International Journal of Pure and Applied Mathematics
Volume 117 No. 20 2017, 325-330
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

An Adaptive Play fair Cipher Algorithm for Secure Communication Using Radix 64 Conversion

Kalaichelvi V, Manimozhi K, Meenakshi P, Rajakumar B, Vimala Devi P
Assistant Professor, SASTRA University, Kumbakonam, India
E-mail : kalaichelvi2k@gmail.com

Abstract

Cryptography plays a vital role in the field of secure communication. Traditional play fair cipher encrypts only the alphabets (A – Z) and it has lot of shortfalls. To overcome these shortfalls, this paper proposes an adaptive playfair cipher algorithm using Radix 64 conversion. It will encrypt any type of text messages such as Lower and Upper case alphabets, digits(0-9), Special symbols, etc., It will provide more security than the traditional playfair cipher.

Keywords: Cryptography, Encryption, Playfair cipher, Radix 64 conversion.

1.0 Introduction:

Security is the primary concern in the field of Information technology. Cryptography is mainly used for Secure communication. There are two types of cryptosystem: i) Symmetric Key Cryptosystem ii) Asymmetric Key Cryptosystem. In Symmetric Key Cryptosystem, single key is shared by both the sender and receiver whereas in asymmetric key cryptosystem two different keys are used. Various algorithms are published in symmetric key cryptosystem such as DES, 3-DES, Blowfish, IDEA, AES, etc.,. Symmetric Key Cryptosystem is faster than the asymmetric key cryptosystem because it uses simple techniques such as Substitution and Transposition. In Substitution technique, each character is replaced by some other character. In transposition technique, the position of the character is interchanged. Different techniques are published under substitution technique such as Caesar Cipher, Playfair cipher, Mono alphabetic cipher, Poly alphabetic Cipher, Hill cipher, One-tome pad, etc,. In this paper, the modified Playfair cipher algorithm is discussed.

The organization of the paper is as follows. Section 2 discuss about the various research papers related to playfair cipher algorithm. Basic concepts of the traditional Play fair cipher algorithm and the merits and demerits are outlined in section 3. Section 4 discuss about the Modified Playfair cipher algorithm for encryption / decryption methods are presented with examples. Finally, section 5 describes the concluding remarks.

2.0 Literature Survey

Recent research in cryptography provided some novel way to enhance the security of the playfair cipher. An extended 8x8 playfair cipher was proposed in[1]. The proposed system was able to encrypt alphabets, numbers, and some special characters. Spaces and duplicate characters are handled using the symbols | and ^ respectively. Yet another modification appeared in [2] with a strong new cipher based on the ASCII codes of characters. However; in both cases, the

proposed 64 grids were not enough to include all the keys on a standard keyboard. Another generalized 8x16 Playfair cipher was introduced in [3], which considered the 128 ASCII characters instead of the 26 characters of the English language. More research efforts are still devoted to overcome these drawbacks in the Playfair cipher. Ravindra Babu K et.al discussed about traditional playfair cipher algorithm[4]. He proposed an enhancement with the traditional playfair cipher algorithm for encrypting alphabets as well as Digits[0-9]. But, this method wont encrypt the other cases like operators, special symbols, Blank space, etc.,

3.0 Radix 64 Conversion

Radix 64 conversion is a binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. Radix 64 conversion table uses 65 characters. It consists of 26 Uppercase letters, 26 Lower case letters, 10 digits and 2 special characters i.e., + and / and a padding character ('='). So, totally it contains 65 characters. Radix 64 encoding and decoding procedure is used in both encryption and decryption side. It takes 3 characters at a time and then it is converted into binary based on the ASCII value of the characters. So, we will get totally 24 bits. These 24 bits are divided into *four* groups of 6 bits and find the corresponding decimal value. Finally, pick the corresponding Radix 64 character from the Radix 64 conversion table. Radix 64 decoding is the reverse process of Radix 64 encoding procedure [5].

4.0 Traditional Play fair Cipher Algorithm

Play fair cipher algorithm is one of the multi-letter encryption cipher. It will take 2 characters at a time for encryption/decryption. The playfair algorithm is based on the use of a 5X5 matrix of letters constructed using a keyword. The matrix is constructed by filling the in the letters of the keyword from left to right and from top to bottom, and then fill the remainder of the matrix with the remaining letters in alphabetical order. We can combine two characters in a cell. Plaintext is encrypted based on the following rules:

1. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
2. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
3. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Suppose, if two characters are same it is separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

Limitations:

- 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 uses only uppercase alphabets.

5.0 Proposed Play fair Cipher Algorithm:

In proposed system [Fig.1], 8 X 8 matrix [***Table 1]*** is used for encryption and decryption. Initially, it is filled with the given keyword called ***"HACKER"*** and then the remaining cells are filled with the remaining uppercase alphabets, lowercase alphabets, numbers (0-9) and with the special characters (+ and /).

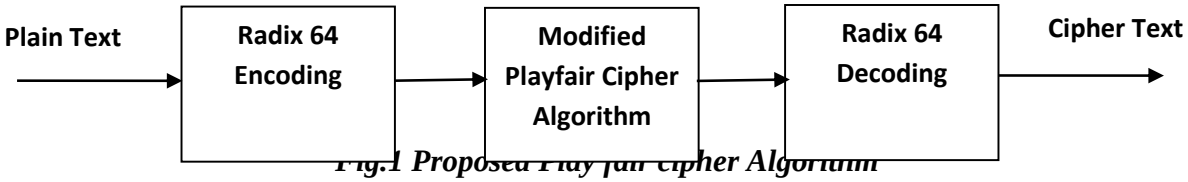


Fig.1 Proposed Play fair cipher Algorithm

H	A	C	K	E	R	B	D
F	G	I	J	L	M	N	O
P	Q	S	T	U	V	W	X
Y	Z	a	b	c	d	e	f
g	H	I	j	k	L	m	n
o	P	q	r	s	t	u	v
w	X	y	z	0	1	2	3
4	5	6	7	8	9	+	/

Table 1. Proposed 8 x 8 Matrix

Encryption and decryption is performed based on the following rules.

1. Get the plaintext in the form of a file.
2. Divide the message into blocks (3 characters per block).
3. To convert it into Radix 64 characters apply Radix- 64 encoding.
4. Apply the following rules to encrypt the message.
   - i) Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
   - ii) Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
   - iii) Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.
5. Finally, Radix 64 decoding is applied on the output of the previous step to get final cipher text.

5.1 Illustration:

Text : CRYPTO

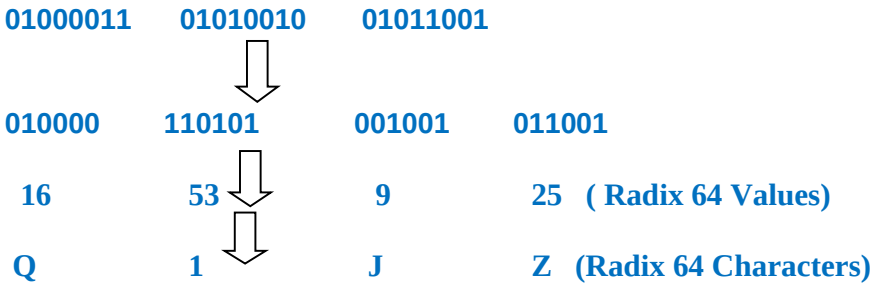
Encryption:

67 82 89 80 84 79 **(ASCII Characters)**

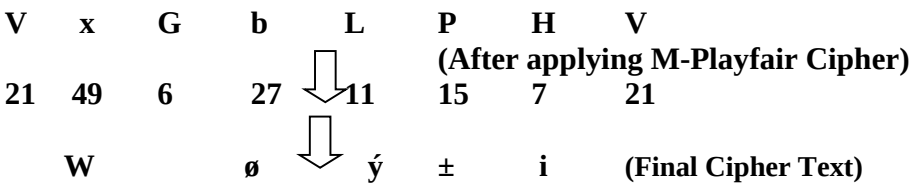
⇩

01000011 01010010 01011001 01010000 01010100 01001111

⇩

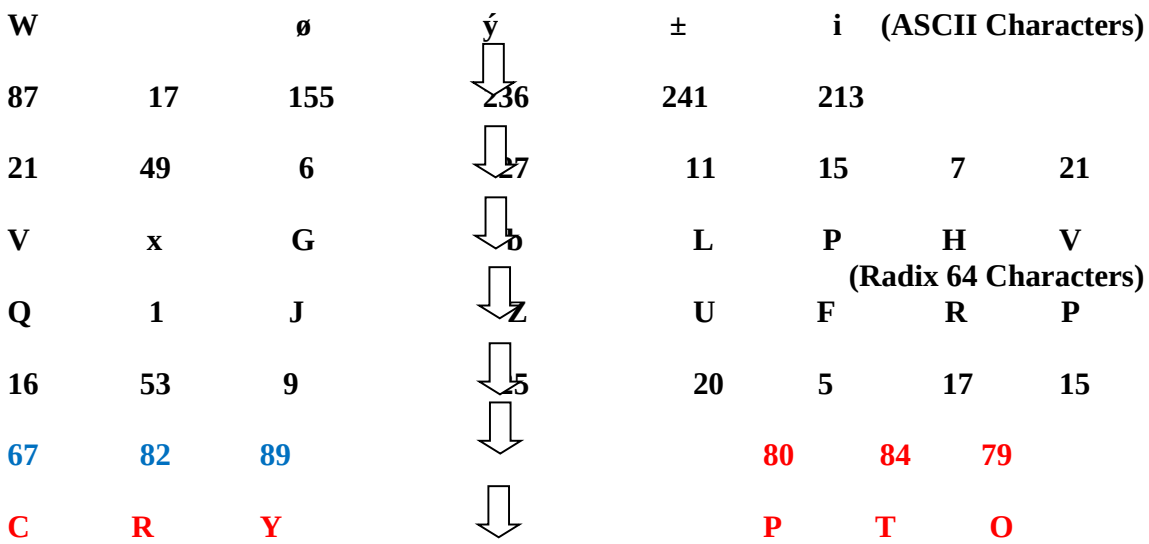


Similarly, the next 24 characters are converted into four Radix 64 characters such as UFRP. At the end of Radix 64 encoding we will get **"Q1JZ UFRP"**. Next, this text is applied to the Proposed Modified Playfair Cipher algorithm using 8 x 8 matrix. Similar to the traditional playfair cipher, the proposed algorithm process *two* characters at a time. Finally, we will get **"VxGbLPHV"** as the intermediate cipher text. Then, Radix 64 decoding is applied to get final cipher text.



Decryption:

Decryption is the reverse process of encryption. The cipher text is divided into groups of four characters and the following procedure is followed.



6.0 Conclusion

In this paper we have pointed the traditional Playfair algorithm, its merits and demerits. In order to overcome the demerits, we have proposed an extension to traditional PlayFair cipher algorithm, can be used more efficiently. It will encrypt any type of messages and it will provide more security than the traditional Playfair cipher.

References:

1. Srivastava SS, N Gupta and R Jaiswal. Modified Version of Playfair Cipher by using 8x8 Matrix and Random Number Generation. in *IEEE 3rd International Conference on Computer Modeling and Simulatio*. 2011. Mumbai.
2. Srivastava SS and N Gupta. A Novel Approach to Security using Extended Playfair Cipher. *International Journal of Computer Applications*. 2011; 20(6): 0975 – 8887.

3. Sastry VUK, NR Shankar and SB Durga. A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration. *International Journal of Network and Mobile Technologies*. 2010; 1(2): 45-53.

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. William Stallings, “Cryptography and Network Security”, 5th Edition.
6. Bruce Schneier, "Applied Cryptography" , John Wiley & Sons, Inc 1996
7. Richard Smith "Internet Cryptography",Pearson Edn Pvt.Ltd
8. Atul Kahate “Cryptography and Network Security”, Tata Mc.Graw Hill