PLAYFAIR CIPHER

Project Report submitted to
Maharaja Sriram Chandra Bhanjadeo University

for the partial fulfilment for the award of the degree of

Master of Computer Application (MCA)

by
Tapas Kumar Nayak
(Roll No. 15101N204011)

Under the supervision of
Dr. Jibendu Kumar Mantri
Associate professor
Dept. of Computer Application
Maharaja Sriram Chandra Bhanjadeo University

August 2022

Dept. of Computer Application
Maharaja Sriram Chandra Bhanjadeo University
Sriram Chandra Vihar, Takatpur, Baripada - 757003, Dist: Mayurbhanj, Odisha

Dr. Jibendu kumar Mantri
Associate professor
Dept. of Computer Application
Maharaja Sriram Chandra Bhanjadeo University
Sriram Chandra Vihar, Takatpur
Baripada - 757003, Dist: Mayurbhanj, Odisha
Email: jkmantri@gmail.com

CERTIFICATE

I certify that **Tapas Kumar Nayak** has completed the project work on **"PLAYFAIR CIPHER"** submitted to Maharaja Sriram Chandra Bhanjadeo University in partial fulfilment of the requirement for the final semester of Master of Computer Application is a bonafide work carried out under my guidance.

.

Dr. Jibendu Kumar Mantri
Associate professor
Maharaja Sriram Chandra Bhanjadeo University
(Supervisor)

DECLARATION

I, **TAPAS KUMAR NAYAK**, Roll No: **15101N204011** do hereby declare that the project report entitled "PLAYFAIR CIPHER" submitted to Dept. of Computer Application, Maharaja Sriram Chandra Bhanjadeo University for the partial fulfilment award of the degree of MASTER OF COMPUTER APPLICATION (MCA), is an authentic and original work carried out by me at under the supervision and guidance of **Dr. Jibendu Kumar Mantri**, **Associate professor**, Dept. of Computer Application, Maharaja Sriram Chandra Bhanjadeo University

Tapas Kumar Nayak

Date :-

EVALUATION

This project report titled "**PLAYFAIR CIPHER**" submitted by **TAPAS KUMAR NAYAK**, Roll No. **15101N204011** is evaluated towards the partial fulfilment of final Semester MCA Examination 2022 of Maharaja Sriram Chandra Bhanjadeo University.

HOD

Dept. of Computer Application

Maharaja Sriram Chandra Bhanjadeo University

External Internal

ACKNOWLEDGEMENT

I would like to express my special thanks and gratitude to my project guide and mentor **Dr. Jibendu Kumar Mantri**, whose earnest suggestion, inspiration and involvement paved the way for the successful completion of the project. I would like to offer our special gratitude to her for sharing the ups and downs during the development and bearing the inconvenience.

I really want to thank our department faculty members, Prof. Himabindu Maringanti, Dr. Prasanta Kumar Swain, Mr. Swarupanda Bissoi, Jyoti Kumar Mahanta and Swabhiman Sarangi along with my mentor **Dr. Jibendu Kumar Mantri** of the Computer Application department for providing us all facilities that are required for our project.

Tapas Kumar Nayak

CONTENTS

1 Preamble

1.1 Introduction

In this age of universal electronic connectivity, of viruses and hackers, of electronic fraud, there is indeed no time at which security does not matter. It is now more important than ever to protect data and resources from disclosure, ensure the integrity of data and messages, and protect systems against network-based attacks due to the exponential growth of computer systems and their interconnection via networks. This increased dependence on the information stored and communicated using these systems by both organizations and individuals has also increased awareness of these issues.

Additionally, the fields of network security and cryptography have advanced, resulting in the creation of useful, easily accessible apps to enforce network security. The design of specific methods to guarantee the secrecy and/or validity of information is known as cryptography. Earlier, physical and administrative measures were primarily used to meet an organization's need for information security. But with the development of computers and then distributed systems, the idea of network security became extremely clear. In order to avoid threats to integrity, privacy, and accessibility, cryptographic algorithms are required.

Cryptography, in its early days was extensively deployed in war-zones where it was utilized in breaking the secret messages of the opponent army. Today, cryptography prevails and is majorly used in hiding personal data or classified credentials and also in securing the social media accounts, bank details and even e-mails.

Cryptography has become an essential tool in transmission of information. Cryptography is the central part of several fields: information security and related issues, particularly, authentication, and access control. Cryptography encompasses a large number of algorithms which are used in building secure applications. Cryptography is the study of Secret (crypto-)-Writing (-graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form. As the field of cryptography has advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances. Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives when we sign our name to some document and for instance and, as we move to world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for such procedures.

Cryptographic systems are generally classified along three independent dimensions:

1. Type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition.

2. The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each use a different key the system is referred to as asymmetric, two key, or public-key encryption.

3. The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

1.2 Objectives and Goals

The Main Goals of cryptography

1. Data Privacy(confidentiality)
2. Data Authenticity(it came from from where it claims)
3. Data integrity(it has not been modified on the way) in the digital world

1. **Confidentiality**

- Confidentiality is most commonly addressed goal
- The meaning of a message is concealed by encoding it
- The sender encrypts the message using a cryptographic key
- The recipient decrypts the message using a cryptographic key that may or may not be the same as the one used by the sender

2. **Data Integrity**

- Integrity Ensures that the message received is the same as the message that was sent
- Uses hashing to create a unique message digest from the message that is sent along with the message
- Recipient uses the same technique to create a second digest from the message to compare to the original one
- This technique only protects against unintentional alteration of the message
- A variation is used to create digital signatures to protect against malicious alteration

3. **Authentication**

- A user or system can prove their identity to another who does not have personal knowledge of their identity
- Accomplished using digital certificates
- Kerberos is a common cryptographic authentication system

2 REQUIREMENT GATHERING & ANALYSIS

2.1 Software Requirements

1. Windows 11
2. Visual Studio Code

2.2 Hardware Requirements

1. Multimedia Keyboard
2. Optical Mouse
3. Laptop
4. 512GB Solid State Drive
5. AMD Ryzen 5 processor

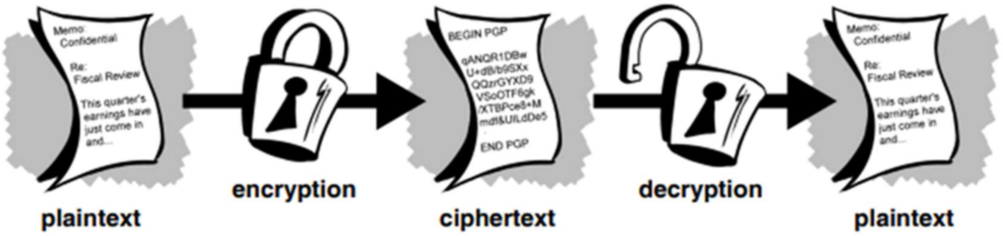
3 METHODOLOGY

CRYPTOGRAPHY :--

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.



There are 2 main types of cryptography in use –

1. Symmetric key cryptography –

   when the same key is used for both encryption and decryption

2. Asymmetric key cryptography –

   when one key is used for encryption and another for decryption

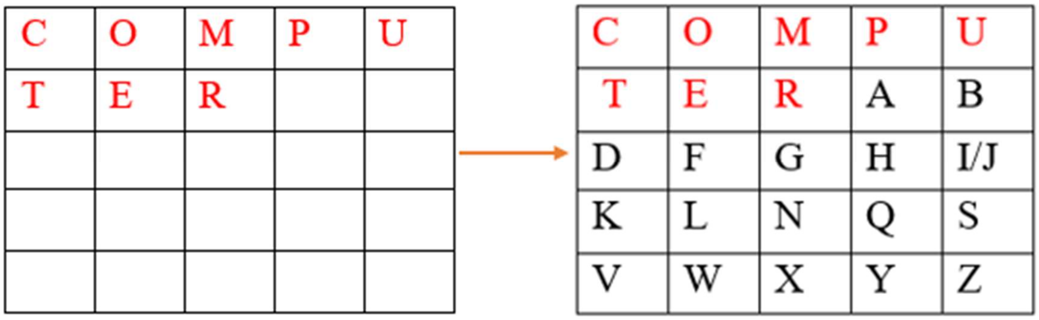
PLAYFAIR CIPHER –

Playfair Cipher Algorithm is one of the famous algorithms in history of block cipher. The Playfair cipher is a method of cryptography invented in 1854 by English physicist Sir Charles Wheatstone (1802–1875). The encryption method was named for Wheatstone's friend, Lyon Playfair, who helped popularize the cipher by successfully lobbying for its official adoption by the British government.

The best - known multiple letter encryption cipher is the Playfair, which creates diagrams in the plaintext as single units and translates these units into cipher text diagrams. The playfair algorithm is based on the use of 5 X 5 matrix of letters constructed using a keyword. Playfair is a substitution cipher.

Procedure:-

The traditional Playfair cipher uses 25 uppercase alphabets. A secret keyword is chosen and the 5 x 5 matrix is built up by placing the keyword without any duplication of letters from left to right and from top to bottom. The other letters of the alphabet are then placed in the matrix. For example if we choose “COMPUTER” as the secret keyword the matrix is given in table.



C	O	M	P	U
T	E	R		

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

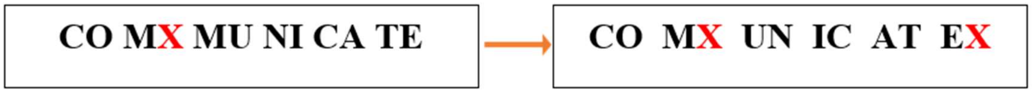
Then finish filling up the remaining squares of the matrix with the remaining letters of the alphabet, in alphabetical order. Since there are 26 letters and only 25 squares, we assign I and J to the same square.

- Divide Plain text into pairs of letters and when a letter is left alone, we can add "X" in the end. i.e.

  Input message – COMMUNICATE

  Plain text: CO MM UN IC AT EX

- If a pair contains repeated letters, we can use a filler letter such as x:
  CO MX MU NI CA TE
- In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies a pair of plaintext characters. So, it needs always even number of characters in plaintext message. In case, the message counts odd number of characters a spare letter X is added at the end of the plaintext message. Further repeating plaintext letters in the same pair are separated with a filler letter, such as X, so that the words "COMMUNICATE" would be treated as:



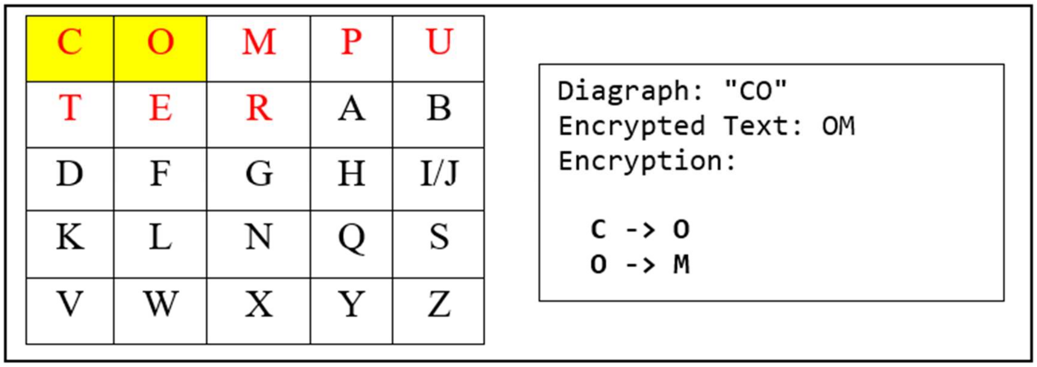
CO MX MU NI CA TE

CO MX UN IC AT EX

- There may be the following three conditions:

1. If a pair letters (diagraph) are in the same row:

In this case, replace each letter of the digraph with the letters immediately to their right. If there is no letter to the right, consider the first letter of the same row as the right letter. Suppose, Z is a letter whose right letter is required, in such case, V will be right to Z.

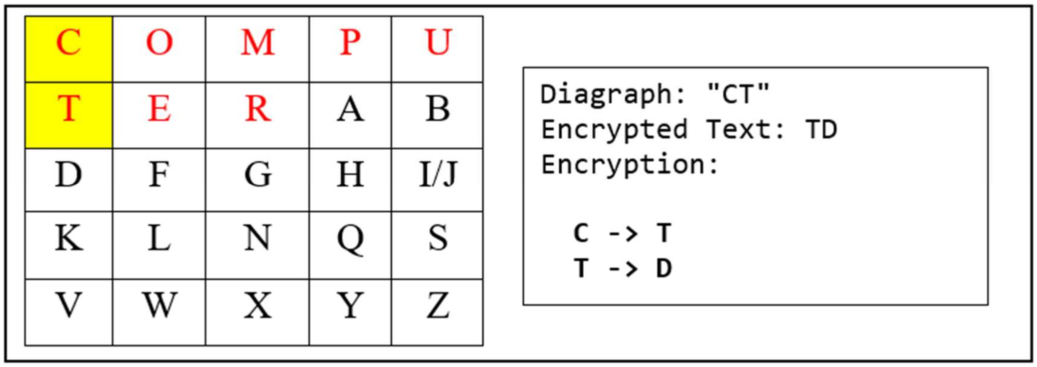


C	O	M	P	U
T	E	R	A	B
D	F	G	H	I/J
K	L	N	Q	S
V	W	X	Y	Z

```
Diagraph: "CO"
Encrypted Text: OM
Encryption:

  C -> O
  O -> M
```

2. If a pair of letters (digraph) appears in the same column:

In this case, replace each letter of the digraph with the letters immediately below them. If there is no letter below, wrap around to the top of the same column. Suppose, W is a letter whose below letter is required, in such case, Z will be below U.

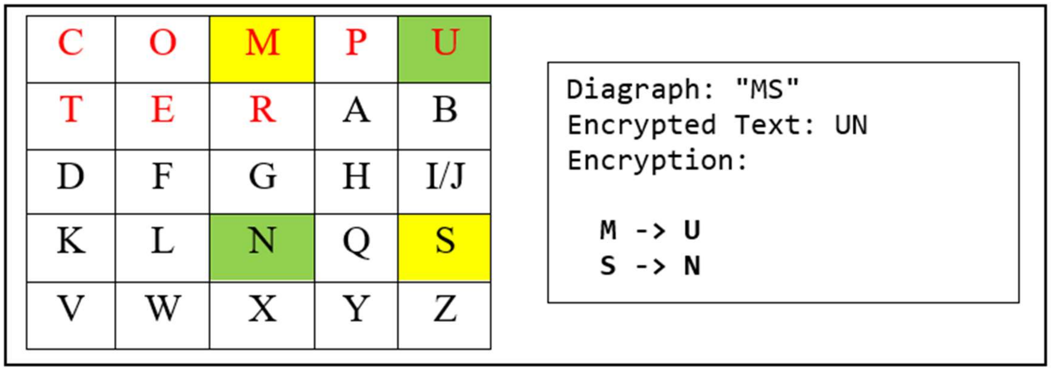


C	O	M	P	U
T	E	R	A	B
D	F	G	H	I/J
K	L	N	Q	S
V	W	X	Y	Z

```
Diagraph: "CT"
Encrypted Text: TD
Encryption:

  C -> T
  T -> D
```

3. If a pair of letters (digraph) appears in a different row and different column:

Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.



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

```
Diagraph: "MS"
Encrypted Text: UN
Encryption:

  M -> U
  S -> N
```

4. If two letters are in the same row, but there is no letter to the right:

we return to the first letter from the left.

Example of Playfair Cipher:--

Suppose, the plaintext is COMMUNICATION and the key that we will use to encipher the plaintext is COMPUTER. The key can be any word or phrase. Let's encipher the message COMMUNICATION.

1. First, split the plaintext into digraph

   i.e. CO MX MU NI CA TE.

2. Construct a 5*5 key-matrix (by rule 3). In our case, the key is COMPUTER

3. Now, we will traverse in key-matrix pair by pair and find the corresponding encipher for the pair.

   - The first digraph is CO. The pair appears in the same row.
     i.e. CO gets encipher into OM.

   - The second digraph is MX. The pair appears in the same column.

     i.e. MX gets encipher into RM.
   - The third digraph is MU. The pair appears in the same row.

     i.e. MU gets encipher into PC.

- The fourth digraph is NI. The pair appears in different rows and different columns.

  i.e. NI gets encipher into SG.

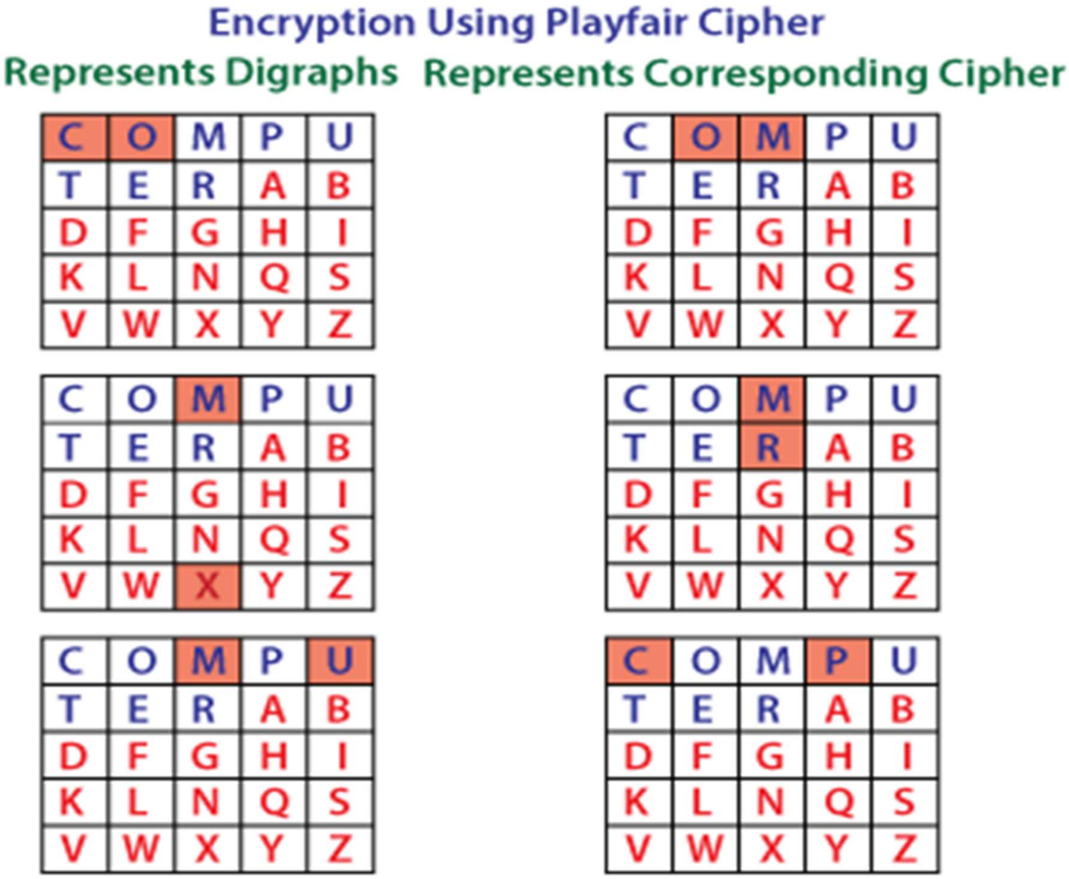
- The fifth digraph is CA. The pair appears in different rows and different columns.

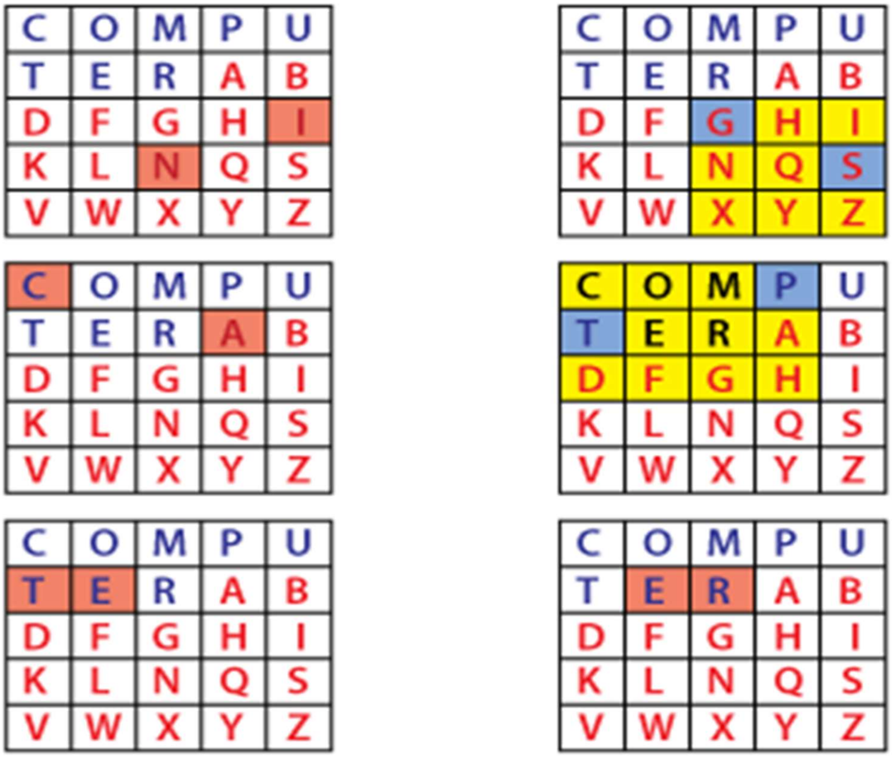
  i.e. CA gets encipher into PT.

- The sixth digraph is TE. The pair appears in the same row.

  i.e. TE gets encipher into ER.

Therefore, the plaintext **COMMUNICATE** gets encipher (encrypted) into **OMRMPCSGPTER.**





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

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

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

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

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

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

Terminology-

- Plaintext: It is the original message that is to be encrypted. It is also known as a message.
- Ciphertext: It is an encrypted message.
- Cipher: It is an algorithm for transforming plaintext to ciphertext.
- Key: It is the key to encrypt or decrypt the plaintext. It is known only to the sender and receiver. It is filled character by character in the matrix that is called key-table or key-matrix.
- Encipher: The process of converting plaintext into ciphertext is called encipher.
- Decipher: The process of removing ciphertext from plaintext is called decipher.
- Cryptanalysis: It is the study of the methods and principles of deciphering ciphertext without knowing the key.

4 LITERATURE REVIEW

1. **Aftab Alam, Shah Khalid, and Muhammad Salam (2013) : A Modified Version of Playfair Cipher Using 7×4 Matrix.**

This paper deals with the modification of playfair cipher. The original 5×5 matrix playfair cipher is modified to 7×4 matrix playfair cipher in which two symbol “*” and “#” are included. The addition of these two symbols in the matrix creates one-to-one correspondence between the plaintext and the ciphertext, which makes the encryption and decryption easy and unambiguous. The text is more unreadable when these symbols appear in the resulting ciphertext. Also, this method can be extended to encrypt and decrypt the messages of any language by taking a proper size matrix.

2. **Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh (2012): 3D (4 X 4 X 4) - Playfair Cipher**

The theme of this research is to provide security for the data that contains alphabets numerals and special characters during its transmission. However, because of the drawbacks inherent in the classical Playfair cipher which adversely affects the security, this research proposed 3D-Playfair Cipher (4 X 4 X 4 Playfair cipher) which works on trigraph rather than using digraph which eliminates the fact that a diagram and its reverse will encrypt in a similar fashion. 3D-Playfair cipher supports all 26 alphabets {AZ}, 10 digits {0-9} and 28 special characters { ! “ # $ % & ‘ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ | } which eliminate the limitation of classical Playfair in which “i” and “j” both character cannot appear at the same time. 3D-Playfair enhances the security by increasing complexity. Various types of cryptography attacks have been taken under consideration for original Playfair cipher but not vulnerable for this proposed cipher.

3. **Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh (2012) : 6 X 6 Playfair Cipher using LFSR based Unique Random Number Generator.**

Playfair cipher is the well-known multiple letter encryption cipher. Where the digraphs in the plaintext are treated as single units and converted into corresponding cipher text digraphs. However because of the drawbacks inherent in the 5 X 5 Playfair cipher which adversely affects the security they proposed a 6 X 6 Playfair cipher and then coupled it with Linear Feedback Shift Register based Unique Random Number Generator. 6 X 6 Playfair cipher supports all 26 alphabets (A-Z) and 10 digits (0-9) which eliminate the limitation of 5 X 5 Playfair in which “i” and “j” both character could not appear at the same time. LFSR not only enhances the security up to a considerable level by generating random sequences but also provides a much faster rate of encryption and decryption, that’s why LFSR based Unique Random Number Generator is chosen for the consideration. This paper deals in with the security issues of the new proposed system. Various types of cryptography attacks have been taken under consideration for original Playfair cipher but not vulnerable for this proposed cipher.

4. **Arvind Kumar, Pawan Singh Mehra, Gagan Gupta, Aatif Jamshed (2012): Modified Block Playfair Cipher using Random Shift Key Generation.**

In this paper conventional Playfair Cipher is being modified by encrypting the plaintext in blocks. For each block the keyword would be the same but the matrix will shift by some random value. As a result of which the diagram analysis would be very difficult which is done in the traditional Playfair Cipher to obtain the plaintext from the ciphertext. The shift value will be generated using SHA-1 which is very secure. Playfair Cipher method, based on polyalphabetic cipher is relatively easy to break because it still leaves much of the structure and a few hundred of letters of ciphertext are sufficient. To add to its security and to make it more usable they are using 6x6 matrix instead of 5x5 which will be able to cover 26 alphabets in English and ten numerals i.e. from 0 to 9. This 6x6 matrix eliminate the case of putting of 2 alphabets (I and J) together in the matrix as it was in the 5x5 matrix. Plaintext as well as key can be numeral, alphabetic or combination of both.

5. **Assia Merzoug, Adda Ali Pacha, Naima Hadj Said (2017): New Approach of the Playfair's Cipher with a Numerical Value of the Keyword**

At least during the last five years there has been an explosion of a public academic research in cryptography for Playfair's cipher. We were interested, and we have proposed a method to improve it, to make it safer and more efficient. We have oversized this encryption matrix by 7x7 coefficients and for its filling, we have combined two chaotic maps (the attractor Henon and logistics map). The attractor Henon of dimension 2, determines the intersection of the row and column of the new matrix playfair. The coefficients of this matrix are calculated from logistic map, each value is a single character of the alphabet used. The secret keyword is formed by the initial conditions of the chaotic attractors.

6. **Denni Kurniawan, April Lia Hananto, Bayu Priyatna (2018): Modification Application of Key Metrics 13x13 Cryptographic Algorithm Playfair Cipher and Combination with Linear Feedback Shift Register (LFSR) on Data Security Based on Mobile Android**

Playfair cipher is a classic encryption method that is difficult to manually manipulate but apart from the advantages found in plyafair cipher there are also many shortcomings, can be solved by using the information frequency of occurrence bigram, can not enter lowercase letters, numbers and special characters when encrypting This research modifies the key matrix of playfair cryptography algorithms and combines with the Linear Feedback Shift Register (LFSR) algorithm, by changing the size of the 13x13 key matrix the playfair cipher is able to insert characters as many as 196 characters consisting of capital letters, lowercase letters. The result of calculation with avalanche effect method got average value 43,59% at playfair cipher done by modification of matrix key 13x13 and combined with LFSR generator, 2,15% at playfair cipher 10x10 matrix key without merged with LFSR and 34,41% at playfair classic 5x5. That the playfair cipher that has been modified and combined with the LFSR generator is stronger than the previous playfair cipher. The result of time complexity testing has fast encryption and decryption.

7. **Ibrahim Abde Al-jalil Sholi, Mohamad A. Mohamed (2019): Modifying Playfair cipher algorithm using KAJ spiral method to fit any language regardless of the number of characters**

In this paper they proposed KAJ Spiral method for supporting Playfair cipher algorithm to use languages other than English and utilize block with more than two characters at once. Original method does not support block of characters and other languages. The method uses a spiral shape with two axes (X, Y) and the letters are spread on the axis within circles depending on the language. They use Friedman method analysis (index of coincidence) as a tool to test and prove the efficiency of KAJ Spiral method, and they found that it is at least equally secure to the original Playfair cipher. The aims of this is making cryptography just like mathematics a universal language such that people with different languages can use this algorithm for secure communication, and at the same time make the algorithm stronger and easy to use, with the ability to fit any language.

8. Jan Carlo T. Arroyo, Ariel M. Sison, Ruji P. Medina, Allemar Jhone P. Delima (2022): An Enhanced Playfair Algorithm with Dynamic Matrix Using the Novel Multidimensional ElementinGrid Sequencer (MEGS)

This study enhanced the Playfair algorithm with the novel Multidimensional Element-in-Grid Sequencer (MEGS). A 16x16 dynamic matrix with a new character sequencing scheme is introduced before substitution for a more secure encryption process. The proposed modification incorporates matrix rotation, matrix shifting, matrix rolling, and crossover operations in producing the ciphertext. The enhanced Playfair algorithm will pave the way for a robust system to secure information where similar plaintext characters may not have the same encryption value. The generated ciphertext will only contain printable ASCII characters. Simulation results revealed that the modified Playfair algorithm obtained an average of 53.54% avalanche effect when tested using plaintext with varying lengths ranging from 10 to 1000 characters, thus, surpassing the Strict Avalanche Criterion (SAC) standard. Applying the modified Playfair algorithm in image steganography or password security is recommended for future works, and other performance metrics such as the randomness test and brute force attack analysis be tested.

9. Jitendra Choudhary, Ravindra Kumar Gupta, Shailendra Singh (2013): A GENERALIZED VERSION OF PLAY FAIR CIPHER

In this paper, they have generalized and modified the play fair cipher. They have introduced confusion and diffusion. The cryptanalysis carried out in this analysis has shown that the proposed play fair cipher is a strong one.

The role of cryptography in today’s world is increasing day by day. Information is flowing from one place to another on the network. One most common cryptography technique is substitution cipher. Play fair is most common substitution cipher. In this paper, they present a generalized version of play fair ciphers. Encryption/decryption is a very popular task. They also explain the fundamentals of sequential cryptography.

10. Mantoo Kumar Gupta, Rajeev Kumar Das (2020): Playfair, The Substitution Cipher: A Review

Playfair Cipher is one of the techniques which encrypts and decrypts a given data and keeps it isolated from several threats. The initial digraph substitution cipher is the playfair cipher. This was introduced by charles wheatstone in 1854, but was mentioned after Lord Playfair who elevated the use of the cipher instead of enciphering the single letter likewise in simple substitution. This paper presents review of existing Playfair ciphers with few variants of it.

11. Mohd Vasim Ahamad, Misbah Urrahman Siddiqui, Maria Masroor, Urooj Fatima (2018): An Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret Key

With the technology advancements and easy availability of internet, every day millions of users share information electronically through emails, file sharing, e-commerce, etc. As, internet is highly vulnerable to various attacks, sending sensitive information over the Internet may be dangerous. One of the ways to protect the sensitive Information is using the cryptographic techniques. So, while sharing sensitive information over the Internet, it should be sent in encrypted form to prevent the access by unauthorized person. Encryption can be defined as the process of transforming information in such a manner that only authorized person can understand the shared information. In this paper, they have taken Playfair encryption algorithm for encryption and modified it by using Fibonacci series. Fibonacci series is used to generate a random key, which is used for encrypting the message in Playfair encryption algorithm. Using Fibonacci numbers and generating random keys provide significant security to shared information.

12. Naveen KM(2016) : Enhanced Play Fair Cipher

The theme of this research work is to design and develop a very strong cryptographic technique, which will be used to provide security for alphanumeric characters, special characters and numbers, when they transmit over the network. This cryptographic technique, very well addresses the problems that were faced by the classical play fair and 3D Play fair techniques and overcomes the problems they faced in those techniques. Here they will consider 4 characters at a time, group them and then use them for encryption.

They have a problem in the classical play fair as it uses i and j as same character. Here they eliminate this problem and they also eliminate the problem with 3D play fair which will use only certain limited character sets for encryption and that is not case sensitive. In our proposed method, they take into consideration all the 256 ASCII characters for encryption and it is also a complex algorithm when compared to previous replacement techniques.

13. Nitya Khare, S. Veena Dhari(2017): A Survey on Playfair Cipher Encryption Technique

The well-known multiletter cipher encryption method is playfair cipher Although, a wide variety of techniques have been employed for encryption and decryption The playfair cipher shows a great advancement over other encryption method. It consists of 5X5 key matrix. Playfair cipher is the form of block cipher which has no limit on the number of characters in a message it can do, but it operates on block of characters encrypting and decrypting two characters at a time cipher. In this, the plain text digraphs are converted to cipher text digraphs and vice versa using a pre-shared key.

14. Ouday Nidhal Ameen Hanosh, BaraaWasfi Salim (2013): 11 × 11 Playfair Cipher based on a Cascade of LFSRs

Playfair cipher is one of the better-known multiple letter encryption ciphers. In this method, the diagrams in the plaintext are treated as a single unit and then these units converted into ciphertext diagrams. This paper implements and discusses a new system which proposed by using 11 × 11 Playfair cipher that supports all 26 alphabets in both: upper case letters (A-Z) as well as lower case letters (a-z), ten digits (0-9), special characters and the extended special characters. This combination will tackle the limitation of 5×5 Playfair cipher in which both “i” and “j” letters could not appear simultaneously. In order to increase the level of security of this method, the output of an 11×11 Playfair procedure will be an input to the complete procedure of a cascade LFSRs. Finally, this system was implemented using MATLAB 8.0 (R2012b).

15. Sakshi Agarwal , Gaurav Agarwal (2019): Play-Fair Encryption Algorithm – A Review

Cryptography is an art of secure information that deals with the encoding and decoding of messages which enhances the security of the data at both ends. In cryptography there are so many algorithms that can encode the plain text into cipher text which can be decode to get the plain text again. The various algorithms are RSA(Rivest, Shamir, Aldeman), DES (Data Encryption Standard), Play-fair cipher and Vignere cipher and Hill Cipher. The traditional Play fair cipher has 5*5 matrix in which the position of I/J is same and only the 26 alphabets of English they used. In this paper, they deal with the enhancement of traditional play-fair as by using some more special characters, numbers and small letters of English alphabet.

16. Sanjay Basu, Utpal Kumar Ray (2012): Modified Playfair Cipher using Rectangular Matrix

One of the well-known polyalphabetic ciphers is the Playfair cipher. In this cipher diagrams or groups of 2 letters in the plain text is converted to cipher text diagrams during encryption using a key. Similarly during decryption cipher text diagrams are converted to plain text diagrams using the same key. However the original 5 x 5 Playfair cipher can support only 25 uppercase alphabets. To overcome this drawback they propose a rectangular matrix having 10 columns and 9 rows which can support almost all the printable characters including white space. This paper analyses the original Playfair cipher, the different variations that have been proposed and the modified Playfair cipher that they propose. Cryptanalysis is done to show that the proposed cipher is a strong one.

17. Sarita Singh (2020) : A Novel Technique for Enhancement of the Security of Playfair Cipher:

In today's world advancement of data transmission over the unsecured channel and data is not secure. In this scenario, data should be in encrypted form and that data transmitted over the network. In cryptography, have two methods to encrypt data are substitution and Transposition. Transposition is referring to changing the position of a character in the given text. On the other hand, Substitution is referring to replacing the character with another character in the given text. Play fair cipher is based on polyalphabetic substitution cipher; classical play fair cipher has a 5*5 matrix. To increase the security of play fair cipher, her paper presents a new approach to introducing double encryption in the sender side and double decryption in the receiver side approach by vigenere cipher, play fair cipher, and linear congruently method.

18. Shiv Shakti Srivastava, Nitin Gupta (2011): A Novel Approach to Security using Extended Playfair Cipher

The well known multiple letter encryption cipher is the Playfair cipher. Here the digrams in the plaintext are treated as single units and converted into corresponding cipher text digrams. However because of the drawbacks inherent in the 5×5 Playfair cipher which adversely affects the security they proposed an 8×8 Playfair cipher. This paper analyses the new proposed system. For this they have carried out cryptanalysis and through the avalanche effect they find out that the proposed cipher is a strong one.

19. V. Subhashini , N. Geethanjali (2016): Analysis of Playfair Algorithm with Different Sizes on Natural Languages (Specialized on Telugu language)

Cryptography is used to encrypt the secret messages. In Cryptography, the Playfair cipher algorithm depending upon different matrices had explained an interesting data encryption technique with very low complexity. This Paper will present a perspective on combination of Playfair techniques. Extending the concept of 5 X 5 matrix of Playfair algorithm into different sizes, encrypting the messages of natural languages is developed. Play fair cipher is one of the popular symmetric encryption methods. The first recorded description of the Play fair cipher was in a document signed by Wheatstone on 26 March 1854. However Lord Play fair promoted the use of this cipher and hence it is called Play fair Cipher. In this paper the original paper of 5 X 5 matrix is modified into N X M matrix and it is possible to encrypt messages written by natural language. In this paper their state language Telugu as a special case is discussed.

20. Zubair Iqbal, Bhumika Gupta, Kamal Kr. Gola, Prachi Gupta (2014): Enhanced the Security of Playfair Technique using Excess 3 Code (XS3) and Ceasar Cipher

The main purpose of their research is to provide security for the data that contains alphabets and integer values during the transmission, when data is transmitted form sender to receiver. As we know that playfair technique if best for multiple letter encryption, which treats the plain text as single units and translates these units into cipher text. It is highly difficult to the attacker to understand or to decrypt the cipher text. The existing playfair technique is based on the use of a 5 X 5 matrix of letters constructed using a keyword. This algorithm can only allow the text that contains alphabets only. But many algorithms have been proposed that allow text which contains alphabets, integers as well as special symbols using 6 * 6 matrix and 10 * 9 matrix etc. In playfair technique a groups of 2 letters in the plain text is converted to cipher text during encryption using a key. Similarly on other hand during decryption cipher text are converted to plain text using the same key. Some time it may be possible for the attacker to understand the plaintext. To overcome this problem they proposed an algorithm that extends the security of playfair technique using excess 3 code and ceasar cipher technique where first each alphabets and integer is converted into binary number and then its equivalent excess 3 code and after that with the help of key encryption process will be apply. In their proposed technique they are using 6 * 6 matrix which contain alphabets and integers only.

5 IMPLEMENTATION

5.1 Programming Language Selection

Here we use JAVA Language for the encryption and the decryption of Playfair Cipher algorithm.

Java is a general purpose programming language that is class based and object oriented. The programming language is structured in such a way that devlopers can write code any where and run it anywhere without worrying about the underlying computer architecture. It is also referred to as write once, run anywhere.

5.2 Coding

PROGRAM-

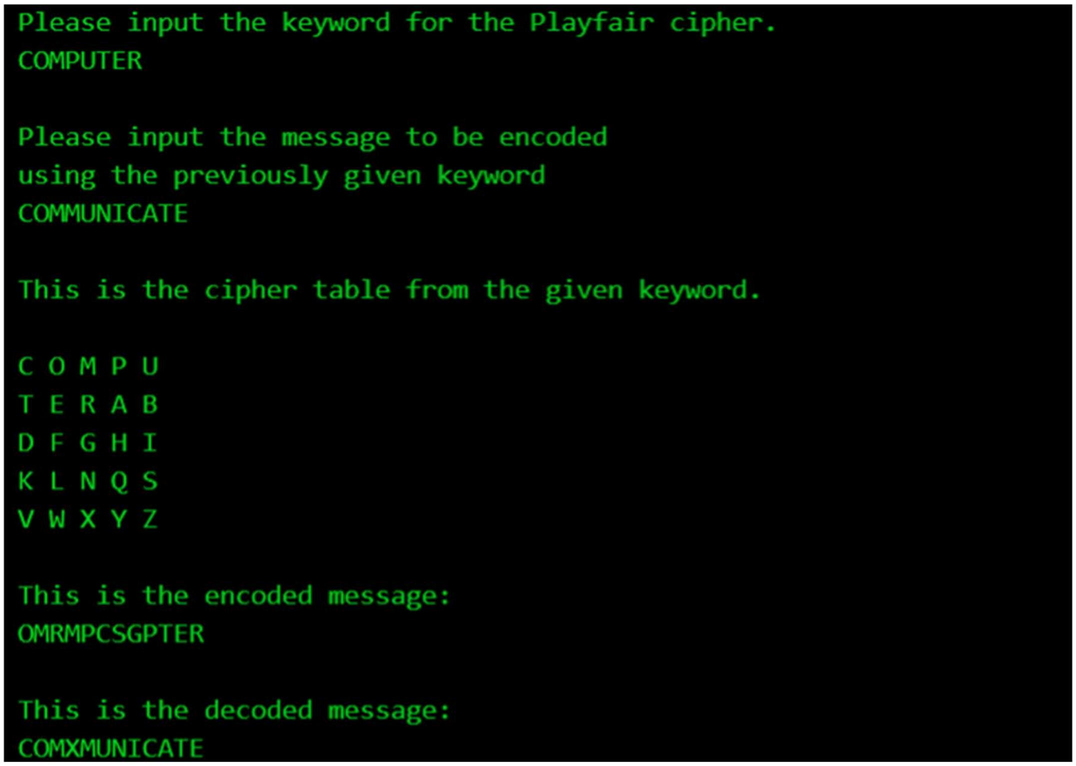
```
// encodes text input using the Playfair cipher

// results (both encode and decode) are output with the table

// requires a user keyword for the cipher

// uses letter 'X' for insertion, I replaces J


import java.awt.Point;

import java.util.Scanner;


public class Playfair{

  // length of digraph array

  private int length = 0;


  // table for Playfair cipher
  private String [][] table;

  // main method to test Playfair method
  public static void main(String[] args){
    Playfair pf = new Playfair();
  }

  // main run of the program, Playfair method
  private Playfair(){

    // prompts user for the keyword to use for encoding & creates tables
    System.out.println("Please input the keyword for the Playfair cipher.");
    Scanner sc = new Scanner(System.in);
    String keyword = parseString(sc);
    while(keyword.equals(""))
      keyword = parseString(sc);
    System.out.println();
    table = this.cipherTable(keyword);



    // prompts user for message to be encoded
    System.out.println("Please input the message to be encoded");
    System.out.println("using the previously given keyword");
    String input = parseString(sc);
    while(input.equals(""))
```

```
      input = parseString(sc);
    System.out.println();

    // encodes and then decodes the encoded message
    String output = cipher(input);
    String decodedOutput = decode(output);

    // output the results to user
    this.printTable(table);
    this.printResults(output,decodedOutput);
  }

  // parses any input string to remove numbers, punctuation,
  // replaces any J's with I's, and makes string all caps
  private String parseString(Scanner s){
    String parse = s.nextLine();
    parse = parse.toUpperCase();
    parse = parse.replaceAll("[^A-Z]", "");
    parse = parse.replace("J", "I");
    return parse;
  }
  // creates the cipher table based on some input string (already
parsed)
  private String[][] cipherTable(String key){
    String[][] playfairTable = new String[5][5];
    String keyString = key + "ABCDEFGHIKLMNOPQRSTUVWXYZ";

    // fill string array with empty string
    for(int i = 0; i < 5; i++)
      for(int j = 0; j < 5; j++)
        playfairTable[i][j] = "";


    for(int k = 0; k < keyString.length(); k++){
      boolean repeat = false;
      boolean used = false;
      for(int i = 0; i < 5; i++){
        for(int j = 0; j < 5; j++){
          if(playfairTable[i][j].equals("" +
keyString.charAt(k))){
            repeat = true;
          }else if(playfairTable[i][j].equals("") && !repeat &&
!used){
            playfairTable[i][j] = "" + keyString.charAt(k);
            used = true;
          }
        }
      }
    }
    return playfairTable;
  }
  // cipher: takes input (all upper-case), encodes it, and returns
output
  private String cipher(String in){
    length = (int) in.length() / 2 + in.length() % 2;


    // insert x between double-letter digraphs & redefines
"length"
```

```
    for(int i = 0; i < (length - 1); i++){
      if(in.charAt(2 * i) == in.charAt(2 * i + 1)){
        in = new StringBuffer(in).insert(2 * i + 1,
'X').toString();
        length = (int) in.length() / 2 + in.length() % 2;
      }
    }

    // adds an x to the last digraph, if necessary
    String[] digraph = new String[length];
    for(int j = 0; j < length ; j++){
      if(j == (length - 1) && in.length() / 2 == (length - 1))
        in = in + "X";
      digraph[j] = in.charAt(2 * j) +""+ in.charAt(2 * j + 1);
    }

    // encodes the digraphs and returns the output
    String out = "";
    String[] encDigraphs = new String[length];
    encDigraphs = encodeDigraph(digraph);
    for(int k = 0; k < length; k++)
      out = out + encDigraphs[k];
    return out;
  }

  // encodes the digraph input with the cipher's specifications
  private String[] encodeDigraph(String di[]){
    String[] enc = new String[length];
    for(int i = 0; i < length; i++){
      char a = di[i].charAt(0);
      char b = di[i].charAt(1);
      int r1 = (int) getPoint(a).getX();
      int r2 = (int) getPoint(b).getX();
      int c1 = (int) getPoint(a).getY();
      int c2 = (int) getPoint(b).getY();

      // case 1: letters in digraph are of same row, shift columns
to right
      if(r1 == r2){
        c1 = (c1 + 1) % 5;
        c2 = (c2 + 1) % 5;

      // case 2: letters in digraph are of same column, shift rows
down
      }else if(c1 == c2){
        r1 = (r1 + 1) % 5;
        r2 = (r2 + 1) % 5;

      // case 3: letters in digraph form rectangle, swap first
column # with second column #
      }else{
        int temp = c1;
        c1 = c2;
        c2 = temp;
      }
      //performs the table look-up and puts those values into the
encoded array
      enc[i] = table[r1][c1] + "" + table[r2][c2];
    }
    return enc;
  }

  // decodes the output given from the cipher and decode methods
(opp. of encoding process)
  private String decode(String out){
    String decoded = "";
    for(int i = 0; i < out.length() / 2; i++){
      char a = out.charAt(2*i);
      char b = out.charAt(2*i+1);
      int r1 = (int) getPoint(a).getX();
      int r2 = (int) getPoint(b).getX();
      int c1 = (int) getPoint(a).getY();
      int c2 = (int) getPoint(b).getY();
      if(r1 == r2){
        c1 = (c1 + 4) % 5;
        c2 = (c2 + 4) % 5;
      }else if(c1 == c2){
        r1 = (r1 + 4) % 5;
        r2 = (r2 + 4) % 5;
      }else{
        int temp = c1;
        c1 = c2;
        c2 = temp;
      }
      decoded = decoded + table[r1][c1] + table[r2][c2];
    }
    return decoded;
  }

  // returns a point containing the row and column of the letter
  private Point getPoint(char c){
    Point pt = new Point(0,0);
    for(int i = 0; i < 5; i++)
      for(int j = 0; j < 5; j++)
        if(c == table[i][j].charAt(0))
          pt = new Point(i,j);
    return pt;
  }

  // prints the cipher table out for the user
  private void printTable(String[][] printedTable){
    System.out.println("This is the cipher table from the given
keyword.");
    System.out.println();

    for(int i = 0; i < 5; i++){
      for(int j = 0; j < 5; j++){
        System.out.print(printedTable[i][j]+" ");
      }
      System.out.println();
    }
    System.out.println();
  }

  // prints results (encoded and decoded)
  private void printResults(String enc, String dec){
    System.out.println("This is the encoded message:");
    System.out.println(enc);
    System.out.println();
    System.out.println("This is the decoded message:");
    System.out.println(dec);
  }
}
```

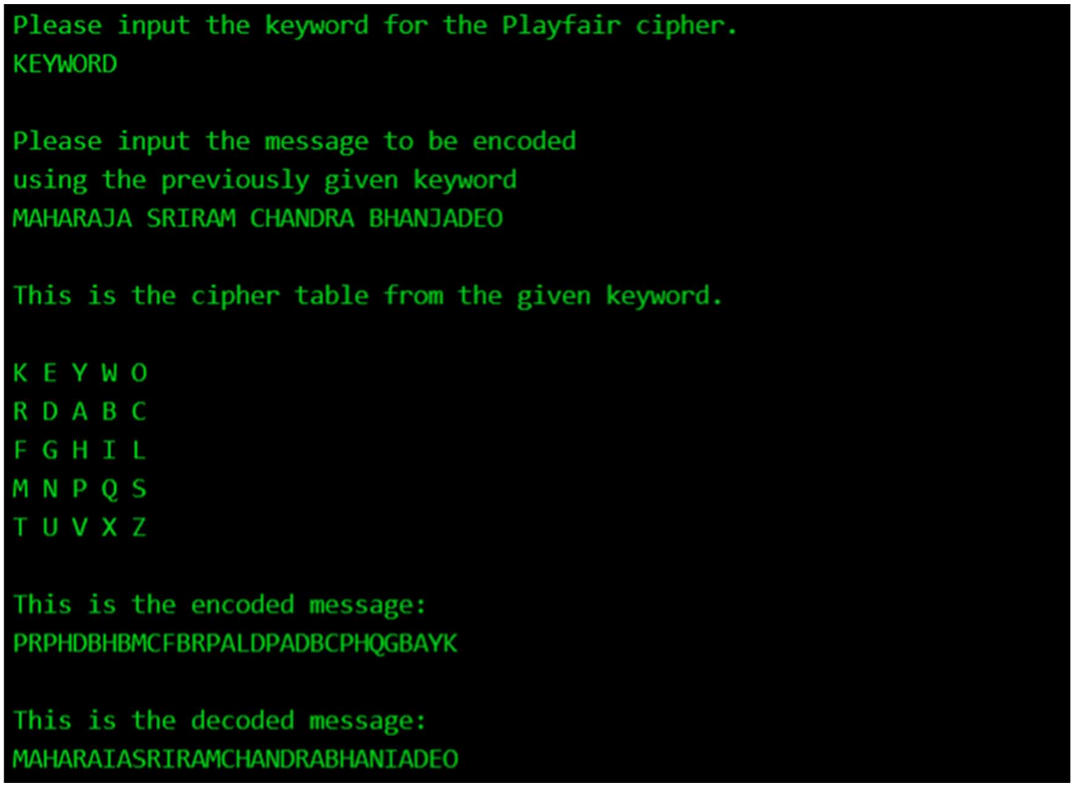
6 SCREENSHOTS

OUTPUT-1



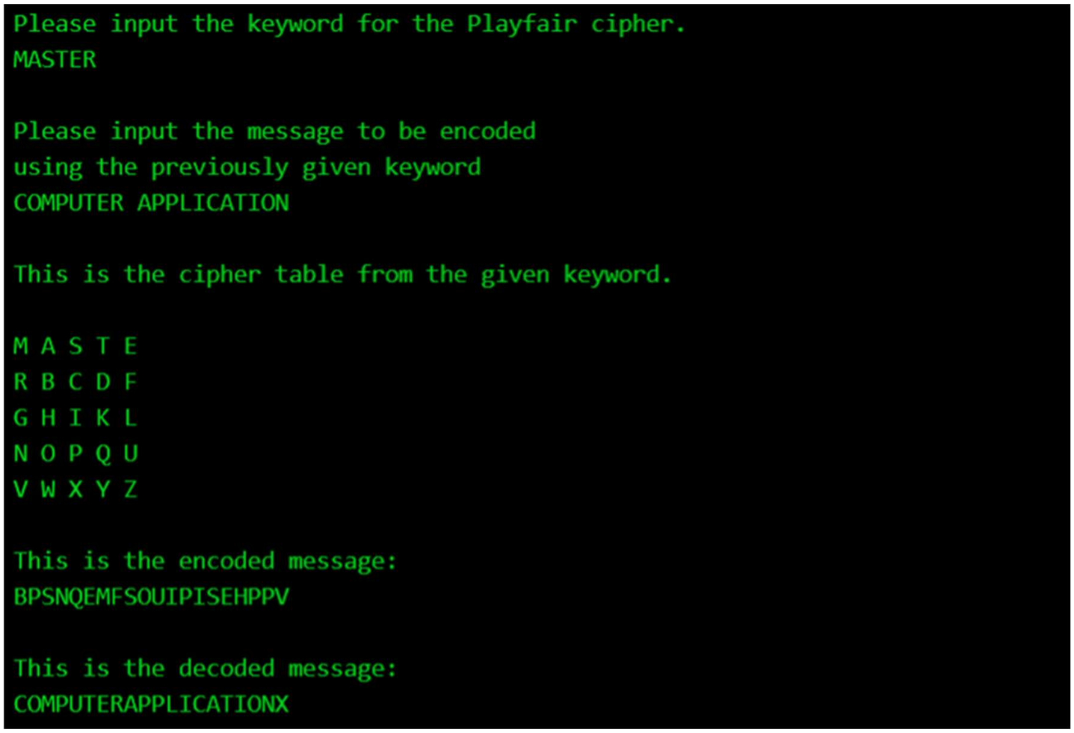
```
Please input the keyword for the Playfair cipher.
COMPUTER

Please input the message to be encoded
using the previously given keyword
COMMUNICATE

This is the cipher table from the given keyword.

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

This is the encoded message:
OMRMPCSGPTER

This is the decoded message:
COMXMUNICATE
```

OUTPUT-2



```
Please input the keyword for the Playfair cipher.
KEYWORD

Please input the message to be encoded
using the previously given keyword
MAHARAJA SRIRAM CHANDRA BHANJADEO

This is the cipher table from the given keyword.

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

This is the encoded message:
PRPHDBHBMCFBRPALDPADBCPHQGBAYK

This is the decoded message:
MAHARAIASRIRAMCHANDRABHANIADEO
```

OUTPUT-3



```
Please input the keyword for the Playfair cipher.
MASTER

Please input the message to be encoded
using the previously given keyword
COMPUTER APPLICATION

This is the cipher table from the given keyword.

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

This is the encoded message:
BPSNQEMFSOUIPISEHPPV

This is the decoded message:
COMPUTERAPPLICATIONX
```

7 CONCLUSION & FUTURE WORK

It is now more important than ever to protect data and resources from disclosure, ensure the integrity of data and messages, and protect systems against network-based attacks due to the exponential growth of computer systems and their interconnection via networks. For the protection of the data, we have used the Playfair Encryption Technique in our project paper . It is one of the most ancient and effective methods of data encryption.

Here we have worked on what is Playfair cipher algorithm, how it works and the implementation. From the above project we learn that Playfair cipher providing security, integrity, confidentiality and authentication while transferring a message.

7.1 Advantages of the System

1. Diverse ciphertext if we scrutinize the Algorithm, we can notice at every stage we are getting diverse ciphertext, thus more trouble to cryptanalyst.
2. Brute force attack does not affect it.
3. Cryptanalyze (the process of decoding cipher without knowing key) is not possible.
4. Overcomes the limitation of simple Playfair square cipher.
5. Easy to perform the substitution.

7.2 Limitations of the System

The limitations of the Playfair cipher are as follows:

- Only 25 alphabets are supported.
- It does not support numeric characters.
- Only either upper cases or lower cases are supported.
- The use of special characters (such as blank space, newline, punctuations, etc.) is prohibited.

- It does not support other languages, except English.
- Encryption of media files is also not supported.

7.3 Future Work

Here we have implemented Playfair cipher in a simple manner. Also we have studied above 20 modified version of Playfair cipher projects for future work.

REFERENCES

1. Aftab Alam, Shah Khalid, and Muhammad Salam (2013), “A Modified Version of Playfair Cipher Using 7×4 Matrix.”, Vol. 5, International Journal of Computer Theory and Engineering, 626-628.

2. Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh (2012), “3D (4 X 4 X 4) - Playfair Cipher” Volume 51, International Journal of Computer Applications, 36 – 38

3. Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh (2012), “6 X 6 Playfair Cipher using LFSR based Unique Random Number Generator”, Volume-51, International Journal of Computer Applications, 30-35.

4. Arvind Kumar, Pawan Singh Mehra, Gagan Gupta, Aatif Jamshed (2012), “Modified Block Playfair Cipher using Random Shift Key Generation”, Volume 58, International Journal of Computer Applications, 10-13

5. Assia Merzoug, Adda Ali Pacha, Naima Hadj Said (2017), “New Approach of the Playfair's Cipher with a Numerical Value of the Keyword”, Vol. 6, Indonesian Journal of Electrical Engineering and Computer Science, 695-703

6. Denni Kurniawan, April Lia Hananto, Bayu Priyatna (2018), “Modification Application of Key Metrics 13x13 Cryptographic Algorithm Playfair Cipher and Combination with Linear Feedback Shift Register (LFSR) on Data Security Based on Mobile Android”, Volume 5, International Journal of Computer Techniques, 65-70

7. Ibrahim Abde Al-jalil Sholi, Mohamad A. Mohamed (2019), “Modifying Playfair cipher algorithm using KAJ spiral method to fit any language regardless of the number of characters”, Vol. 9, International Journal of Electrical and Computer Engineering, 5400-5411

8. Jan Carlo T. Arroyo, Ariel M. Sison, Ruji P. Medina, Allemar Jhone P. Delima (2022), “An Enhanced Playfair Algorithm with Dynamic Matrix Using the Novel Multidimensional ElementinGrid Sequencer (MEGS)”, Volume-70, International Journal of Engineering Trends and Technology, 132-139

9. Jitendra Choudhary, Ravindra Kumar Gupta, Shailendra Singh (2013), “A GENERALIZED VERSION OF PLAY FAIR CIPHER”, Volume-2, International Journal of Computer Applications, 176 – 179

10. Mantoo Kumar Gupta, Rajeev Kumar Das (2020), “Playfair, The Substitution Cipher: A Review”, Vol.-03, Journal of Science and Engineering, 31 – 34

11. Mohd Vasim Ahamad, Misbah Urrahman Siddiqui, Maria Masroor, Urooj Fatima (2018), “Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret Key”, vol.-7, International Journal of Engineering & Technology, 347 – 351

12. Naveen KM (2016), “Enhanced Play Fair Cipher”, Vol. 3, International Journal of Innovative Science, Engineering & Technology, 335-341

13. Nitya Khare, S. Veena Dhari (2017), “A Survey on Playfair Cipher Encryption Technique”, Vol. 5, International Journal for Scientific Research & Development, 568-569

14. Ouday Nidhal Ameen Hanosh, BaraaWasfi Salim (2013), “11 × 11 Playfair Cipher based on a Cascade of LFSRs”, Volume 12, IOSR Journal of Computer Engineering, 29-35

15. Sakshi Agarwal , Gaurav Agarwal (2019), “Play-Fair Encryption Algorithm – A Review”, Volume-10, International Journal of Computer Science & Communication, 201-210 .

16. Sanjay Basu, Utpal Kumar Ray (2012), “Modified Playfair Cipher using Rectangular Matrix”, Volume 46, International Journal of Computer Applications, 28 – 30

17. Sarita Singh (2020), “A Novel Technique for Enhancement of the Security of Playfair Cipher”, Volume-7, International Journal of Computer Engineering in Research Trends, 8-12

18. Shiv Shakti Srivastava, Nitin Gupta (2011), “A Novel Approach to Security using Extended Playfair Cipher”, Volume 20, International Journal of Computer Applications, 39-43

19. V. Subhashini , N. Geethanjali (2016), “Analysis of Playfair Algorithm with Different Sizes on Natural Languages (Specialized on Telugu language)”, Volume 2, International Research Journal of Advanced Engineering and Science, 27-30

20. Zubair Iqbal, Bhumika Gupta, Kamal Kr. Gola, Prachi Gupta (2014), “Enhanced the Security of Playfair Technique using Excess 3 Code (XS3) and Ceasar Cipher”, Volume 103, International Journal of Computer Applications, 16 – 20

REFERENCE BOOKS:

1. Cryptography and Network Security - Principles and Practice | Seventh Edition | By Pearson

2. Cryptography and Network Security Principles and Practice (7th Edition) William Stallings - Mar 05, 2016

REFERENCE LINKS:

1. https://www.geeksforgeeks.org/playfair-cipher-with-examples/
2. https://www.javatpoint.com/playfair-cipher-program-in-java
3. https://www.jigsawacademy.com/blogs/cyber-security/playfair-cipher/
4. https://towardsdatascience.com/playfair-cipher-encryption-fa8ed7df8ea5