International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Analysis of Playfair Algorithm with Different Sizes on Natural Languages (Specialized on Telugu language)

V. Subhashini[1], Dr. N. Geethanjali[2]
[1]Research Scholar, Department of Computer Science & Technology, Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India
[2]Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University, Ananthapuramu, Andhra Pradesh, India

Abstract*—** *Cryptography is used to encrypt the secret messages. In Cryptography, the Playfair cipher algorithm depending upon different matrices had explained an interesting data encryption technique with very low complexity. This Paper will present a perspective on combination of Playfair techniques. Extending the concept of 5 X 5 matrix of Playfair algorithm into different sizes, encrypting the messages of natural languages is developed. Play fair cipher is one of the popular symmetric encryption methods. The first recorded description of the Play fair cipher was in a document signed by Wheatstone on 26 March 1854. However Lord Play fair promoted the use of this cipher and hence it is called Play fair Cipher. Previously, this paper is improved the algorithm to support 6 X 6 matrix for 0-9 numeric values and alphabets, 8 X 8 matrix for Interweaving on DNA – encoded data, 7 X 4 matrix for non repeating alphabets with #,*.10 X 9 matrix for alpha-numeric values and special characters. The 16 X 16 matrix is used of Urdu language, 256 X 256 a matrix is used for Kurdish Language. In this paper the original paper of 5 X 5 matrix is modified into N X M matrix and it is possible to encrypt messages written by natural language. In this paper our state language Telugu as a special case is discussed.**

***Keywords*—** *Cryptography, Keys, Digraphs, Encryption, Decryption, Cryptanalysis.*

I. INTRODUCTION

Cryptography has become an essential tool in transmission of information. Cryptography is the central part of several fields: information security and related issues, particularly, authentication, and access control. Cryptography encompasses a large number of algorithms which are used in building secure applications. Cryptography is the study of Secret (crypto-)-Writing (-graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form. As the field of cryptography has advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances. Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives when we sign our name to some document and for instance and, as we move to world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for such procedures. Cryptographic systems are generally classified along three independent dimensions:

1. Type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition.
2. The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each use a different key the system is referred to as asymmetric, two key, or public-key encryption.
3. The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

II. PLAYFAIR CIPHER

The best - known multiple letter encryption cipher is the Playfair, which creates diagrams in the plaintext as single units and translates these units into cipher text diagrams. The playfair algorithm is based on the use of 5 X 5 matrix of letters constructed using a keyword. Playfair is a substitution cipher. Playfair cipher was originally developed by Charles Wheatstone in 1854 but it bears the name of Lord Playfair because he promoted the use of this method.

The traditional Playfair cipher uses 25 uppercase alphabets. A secret keyword is chosen and the 5 x 5 matrix is built up by placing the keyword without any duplication of letters from left to right and from top to bottom. The other letters of the alphabet are then placed in the matrix. For example if we choose "DIGITAL LIBRARY" as the secret keyword the matrix is given in table 1.

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

V. Subhashini and Dr. N. Geethanjali, "Analysis of playfair algorithm with different sizes on natural languages (Specialized on Telugu language)," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 3, pp. 27-30, 2016.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

So, the Using the word “DIGITAL LIBRARY”, we get the following code:

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

In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies a 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.

So using the Keyword “DIGITAL LIBRARY” the word “COMMUNICATE” can be decoded as follows

CO	MX	UN	IC	AT	EX
GK	FW	SH	YG	DQ	AW

III. Existing Playfair on Different Sizes

Originally the PlayFair Algorithm was developed for 5 X 5 Matrix to encrypt and decrypt the message. Later it was developed for different sizes: 6 X 6 matrix for 0-9 numeric values and alphabets, 8 X 8 matrix for Interweaving on DNA – encoded data, 7 X 4 matrix for non repeating alphabets with #,*.10 X 9 matrix for alpha-numeric values and special characters. The 16 X 16 matrix is used of Urdu language, 256 X 256 a matrix is used for Kurdish Language. The 9 x 9 Playfair cipher uses 9 x 9 matrix which contains the key at the beginning of the matrix. The key should not be more than 81 characters (pertaining to the size 9 x 9) decided by the security administrator.

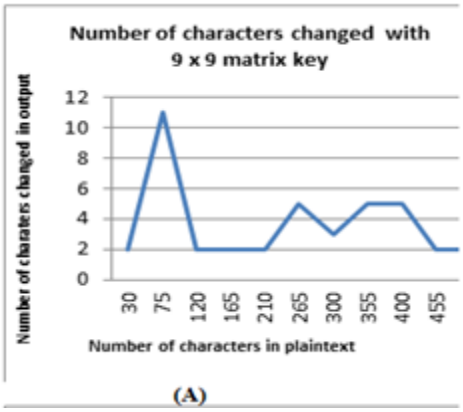
IV. Results and Analysis of Various Matrix Sizes for the Key

A. Different sizes of the matrices for the key were implemented ranging from 9 x 9 to 11X11 accordingly, a 10 x 10 matrix contained 100 characters, and an 11 x 11 matrix consisted of 121 characters. Two set of experiments were done. In the first set, the plaintext was variable but the key was kept the same. In the second set, the plaintext was kept the same but the key was changed. For both sets, avalanche effect was measured. Avalanche effect measures the change in the output when the input or the key is slightly changed. Details of these experiments and results are given below.

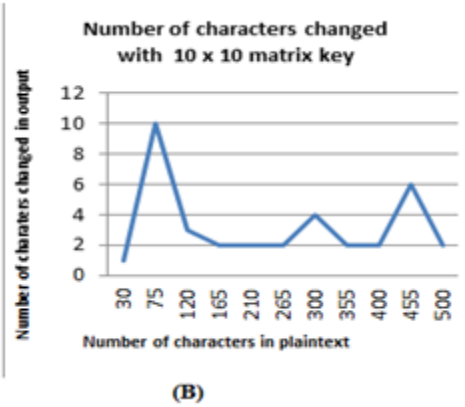
Number of Characters in Plaintext	Number of Characters Changed in Output after Flipping One Bit in Input		
	9 X 9	10 X 10	11 X 11
30	2	1	1
75	11	10	12
120	2	3	2
165	2	2	2
210	2	2	2
265	5	2	5
300	3	4	4
355	5	2	2
400	5	2	6
455	2	6	2
500	2	1	1

B. Results with fixed key and variable plaintexts

This set of experiments was performed with fixed matrix, fixed key (27 distinct characters including space) which is “A quick brown fox jumps over the lazy dog”, and ten different sizes of plaintexts ranging from 30 characters to 500 characters. In each of these plaintexts, one bit in the input was changed (note that each character in the plaintext is represented in ASCII format, and changing one bit input anywhere will affect that particular character in which the change has taken place). It is observed from this table that the change in the output characters ranged between 1 and 12 characters. A clearer picture of the trends is visible which shows that an increase in the size of plaintext does not contribute much to the avalanche effect. The reason for this is that there is only one bit change in the whole plaintext input, and this one bit change does not depend on the size of the plaintext. Moreover, it is also observed that for all three matrix sizes, the biggest change was observed for plaintext of 75 characters. This could be attributed to the structure of the plaintext itself, which, in this particular case, might have a strong impact on the output due to the particular key selected for encryption.



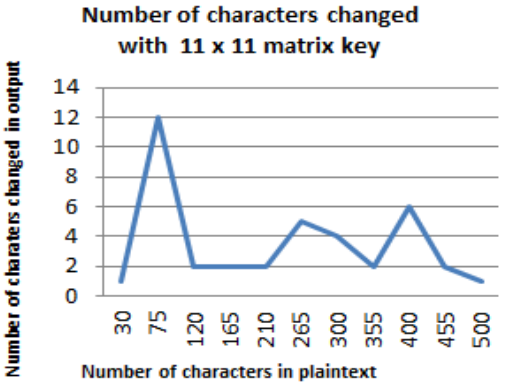
(A)



(B)

V. Subhashini and Dr. N. Geethanjali, “Analysis of playfair algorithm with different sizes on natural languages (Specialized on Telugu language),” *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 3, pp. 27-30, 2016.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024



(C)

Fig. Change In Output With 1 Bit Change In Plaintext Input Using (A) 9 X 9 matrix (B) 10 X 10 Matrix (C) 11 X 11 Matrix

Cresols with variable key and fixed plaintexts

The second set of experiments was having fixed plaintext (32 distinct characters including space) which was "A quick brown fox jumps over the lazy dog l, 5mp? /." Three different sizes of keys (i.e. 10, 20, and 30 characters) were used with each of configuration of the matrices. Table II shows the results of these experiments. It is observed from the table that with key size of 10 characters, there was no effect on the output for 9 x 9 and 10 x 10 matrices, but had a notable effect with 8 characters changed with 11 x 11 matrixes. Moreover, when the key size was increased for any matrix size, the general trend was that the number of characters changed in the output increased sharply and steadily, with the exception of 11 x 11 matrix where change in key size from 20 to 30 and flipping one bit in the key resulted in the same effect in the output with change of 14 characters each time. Overall, it can be fairly claimed that increasing the key size proportionally increased the number of characters changed in the encrypted output.

Playfair cipher has a strong potential for usage in wireless and mobile communications in which the sender is constrained by limited power. This potential of Playfair cipher lies in its simple design which allows for less power consumption than more complex algorithms such as RSA, DES, and AES. This paper presented a comparative analysis of three different matrix sizes, namely 9 x 9, 10 x 10, and 11 x 11, for keys of Playfair cipher.

V. PROPOSED ALGORITHM

A Playfair Algorithm for any Natural Language (Telugu)

The problem in 5X5 matrix playfair cipher arises when the language size exceeds 26 characters i.e. suppose we want to encrypt a message in Telugu language; the 5X5 matrix is unable to cope with the situation. In this study we proposed a NXM matrix playfair cipher which efficiently improves the performances of 5X5 Matrix.

In case of using NXM matrix first of all identify the,

1. Size of natural language i.e. number of characters.
2. Identify the size of NXM matrix.

Size (M)=2N+2

3. Make digraphs
4. Build mapping of the natural language characters with Unicode.
5. Fill all the cells of the matrix with language characters.
6. A key may be selected as per 5X5 playfair cipher having no repeating characters.
7. Use # for completing the odd pair and * for repeating characters.
8. After decryption ignore the # and * in the plain text.

Example of using NXM matrix for encryption of any natural language (A special case of TELUGU language)

In case of Telugu language we are using the Unicode concepts "Unicode provides a unique number for every character no matter what the platform, no matter what the program, no matter what the language"

Suppose to encrypt the word " □□□□□□□"

To encrypt the data we need to follow 8 X 8 matrix. As in the Telugu language we find 52 characters and 12 special character.(52 +12=64). Then for the word "□□□□□□□" the 8 X 8 matrix is as follows:

భ	ర	త	□□	□□	అ	ఆ	ఇ
ఈ	ఉ	ఊ	ఋ	□□	ఎ	ఏ	ఐ
ఒ	ఓ	ఔ	□□	□□	క	ఖ	గ
ఘ	జ	చ	ఛ	జ	ఝ	ఞ	ట
ఠ	డ	ఢ	ణ	థ	ధ	న	ప
ఫ	బ	మ	య	ల	వ	ష	స
హ	ళ	□□□	ఱ	□	□	□	□
□	□	□	□	□	□	□	□

After encrypted matrix with the keyword is as follows:

భ అ	ర ఆ	త ఇ	□□ ఈ	□□ ఉ	అ ఊ	ఆ ఋ	ఇ ఋ
ఈ ఎ	ఉ ఏ	ఊ ఐ	ఋ ఒ	□□ ఓ	ఎ ఔ	ఏ □□	ఐ □□
ఒ క	ఓ ఖ	ఔ గ	□□ ఘ	□□ జ	క చ	ఖ ఛ	గ జ
ఘ ఝ	జ ఞ	చ ట	ఛ ఠ	జ డ	ఝ ఢ	ఞ ణ	ట త

V. Subhashini and Dr. N. Geethanjali, "Analysis of playfair algorithm with different sizes on natural languages (Specialized on Telugu language)," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 3, pp. 27-30, 2016.

థ థ	డ ద	ఢ ధ	ణ న	ఫ ప	ద ఫ	ధ బ	న భ
ప మ	ఫ య	బ ర	మ ల	య వ	ల ష	వ స	ష హ
స ళ	హ □□□	ళ అ	□□□ □	అ □	□ □	□ □	□ □
□ □	□ □	□ □	□ □	□ □	□ □	□ □	□ □

So the encrypted text message for the word "□□□□□□□" is

భ అ	ర ఆ	త ఇ	□□ ఈ	□□ ఉ

VI. CONCLUSION

a. In this paper the original 5X5 matrix playfair cipher is modified to NXM matrix. By using NxM matrix it is possible to encrypt messages written in any natural language. In this paper Telugu as a special case is discussed.

b. This paper strongly depends upon lipi of the language.

REFERENCES

[1] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, 2001

[2] http://en.wikipedia.org/wiki/Playfair_cipher. Retrieved on 26 May 2015

[3] S. S. Srivastava and N. Gupta, "A novel approach to security using extended Playfair Cipher," *International Journal of Computer Applications*, vol. 20, no. 6, pp. 39-43, 2011.

[4] Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I. V. N. S. Aditya, and P. Komuraiah, "An extension to traditional Playfair cryptographic method," *International Journal of Computer Applications*, vol. 17, no. 5, pp. 34-36, 2011.

[5] R. Babu Kallam, Dr. A. Vinaya Babu, Dr. S. Udaya Kumar, and S. Swetha, "An improved Playfair Cipher cryptographic substitution algorithm," *International Journal of Advanced Research in Computer Science*, vol. 2, no. 1, pp. 211-214, 2011.

[6] O. Hassan Ahmed, A. Mahmood Ahmed, and S. Hasan Ahmed, "Improving playfair algorithm to support user verification and all the languages in the world including kurdish language," *International Journal of Engineering and Computer Science*, vol. 4, issue 8, pp. 14058-14062, 2015.

[7] S. A. Khan, "Design and analysis of playfair ciphers with different matrix sizes," *International Journal of Computing and Network Technology*, vol. 3, no. 3, pp. 117-122, 2015.

[8] G. Shrivastava, M. Chouhan, M. Dhawan, "A modified version of extended Plafair Cipher (8x8)," *International Journal of Engineering and Computer Science*, vol. 2, issue 4, pp. 956-961, 2013.