ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Generalization for Multidimensional Playfair Cipher

Krishnaraj Bhat, Dindayal Mahto and Dilip Kumar Yadav
Department of Computer Applications
National Institute of Technology
Jamshedpur, India

Abstract: Playfair cipher is a multi letter, poly alphabetic, symmetric cipher having a 2 dimensional key matrix supporting the security of 26 English alphabets. From the survey it is found that there are other variants which have key matrices with 3 and 4 dimensions. The main aim of this research is to provide the generalization for multidimensional Playfair cipher which includes choosing the dimension based on the number of values/characters supported by the Playfair cipher variant and the corresponding encryption and decryption processes. It is found from the dimensional analysis that more is the dimension for the fixed number of values/characters supported, stronger is the cipher against brute force attack with respect to possible number of groups.

Keywords: Information security; Cryptography; Conventional cipher; Classical cipher.

I. INTRODUCTION

Playfair cipher (Classical Playfair cipher or Wheatstone cipher) is one of the oldest conventional ciphers. It is found by Sir Charles Wheatstone in 1854. It is named after his friend Playfair who championed it at the British office. It has played a decisive role in World War I and World War II [1]. It works with digrams supporting 26 English letters, having X as filler letter and I and J treated as same. It uses a 2 dimensional key matrix of size 5 × 5 [2].

There are proposals of new variations of 2 dimensional Playfair cipher supporting different character sets [3-7]. Kaur *et al* [8] proposed the 3 dimensional Playfair cipher supporting 64 characters, working with trigrams and having the key matrix of size 4 × 4 × 4. There are articles [9-12] proposing the extensions of 3 dimensional Playfair cipher supporting the same character set but combined with Linear Feedback Shift Register. Bhat *et al* [13], [14] proposed the 4 dimensional Playfair cipher supporting 260 values, working with quartets and having the key matrix of size 2 × 2 × 13 × 5.

The objective of this research is to find the general formula for encryption and decryption of D dimensional Playfair cipher where D is a natural number greater than 1 and to find the maximum dimension of a Playfair cipher variant based on the number of values/characters it supports.

The organization of this article is as follows. Section II discusses the generalization. Section III gives an illustration of a 5 dimensional Playfair cipher variant using generalization. Section IV elaborates on the dimensional analysis.

II. GENERALIZATION

Choosing the dimension for the key matrix of a Playfair cipher variant depends on the number of values/characters supported by that variant. If N is the number of values/characters supported by the variant then the maximum dimension of the key matrix is the number of prime factors in the factorized form of N i.e. if $N = F_1 \times F_2 \times \ldots \times F_{D-1} \times F_D$ where F_1, F_2, …, F_{D-1}, F_D are primes then the maximum dimension is D. For N = 32 = 2 × 2 × 2 × 2 × 2, the maximum dimension is 5. In order to have a 4 dimensional key matrix with N = 32, 32 is factored as 4 × 2 × 2 × 2. Since Playfair cipher is a multi letter cipher, minimum dimension of the key matrix is 2.

In a key matrix with D dimensions, each element in the key matrix is represented using D co-ordinates $(X_1, X_2 \ldots X_{D-1}, X_D)$. If N = 32 = 2 × 2 × 2 × 2 × 2 then D = 5 and X_1, X_2, X_3, X_4, X_5 = 0 or 1. The first and last cell elements in the key matrix are represented by the co-ordinates (0, 0, 0, 0, 0) and (1, 1, 1, 1, 1) respectively.

A. *Encryption Process*

A group having D elements is considered at once while encrypting. If E_0, E_1, …, E_{D-1} are the elements in the group according to the order they appear then each element E_i where $0 \le i \le D-1$ is substituted by the element with the co-ordinates: $(E_{(i+2) \bmod D}.X_1, E_{(i+3) \bmod D}.X_2, \ldots, E_{(i+D-2) \bmod D}.X_{D-3}, E_{(i+D-1) \bmod D}.X_{D-2}, E_i.X_{D-1}, E_{(i+1) \bmod D}.X_D)$. Here, $E_i.X_j$ represents the X_j co-ordinate value for the element E_i where $1 \le j \le D$. Encryptional substitutions for dimensions 2 to 8 are shown in Table I.

Table I. Encryptional substitutions for dimensions 2 to 8

Dimension	***Substitution***
2	$(E_i.X_1, E_{(i+1) \bmod 2}.X_2)$
3	$(E_{(i+2) \bmod 3}.X_1, E_i.X_2, E_{(i+1) \bmod 3}.X_3)$
4	$(E_{(i+2) \bmod 4}.X_1, E_{(i+3) \bmod 4}.X_2, E_i.X_3, E_{(i+1) \bmod 4}.X_4)$
5	$(E_{(i+2) \bmod 5}.X_1, E_{(i+3) \bmod 5}.X_2, E_{(i+4) \bmod 5}.X_3, E_i.X_4, E_{(i+1) \bmod 5}.X_5)$
6	$(E_{(i+2) \bmod 6}.X_1, E_{(i+3) \bmod 6}.X_2, E_{(i+4) \bmod 6}.X_3, E_{(i+5) \bmod 6}.X_4, E_i.X_5, E_{(i+1) \bmod 6}.X_6)$
7	$(E_{(i+2) \bmod 7}.X_1, E_{(i+3) \bmod 7}.X_2, E_{(i+4) \bmod 7}.X_3, E_{(i+5) \bmod 7}.X_4, E_{(i+6) \bmod 7}.X_5, E_i.X_6, E_{(i+1) \bmod 7}.X_7)$
8	$(E_{(i+2) \bmod 8}.X_1, E_{(i+3) \bmod 8}.X_2, E_{(i+4) \bmod 8}.X_3, E_{(i+5) \bmod 8}.X_4, E_{(i+6) \bmod 8}.X_5, E_{(i+7) \bmod 8}.X_6, E_i.X_7, E_{(i+1) \bmod 8}.X_8)$

ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

B. *Decryption Process*

During decryption, each element E_i in the group is substituted by the element with the co-ordinates: $(E_{(i+D-2) \bmod D}.X_1, E_{(i+D-3) \bmod D}.X_2, \ldots, E_{(i+2) \bmod D}.X_{D-3}, E_{(i+1) \bmod D}.X_{D-2}, E_i.X_{D-1}, E_{(i+D-1) \bmod D}.X_D)$. Decryptional substitutions for dimensions 2 to 8 are shown in Table II.

Table II. Decryptional substitutions for dimensions 2 to 8

Dimension	*Substitution*
2	$(E_i.X_1, E_{(i+1) \bmod 2}.X_2)$
3	$(E_{(i+1) \bmod 3}.X_1, E_i.X_2, E_{(i+2) \bmod 3}.X_3)$
4	$(E_{(i+2) \bmod 4}.X_1, E_{(i+1) \bmod 4}.X_2, E_i.X_3, E_{(i+3) \bmod 4}.X_4)$
5	$(E_{(i+3) \bmod 5}.X_1, E_{(i+2) \bmod 5}.X_2, E_{(i+1) \bmod 5}.X_3, E_i.X_4, E_{(i+4) \bmod 5}.X_5)$
6	$(E_{(i+4) \bmod 6}.X_1, E_{(i+3) \bmod 6}.X_2, E_{(i+2) \bmod 6}.X_3, E_{(i+1) \bmod 6}.X_4, E_i.X_5, E_{(i+5) \bmod 6}.X_6)$
7	$(E_{(i+5) \bmod 7}.X_1, E_{(i+4) \bmod 7}.X_2, E_{(i+3) \bmod 7}.X_3, E_{(i+2) \bmod 7}.X_4, E_{(i+1) \bmod 7}.X_5, E_i.X_6, E_{(i+6) \bmod 7}.X_7)$
8	$(E_{(i+6) \bmod 8}.X_1, E_{(i+5) \bmod 8}.X_2, E_{(i+4) \bmod 8}.X_3, E_{(i+3) \bmod 8}.X_4, E_{(i+2) \bmod 8}.X_5, E_{(i+1) \bmod 8}.X_6, E_i.X_7, E_{(i+7) \bmod 8}.X_8)$

III. AN ILLUSTRATION OF 5 DIMENSIONAL PLAYFAIR CIPHER

A 5 dimensional Playfair cipher variant is considered supporting 32 characters among which 26 are English alphabets (A to Z) and 6 are symbols (!, @, #, $, ^, &). The key matrix formation is similar to that of Classical Playfair cipher. The key matrix for the key KRISHNA is shown in Table III.

Table III. Key matrix for the key KRISHNA

K	R	I	S
H	N	A	B
C	D	E	F
G	J	L	M
O	P	Q	T
U	V	W	X
Y	Z	!	@
#	$	^	&

Table IV shows the co-ordinates representing each element of the key matrix shown in Table III.

Table IV. Co-ordinates representation of elements of the key matrix shown in Table III

Element	X_1	X_2	X_3	X_4	X_5	*Element*	X_1	X_2	X_3	X_4	X_5
K	0	0	0	0	0	O	1	0	0	0	0
R	0	0	0	0	1	P	1	0	0	0	1
I	0	0	0	1	0	Q	1	0	0	1	0
S	0	0	0	1	1	T	1	0	0	1	1
H	0	0	1	0	0	U	1	0	1	0	0
N	0	0	1	0	1	V	1	0	1	0	1
A	0	0	1	1	0	W	1	0	1	1	0
B	0	0	1	1	1	X	1	0	1	1	1
C	0	1	0	0	0	Y	1	1	0	0	0
D	0	1	0	0	1	Z	1	1	0	0	1
E	0	1	0	1	0	!	1	1	0	1	0
F	0	1	0	1	1	@	1	1	0	1	1
G	0	1	1	0	0	#	1	1	1	0	0
J	0	1	1	0	1	$	1	1	1	0	1
L	0	1	1	1	0	^	1	1	1	1	0
M	0	1	1	1	1	&	1	1	1	1	1

Encryption and decryption of a plain message KITTA of length 5 and its cipher message respectively are discussed in following subsections.

A. *Encryption*

Using Table IV as reference, Table V shows the substitution done for each character in the plain message. The substitution formula is taken from Table I corresponding to dimension 5. K is substituted by U which has the X_1 co-ordinate value as that of T, X_2 co-ordinate value as that of T, X_3 co-ordinate value as that of A, X_4 co-ordinate value as that of K and X_5 co-ordinate value as that of I. In a similar way, other characters are substituted. The cipher message formed is UTSII.

Table V. Encryptional substitutions for plain message KITTA

Plain message	X_1	X_2	X_3	X_4	X_5	*Cipher message*
K	1	0	1	0	0	U
I	1	0	0	1	1	T
T	0	0	0	1	1	S
T	0	0	0	1	0	I

A	0	0	0	1	0	I

B. Decryption

Using Table IV as reference, Table VI shows the substitution done for each character in the cipher message. The substitution formula is taken from Table II corresponding to dimension 5. U is substituted by K which has the X_1 co-ordinate value as that of I, X_2 co-ordinate value as that of S, X_3 co-ordinate value as that of T, X_4 co-ordinate value as that of U and X_5 co-ordinate value as that of I. Likewise, other characters are substituted. The decrypted message formed is KITTA.

Table VI. Decryptional substitutions for cipher message UTSII

Cipher message	X_1	X_2	X_3	X_4	X_5	***Decrypted message***
U	0	0	0	0	0	K
T	0	0	0	1	0	I
S	1	0	0	1	1	T
I	1	0	0	1	1	T
I	0	0	1	1	0	A

IV. DIMENSIONAL ANALYSIS

In the above illustration, possible number of groups of size 5 for N = 32 is 32^5. If the dimension was 4 for the same N then possible number of groups is 32^4. In general, if D is the dimension and N is the number of elements in the key matrix then possible number of groups is N^D. In order to be strong against brute force attack with respect to possible number of groups, dimension chosen must be the maximum.

V. CONCLUSION

Generalization for multidimensional Playfair cipher can be used to find the maximum dimension of the key matrix having a set of characters/values supported by a Playfair cipher variant and its encryption and decryption procedures and to make the brute force attack hard with respect to possible number of groups.

VI. REFERENCES

[1] W. Stallings, Cryptography and Network Security Principles and Practice, 6th ed., Pearson Education: United States, 2014.

[2] B. Schneier, Applied cryptography: protocols algorithms and source code in C, 2nd ed., Wiley Computer Publishing, John Wiley and sons, Inc: New York, 1996.

[3] V. U. Sastry, N. R. Shankar, S. D. Bhavani, "A Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering, vol. 1, no. 5, Dec. 2009, pp. 597-601.

[4] S. S. Srivastava, N. Gupta, "Optimization and Analysis of the Extended Playfair Cipher", International Conference on Emerging Trends in Networks and Computer Communications, 2011, pp. 267-270.

[5] S. Basu, U. K. Ray, "Modified Playfair Cipher using Rectangular Matrix", International Journal of Computer Applications, vol. 46, no. 9, May 2012, pp. 28-30.

[6] S.S.Dhenakaran, M. Ilayaraja, "Extension of Playfair Cipher using 16X16 Matrix", International Journal of Computer Applications, vol. 48, no. 7, June 2012, pp. 37-41.

[7] A. Kaur, H. K. Verma, R. K. Singh, "6 X 6 Playfair Cipher using LFSR based Unique Random Number Generator", International Journal of Computer Applications, vol. 51, no. 2, Aug. 2012, pp. 30-35.

[8] A. Kaur, H. K. Verma, R. K. Singh, "3D (4 X 4 X 4) - Playfair Cipher", International Journal of Computer Applications, vol. 51, no. 2, Aug. 2012, pp. 36-38.

[9] A. Kaur, H. K. Verma, R. K. Singh, "3D - Playfair Cipher using LFSR based Unique Random Number Generator", Sixth International Conference on Contemporary Computing (IC3), 2013, pp. 18-23.

[10] S. Singh, R. K. Singh, A. Kaur, "3D - Playfair Cipher using Linear Feedback Shift Register", Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Sept. 2013, pp. 164-171.

[11] V. Verma, D. Kaur, R. K. Singh, A. Kaur, "3D - Playfair Cipher with additional Bitwise Operation", International Conference on Control, Computing, Communication and Materials (ICCCCM), 2013.

[12] S. Singh, A. Kaur, R. K. Singh, D. Kaur, "Developing 3D-Playfair Cipher Algorithm Using Structure Rotation", International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015, pp. 1004-1008.

[13] K. Bhat, D. Mahto, D. K. Yadav, "A Novel Approach to Information Security using Four Dimensional (4D) Playfair Cipher Fused with Linear Feedback Shift Register", Indian Journal of Computer Science and Engineering, vol. 8, no. 1, Feb-March 2017, pp. 15-32.

[14] K. Bhat, D. Mahto, D. K. Yadav, "Comparison Analysis of AES-256, RSA-2048 and Four Dimensional Playfair Cipher Fused with Linear Feedback Shift Register", International Journal of Advanced Research in Computer Science, vol. 8, no. 3, March-April 2017.