Message Encryption with Modification in Playfair Cipher

Snehal Patil
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune, India.
sneva2913@gmail.com

Shivani Parihar
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune, India.
shivaniparihar.2110@gmail.com

Swapnajit Patil
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune, India.
swapnajitp223@gmail.com

Rahul Patil
Professor, Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune, India.
rahulpatilpink@gmail.com

***Abstract* - In present era, data is the most valuable assets for everyone. We all share data to each other via any mode of communication. For secure communication data can be encrypted during its transmission. There are many techniques available to encrypt data in which Play fair Cipher is best known for its multiple letter encryptions. It is highly tedious for opponent to decipher the cipher text encrypted using Play fair. The goal of this research paper is to provide security for the alphanumeric data during its transmission.**

Keywords - Encryption, Decryption, Plaintext, Cipher text, key,Playfair cipher.

I. INTRODUCTION

Information security is the biggest challenge now days. We have several methods to provide security for the information that is exchanged by sender and receiver. Encryption is highly trusted and well known method for data/ information protection during its transmission between sender and receiver.

In today's scenario, 'information' has become indispensable to both individuals and organizations. When any information is stored or transmitted by a message there should be some mechanism to protect that information from hackers . If information reaches the unauthorized person they might arise a lot of complications. Hence there is a need to hide the data so that a third person or irrelevant person cannot extract the exact message. Even for static data, to prevent misuse of the data there should be some mechanism so that if a third party manages to get hold of the data he will not be able to find out the meaning of the data. Hence Cryptography plays an vital role in data communication in today's world.

Cryptography is an area of data security which is developed to provide security for the senders and receivers to transmit and receive sensitive data through an insecure channel by a means of process called Encryption and Decryption. Cryptography ensures that the message should be sent without any alterations and only be authorized person can be able to open and read the message. A number of cryptographic methods and algorithms are developed for achieving secure communication.

The traditional model of encryption system comprises plaintext, encryption algorithm, secret key, cipher text and decryption algorithm. We need a powerful encryption algorithm to generate a stable and robust cipher text from given plaintext. The secret key has to be secure and must be acquired in a secure way by both sender and receiver.

Playfair cipher has great significance among all of the existing cryptographic systems. Encryption process of classical Playfair cipher uses a matrix in which letters are arranged in 5 rows and 5 columns. Arrangement of letters is based on a keyword (non-repeating letters) and formation of matrix starts by filling the letters of that keyword. Filling of letters in matrix is done from left to right and top to bottom. So after filling the keyword letters, matrix is filled by remaining letters of alphabets in ascending order (i.e. from a to z). This algorithm works only for alphabetic plaintext and numeric plaintext are not allowed to encrypt. It is the drawback of classical Playfair cipher.

we have proposed an enhancement to the existing Playfair encryption algorithm and also made a encryption decryption mechanism for message encoding and decoding by:

- Two more parameters along with key to encode and decode the plaintext.
- These parameters will be exchanged like key and without knowledge of the two additional parameters one cannot decrypt the cipher text even if they have key.

This will help in assuring the data integrity.

II. RELATED WORK

In paper [1], the authors have outlined the pros and cons of the classical Playfair cipher and by using alphanumeric keyword, they have proposed an enhancement to the existing encryption process. Paper [2] deals with some of the limitations and extensibilities of the traditional Playfair cipher. They have proposed a modification which uses 7 x 7 matrix with matrix randomization algorithm to extend the data holding capability and security at the same time. Paper [3] deals with the variations in the Playfair Cipher made by different authors on the basis of parameters. In paper [4], the authors have proposed an adaptive Playfair cipher algorithm using Radix 64 conversion. It encrypts any type of text messages such as Lower and Upper case alphabets, digits (0-9), Special symbols, etc. in order to provide more security. Paper [5] is the survey on the traditional Playfair Cipher encryption technique along with its limitations and drawbacks.

III. EXISTING SYSTEM

A. Traditional Playfair Cipher

Playfair is a symmetric polyalphabetic encryption system that uses block substitution. It was invented by Charles Wheatstone in 1954 but implementation was popularized by Lord Playfair. This cipher was also used as a British field cipher. Playfair cipher uses a 5 × 5 matrix which is shown in Table 1.

TABLE 1

A PLAYFAIR MATRIX

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

The matrix is constructed by choosing a keyword from which duplicate characters are removed and placed in the matrix. Then the rest of the empty spaces are filled with remaining characters by following an alphabetic order. Consistency with English alphabet is kept by putting any two characters in a single entry (Traditionally, these characters are I and J). Then plaintext is considered as a construction of two character blocks. A plaintext with odd length is normalized by appending a padding character at the end. Each block is substituted by following the rules below:

- If both characters are same, a filler character e.g., x is added after the first character.
- If both characters are on the same row of the matrix, they are replaced by their immediate next with the first element of the row circularly following the last
- Two characters that are on the same column are replaced by the character beneath them with the top element of the row circularly following the bottom
- Two characters when neither on the same column or on the same row, replaced by the character on its row that intersects another character by column.

For every possible key there is different number of matrix arrangements. So, for 25 letters, a permutation of 25 (which is approximately 1025) number of possible matrix can be generated. Also, with 26 letters there is a possibility of 676 diagrams, which was considerably secure for the time when Playfair invented. But, with the change of time, different cracking method arisen, some of which doesn't even require technical device and can be solved by pencil and paper.

B. 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.

IV. PROPOSED MODEL

In our proposed system we have made an Encryption and Decryption mechanism where messages will be encoded and decoded using a modified Playfair cipher. In the modified Playfair cipher, we will add 2 more parameters along with the key to encode and decode the plaintext. These two parameters will be exchanged like keys and without knowledge of the two additional parameters, one cannot decrypt the ciphertext even if they have a key. This will help in assuring data integrity.

Figure 1 shows us the Proposed System Diagram for the Sender side.

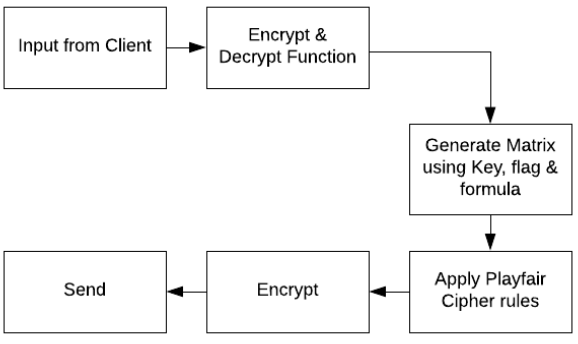

Fig. 1. Sender Side Proposed System Diagram

Figure 2 shows us the Proposed System Diagram for the Receiver side.

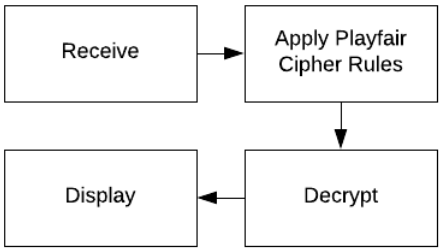

Fig. 2. Receiver Side Proposed System Diagram

A. Encryption and Decryption Rules

1) Take Keyword, Formula, and Flag value as the input data.
2) Generate 20 numbers using the formula.
3) **If Flag = 0 (9 x 5 matrix)**
   a) Create sets of 5 numbers from 20 numbers generated.
   b) Add these sets alternately with an alphabet matrix.

   If Flag = 1 (5 x 9 matrix)
   a) Create sets of 4 numbers from 20 numbers generated.
   b) Merge the rows of alphabet list and number list such that it starts with the alphabet and ends with the alphabet.
4) Encrypt the ciphertext by using the same rules as the Playfair cipher.
5) Decrypt by applying the same rules as Playfair cipher.

B. Illustration

Keyword: WorldPeace

Flag = 1

Formula value = " even"

TABLE Matrix 5 x 9

	1	2	3	4	5	6	7	8	9
1	w	2	o	4	r	6	l	8	d
2	p	10	e	12	a	14	c	16	b
3	f	18	g	20	h	22	i	24	k
4	m	26	n	28	q	30	s	32	t
5	u	34	v	36	x	38	y	40	z

5x 9 matrix

Rules:

Rule1:Same row "next element

Rule2:Same column : below element

Rule3: Otherwise : diagonally opposite

Using the generated matrix and input parameter from user Encryption will be as

plaintext=Warwillend

1. Split plaintext into pair of two letters

   wa rw il le nd

2. Encryption using Playfair cipher rules
   a. w a → r p (by rule3)
   b. r w → 6 2(by rule1)
   c. i l → s c (by rule2)
   d. l e → o c (by rule3)
   e. n d → t o (by rule3)
3. Ciphertext= rp62scocto

For Decryption

Rules:

Rule1:same row left element

Rule2:same column above element

Rule3:Otherwise = diagonally opposite

1. Split Cihertext into pair of two

   r p l o 28 8 o c t o

2. Applying decryption rules on 5 x 9 matrix
   a. r p → w a(by rule3)
   b. 6 2 → r w(by rule1)
   c. s c → i l (by rule2)
   d. o c → l e (by rule3)
   e. t o → n d (by rule3)

Keyword: WorldPeace

Flag = 0

Formula value = "even "

TABLE Matrix 9 x 5

	1	2	3	4	5
1	w	o	r	l	d
2	2	4	6	8	10
3	p	e	a	c	b
4	12	14	16	18	q
5	f	g	h	i	k

6	22	24	26	28	30
7	m	n	q	s	t
8	32	34	36	38	40
9	u	v	x	y	z

9 x 5 matrix

Plaintext = Warwillend

1. Split plaintext into pair of two letters

   w a r w i l l e n d

2. Encryption using Playfair cipher rules
   a. w a → r p (by rule3)
   b. r w → l o(by rule1)
   c. i l → 28 8 (by rule2)
   d. l e → o c (by rule3)
   e. n d → t o (by rule3)

3. Ciphertext=rplo288octo

For Decryption

Rules:

Rule1:same row: previous element

Rule2:same column: above element

Rule3:Otherwise: diagonally opposite

3. Split Cihertext into pair of two

   r p l o 28 8 o c t o

4. Applying decryption rules on 9 x 5 matrix
   f. r p → w a(by rule3)
   g. l o → r w(by rule1)
   h. 28 8 → i l (by rule2)
   i. o c → l e (by rule3)
   j. t o → n d (by rule3)

V. GUI IMPLEMENTATION

Users can input plaintext or ciphertext, flag parameter, and the formula with which the user wants to encrypt or decrypt the plaintext or ciphertext respectively. Using encrypt or decrypt button user can perform encryption or decryption.

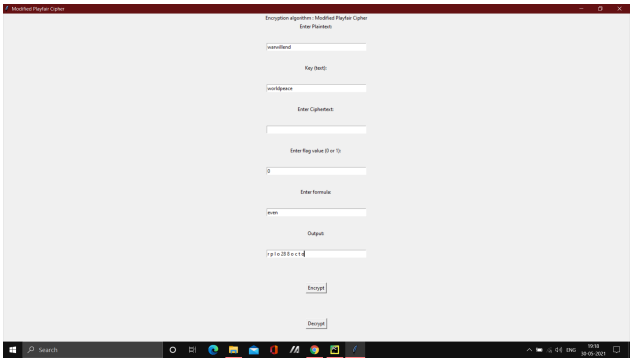

Figure 3 Encryption using flag=0,formula=even

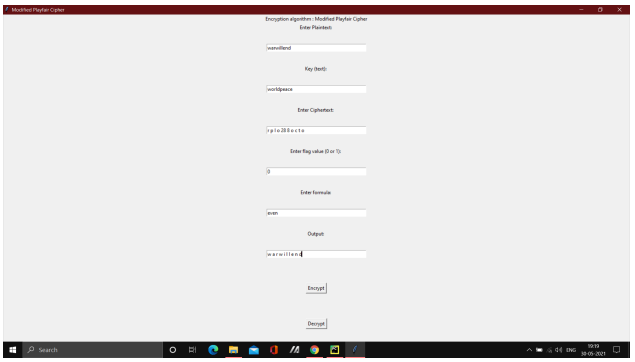

Fig.4 Decryption using flag=0,formula=even

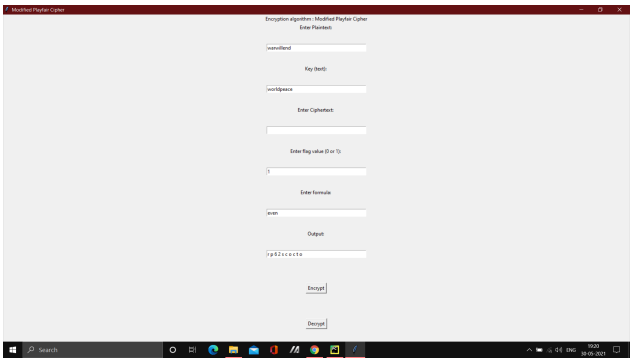

Fig.5 Encryption using flag=1,formula=even

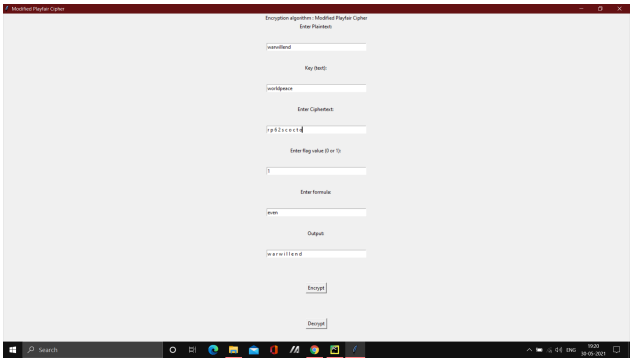

Fig6.Decryption using flag=1,formula=even

VI. CONCLUSION

The use of the internet is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different security services. To provide security to the network and data different encryption methods are used.

In this paper, we have proposed a system by modifying the traditional Playfair cipher for safe and secure encryption and decryption. Hence, after applying a proper algorithm for key and parameter exchange, we can prevent the man-in-middle attack for the integrity of the data. This algorithm would enhance the security of the data.

References

[1] Ashish Pandey, Neelendra Badal, "A Modified Circular Version of Playfair Cipher", 2nd International Conference on Advanced Computing and Software Engineering (ICACSE), 2019.

[2] Md. Ahnaf Tahmid Shakil, Md. Rabiul Islam, "An Efficient Modification to Playfair Cipher", ULAB Journal of Science and Engineering, Vol. 5, No. 1, November 2014.

[3] R. Deepthi, "A Survey Paper on Playfair Cipher and its Variants", International Research of Engineering and Technology (IRJET), Vol. 04, Issue. 04, April 2017.

[4] Klaichelvi V, Manimozhi K, Meenakshi P, Rajakumar B, Vimala Devi P, " An Adaptive Playfair Cipher Algorithm for Secure Communication Using Radix 64 Conversion", International Journal of Pure and Applied Mathematics, Vol. 07, No. 20, 2017.

[5] Mrs. Nitya Khare, De. S. Veena Dhari, "A Survey on Playfair Cipher Encryption Technique", International Journal of Scientific Research and Development, Vol. 05, Issue. 10, 2017.

/