IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 10, Iss 9, Aug 2021

An approach towards modification of playfair cipher using 16 x 16 matrix

Dr. S.Radha Krishna,Assistant Professor in CSE Department,JNTUA College of Engineering Pulivendula

***Abstract*—The Play fair cipher is a popular poly alphabetic encryption.It mathematically secures information by encrypting the message with a key.The same key is used to change cipher text diagrams into plain text diagrams during decryption.However, only 25 capital alphabets can be supported by the original 5 x 5 play fair cipher.The play fair cipher's current approaches are researched.The suggested method circumvents the limitations of past studies that used a play fair cipher using a 5x5 matrix, 7x4 matrix, and 6x6 matrix.The suggested technique utilises a 16x16 matrix and provides strength for fair cipher play.The suggested work is an improvement to the current technique that makes use of matrix rolling, shifting, and rotation.It uses alphabets, both lowercase and uppercase letters, numbers, and special characters to build the matrix's content.**

***Index Terms*—Encryption, Decryption, Play fair cipher, matrix rotation,matrix shifting,matrix rolling**

I. Introduction

Data security is more important than ever in the modern world due to the substantial growth in internet traffic caused by remote work. To safeguard private information, sensitive data, and the security of both the sender and receiver, encryption techniques like cryptography are crucial. [1]

Cryptography involves converting plain text into indiscernible text to make it readable only to the intended recipient and sender. It has several applications, including preventing data theft, user authentication, and ensuring user security. Cryptography is divided into two categories: symmetric and asymmetric. Classical ciphers like the hill and playfair ciphers have long been staples in the world of cryptography. The playfair cipher is the most often used cipher algorithm for a variety of reasons. The algorithm is more difficult for the cryptanalyst to decipher because each step produces a unique ciphertext, as can be seen by carefully examining it. It is unaffected by attacks using brute force. It is incredibly difficult to decode the cipher without the key. The substitution is made simple by it. [2]

The traditional playfair cipher, however, is less trustworthy in the present world due to technological advancements. Classical playfair ciphers produce encrypted data that is simple to decode and offers very little security. The traditional playfair encryption has already undergone numerous modifications that increase security over the traditional playfair cipher.
In this study, we also suggest a variation that primarily relies on a lightweight cryptography technique.It offers secure solutions for constrained resources in a network while using less memory, less computer power, and less energy. In order to add an additional degree of protection, we are adding rotation, shifting, and rolling in addition to the standard confusion and diffusion techniques. We are also correcting the playfair cipher's fundamental flaw, which is its restriction to only 25 characters. The proposed method uses a 16*16 matrix rather than a 5*5 matrix to take into account all of the lowercase and uppercase alphabets, integers and many symbols. [3]

II. Review and Literature

A. Traditional Play fair Algorithm

The Playfair cipher is a traditional encryption method that was developed in 1854 by Charles Wheatstone, but it was given the name Lyon Playfair in honour of their mutual acquaintance. It encrypts plaintext messages using a polygraphic substitution technique. Every letter of the alphabet is employed in the method's 5x5 letter matrix, known as a Playfair square, with the exception of "J," which is mixed with "I." The keyword is then entered into the matrix, followed by the orderly entry of the remaining letters. Each pair of two letters from the plaintext message is then encrypted according to a set of criteria.If the letters are not in the same row or column, the letters at the corners of the rectangle the two letters make take their place. The recipient receives the generated ciphertext and uses the identical playfair square to decrypt the message. The conventional playfair cipher is a straightforward but efficient encryption method, however it is susceptible to several attacks, such as frequency analysis and assaults using known plaintext.

B. Limitation of traditional play fair:

The conventional Playfair cipher uses an alphabetic 5x5 matrix and a polygraphic substitution cipher that works on pairs of letters. It is, nevertheless, susceptible to some attacks because of a number of flaws. The following are some of them: a constrained key space, susceptibility to known-plaintext assaults, frequency analysis attacks, a lack of authentication, and a constrained character set.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 10, Iss 9, Aug 2021

TABLE I
STEPS OF TRADITIONAL PLAYFAIR CIPHER

Ref.	Process	Description
[4]	Generating Matrix	• A 5x5 grid of alphabets known as the key square serves as the encryption key for plaintext. • One letter of the alphabet, typically J, is left off the table (the letter I might be used in its place instead), and each of the 25 alphabets must be distinct.
[5]	Encryption	• The plaintext is split into pairs of letters (digraphs). • Replace each letter with the letter to its right (wrapping around to the left side of the row if necessary) if both letters are in the same row of the key square. • Replace each letter with the letter below it (wrapping around to the top if necessary) if both letters are in the same column of the key square. • If neither of these conditions is true, use these two letters to make a rectangle and swap out each letter with the letter in the corner opposite.
[6]	Decryption	• If it happens that two letters are in the same row, replace them with the letter on their left. Return to the end of the same row and only change a letter that is at the beginning with the start letter. • If, by chance, two letters appear in the same column, replace them with the letter above. If the letter is at the top, replace it by moving the letter from the column's bottom to the top. • Imagine drawing a rectangle and writing the alphabets on the corners if neither alphabet is in the same column or row.

The key space may be quite big, but it is still small in comparison to most contemporary encryption techniques, leaving it open to brute-force attacks. The Playfair cipher is additionally unprotected against tampering attempts since it lacks authentication and integrity verification.Due to these restrictions, the classic Playfair cipher is typically regarded as less safe when compared to contemporary encryption techniques, and it is ineffective for encrypting messages that contain characters other than the restricted character set. [7]

C. Modifications on Traditional Play fair Algorithm

To improve the security and dependability of the traditional Playfair cipher in the present day, numerous modifications can be made. The main focus of the change is the security it offers against various threats. [8]

The traditional Playfair Cipher can be improved in the following ways to increase security and benefit:

The table below lists modifications to the Playfair Cipher along with their complexity and drawbacks. The modifications are listed in the first column, while the second column describes the complexity of each modification, ranging from low to high. The third column lists the drawbacks of each modification. The modifications listed are Multiple Rounds of Encryption, Variable Matrix Size, Substitution and Transposition, Key Management, and Modified Playfair Cipher. This table can be used as a reference to compare the different modifications and their respective trade-offs.

III. PROPOSED MODIFICATION ON PLAYFAIR CIPHER

In this work, we provide a modification to the play fair 16x16 matrix to strengthen the correctness and compatibility of the play fair cipher with data content.

The technique starts by creating a 16x16 matrix using the matrix with all capital and lowercase letters, the numbers 0 to 9, the arrow, the mathematical symbols +, -, /, and *, and many other symbols, the result is a total of 256 characters we start the encryption of the plain text.

A. Encryption

Certain steps in the encryption process give the algorithm an additional layer of security. The stages are explained in detail below:

- **Rotation**: The 16x16 matrix is rotated by 90 degrees clockwise as the initial stage in encrypting plain text. Rows and columns are transformed in this procedure from one another.Here is a section of above matrix showing the rotation process.

  The algorithm used to rotate the matrix is shown in the pseudo code below.

---

cipher key and plain text as input. After creating a 16x16

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 10, Iss 9, Aug 2021

Algorithm 1 Matrix Rotation Algorithm N ← 5Fun rot90Clkwse(arr)global Nfor j ← N dofor i ← N-1 to -1 step -1 dowrite(arr[i][j], end ←" ")x=arr[i][j]end forwrite(x)end forarr1 ← [row 1,row2,row 3,row 4,row 5... row 16]rot90Clkwse(arr1);=0

- **Shifting**: Matrix shifting goes through the elements of each row and shifts them in accordance with an offset value. To start the shift row operation, the elements ofthe second row of the matrix are moved one (1) time to the right.In addition, rows after that experience a number of shifts dependent on their row number less one. The pseudo code below demonstrates the algorithm that was used to shift the matrix.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 10, Iss 9, Aug 2021

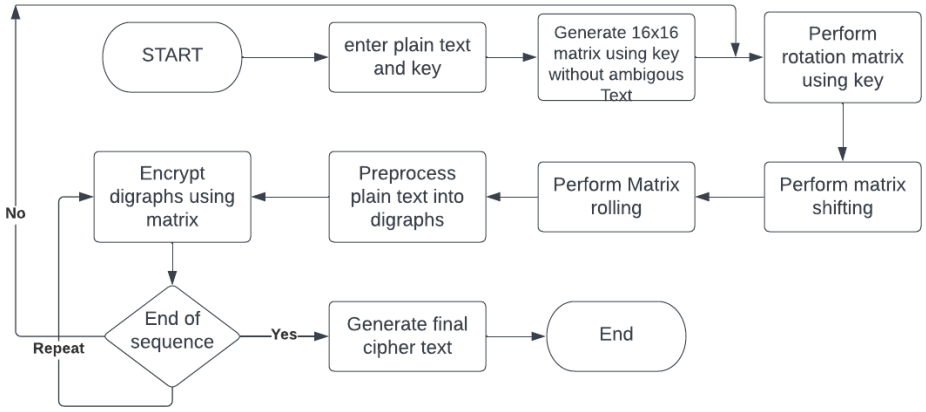

Fig. 1. Proposed methodology flowchart

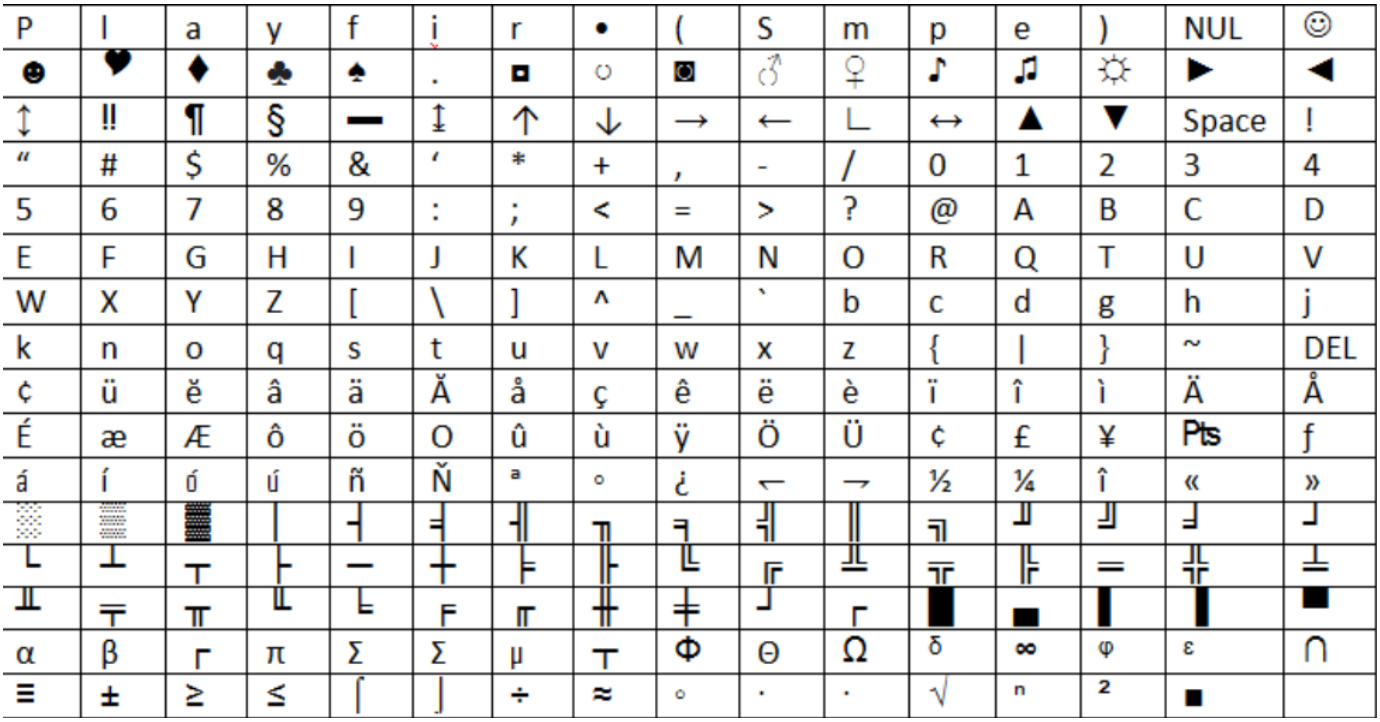

Fig. 2. Structure of proposed architecture

- **Rolling**: The third operation, called ”matrix roll” shifts an array of items while iterating across a set of axes. In the advised method, a full row is raised by the roll action. The algorithm used to roll the matrix is shown in the pseudo code below.

  We will preprocess plain text into digraphs as the matrix rolls.Then, after utilising the matrix to encrypt digraphs, we will wait for the sequence to come to a conclusion. If it does, we will then produce the final cipher; otherwise, we should return to the stage that involved creating the 16-by-16 matrix using the key.

B. Decryption

As we did during encryption, we take the key and use it to form a 16*16 matrix in order to decrypt the encrypted text. Then we split the cipher text into digraphs and apply the decryption method similarly to the conventional Playfair cipher by employing one diagraph at a time. The matrix is then subjected to all three operations, rolling, shifting, and rotating in the appropriate order. The aforementioned procedure will

IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 10, Iss 9, Aug 2021

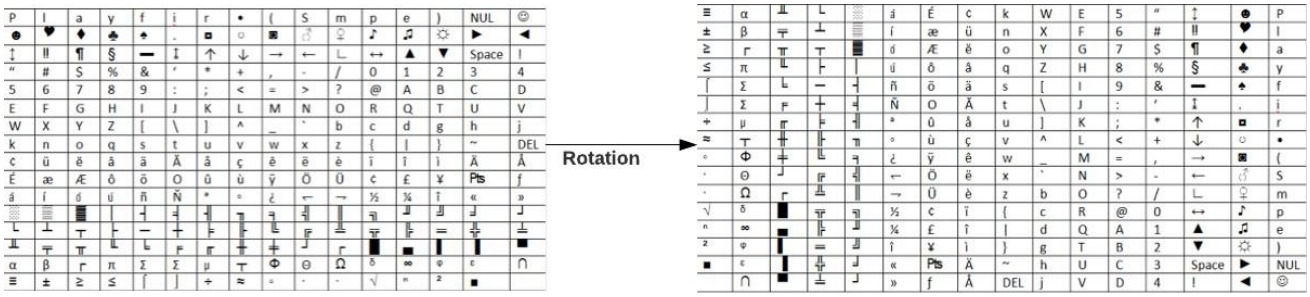

Fig. 3. Matrix Rotation

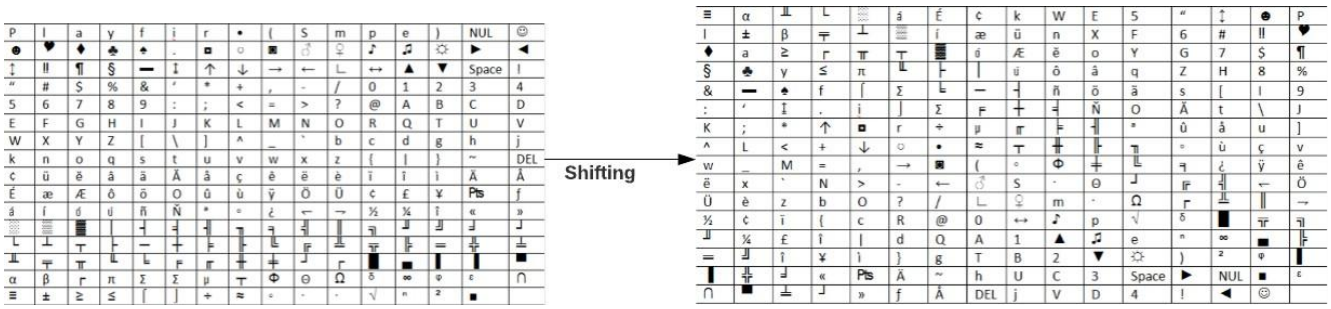

Fig. 4. Matrix Shifting

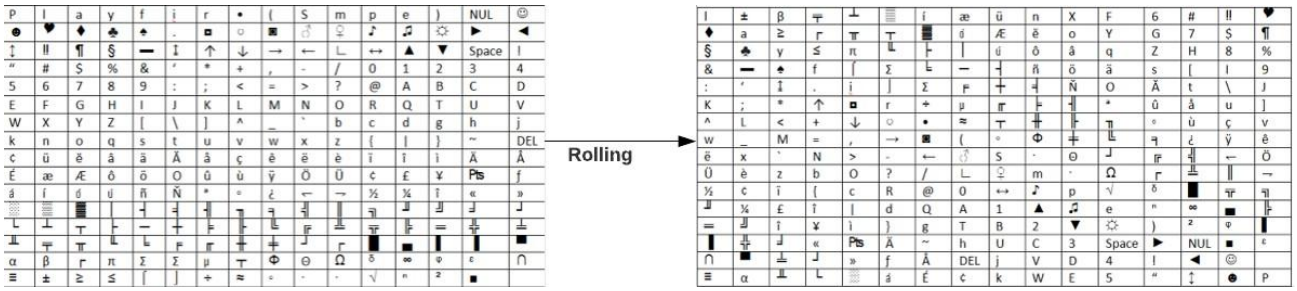

Fig. 5. Matrix Rolling

be repeated until all of the digraphs have been transformed into plain text.

IV. Result and Analysis

After testing the proposed algorithm into the system with keyword ”playfair” and plaintext as ”crpyptography”, we get the cipher text as below: Keyword: Playfair

A poly-graphic substitution cipher that works with pairs of letters rather than single letters is the playfair cipher algorithm. In order to encrypt and decrypt messages, it employs a 16x16 matrix of letters. The alphabetical letters of the alphabet are commonly used to fill the matrix, while additional characters like numerals and punctuation marks are also permitted.

A. Brute Force Attack

A cryptographic system can be broken via a brute force attack, which involves attempting every potential key until the right one is discovered. Although it can work well against weak systems, strong encryption with vast key spaces is

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 10, Iss 9, Aug 2021

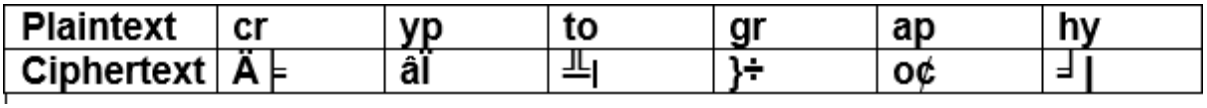

Fig. 6. Example

TABLE II
WAYS OF MODIFICATIONS IN TRADITIONAL PLAYFAIR CIPHER

Ref.	Modifications	Description
[9]	Key Management	The encryption key used in the classic playfair Cipher is a 5x5 matrix of letters that both the sender and the recipient share. The decoding of messages is possible, nevertheless, if this key is compromised. The security of the cipher can be considerably improved by altering the key management procedure, for as by employing a more powerful key generation method or a bigger key space.
[10]	Multiple Rounds of Encryption	Applying the encryption algorithm to the plaintext message numerous times is one method for enhancing the security of the playfair Cipher. Several rounds of encryption is the name given to this procedure. This increases the complexity and decryption difficulty of the cipher text, increasing its security.
[11]	Substitution and Transposition	The plaintext message is encrypted using just substitution in the classic playfair Cipher. The cipher text generated by the encryption process is made more complex by the addition of a transposition phase, making it more challenging for attackers to decrypt.
[12]	Variable Matrix Size	Another change to the playfair Cipher is the substitution of a variable matrix size for the conventional 5x5 matrix. The key space is expanded by increasing the matrix size, strengthening the cipher's security.

typically impossible to implement. Using strong encryption and key management procedures, as well as capping the number of attempts permitted, can reduce the likelihood of brute force assaults. [18]

B. Frequency Analysis Attack

Frequency analysis attack is a method of breaking a cryptographic system by analyzing the frequency distribution of characters or symbols in the ciphertext. It's most effective against simple substitution ciphers. To mitigate the risk, more complex substitution ciphers should be used, and techniques like adding random data or padding the ciphertext can further disrupt the frequency distribution. [19]

Algorithm 2 Matrix Shifting Algorithm

```
Fun cir_st(arr, st)
st ¸stmodlen(arr)
arr[—st], arr[: − st]¸arr[: st], arr[st :]
m_trans(m)
cir_st(m[1], 4)
cir_st(m[2], 3)
cir_st(m[3], 2)
cir_st(m[4],                    1)
m¸[row1, row2, row3, row4, row5...row16]
m_trans(m)
ms¸m
write(ms)
= 0
```

Algorithm 3 Matrix Rolling Algorithm

```
mr ← np.roll(ms, -1, axis=0)write(mr)=0
```

C. Man in the Middle Attack

A man-in-the-middle (MITM) attack is where an attacker intercepts and alters communications between two parties without their knowledge. It can be carried out by exploiting vulnerabilities or tricking users. To mitigate the risk, cryptographic protocols like SSL/TLS can be used, and user education can help prevent phishing and untrusted network connections. [20]

The playfair cipher algorithm encrypts data using a number of operations, such as matrix rotation, matrix rolling, and matrix shifting. By making the encryption process more complex, these activities contribute to improving the security of the cipher. The analysis shows that doing the aforementioned raises the algorithm's resistance against attacks like brute force, man in the middle and frequency analysis. The attacker would not gain any significant information in a reasonable amount of time.

The number of distinct keys that can be generated by the matrix determines the size of the key domain. A square matrix that is filled with alphabetic or other characters serves as the Playfair cipher's key.

The matrix has 16 rows and 16 columns, thus there are 16x16 = 256 places in the matrix where characters could be placed. However, as no letter can appear twice in a row or column, the first character of the key can be any of the 26 letters of the alphabet, and each succeeding character can only be one of the remaining 25 letters.

As a result, there are the following number of keys that could be used with a 16 by 16 Playfair cipher matrix:

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 10, Iss 9, Aug 2021

TABLE III
STUDY OF VARIOUS MODIFIED PLAYFAIR ALGORITHM TYPES

Ref.	Modification	Complexity	Drawbacks
[13]	Uses a rectangular matrix of size MxN. apply a series of substitution and transposition steps using the rectangular matrix.	Medium(uses a rectangular matrix). substitution and transposition make its time complexity average.	Although difficult but can be Broken. Limited key space, more time-consuming and resource-intensive.
[14]	Uses random swap patterns and rotation to make the cipher more secure.	Medium(uses 6*6) can range from $O(n^2)toO(k)orO(n)$,n is the number of rows.	Rotation and random swap lead to a larger number of possible keys difficult to manage and securely distribute.
[15]	Uses 8*8 matrix combined with LFSR.Circular Shift Rule, alternate Pair Rule	High as it uses LSFR, which requires more hardware resources and power consumption.	i) LFSR is limited by the size of the register ii) Vulnerable to correlation attacks.
[16]	Uses 4*19 cipher matrix RSA stenography RMPS keyless transposition	Medium (4x19, which makes it slightly slower than the standard 5X5. the use of steganography, RSA and RMPS keyless transposition.)	Limited by the size of the RSA key.complex and computationally intensive.
[17]	Uses 6*6 Key matrix Combined with block cipher Uses Transposition Technique	Medium(addition of block cipher increases the complexity) Permutation matrix take O(n!) time	Limited amount of data at a time and Vulnerable against attacks

26 × 25255 is roughly equivalent to 1.045 x 10472.
This indicates that a 16 by 16 Playfair cipher has a very vast key space, making it challenging for an attacker to find the right key using brute-force attacks.

V. CONCLUSION

We have examined the drawbacks of the original play fair cipher in this essay.Then by enlarging the dimension of the key matrix,we improved the conventional play fair cipher and strengthened security against Brute force attack,Dictionary attack,chosen plain text/cipher text attack and known plain text attack.the fastest method of encryption,the play fair cipher uses a 16x16 matrix that contains all the printed extended ASCII values,making it more difficult to crack.we demonstrated through crypt analysis that the modified play fair cipher is more robust than the original.Two distinct keys can be used for encryption and decryption in this application in the future for enhancement.public key applied to the decryption.To further improve the security of information ,additional,more sophisticated encryption techniques can be added.

REFERENCES

[1] G. Agrawal, S. Singh, and M. Agarwal, "An enhanced and secure playfair cipher by introducing the frequency of letters in any plain text," *Journal of Current Computer Science and Technology*, vol. 1, no. 3, pp. 10–16, 2011.

[2] J. C. C. Ferrer, F. E. D. Guzman, K. L. E. Gardon, R. J. R. Rosales, D. Dell Michael Badua, and D. R. Marcelo, "Extended 10 x 10 playfair cipher," in *2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM)*, pp. 1–4, 2018.

[3] V. U. Sastry, N. R. Shankar, and S. D. Bhavani, "A modified playfair cipher involving interweaving and iteration," *International journal of Computer theory and Engineering*, vol. 1, no. 5, p. 597, 2009.

[4] S. Basu and U. K. Ray, "Modified playfair cipher using rectangular matrix," *International Journal of Computer Applications*, vol. 46, no. 9, pp. 28–30, 2012.

[5] H. Tunga, A. Saha, A. Ghosh, and S. Ghosh, "Novel modified playfair cipher using a squarematrix," *International Journal of Computer Applications*, vol. 101, no. 12, pp. 16–21, 2014.P. Goyal, G. Sharma, and S. S. Kushwah, "Network security: A survey paper on playfair cipher and its variants," *Int. J. Urban Des. Ubiquitous Comput*, vol. 3, no. 1, p. 9, 2015.

[6] S. Dhenakaran and M. Ilayaraja, "Extension of playfair cipher using 16x16 matrix," *International Journal of Computer Applications*, vol. 48, no. 7, 2012.

[7] M. M. Maha, M. Masuduzzaman, and A. Bhowmik, "An effective modification of play fair cipher with performance analysis using 6x6 matrix," in *Proceedings of the International Conference on Computing Advancements*, pp. 1–6, 2020.

[8] P. Murali and G. Senthilkumar, "Modified version of playfair cipher using linear feedback shift register," in *2009 International Conference on Information Management and Engineering*, pp. 488–490, 2009.

[9] R. S. Villafuerte, A. M. Sison, and R. P. Medina, "i3d-playfair: An improved 3d playfair cipher algorithm," in *2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)*, pp. 538–541, 2019.

[10] M. S. Sannidhan, K. B. Sudeepa, J. E. Martis, and A. Bhandary, "A novel key generation approach based on facial image features for stream cipher system," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 956–962, 2020.

[11] A. A. Alam, B. S. Khalid, and C. M. Salam, "A modified version of playfair cipher using 7? 4 matrix," *International Journal of Computer Theory and Engineering*, vol. 5, no. 4, p. 626, 2013.

[12] R. Patil, S. V. Bang, and R. B. Bangar, "Improved cryptography by applying transposition on modified playfair algorithm followed by steganography," *Int. J. Innov. Sci. Res. Technol*, vol. 6, no. 5, pp. 616–620, 2021.

[13] S. Hans, R. Johari, and V. Gautam, "An extended playfair cipher using rotation and random swap patterns," in *2014 International Conference on Computer and Communication Technology (ICCCT)*, pp. 157–160, IEEE, 2014.

[14] S. S. Srivastava and N. Gupta, "A novel approach to security using extended playfair cipher," *International Journal of Computer Applications*, vol. 20, no. 6, pp. 0975–8887, 2011.

[15] S. S. Chauhan, H. Singh, and R. N. Gurjar, "Secure key exchange using rsa in extended playfair cipher technique," *International Journal of Computer Applications*, vol. 104, no. 15, 2014.

[16] R. Babu K, S. Uday Kumar, A. Vinay Babu, I. Aditya, and P. Komuraiah, "An extension to traditional playfair cryptographic method," *International Journal of Computer Applications*, vol. 17, no. 5, pp. 34–36, 2011.

[17] A. Kaur, H. K. Verma, and R. K. Singh, "3d—playfair cipher using lfsr based unique random number generator," in *2013 Sixth International Conference on Contemporary Computing (IC3)*, pp. 18–23, IEEE, 2013.

[18] N. Chand and S. Bhattacharyya, "A novel approach for encryption of text

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 10, Iss 9, Aug 2021

International Journal of Engineering Science and Innovative Technology (IJESIT) Volume, vol. 3, pp. 478–484, 2014.

[19] M. S. Yousif, R. K. Salih, and N. M. G. Alsaidi, "A new modified playfair cipher," in *AIP Conference Proceedings*, vol. 2086, p. 030047, AIP Publishing LLC, 2019.