National Journal of Advanced Research
ISSN: 2455-216X; Impact Factor: RJIF 5.12
Received: 05-12-2018; Accepted: 09-01-2019
www.allnationaljournal.com
Volume 5; Issue 1; January 2019; Page No. 73-77

Enhanced 16x16 playfair techniques for secure key exchange using RSA algorithm

Pawan Tiwari[1], Dr. Sunil Gupta[2], Dr. Deepak Choudhary[3]
[1] M.Tech Research Scholar I.E.T, Alwar, Rajasthan, India
[2] Professor and H.O.D, Department of CSE, L.I.E.T, Alwar, Rajasthan, India
[3] Associate. Professor, Department of CSE, I.E.T, Alwar, Rajasthan, India

Abstract
In the time of internet when we are sending and receiving the information over the network in the presence of the third party then it is very necessary to protect our data from the attacker's, in the series to protect the data we are using the cryptography algorithms. According to the key the encryption algorithm are of two types. First is symmetric key algorithm and second is asymmetric key algorithms.
The proposed work is an example of the symmetric key with asymmetric key together. In the work I done the improvement in the play fair matrix technique. I used the all the rules of the basic play fair algorithm with some changes (changes in matrix)..
The objective of this work is to securing the key of extended play fair technique of size16x16 using RSA algorithm (which is an Asymmetric key algorithm). It is a two stage algorithm.
In the first stage existing methods of playfair cipher modified by increasing in the size of matrix, so that restrictions of earlier works of playfair (PF) cipher using 5×5 matrix were overcome in the proposed work. In this proposed method use a 16×16 matrix which contains all the alphabetic, numeric and special character use in the keyboard as input. This work is an enhancement to existing algorithms that uses 5×5 matrix to pick cipher characters. It makes use of alphabets both lower case and upper case characters, number and special characters for constructing the contents of the matrix and after this we use the rotation factor to rotate the matrix.
In the second stage, the RSA public key encryption technique is used for sending key of the playfair ciphers securely and by this key we make the playfair matrix at the receiver end and we use the rotation factor to rotate the matrix after fill the key. By this matrix we can decrypt the cipher text and get the plain text finally, the security strength of the whole system has been analyzed and tried to fulfill requirement of security. At the last, thesis presents the scope for further work and concludes the thesis.

Keywords: RSA algorithm, playfair, cryptography algorithms

Introduction
In the era of digital world, security of 'information' has very important to both organization and individuals. When information is stored or transmitted by a message or packets of messages by some channel there should be some mechanism or method to protect that information from interruption and hacking. If information hacked by the wrong person there might arise a lot of problems. So we need to hide the data in such a way that no any third person or party can't hack the exact message. Even for static data, to prevent the misuse of data there should be some mechanism so that if a third party hack the data he will not be able to find out the right meaning of the data. Hence Cryptography plays an important role in data communication in today's digital world or in internet. Modern cryptography is part of mathematics and technology of computer science. Applications of cryptography include all computer passwords, ATM cards, and electronic commerce possible on information and tackle them with right types of counter measures. Also optimize process of the countering by proposing new method and increase the security, confidentiality, integrity and availability.

Playfair Algorithm
In the Playfair cipher, the alphabets are arranged in a 5×5 key matrix based on secret key. Though there are 26-alphabets in English language but PF cipher can handle only 25-alphabets. So, any one of i/j is used. To fill-in the key matrix table of size 5X5, the letters of the keyword (dropping all duplicate letters) are put in serially, and then remaining spaces are filled with rest of the letters of the alphabet in order [31, 32, 33].

Table 1: Key matrix

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

To encrypt a message, the message is broke into groups of 2 letters such that, for example, "Hello How Are You" is to be treated as "HE LL OH OW AR EY OU", and then mapped them out on the key table. Then these 4 rules are applied, in order, to each pair of letters in the plaintext:

Rules for making the CT using PF Matrix
1. Add an "X" letter after the first letter, if both letters are the same (or only one letter is left). Encrypt the new pair and continue doing this. Some variants of play fair use "Q" instead of "X", but any uncommon monograph will do.
2. If both alphabets appear on the same row in play fair matrix table, replace them with the letters to their immediate right side respectively (wrapping around to the left side of the row if a letter in the original plain text pair was on the right side of the row).

3. If both the alphabets appear on the same column in play fair matrix table, replace them with the letters immediately below side respectively (wrapping around to the top side of the column if a letter in the original plain text pair was on the bottom side of the column).
4. If both alphabets are not on the same column or row, replace them with the letters on same row respectively but at other pair of corners of the rectangle defined by the original pair. The order is important first letter of encrypted pair is one that lies on the same row as the first letter of the PT pair.

The decryption process (DP), use the INVERSE (opposite) of the last 3 (2, 3, 4) rules, and the first as-is (dropping any extra "X"s (or "Q"s) that do not make any sense in the final result message when finished) [31, 32, 33].

RSA cryptosystem

RSA cryptosystem was developed by these three, Ronald Rivest, Adi Shamir and Leonard Adleman in 1978. It has become a standard public- key cryptography used to encrypt private data, and it was the first published public key system. The high level of security of RSA algorithm depends on the difficulty of factoring the large numbers which are products of two large primes. Around the 1980s, scientists noticed that even though this difficulty occurred, it still did not achieve sufficient security. Therefore, they developed a strong method for security which created a hypothesis about the weaknesses of an adversary. This method is used with specific computational algorithms to meet the requirements of security. In 1984 the ElGamal public-key encryption appeared. It was based on the discrete logarithm problem and competed with the RSA cryptosystem [29-36, 38].

Literature Review

The main limitation of the play fair algorithm is that it supports only 25-alphabets of English language. Over years several attempts have been made to increase character limit of its dataset some of these are discussed here.

According to Aftab Alam, Shah Khalid, and Muhammad Salam, *et al.* [1] has discussed in this paper, a keyword is used to construct the 7x4 playfair matrix using letters and symbols, "#" and "*" two special symbols and upper case letters are the base for this Playfair Algorithm. The 7x4 playfiar matrix is constructed by filling keyword with no repeating (duplicate) letters. There is I and J are in different cells.

According to Ravindra babu, Udaya Kumar, Vinaya babu, *et al.* [2] has discussed in this paper proposed a 6×6 size of matrix use of a larger key. There is total 36 character, where all the 10-decimal numbers (0-9) and 26-alphabets of English language in upper case. But it needs more characters support in order to be able to work over a large range of text file. They also proposed use of transposition ciphers to preserve frequency distribution of the single letters to destroy the diagram and higher order distribution.

According to Lt. Ravindra Babu Kallam, Dr. S. Udaya Kumar, Dr. A. Vinaya Babu3 and Dr. M. Thirupathi Reddy, *et al.* [4] has discussed in this paper, it addresses the problem in a completely different way by generating a Block Cipher using Color Substitution. Binary values of the 7-bit ASCII codes are used along with corresponding colors of ARGB color model. Proposed "Play Color Cipher" substitutes each character of plaintext with a color block from an 18 decillions of colors. Color limit of the ARGB color model is N = 256×256×256×256 = 4294967296.

According to Subhajit Bhattacharyya, Nisarga Chand & Subham Chakraborty, *et al.* [6] has propos the effective way to show the 90 characters. This extended play fair algorithm is based on use of a 10 by 9 matrix of letters constructed using a keyword. This 10 x 9 matrix contains almost all printable characters. This includes lowercase, uppercase alphabets, punctuation marks, numbers and special characters. The playfair matrix is constructed by filling in letters, numbers or special characters of keyword from the left side to right side and from top side to bottom side, and filling in the remainder of the matrix with remaining letters in the alphabetic order and the digits in ascending order form 0 to 9 and special characters.

Implementation

Tools Used

In this dissertation, Turbo C/ C++ is use for simulate the algorithm.

Execution Process

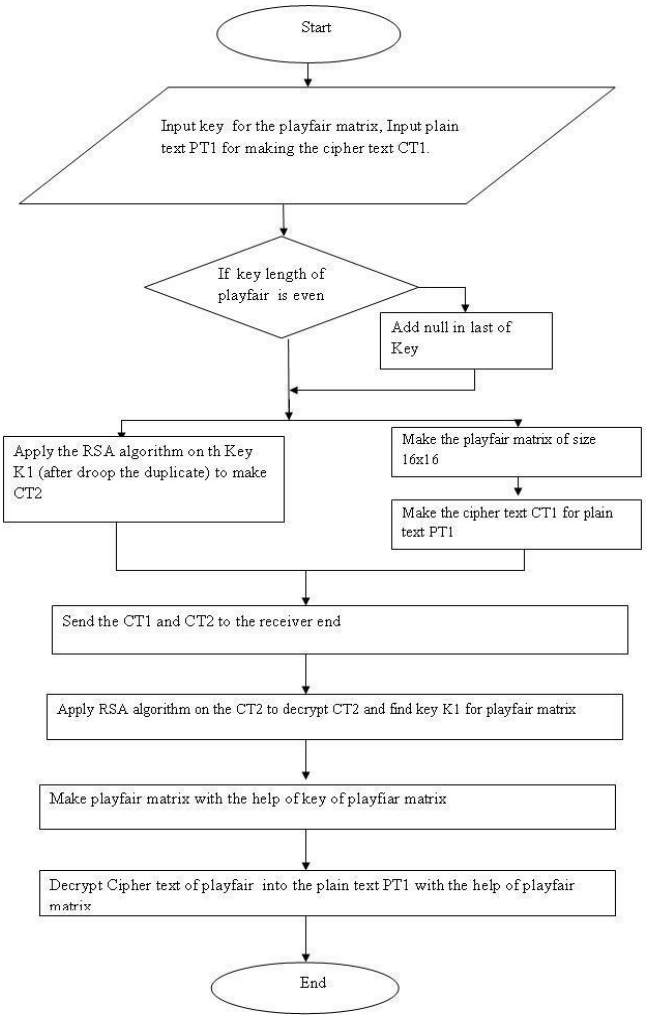

Fig 1: Shows the diagram of the complete methodology followed in this dissertation

The proposed work consists of the following these steps:
At the Sender ends

Step 1: construct a modified table of Playfair cipher technique of size 16X16, which contain all the alphabets from A to Z upper case and a to z in lower case, all the special characters which are on the keyboard and all numeric values (from 0 to 9). The PF encryption technique is divide into two phases:

a. First phase is creation and population of Matrix (by using the key and rotate the matrix with rotation factor after insert the key without duplicate).
b. The second phase is encryption process of the plain text message with the help of the Matrix. Make the Cipher text (CT1) of the plain text.

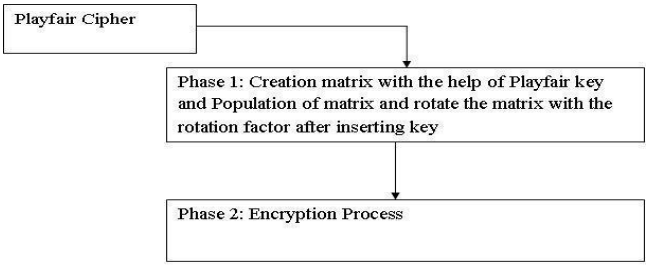

Fig 2: Playfair cipher encryption steps [32]

Step 2: use the key of Playfair technique as a Plain Text in RSA algorithm to make the Cipher text (CT2) of the key and send to the receiver.

At the Receiver ends

Step 3: decrypt the Cipher Text (CT2) into Plain Text (Playfair matrix key).

Step 4: construct a modified table of Playfair cipher technique of size 16X16, which contain all
the alphabets form A to Z upper case and a to z in lower case, all the special characters which are on the keyboard and all numeric values (from 0 to 9). The PF decryption technique is divided into two phases:

a. First phase is creation and population of Matrix (by using the key).
b. The second phase is decryption process of the cipher text (CT1) message with the help of the matrix and makes the plain text.

Example

Example 1 with P=17, Q=19 and E=7

Key = playfair example Key after dropping the duplicate = playfirexm
The key array at the sender end is:

Table Key array at the sender end

p	l	a	y	f	i	r	e	x	m

By the help of the key array shown in TABLE, make the matrix of size 16×16 for play fair cipher as shown in TABLE, first insert the character of TABLE from left to right and then from top to bottom As shown in TABLE When all element of TABLE are filled, and then insert all the remaining element of ASCII value by dropping all duplicates. By this TABLE will be created at the sender end (according to proposed algorithm).

Table 2: converting the cipher text 1 by plain text due to the 16x16 play fair matrix

S.no. of character	Plain text character and ASCII value	Row	Column	ASCII value Cipher text character and
1	i (105)	1	7	(109) m
2	blank space (32)	3	1 1	(28) file separator
3	a (97)	1	4	(121) y
4	m (109)	1	11	0 NUL
5	blank space (32)	13	1 1	(109) m
6	r (114)	1	8	(29) group separator
7	a (97) 9	1	4	(121) y
8	m (109)	1	11	0 NUL

So the cipher text at the sender end will be:
Cipher text 1 (CT1) = m∟y ↔my

Now the RSA algorithm will be used on the key exchange it securely.
At the sender's end: After dropping duplicates from the key the key will become:
Key = playfirexm
The ASCII code of this key character by character is

Table ASCII code of this key character by character

112	108	97	121	102	105	114	101	120	109

Now select two large prime numbers 'P' and 'Q'. To make the calculation simple two small prime no. have been taken.
P= 17, Q= 19
N=17 × 19= 323
Select any integer value of encryption key 'e' let it be 7.
Then apply encryption process on each (cipher text) values provided in TABLE. It will give cipher text 2(CT2)
$CT2 = (key)^e \bmod N$
$CT2 = 112^7 \bmod 323 = 5$
$CT2 = 108^7 \bmod 323 = 48$
$CT2 = 97^7 \bmod 323 = 109$
$CT2 = 121^7 \bmod 323 = 26$
$CT2 = 102^7 \bmod 323 = 102$
$CT2 = 105^7 \bmod 323 = 300$
$CT2 = 114^7 \bmod 323 = 228$
$CT2 = 101^7 \bmod 323 = 237$
$CT2 = 120^7 \bmod 323 = 256$
$CT2 = 109^7 \bmod 323 = 250$
So the CT2 at the sender end will be in the ASCII code as shown in the TABLE
TABLE ASCII code of CT2 character by character at sender end

5	48	109	26	102	300	228	237	256	250

Sender will send the CT1 and CT2 to the receiver.
At the receiver end, the value of decryption key 'd' will be 247
So the CT2 received at the receiver end will be as shown in TABLE.
Apply the decryption process on cipher text values of key
$Key = (CT2)^d \bmod N$
$Key = 5^{247} \bmod 323 = 112$
$Key = 48^{247} \bmod 323 = 108$
$Key = 109^{247} \bmod 323 = 97$
$Key = 26^{247} \bmod 323 = 121$
$Key = 102^{247} \bmod 323 = 102$
$Key = 300^{247} \bmod 323 = 105$

Key = 228^{247} mod 323= 114
Key = 237^{247} mod 323= 101
Key = 256^{247} mod 323= 120
Key = 250^{247} mod 323= 109
So the total key at the receiver end (ASCII Code) will be

Table 3: converting the plain text from cipher text 1 due to the 16x16 playfair matrix

S.no. of character	ASCII value Cipher text character and	Row	Column	Plain text character and ASCII value
1	(109) m	1	11	i (105)
2	(28) file separator	3	7	blank space (32)
3	(121) y	1	5	a (97)
4	**(0)** NUL	1	12	m (109)
5	(109) m	11	8	blank space (32)
6	(29) group separator	3	8	r (114)
7	(121) y	1	5	a (97)
8	0 NUL	1	12	m (109)

PT= i am ram

Experimental result

Performance Analysis

This chapter delineates the techniques applied in keeping the content secret through character supported, frequency analysis, and required matrix for brute force attack.

Character Supported

From the above example, we can see that there is no any two results of cipher text 1 and cipher text 2 are same. So we can say that this algorithm is enough safe from the attacks. With the comparison with existence algorithm this proposes algorithm takes the advantage on them in number of character supported. Fig shows this comparison.

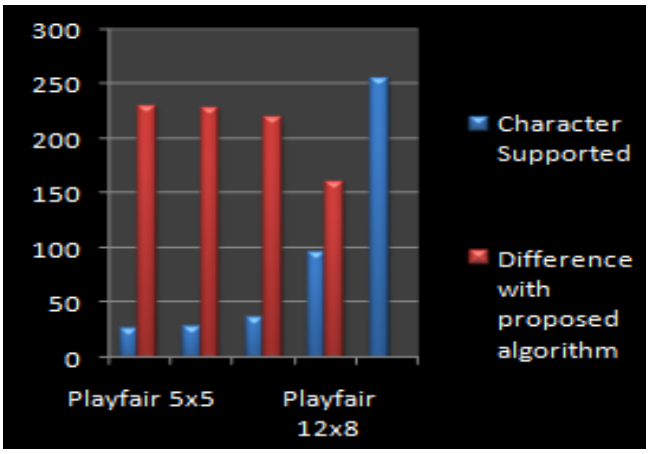

Fig 3: Graph number of character supported by different algorithm.

Frequency Analysis

Now, with the comparison with existence algorithm this proposes algorithm takes the advantage on them in frequency analysis attack. Fig 4 shows this comparison.

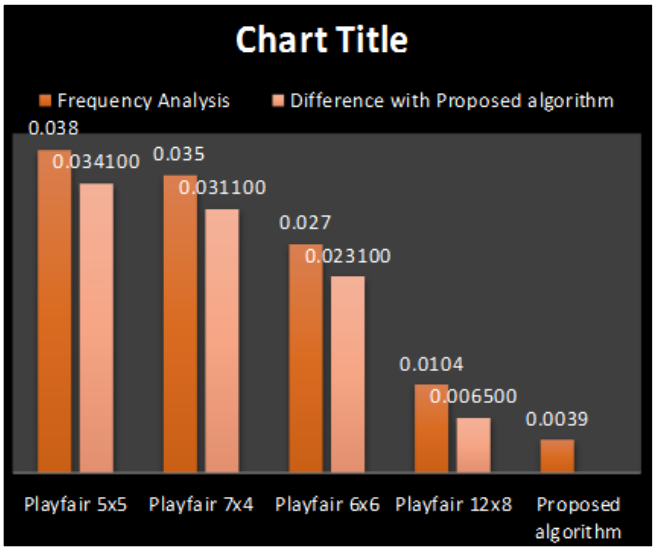

Fig 4: Graph of frequency analysis attack by different algorithm.

Advantage of Algorithm

- In this algorithm 256 character are used so it takes advantage on 5x5 matrix which used the 26 characters.
- The proposed 16×16 Playfair cipher can be said to be safe from Brute Force Attack, as the attacker has to find in a 256×256 = 65536 digraphs.
- Increasing the key size also reduces the chances to break the cipher by the Frequency Analysis. The probability of occurrence of an element in the original Playfair (PF) matrix table of size 5×5 was 1/26 = 0.0384, whereas in the extended 16×16 Playfair matrix the probability is 1/256 = 0.00390625, which is far less when compared and it makes the frequency analysis a tougher job.
- The 'I' and 'J' character are in different cell. Space between two words in the Plain Text is considered as one character. Special characters are used in this algorithm.
- The uppercase and lower case alphabets are in this algorithm.
- An extra letter NULL is added when the PT word consists of odd number of character. In the Decryption Process this NULL is ignored.
- The solution should be completely secure. The key distribution problem must be solved by this solution.
- There are some ASCII values which can't printable on the screen so it is hard to retrieve the message by the hacker.

Conclusion and Future Work

Conclusion

So far the encryption technique adopting concept of PLAY-FAIR CIPHER MATRIX of size 5X5 has been programmed for calculating the Cipher Text CT1. Finally, we have pointed the merits and demerits of traditional PF algorithm. In this algorithm playfair matrix is used for creating the cipher text and the RSA algorithm is used for providing the secure channel.

Future work

In the future when new technology of cryptanalysis will come in the market, to prevent the data form that kind of attack, enhance this work in such type that it will be save our data from that kind of attack on data. There are some suggestions for the future work.

1. Work on the algorithm for encryption and decryption of the image, audio, video.
2. Try to generate the algorithm which provides more security than this algorithm, because security of key is depends on the RSA algorithm so take the large prime number as the value of P and Q.
3. Make easy key distribution, if there is more than on receiver.
4. Decrease the decryption time of the RSA algorithm.

References

1. Aftab Alam, Shah Khalid, Muhammad Salam. A Modified Version of Playfair Cipher Using 7×4 Matrix. International Journal of Computer Theory and Engineering. 2013; 5:4.
2. Ravindra babu, Udaya Kumar, Vinaya babu. An Extension to Traditional Play Fair Cipher Cryptographic Substitution Method, IJCA, 0975-8887. 2011; 17:5.
3. Umakanta Sastry V, Ravi Shankar N, Durga Bhavani S. A Modified Playfair Cipher Involving Interweaving and Iteration. International Journal of Computer Theory and Engineering. 2009; 1(5):1793-8201.
4. Lt. Ravindra Babu Kallam, Udaya Kumar S, Vinaya Babu A, Thirupathi Reddy M. A Block Cipher Generation Using Color Substitution, ©2010 International Journal of Computer Applications. 0975 – 8887; 1:28.
5. Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa. A DNA and Amino Acids-Based Implementation of Playfair Cipher, (IJCSIS) International Journal of Computer Science and Information Security. 2010; 8:3.
6. Subhajit Bhattacharyya, Nisarga Chand, Subham Chakraborty. A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps. International Journal of Advanced Research in Computer Engineering & Technology. 2014; 3:2.
7. Packirisamy Murali, Gandhidoss Senthil Kumar. Modified Version of Playfair Cipher using Linear Feedback Shift Register, International Conference on Information Management and Engineering, 2009, 488-490.
8. Fauzan Saeed, Mustafa Rashid. Integrating Classical Encryption with Modern Technique, IJCSNS International Journal of Computer 280 Science and Network Security. 2010; 10(5):280-285.
9. Sriram Ramanujam, Marimuthu Karuppiaj. Designing an algorithm with High Avalanche Effect, IJCSNS International Journal of Computer Science and Network Security. 2011; 11(1):106-111.
10. Shiv Shakti Srivastava, Nitin Gupta. A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications (0975 – 8887). 2011; 20:6.
11. Gaurav Agrawal, Saurabh Singh, Manu Agarwal. An Enhanced and Secure Playfair Cipher by Introducing the Frequency of Letters in any Plain text". Journal of Current Computer Science and Technology. 2011; 1(3):10-16
12. Packirisamy Murali, Gandhidoss Senthilkumar, Modified Version of Playfair Cipher using Linear Feedback Shift Register, IJCSNS International Journal of Computer Science and Network Security. 2008; 8:12.
13. Harinandan Tunga, Soumen Mukherjee A New Modified Playfair Algorithm Based On Frequency Analysis. International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459. 2012; 2:1.