World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:5, No:1, 2011

A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)

Muhammad Salam, Nasir Rashid, Shah Khalid, Muhammad Raees Khan

***Abstract*—**In this paper a modified version NXM of traditional 5X5 playfair cipher is introduced which enable the user to encrypt message of any Natural language by taking appropriate size of the matrix depending upon the size of the natural language. 5X5 matrix has the capability of storing only 26 characters of English language and unable to store characters of any language having more than 26 characters. To overcome this limitation NXM matrix is introduced which solve this limitation. In this paper a special case of Urdu language is discussed. Where # is used for completing odd pair and * is used for repeating letters.

***Keywords*—**cryptography, decryption, encryption, playfair cipher, traditional cipher.

I. Introduction

CRYPTOPGAPHY comes from the Greek words for "secret writing" [1] so we can define cryptography as the art of writing secret words is called cryptography.

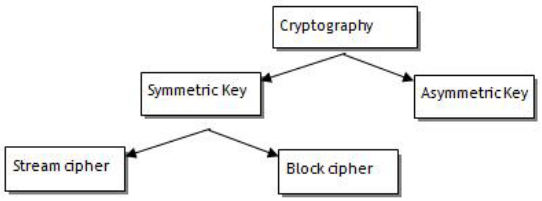


Fig. 1 Taxonomy of Cryptographic algorithms

"There are two basic types of cryptography systems: symmetric (also known as conventional or secret key) and asymmetric (public key)" [2]. "A symmetric cipher is one in which a given key is used to encrypt data, and that same key must be used to decrypt the data" [3]

In Symmetric Key Cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message. The receiver uses the shared key end decryption algorithm to decrypt the message. In Asymmetric Key Cryptography each user is assigned a pair of keys, public key and private key. The public key is announced to all members while the private key is kept secret by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message.

According to [5] A symmetric encryption scheme has five components i.e. plaintext, encryption algorithm, secret key, cipher text, Decryption algorithm shown in Fig. 2.

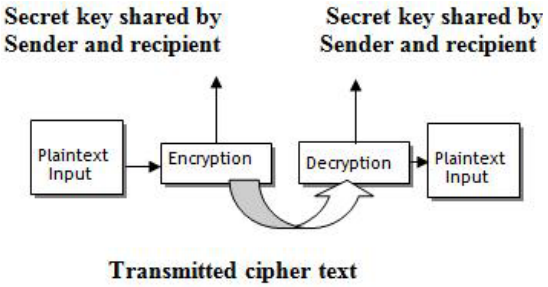


Fig. 2 Components of encryption scheme

In Symmetric Key Cryptography two types of ciphers, substitution cipher and transposition cipher are used [4]. In substitution cipher one symbol of the plane text is replaced by anther symbol. Substitution ciphers has further two types.

In Mono-alphabetic substitution cipher, a character in the plain text is always changed to the same character in the cipher text. The well-known example of Mono-alphabetic substitution cipher is the CAESAR Cipher which always change a to d. In polyalphabetic substitution cipher a single character in the plain text is changed to many characters in the cipher text. The well-known example of polyalphabetic substitution cipher is VIGENERE Cipher which changes a single character in the plain text into many characters in the cipher text by considering position of the character in the plain text.

In transposition cipher the characters in the plain text are swapped to get the cipher text i.e. the characters retain their plain text form but their position is changed. The plain text is organized into two dimensional table and columns are interchanged according to a predefined key.

II. The Playfair Cipher

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 [6].

Playfair is digraph substitution cipher which uses a 5x5 matrix, in which the key word is written first and the remaining cells of the matrix are filled with other letter of

[1]Muhammad Salam (msmdir@gmail.com),
[2]Nasir Rashid (nasir@uom.edu.pk)
[3]Shah Khalid (shahkhalid@uom.edu.pk),
[4]Raees Khan ShahSani (shahsani@uom.edu.pk),
Department of Computer Science & IT, University of Malakand, Pakistan

alphabets with I and J taken in the same cell. The message is divided into digraphs, in which repeating letters in the same pair are separated by filler letter X. in case of odd number of letters in the message a spare letter X is padded with the word to complete the pair. Then the plain text is encoded according to the four rules presented in [5].

Any word with no repeating letters can be selected as a key word to fill the matrix. The problem arises when we want to encrypt a message written in any natural language (URDU).

III. NXM Version of Playfair Cipher for any Natural Language (URDU)

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 URDU 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)=N+2
3. Make digraphs
4. Build mapping of the natural language charters 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 URDU language)

In case of Urdu 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” [7].

Following is the Unicode table for Urdu language [8], [9].

062B	0679	062A	067E	0628	0627	0622
ث	ٹ	ت	پ	ب	ا	آ
0630	0688	062F	062E	062D	0686	062C
ذ	ڈ	د	خ	ح	چ	ج
0635	0634	0633	0698	0632	0691	0631
ص	ش	س	ژ	ز	ڑ	ر
0642	0641	063A	0639	0638	0637	0636
ق	ف	غ	ع	ظ	ط	ض
0648	06BA	0646	0645	0644	06AF	06A9
و	ں	ن	م	ل	گ	ک
06D2	06CC	0626	06BE	06C1	0621	0624
ے	ی	ئ	ھ	ہ	ء	ؤ

Example 1

Consider the following Urdu plain text:

پاکستان زندہ باد

Key:

خیبر

Now to encrypt the above plain text in Urdu language

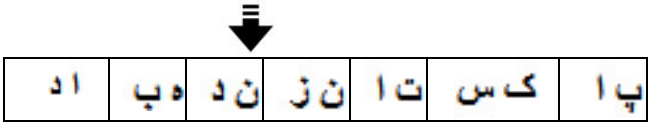
Number of characters in Urdu: N=42
Size (M) =N+2
Size (M) =42+2
Size (M) =44

Digraphs:

اد	ہ ب	ن د	ن ز	ت ا	ک س	پ ا

Cipher text using above table:

ث ڑ	پ ×	ء ڑ	م ڑ	پ آ	ل ڑ	آ ا



اد	ہ ب	ن د	ن ز	ت ا	ک س	پ ا

Example 2
Consider the following Urdu plain text:

ششماہی

Key:

خیبر

Digraphs:

ی #	ا ہ	ش م	ش ×

Cipher text using above table:

ی #	ا ہ	ش م	ش ×

ے ر	ء پ	ظ ڤ	ئ ض

ی #	ا ہ	ش م	ش ×

Now we drop pillars # and x to get the original Plain text:

ششماہی

IV. Cryptanalysis

In cryptography, confusion and diffusion play an important role in the development of a cipher [10, 11, 12]. Confusion refers to making the relationship between the key and cipher text as complex as possible and can be achieved by transposition. Diffusion refers to making the relation between the plaintext and cipher text as complex as possible. Strong confusion and diffusion make it difficult for the attacker to find the key or plaintext if the attacker has large number of plaintext and cipher text pairs.

Like the original playfair cipher, the algorithm proposed in this study can also be easily cracked if someone has enough cipher text and plaintext pairs. The addition of the " * " and " # " symbols have greatly increased the diffusion but still the proposed algorithm can be cracked by the same methods as the original 5x5 matrix playfair.

V. Conclusion

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 Urdu as a special case is discussed.

References

[1] Andrew S. Tanenbaum, "Networks Computer", 4th Edition
[2] http://www.sirraksbey.com/cryptography.html
[3] http://eclipsed.net/~gr/20030702/320000- symmetric_v_pki.html
[4] Behrouz A. Forouzan, "Data Communications and Networking", 4th Edition, McGraw-Hills, 2006
[5] William Stallings, "Cryptography and Network Security: Principles and Practice", 4th Edition, Prentice Hall, 2005
[6] http://en.wikipedia.org/wiki
[7] http://unicode.org/standard/WhatIsUnicode.html
[8] http://www.tremu.gov.pk/tremu1/workingroups/pdfpresentations/UZT%20UNICODE%20MAPPING.pdf
[9] http://unicode.org/charts/PDF/U0600.pdf
[10] H. A. A. Hassan, M. Saeb, and H. D. Hamed, "The PYRAMIDS block cipher", International Journal of Network Security, Vol. 1, No. 1, pp. 52-60, 2005.
[11] Y. Kurniawan, A. S. A., M. S. Mardiyanto, I. S. S., and S. Sutikno, "The new block cipher: BC2", International Journal of Network Security, Vol. 8, No. 1, pp. 16-24, 2009.
[12] P. Lin, W. L. Wu, C. K. Wu, "Security analysis of double length compression function based on block cipher" International Journal of Network Security, Vol. 4, No. 2, pp. 121-127, 2007.