 different characters can be accepted as input characters into plaintext, password texts can have up to 128 different characters. (Siddiqui et al., 2017).

Oweoya, 2013 (Oweoya, 2013) proposed playfair encryption and decryption, which would be difficult to solve with a brute force procedure, where the matrix size became 16x16 which allowed all alphabetic letters (A-Z) and almost all special characters to be entered.

Kumar, 2013 (Kumar et al., 2013) introduced a new technique, namely safe message transmission with a modified version of playfair cipher combined with a random number generator and a transpose matrix concept. This method uses a simple method of generating random numbers called Linear Feedback Shift Register and the Transpose Matrix concept.

Shrivastava, 2013 (Shrivastava et al., 2013) proposed a simple column transposition method in several rounds using an 8x8 size matrix. With a transposition of several turns, encryption becomes more complex.

From the results of the study, Haris said that all the existing proposed variants of Playfair cipher missed one of the most important security parameters (Haris & Alankar, 2014).

Bhattacharyya modifyied the playfair table to 10 x 9. This matrix used all alphanumeric characters as well as some special characters. In this modified playfair cipher, six different

keys and six iteration steps were used to make the encrypted message stronger than the traditional playfair cipher (Bhattacharyya et al., 2014).

Sharma's research said that the implementation of the advanced encryption algorithm generates cipher text which is very complex. It is concluded that by changing the encryption mechanism, by including a random number, the complexity of the encrypted text can be significantly increased (Sharma et al., 2014).

Kurniawan's results ontained a playfair cipher algorithm with a 13x13 matrix and this, combined with the LFSR generator, had a more random ciphertext than the previous playfair cipher (Kurniawan et al., 2018).

Kumar et al, improved the traditional Playfair Cipher with encrypt text in blocks. For each block the keyword will become the same but the matrix will shift with some random values. (Kumar et al., 2013)

From the research above, it can be concluded that the main purpose of developing and modifying the Playfair algorithm is to complicate the process of cryptanalysis and fulfill the needs of the characters needed in the plaintext message.

Based on observations, it is very interesting to develop a method that does not only prioritize the default matrix size, by making not only one matrix, but two matrices, which are named Key Layer Matrix (KLM). With this method, it is expected that it will be increasingly difficult to do cryptanalysis on the Playfair Algorithm.

Related Work

Playfair Chiper

The Playfair algorithm was discovered by Sir Charles Wheatstone and Baron Lyon Playfair in 1854. The Playfair Cipher was used by British soldiers in the Boer War (World War I).

This algorithm is the most famous encoding algorithm for letters [Ravindra]. The Playfair Cipher algorithm uses a keyboard (Chiper table) with a 5x5 square matrix, containing capital letters (A-Z), by removing the letter J to encrypt. The keyboard comes from the default table containing sequential capital letters that have been modified based on the selected Keywords.

By using selected keywords, for example FROZEN AIR, the Chiper Table is obtained as shown below.

The process of using Playfair Algorithm for encryption and decryption can be divided into 3 stages, namely: (1) Stage of Chiper Table Making, (2) Plaintext Preparation Phase, (3) Encryption Phase, (4) Decryption stage.

Stage of Chiper Table Making

At this stage, the first step is to do the encryption using the Playfair Algorithm. The steps that must be taken are as follows:

1. Create a default (original) matrix, measuring 5x5 with an alphabet letter (A-Z) element by negating the letter J.
2. Determine which keywords to use, the longer the better.
3. Replace all of the letters J in the Keyword with the letter I.
4. Replace each letter of the keyword into the default table starting from the first row and from the left, by removing duplicate letters and shifting the letters in the default table.
5. Expand the cipher matrix formed by adding row 1 to line 6 and column 1 in column 6.

Plaintext Preparation Phase

The second step after preparing the Chiper table, is to prepare the plaintext before being encrypted with the following rules [Stallings, 2010]:

1. Remove all spaces and non-letter characters from plaintext.
2. Change all the letters J in the text with the letter I.
3. Write the Plaintext in a bigram.
4. If there are the same letters in each pair of letters, then insert the letter Z in the middle, so that each pair of letters consists of different letters.
5. If there are letters that have no pairs, then add the letter Z at the end of the pair.

Encryption Phase

The encryption process in the Playfair Algorithm is done after the Chiper table is ready and the plaintext preparation stage is complete. This process forms an encrypted message from the Plaintext message. Each pair of letters (bigram) takes the following steps:

1. If the two letters are on the same line in the Chiper table, then each letter is replaced with the letter on the right.
2. If the two letters are in the same column in the Chiper table, then each letter is replaced with a letter below it.
3. If the two letters are not in the same row or column, then the first letter is replaced by the letter in the first line intersection with the second letter column. Instead the second letter is replaced by the letter in the intersection of the second letter row with the first letter column.

Decryption stage

The decryption process is the opposite of the encryption process, which is returning an

encrypted message (ciphertext) to the original message (Plaintext). Each pair of gamers (bigram) from encrypted messages undertake the following steps:

1. If the two letters are in the same line on the Chiper table, then each letter is replaced with the letter on the left.
2. If the two letters are in the same column in the Chiper table, then each letter is replaced with a letter on the top.
3. If the two letters are not in the same row or column, then the first letter is replaced by the letter in the first line intersection with the second letter column. Instead the second letter is replaced by the letter in the intersection of the second letter row with the first letter column.

Modify the Key Layer Matrix

To improve the reliability of the Playfair Algorithm, while maintaining the size of the Chiper 5x5 matrix, it is proposed that we introduce two default matrices whose elements are alphabetical letters (A-Z), where the position of letters in matrix elements is randomly assigned, so the first and second default matrices differ. The first matrix is called the Layer 1 Matrix and the second matrix is called the Layer 2 Matrix.

The proposed method is expected to increase the level of difficulty in the cryptanalysis process, so that message security can be maintained.

The two default tables are used to create Layer 1 and Layer 2 Chiper Tables based on the given keywords. Chiper Layer 1 and Layer 2 tables, are used for the encryption process for each pair of letters with rules that will be discussed in the next sub section. Modified Diagram of the Playfair Algorithm can be seen in Figure 1 below.

Stage of Chiper Table Making

As in the Playfair Algorithm, the Chiper Table creation process can be done using the given keywords by applying to the two default tables in each layer. For Yabel Chiper Layer 1 it is specified using the default Layer 1 table. For example, given the keyword FROZEN AIR, then using rule 3.1.1, obtained: The Layer 1 and Layer 2 Chper tables shown below.

Plaintext Preparation Phase

The process stage is done exactly like the previous Playfair algorithm. Suppose the plaintext to be encrypted is: VERY SECRET, then the steps that must be taken are:

1. Remove all spaces and non-letter characters from plaintext:

   "VERYSECRET"

2. Change all letters J in the text with letter I. Because there is no letter J, continue the next step.
3. Write down the Plaintext in a letter pair (bigram):

   "VE RY SE CR ET"

4. Because there are no twin letters on each bigram, step 4 is jumped.
5. If there are letters that have no pairs, then add the letter Z at the end of the pair.

After obtaining the complete bigram from the plaintext, the next step is to encrypt it using the previously created cipher table.

Encryption Phase

The encryption process proposed in the modification of the Playfair Algorithm with the KLM method is to use each pair of letters (bigram) to be encrypted in layer 1 and layer 2 cipher.

Where the first letter of each pair is taken from layer 1, while the second letter is taken from layer 2. The complete process for each pair of letters (bigram) takes the following steps:

First letter encryption:

1. Determine the position of the first letter on the Chiper Layer 1 Matrix, Determine the position of the second letter on the Layer 2 Chiper Matrix.
2. Vertically drag the position of the second letter on the Chiper Layer 1 matrix, so that the letters found in the Layer 1 Chiper Matrix are found.
3. If the two letters are in the same line on the Chiper Layer 1 Matrix, then the first letter is replaced with the letter on the right.
4. If the two letters are in the same column on the Chiper Layer 1 Matrix, then the first letter is replaced with a letter below it.
5. If the two letters are not in the same row or column, then the first letter is replaced by the letter in the first letter line intersection with the second letter column in the Chiper Layer 1 Matrix.

Second letter encryption:

1. Determine the position of the first letter on the Chiper Layer 1 Matrix, Determine the position of the second letter on the Layer 2 Chiper Matrix.
2. Vertically drag the position of the "first" letter on the Chiper Layer 2 matrix, so that the letters found in the Chiper Layer 2 Matrix.
3. If the two letters are in the same line on the Chiper Layer 2 matrix, then the second letter is replaced with the letter on the right.
4. If the two letters are in the same column on the Chiper Layer 2 matrix, then the second letter is replaced with a letter below it.

5. The second letter is replaced by the letter in the intersection of the second letter row with the first letter column.
6. If the two letters are not in the same row or column, then the second letter is replaced by the letter in the intersection of the second letter line with the column first in the Chiper Layer 2 Matrix.

Following is the Encryption process, one installs the first letter "VE".

So that the result of encryption "VE" is "DC". With the same steps, the total results of encryption are obtained:

"DC ZX MU RA ZU"

Based on the manual results it can be seen that the encryption results are becoming increasingly random, making it difficult for cryptanalysis.

Decryption stage

The decryption process, proposed in modifying the Playfair algorithm with the KLM method, is to reverse the process of encryption for each pair of letters (bigram). Where the first letter of each pair is taken from layer 1 while the second letter is taken from layer 2. The complete process for each pair of letters (bigram) takes the following steps:

Description of the first letter:

1. Determine the position of the first letter on the Chiper Layer 1 Matrix, Determine the position of the second letter on the Chiper Layer 2 Matrix.
2. Vertically drag the position of the second letter on the Chiper Layer 1 matrix, so that the letters found in the Chiper Layer 1 Matrix are found.

3. If the two letters are in the same line on the Chiper Layer 1 matrix, then the first letter is replaced with the letter on the left.
4. If the two letters are in the same column on the Chiper Layer 1 matrix, then the first letter is replaced with the letter on the top.
5. If the two letters are not in the same row or column, then the first letter is replaced by the letter in the first letter line intersection with the second letter column in the Chiper Layer 1 matrix.

Description of the second letter:

1. Determine the position of the first letter on the Chiper Layer 1 Matrix, Determine the position of the second letter on the Chiper Layer 2 Matrix.
2. Vertically drag the position of the "first" letter on the Chiper Layer 2 matrix, so that the letters found in the Chiper Layer 2 Matrix.
3. If the two letters are in the same line on the Chiper Layer 2 matrix, then each letter is replaced with the letter on the right.
4. If the two letters are in the same column on the Chiper Layer 2 matrix, then each letter is replaced with a letter below it.
5. If the two letters are not in the same row or column, then the second letter is replaced by the letter in the intersection of the second letter line with the column first in the Chiper Layer 2 Matrix.

So that the "DC" decryption result is "VE". With the same steps, the total decryption results are obtained:

"VE RY SE CR ET"

Conclusions and recommendations

Conclusions

The Playfair algorithm that uses a 5x5 size matrix, using the standard alphabetical order, makes the cryptanalyst have the possibility of making the cipher key table where they are able to guess the keyword. Therefore, this standard algorithm can be hacked. To minimize the possibility of cryptanalysts being able to hack the message, we can create a default matrix in a random arrangement. This can make it difficult for cryptanalysts to make cipher keys. So, the possibility of being hacked is very unlikely even though the cryptanalyst is able to guess the keywords that are used.

By making the matrix into 2 layers, the 'Key Layer Matrix (KLM)', the Playfair Algorithm is more reliable; where the encryption process and decryption process takes a long time with more focused concentration. Based on a program created using C ++ programming language, the author can make the encryption and decryption process faster. The following is the comparison of the two algorithms using the keyword "FROZEN AIR" with Plaintext "VERY SECRET":

Table 1. Significance test for each relationship

Algorithm	Time Create Chiper Key	Time Enkripsi	Time Dekripsi
Playfair Algorithm	3 seconds	8 seconds	11 seconds
KLM-2 Algorithm	5 seconds	18 seconds	21 seconds

Based on the results of running the program, it is clearly seen that the KLM-2 algorithm is still longer in terms of processing time. Therefore, it can be concluded that the KLM-2 algorithm is feasible to be calculated.

Recommendations

The proposed method used is still a prototype which only uses the 5x5 matrix size, as in the Playfair Algorithm, but has been added with a Layer consisting of 2 layers. The development of the KLM Method still requires further study and development, with a larger matrix size to accommodate other characters that might be included in the text. It is still possible to increase the number of layers to complicate the process of cryptanalysis and borders.

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

Figure 1. Default Table

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

Figure 2. Chiper Table

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

Figure 3. Default Table 1

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

Figure 4. Default Table 2

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

Figure 5. Layer 1 Chiper Table

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

Figure 6. Layer 2 Chiper Table

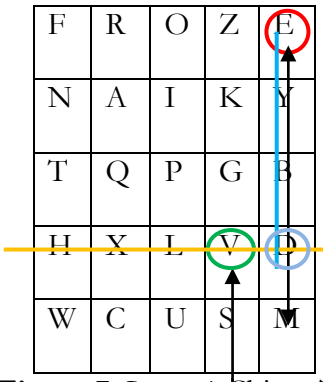

Figure 7. Layer 1 Chiper Table

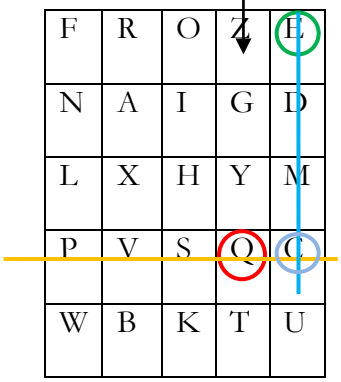

Figure 8. Layer 2 Chiper Table

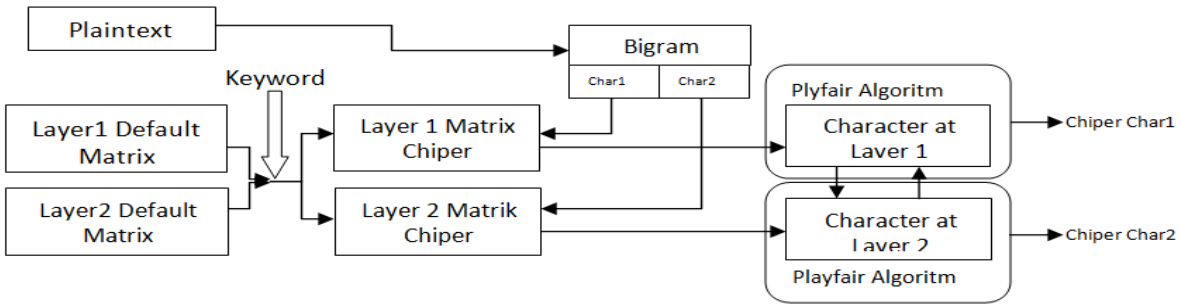

Figure 9. Diagram Key Layer Matrix

References

Alam, A. A., Khalid, B. S., & Salam, C. M. (2013). A Modified Version of Playfair Cipher Using 7x4 Matrix. *International Journal of Computer Theory and Engineering*, *5*(4), 626.

Babu, K. R., Kumar, S. U., & Babu, A. V. (2011). • A Survey On Recently Modernized Cryptographic Algorithms And Analysis On The Block Cipher Generation Using Play Color Cipher Algorithm. *International Journal of Mathematical Archive EISSN 2229-5046*, *2*(10).

Basu S., Kumar U.R, (2012), Modified Playfair Cipher using Rectangular Matrix, International Journal of Computer Applications (0975 – 8887), Volume 46, No. 9

Bhattacharyya, S., Chan, N., Chakraborty, S., (2014)., A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps., *IJARCET*, Volume 3, Issu 2, ISSN: 2278-1323, p 307-312.

Choudhary, J., Kumar, R. G., & Singh, S. (2013). A Generalized Version of Play Fair Cipher., *International Journal of Advanced Computer Technology. Volume*, *2*, 2–6.

Eweoya, I., Daramola, O., & Omoregbe, N. (2013). Improving Security Using Refined 16 X 16 Playfair Cipher for Enhanced Advanced Encryption Standard (AES). *Covenant Journal of Informatics and Communication Technology*, *2*(1).

Haris, M., Alankar B., (2017). A Survey Paper on Different Modification of Playfair Cipher., *International Journal of Advanced Research in Computer Science, Volume 8., No. 5., ISSN:0976-5697.*

Harinandan T., Soumen, M., (2012). A New Modified Playfair Algorithm Based On Frequency Analysis, *International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1.*

Harinandan T., Arnab S., Ghosh A., Ghosh S., (2014). Novel Modified Playfair Cipher using a SquareMatrix, *International Journal of Computer Applications (0975 –8887), Volume 101–No.12.*

Kumar, V., kr Upadhyay, S., Mishra, S. K., & Singh, D. (2013). Modified Version of Playfair Cipher Using Linear Feedback Shift Register and Transpose Matrix Concept. *International Journal of Innovative Technology and Exploring Engineering*, *3*.

Kumar, V., Mehra P., Gupta G., Sarma M. (2013). Enhanced Block Playfair Chiper. 9th *International Conference, QShine 2013, Greader Noida, India, January 11-12, 2013* (pp.689-695).

Kurniawan, D., Hananto, AL., Priyatna, B., (2018), Modification Application of Key Metrics 13x13 Cryptographic Algorithm Playfair Cipher and Combination with Linear Feedback

Shift Register (LFSR) on Data Security Based on Mobile Android., *International Journal of Computer Techniques — Volume 5 Issue 1,p 65-70.*

Negi A., Farswan J.S., Thakkar V.M., Ghansala S., (2012), Cryptography Playfair Cipher using Linear Feedback Shift Register, *IOSR Journal of Engineering, Vol. 2(5) pp: 1212-1216*

Murali, P., Senthilkumar, G.: Modified Version of Playfair Cipher Using Linear Feedback Shift Register, *International Conference on Information Management and Engineering, ICIME 2009, pp. 488–490. IEEE Conference (2009)* .

Menezes AJ, Oorschot PCV, Vanstone SA., (1997). Handbook of applied cryptography. *Boca Raton, Florida, USA: CRC Press.*

Shakil A. T., Islam R., (2014) An Efficient Modification to Playfair Cipher, *ULAB Journal of Science and Engineering, Vol. 5, No. 1, November 2014, ISSN: 2079-4398.*

Sharma, S., Shambhavi, S., Chaudhary, S., Khan, A., (2014)., Improvement of 16X16 Playfair Cipher using Random Number Generator, *International Journal of Computer Applications (0975 –8887)*, Volume 94, No. 1.

Shrivastava, G., Chouhan, M., & Dhawan, M. (2013). A Modified Version Of Extended Plafair Cipher (8x8). *International Journal Of Engineering And Computer Science*, *2*(956–961).

Siddiqui, M.S.N., Biswas, S.S., Agarwal, P., (2017), Genetic Extension of Playfair Cipher Using Modified Matrix, *International Journal of Computer & Mathematical Sciences (IJCMS) ISSN 2347 –8527, Volume 6, Issue 6, p 25-30.*

Srivastava, S.S., Gupta, N., (2011). Security Aspects of the Extended Playfair Cipher, I*nternational Conference on Communication Systems and Network Technologies (CSNT), pp. 144–147. IEEE Conferences.*

.