International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

Enhanced Security by Modifying Playfair Cipher

Amandeep Kaur[1], Tanisha Jain[2], Gurjyot Singh[3]

[1, 2, 3]Guru Gobind Singh Indraprastha University, Guru Tegh Bahadur Institute of Technology, Rajouri Garden, New Delhi 11064, India

Abstract: ***Cryptography is the way and research of concealing information. It is basically a mathematical way to keep information safe and unthreatened. Nowadays, storage systems are increasingly subject to attacks. So, cryptography is a means of security and protection from harm.Cryptography is achieved by using various ciphers, in this paper we have studied the playfair cipher and have generated a comparison in timings of bruteforce attack on a normal playfair versus a modified playfair.***

Keywords: Cipher, Playfair Cipher, Substitution Cipher, Cryptography

1. Introduction

1.1 Security

Computer Security is the protection of information assets through the use of technology processes. The main of security is to provide Confidentiality or privacy, integrity, Authentication, Non Repudiation of data. In order to maintain confidentiality of data from unauthorised access we need to various techniques such as cryptography or stenography.

1.2 Cryptography

Cryptography is art of securing the data. It is a mathematical way and research of concealing information to keep it safe and unthreatened. It deals with encrypting the data first with the key which is kept secret to the legitimate user and the receiver end the enciphered data is deciphered with the appropriate keys.

1.3 Related Work

The existing Playfair cipher is based on the use of 5x5 matrix of letters constructed using a keyword. Usage of 5x5 matrix can only allow 25 characters, hence I/J counted as one.

Example: Major and Maior, the user may get ambiguity at the time of decipherment whether to choose Major or Maior.

To overcome the existing limitations extended Playfair 6x6 matrix algorithm has been proposed.

2. Preliminaries

There are few basic terminologies that are needed to be followed.

- **Encryption –** It is the way to conceal information given in a message so that only those users for whom the message is intended can analyse it.
- **Plaintext –** The message to be disguised
- **Ciphertext –** The coded message
- **Decryption –** The process of reinstating the plaintext from ciphertext.
- **Encryption Algorithm –** Various replacements and alterations in the plaintext are done with the help of encryption algorithm to produce cipher text.
- **Secret Key –** Input given to the encryption algorithm. Cipher text is generated depending upon the specific key being used at the time.
- **Decryption Algorithm –** Plaintext can be restored through this algorithm. It takes cipher text and secret key as an input to reinstate the plaintext.
- **Cryptanalysis –** It is the process of breaking the code without any knowledge of the encryption system
- **Brute Force Attack –** It is one of the approaches to attack a ciphertext by trying every possible key on a ciphertext until the plaintext is restored.
- **Substitution Cipher -** It works by replacing each letter of the plaintext with another letter adjacent to it. Example: "A SIMPLE EXAMPLE" become "B TJNQMF NFTTBHF".

3. Playfair Cipher

Playfair cipher is the best-known multiple letter encryption cipher. It was invented by Charles Wheatstone in 1854 who bears the name of Lord Playfair.

It is a trailblazing work by Charles Wheatstone to encrypt multiple letters, instead of single letters.

The playfair cipher used a 5 by 5 table containing a keyword or phrase.

To generate the key table, one would first fill in the spaces in the table with the letters of the keyword(dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order("I" and "J") in the same spaces. The keys can be written in the top rows of the table, from left to right.

Example: The following example shows the illustrations of 5x5 playfair matrix algorithm for the keyword "MONARCHY".

Taking the keyword any text can be converted into cipher text using three rule:

1) In case of letters in the same row, the letters to the right of each letter are taken.
2) In case the letters in the same column, the letters to the bottom of each letter are taken.

3) In case the letters are neither in the same row or column a rectangle is made with the letters and the letters at the opposite corners are taken.
   Using keyword "MONARCHY" the plaintext "BALLOON" could be converted to ciphertext using the above rules.

4. Modified Playfair Algorithm

The extended playfair algorithm is based on the use of a 6x6 matrix of letters of keyword. The matrix of letters of keyword. The matrix is constructed by filling the letters of keywords from left to right and from top to bottom and filling the remainder letters in alphabetic order and with the digits in ascending order from 0 to 9. In this algorithm both uppercase and lowercase characters could be handled. This algorithm handles I and J letters separately.

The following example shows the illustration of extended 6x6 playfair matrix algorithm for keyword "MONARCHY".

Table 1: Implementation of 6x6 Playfair

M	O	N	A	R	C
H	Y	B	D	E	F
G	I	J	K	L	P
Q	S	T	U	V	W
X	Z	0	1	2	3
4	5	6	7	8	9

The user can encrypt digits along with characters.

For Example using keyword "MONARCHY" the plain text "FROM1972" could be converted into ciphertext.

Table 2: Conversion using 6x6 Playfair

FR	OM	19	72
EC	CM	37	81

5. Proposed Solution

In[1] et.al 6x6 matrix instead of usual 5x5 playfair matrix, if we want to encrypt any numeric characters it is fairly easy to decrypt those numbers without knowing the keys. Here we are proposing a modified algorithm on 6x6 playfair so that all the alpha numeric data will be encrypted securely the complexity will be increased in order to decrypt without key or doing cryptanalysis on this matrix.

Solution

1) Create 6x6 matrix to store alphanumeric numbers.
2) Take secure key (Key must be alphanumeric).
3) Place key in matrix cell by cell without repeating any alphanumeric character.
4) Place rest of the alphabets and numeric to fill the matrix completely.
5) Apply all rules of playfair cipher on required data.

The following example shows the illustration of proposed solution 6x6 playfair matrix algorithm for keyword "COMPUTER1984".

Table 3: Proposed Solution

C	O	M	P	U	T
E	R	1	9	8	4
A	B	D	F	G	H
I	J	K	L	N	Q
S	V	W	X	Y	Z
0	2	3	5	6	7

For example using keyword "COMPUTER1984" could be converted into ciphertext.

Table 4: Conversion using Proposed Solution

GT	BI	T1	9X	X8
HU	AJ	M4	F5	Y9

If we take the data 3456 we will be able to generate the following ciphertext.

Table 5: Comparison

Encryption Technique	34	56
Playfair Cipher	Not Possible	Not Possible
6x6 playfair[1]	X9	67
Proposed Playfair	71	67

6. Result

The time analysis bruteforce attack on the 5x5 Playfair has been depicted in the table below:

Table 6: Bruteforce attack on 5x5 Playfair

Plaintext length(words)	Ciphertext length(words)	Time(seconds)
50	50	0.0322
100	100	0.0358
150	150	0.0479
200	200	0.0565
250	250	0.0631

The time analysis bruteforce attack on the 6x6 Playfair has been depicted in the table below:

Table 7: Bruteforce attack on 5x5 Playfair

Plaintext length(words)	Ciphertext length(words)	Time(seconds)
50	50	0.0343
100	100	0.0374
150	150	0.0512
200	200	0.0583
250	250	0.0652

The comparison graph depicts brute force on 6x6 Playfair matrix takes more time than 5x5 Playfair matrix hence adding a row of numbers in the key matrix increases the complexity and makes the system more secure.

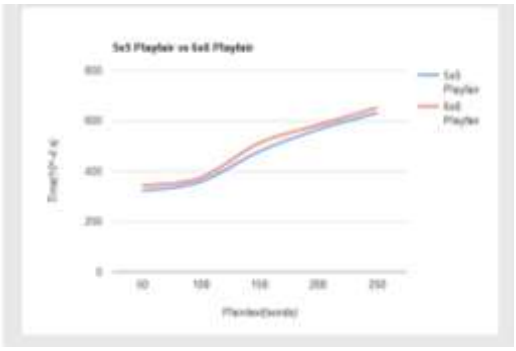

Figure 1: 5x5 vs 6x6 Playfair

References

[1] Monika Arora, Anish Sandiliya, Jawad Ahmad Dar,“ Modified encryption technique by triple substitution on playfair square cipher using 6by6 matrix with five iteration steps”, International Journal of Advanced Research in Computer Science and Software Engineering, XXIII (4), ISSN:2277 128X

[2] Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh, “3D (4 X 4 X 4) – Playfair Cipher,” Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India.

[3] William Stallings, “Cryptography and Network Security,” Principles and Practice, Global Edition, 7th Edition, Pearson Education, 2017.

[4] Subhajit Bhattacharya, Nisarga Chand, Shubham Chakraborty,“ Modified encryption technique using playfair cipher 10x9 matrix with six iteration steps”, International Journal of Advanced Research in Computer Engineering and Technology.

Author Profile

Amandeep Kaur received the M.Tech degree in Information Security, GGSIPU 2014, working as Assistant Professor in Guru Tegh Bahadur Institute of Technology since 2014. Her area of interest is cryptography, optimization algorithms, manets, cyber forensic.