Extended 16x16 Play-Fair Algorithm for Secure Key Exchange Using RSA Algorithm

Sanjay Kumar Mathur¹* Sandeep Srivastava²
Assistant Professor, Department of Computer Science & Engineering
Shekhawati Institute of Engineering & Technology, Sikar,

Abstract – With the world entering in the 21st century rigorous efforts are being made to secure data and flow of information among the users. Though with the advancements are fast and efficient the third party intervention and security threats has also increased many folds. The algorithms being used to encrypt and decrypt data needs to be strong enough to secure the data but also simple enough for a user to handle the process. With this article a novel, practical approach is presented which not only makes the information more secured but also being based on RSA algorithm is easy enough for users to understand and implement into the systems.

Key Words: Play Fair Cipher, RSA Algorithm.

1. INTRODUCTION

In the time of digital world, security of "information" has become critical to both organization and individuals. At the purpose once info is place away or transmitted by a message or bundles of messages by some channel there ought to be some mechanism or technique to defend that info from interruption and hacking.

The interrupted data flow and hacking may lead to unwanted avalanche of events that can hinder with a security of nation and/or privacy of an individual(s). Thus there's a needs of certain mechanism which can protect the information all through the channel from any outside intervention and provide robust against the changing environmental conditions which may lead to wrong interpretation of the data at the receiver.

Consequently, Cryptography assumes an imperative part in data communication in today's digital world or in internet. Current cryptography is a piece of mathematics and innovation of software engineering. Applications of cryptography incorporate all PC passwords, ATM cards, and electronic trade.

The present research concentrates on the attempting to being improve the existing Play-fair technique (5x5 matrix) to 16x16 size of rectangular matrix with the assistance of RSA algorithm (asymmetric key cryptography), to provide information security and handle them with right sorts of counter measures. The security of key will lead us to secure data from being hacked and make data more robust against noise.

2. CRYPTOGRAPHY

Cryptography can be defined as a practice and study of science which leads to hiding of user data from any external intervention (like noise, security hacks, etc.) and provide a safer way to commute between the transmitting and receiving party. Cryptography leads to various aspects of information security such as data confidentiality, data integrity, authentication and non-repudiation. Cryptography in its most primitive definition is the process of encryption and decryption. Encryption is the process of converting the user's message (plaintext) to a certain unreadable nonsense text (ciphertext). This will allow the system to become robust against the possible data security threats. On the other hand, Decryption is the process of reconverting the cipher text back to original plaintext of the user. Here the important point is the data should not get changed during the process which will lead to different conclusions. During recent decades the cryptography has been extended further to include message integrity checking, sender/receiver identity authentication, digital signatures and interactive proofs and secure computation, among others.
very hard to calculate. The user of RSA algorithm generates and publically issues a public key along with one auxiliary value that is used during calculations. The prime numbers must be kept private. The receiver with the public key and with its own private key decrypts the plaintext back from ciphertext.

4. PLAY FAIR ALGORITHM

The Play-fair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher. 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 (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitutes the cipher key. To encrypt a message, one would break the message into bigrams (groups of 2 letters) such that, for example, "Hello World" becomes "HE LL OW OR LD", and map them out on the key table. If needed, append an uncommon monogram to complete the final bigram. The two letters of the bigram are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Play-fair use "Q" instead of "X", but any letter, itself uncommon as a repeated pair, will do.

2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).

3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).

4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first
letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

5. PROPOSED ALGORITHM

At the Sender ends:

Step one: Construct a modified table of Play-fair cipher technique of size 16X16, that contain each one of the alphabets frame begin to end capitalized and a to z in lower-case letter, all the special characters that are on the keyboard and each numeric esteem (from zero to 9).

The PF encryption technique is separation into 2 stages:

a) First stage is creation and population of Matrix (by mistreatment the key).

b) The second stage is encryption process of the plain text message with the assistance of the Matrix. Make the Cipher text (CT1) of the plain text.

Step Two: Utilize 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 Three: decrypt the Cipher Text (CT2) into Plain Text (Playfair matrix key).

Step Four: 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 every one numeric values (from zero to 9). The PF decryption technique is split into 2 phases:

c) First part is creation and population of Matrix (by using the key).

d) The second section is decryption method of the cipher text (CT1) message with the help of the matrix and makes the plain text.

5.4 Experiment Analysis

The proposed work is dividing in two phases:

- The principal stage for Matrix construction utilizes every one of the standards of customary Play fair matrix with these changes:
  - The 2 I and J letters in upper case and lower-case letter are considered as 2 unique letters (I and J are different and that i and j are distinctive).
  - It enables more than 26(up to 256 characters with no duplicate) characters as key.
  - It is case sensitive; it utilizes the upper case as well as lower case characters.

![Fig.5.1 Algorithm for Proposed Methodology](http://www.ijfrcsce.org)

6. RESULTS AND DISCUSSION

Performance Analysis

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

Character Supported

From the over 9 illustration, we can see that there is no any two consequences of cipher text 1 and cipher text 2 are same. So we can state that this algorithm is sufficient safe from the attacks.
With the comparison with existence algorithm this proposes algorithm takes the preferred standpoint on them in number of character upheld. Fig 6.1 shows this comparison.

**Frequency Analysis**

Now, with the comparison with existence algorithm this proposes algorithm takes the advantage on them in frequency analysis attack. Fig 6.2 shows this comparison.

**Brute Force Attack**

In the last comparison with existence algorithm this proposes algorithm takes the advantage on them in Brute Force Attack. Fig 6.3 shows this comparison.

**6.2 Advantage of Algorithm**

- In this algorithm 256 characters are utilized therefore it exploits on 5x5 matrix that utilized the 26 characters.
- The planned 16×16 Playfair cipher may be said to be protected against Brute Force Attack, because the attacker must find in a 256×256 = 65536 digraphs.
- Increasing the key size likewise reduces the probabilities to interrupt the cipher by the Frequency Analysis. The chance of occurrence of a part within the original Playfair(PF) matrix table of size 5×5 was 1/26 = 0.0384, though within the extended16×16 Playfair matrix the likelihood is that 1/256 = 0.00390625, which is way less when compared and it makes the frequency analysis a more durable employment.
- The "I" and "J" character are in various cell house between 2 words within the Plain Text is considered together character. Special characters are utilized as a vicinity of this formula.
- The uppercase and graphic symbol alphabets are during this formula.
- An extra letter NULL is included once the word consists of weird number of character within the decryption method this NULL is disregarded.
• The arrangement ought to be completely secure. The key dispersion issue must be settled by this arrangement.

• There are some ASCII values which can’t printable on the screen so it is hard to retrieve the message by the hacker.

7. CONCLUSION AND FUTURE WORK

Conclusion
Keeping in mind the end goal to beat demerits, we’ve got proposed an extension to customary PF cipher algorithm; which may be utilized all the additional with efficiency notwithstanding for the Plain Text containing alphanumeric esteemed and special characters and utilize the flip factor for the high avalanche result. Then a public key encryption system has been designed that provides the authentication and confidentiality but there are a couple of limitations. Complete mathematical reasoning is given to demonstrate the exact outcome at each sender and receiver sides the previous encryption technique is likewise a chunk of this technique. Once completion of program the strength of the technique has been checked and this encryption technique will likewise be utilized for alternative networks. During this algorithm play-fair matrix is employed for making the cipher text and also the RSA algorithm is used for providing the secure channel.

Future work
1. Later on when new technology of cryptanalysis will come in the market, to prevent the data frame that kind of attack, enhance this work in such sort that it will be spare our data from that kind of attack on data. There are a few proposals for the future work.

2. Work on the algorithm for encryption and decryption of the picture, sound, video.

3. Try to create the algorithm which provides more security than this algorithm, because security of key is relies on upon the RSA algorithm so take the vast prime number as the estimation of P and Q.

4. Make simple key dispersion, if there is more than on receiver.

5. Decrease the decryption time of the RSA algorithm.

REFERENCES


Corresponding Author

Sanjay Kumar Mathur*
PG Scholar
E-Mail – sameer.sanjaymath0@gmail.com