International Journal of Engineering & Technology, 7 (4.5) (2018) 347-351

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret Key

Mohd Vasim Ahamad[1]*, Misbah Urrahman Siddiqui[2], Maria Masroor[3], Urooj Fatima[4]

[1, 2, 3, 4] *Computer Engineering Section, University Women's Polytechnic*
Aligarh Muslim University, India
**Corresponding author E-mail: vasim.iu@gmail.com*

Abstract

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, we 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.

Keywords: *Use about five key words or phrases in alphabetical order, Separated by Semicolon.*

1. Introduction

The technology advancements and easy availability of internet enables millions of users to share information every day electronically through emails, file sharing, e-commerce, etc. [1] Security is the main concern while sharing the sensitive information over the internet. To ensure the security of information, encryption is used. Encryption is the process of transforming the information into some scrambled or unreadable form. The purpose of encryption is to keep information secure from unauthorized person. Decryption is the reverse of encryption; it is the process of getting back the original information from the encrypted data. Cryptography can be defined as the study of encryption and decryption of sensitive information. In cryptography, encryption process transforms the information with the help of an algorithm and a key to make it unreadable to anyone except authorized person. The result of the encryption is scrambled or encrypted information. The reverse to the encryption process is referred to as decryption, which converts scrambled information to readable information using a decryption algorithm and a key [2].

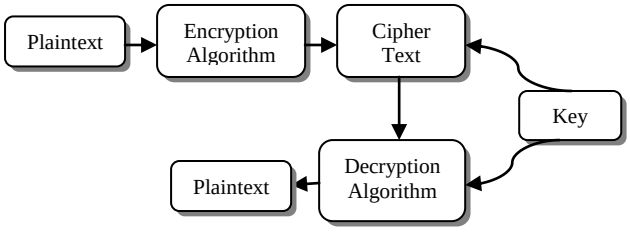


Fig. 1: The Encryption Process

Fig. 1 describes the process of cryptography. The plaintext is the original information to be shared and it is given to the encryption algorithm as an input. The encryption algorithm can be considered as the mathematical algorithm used for transforming the plaintext to the cipher text. The encryption algorithm takes the plaintext and a secret key as input and generates the cipher text as the output. The cipher text is the scrambled or encrypted message which is generated by encryption algorithm using plaintext and a secret key as input. The secret key comprises of some code to transform the plaintext to cipher text and vice versa. The decryption algorithm can be considered as the mathematical algorithm used for transforming the scrambled or cipher text to the original plain text. The decryption algorithm takes the cipher text and a secret key as input and generates the original plain text as the output.

In this paper, we have considered the playfair encryption algorithm. Playfair encryption algorithm takes a key to transform the plaintext to cipher text. We have generated this secret key using Fibonacci numbers. Using Fibonacci numbers and generating random keys provide significant security to shared information. The remaining sections of this paper is organized as follows: A review of the research work previously carried out in this field is listed in section 2. Basic concepts related to encryption and Playfair technique are presented in section 3. In Section 4, we have provided the detailed description of proposed work. Results and discussion are described in section 5 followed by the conclusion and future work in the last section.

2. Literature Review

Nowadays, Information security is the main concern while communicating with other parties and sharing the sensitive and private information over the internet. To ensure the security of

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Information, it is transformed into some unreadable or scrambled form using encryption techniques. The authors in [3], described the Playfair encryption technique and proposed a modified version of it. Authors considered the digraph in the plaintext as single units and transformed them into corresponding cipher text digraphs. Authors in [4], have got some better performance by proposing the extended version of Playfair encryption technique.
In [5], authors studied, analyzed and compared the hybrid data encryption techniques using Fibonacci series, XOR logic and PN sequence. To analyses the performance, the message is divided into three parts and different techniques are applied to these parts with different encryption technique. Furthermore, in [6], they have implemented a new Playfair encryption technique which includes 10 x 9 matrix and six iteration steps for encryption and decryption. This 10 x 9 rectangular matrix includes all alphanumeric characters and some special characters.

3. Basic Concepts

3.1. Encryption

Encryption can be defined as the process of transforming the message into some scrambled or unreadable form so that it can prevent the unauthorized access of the sensitive information. The purpose of encryption is to keep information, to be shared between two parties, secure from third person. Each encryption algorithm is based on two general principles namely substitution and transposition. In substitution principle, each element in the plaintext is substituted or mapped to another element.
In transposition principle, elements in the plaintext are rearranged in some manner so that it can generate unreadable pattern of original message. While using any of the above mentioned principle, the fundamental rule is that no information be lost.
In general, we use either substitution or transposition principle in encryption algorithms, but most of the times we use hybrid techniques involving multiple stages of substitutions and transpositions. Substitution cipher can be categorized into monoalphabatic (simple substitution) cipher and polygraphic cipher. A Monoalphabatic cipher operates on single letters and uses fixed substitution throughout the entire message. A polyalphabetic cipher operates on larger groups of letters and uses a different substitutions at different positions in the message.
The best example of monoalphabatic cipher (simple substitution cipher) is the Caesar Cipher, whereas Playfair technique is the example of polyalphabetic cipher. These two encryption techniques are explained as follows.

3.2. Caesar Cipher

Caesar cipher is a monoalphabetic cipher in which the cipher text is generated by substituting each and every letter of the plaintext by another letter. It is considered as the simplest of all the substitution cipher techniques. It is generally referred to as the Shift Cipher. The concept behind the shift cipher is to shift each letter in the plaintext by another letter by some fixed number ranges between 0 and 25. In Caesar cipher, the secret key is the fixed number between 0 and 25.
The encryption and the decryption algorithms are reverse to each other, and hence, both the sender and the receiver of the message shares the same secret key. Specifically, for the Caesar cipher, each letter of the plaintext is shifted by three [8].

Table 1: Caesar Cipher Example

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

If sender wants to send a message “encryption” to receiver, then shifting of letters (encryption algorithm) can be done as given in the table 1. The receiver will get the cipher text “hqfubswlrq”. By applying the reverse of encryption algorithm i.e. shifting letter three places left, the receiver will get the exact message sent by the sender. The encryption and decryption algorithm can be expressed in mathematical terms as follows. For each letter p of plaintext

$$c = (p+3) \bmod 26 \quad (1)$$

Where c is the cipher text. To recover each letter of plaintext P from cipher text c, use the following equation.

$$p = (c-3) \bmod 26 \quad (2)$$

The key value (say k) for shifting the letters of plaintext may be any value from 1 to 25. If this value is other than three, we consider it as a general Caesar cipher. The general Caesar cipher encryption algorithm can be represented mathematically as follows.

$$c = (p + k) \bmod (26) \quad (3)$$

The decryption algorithm for Caesar cipher can be written as:

$$p = (c – k) \bmod (26) \quad (4)$$

The problem associated with the Caesar cipher is that, if it is clear that the intercepted cipher text is a Caesar cipher, then a brute-force cryptanalysis can be easily performed to recover the original message. It is so because, encryption and decryption algorithms of Caesar cipher are known to everyone. They have to simply the 25 possible keys for cracking the encrypted message. To deal with this problem, more secured polyalphabetic cipher is used.

3.3. Playfair Cipher

In Playfair cipher, pairs of letters from plaintext are encrypted, unlike as in the case of simple substitution cipher where single letter from plaintext is encrypted at one go. The Playfair cipher is the best known example of polyaphabatic cipher, which treats digraphs (combination of two letters) in the plaintext as a single unit and converts these digraphs into ciphertext digraphs. Due to pairwise encryption, the Playfair cipher is significantly harder to break than the monoalphabatic ciphers. Although the cryptanalysis of Playfair is considerably more difficult that monoalphabatic cipher, but it is still possible with 600 possible digraphs. With 600 (25 x 24) possible digraphs, a considerably larger cipher text is required in order to make it more difficult to break [7] [8].
In Playfair cipher, we use 25 uppercase alphabets. The Playfair cipher starts with creating a key table. The key table is generated by creating a 5×5 grid of unique uppercase alphabets which act as the key for encrypting the plaintext.

As we have only 25 cell to store 26 alphabets, both I and J are placed in the same cell of 5 x 5 grid. This key table is created by choosing a secret keyword and placing the keyword in the 5 x 5 grid, without any duplication of alphabets, starting from left to right and from top to bottom. Once done with placing the alphabets of keyword, remaining alphabets are placed in the 5 x 5 grid in their order. Let us suppose, the common secret key “tutorials” is decided by both the communicating parties. The key table is generated as explained above.
The final key table will look alike:

Table 2: The Key Table

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

Now, suppose the sender wants to send the message "hide gold" to other communicating party. In order to apply Playfair cipher, the plaintext message is splited into digraphs (pairs of letters). There may be a possibility of having odd number of letters in plaintext. In this case append Z as the last letter. The final plaintext digraphs will be written as

HI DE GO LD

We have the secret key and the plaintext message to be communicated. The next thing we need, to transform the plaintext into cipher text, is the encryption algorithm. The following are the simple rules of encryption in Playfair cipher:

- If both letters of digraph belongs to the same column, take the letter below each letter of digraph. If a letter is at the bottom of the grid, take the letter at the top. As shown in Table 3, H and I belongs to the same column. So according to the rule, they are replaced by the letters just below them.

HI → QC

Table 3: Using the First Rule

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

- If both letters of digraph belongs to the same row, substitute with the letter to the right of each one. If one of the letters in digraph is the rightmost letter, then choose the leftmost letter in the same row. As shown in Table 4, D and E belongs to the same column. So according to the rule, they are replaced by the letters just next to them.

DE → EF

Table 4: Using the Second Rule

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

- If the digraph doesn't falls under both rules mentioned above, then create a rectangle with the two letters of digraph, and substitute with the letters on the horizontal opposite corner of the same row. According to Table 5, G and O neither belong to the same column nor to the same row. So according to the third rule, they are replaced by the letters on the horizontal opposite corner of the rectangle they form.

GO → FR

Table 5: Using the Third Rule

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

- In Table 6, L and D neither belong to the same column nor to the same row. So according to the third rule, they are replaced by the letters on the horizontal opposite corner of the rectangle they form.

LD → AE

Table 6: Using the Third Rule

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

Using the above mentioned rules, the plaintext "HIDE GOLD" is converted into cipher text "QC EF FR AE". To decrypt this Playfair cipher, follow the same process in reverse. This process is very simple. As receiver also shares the same secret key, and hence can create the key table in the same manner as the sender did. After that, receiver can decrypt the Playfair cipher by following the encryption rules in reverse manner.

4. Proposed Work

4.1 Problem Statement

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. Encryption is the process of transforming the information into unreadable form. Decryption is the reverse of encryption; it is the process of getting back the original information from the encrypted data. Cryptography can be defined as the study of encryption and decryption of sensitive information.

In cryptography, encryption process transforms the information with the help of an algorithm and a key to make it unreadable to anyone except authorized person. The result of the encryption is scrambled or encrypted information. The reverse to the encryption process is referred to as decryption, which converts scrambled information to readable information using a decryption algorithm and a key. The main purpose of this work is to encrypt and decrypt the textual messages using Playfair cipher. The Playfair cipher, like other encryption algorithms, takes input plaintext cipher and a secret key to produce the scrambled cipher text. The same secret key is shared with both the sender and receiver.

Generally, the secret key is selected by one of the communicating parties and shared to other authorized party.

This may cause security problems and cipher text can easily be cracked. To deal with this, we generate the key using Fibonacci terms. We used Fibonacci term to randomly generate the secret key for encryption and decryption purpose. Using Fibonacci numbers and generating random keys provide significant security to shared information. There are following advantages of using Fibonacci terms for generating the secret key for Playfair cipher:

- The key generation steps using Fibonacci terms are highly user friendly. Users need to just enter any number, and the background algorithm checks it for the valid Fibonacci term. If it is a Fibonacci term, then algorithm, explained in the next section, generates the random secret key.
- It uses random key for encryption using Fibonacci series. This secret key is generates from Fibonacci series and this key is of fixed length i.e. seven characters.
- The plaintext message can be encrypted with the random key generated and also can be decrypted with the same key.
- This encryption and decryption mechanism provides the integrity of secure information to be communicated.

4.2 Proposed Algorithm

The proposed algorithm is divided into three steps namely, the key generation, the encryption and the decryption algorithm.

The Key Generation Algorithm: The proposed Playfair cipher uses a random secret key. This key is generates by using Fibonacci series and placed into 5 x 5 grid. This secret key is generated using the following steps:

- Input a number (usually small)
- Check whether the input number is Fibonacci or not. If the number is not Fibonacci then prompt an alert message. If the term is correct than generate next 6 Fibonacci term of the series.
- After getting the series, limit the series terms into ASCII range of alphabets. Then covert the new series into characters, which is the resulting random key.

The Encryption Algorithm: Once, we have the secret key and the plaintext message to be communicated, we need an encryption algorithm to transform the plaintext into cipher text. In order to apply Playfair cipher, the plaintext message is splited into digraphs. There are following rules of encryption in Playfair cipher:

- Make a 5x5 grid and place the generated key into that matrix (duplicate letter must be omitted).
- After placing the key fill out the remaining spots of the grid with remaining letters.
- If both letters of plain text digraph comes under the same column, take the letter below each letter of digraph. If a letter is at the bottom of the grid, take the letter at the top.
- If both letters of digraph are in the same row, substitute with the letter to the right of each one. If one of the letters in digraph is the rightmost letter, then choose the leftmost letter in the same row.
- If the digraph doesn't falls under both rules mentioned above, then create a rectangle with the two letters of digraph, and substitute with the letters on the horizontal opposite corner of the same row.

The Decryption Algorithm: The decryption process is very simple. Create the key table in the same manner as done in the encryption. After that, the cipher text can be decrypted by using the following rules:

- If both letters are in the same column, take the letter above each one (going back to the bottom if at the top).
- If both letters are in the same row, take the letter to the left of each one (going back to the right if at the farthest left).
- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

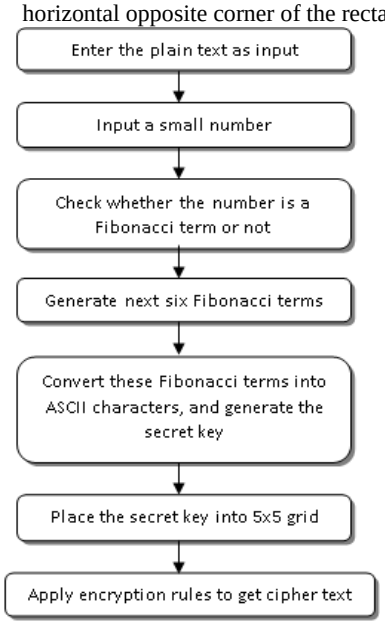


Fig. 2: Basic Steps of Proposed Algorithm

5. Results and Discussion

We have used C-Free editor for writing the codes of algorithm in C language. After execution of implemented algorithm, here are the snapshots of each important steps.

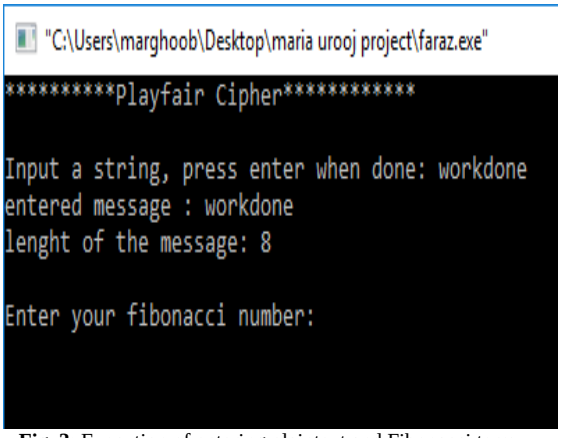


Fig. 3: Execution of entering plaintext and Fibonacci term

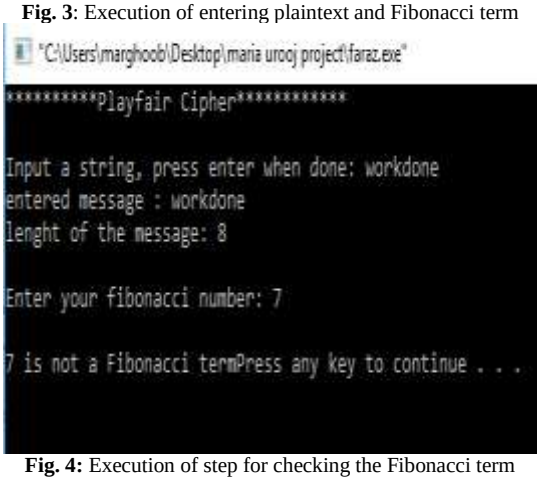


Fig. 4: Execution of step for checking the Fibonacci term

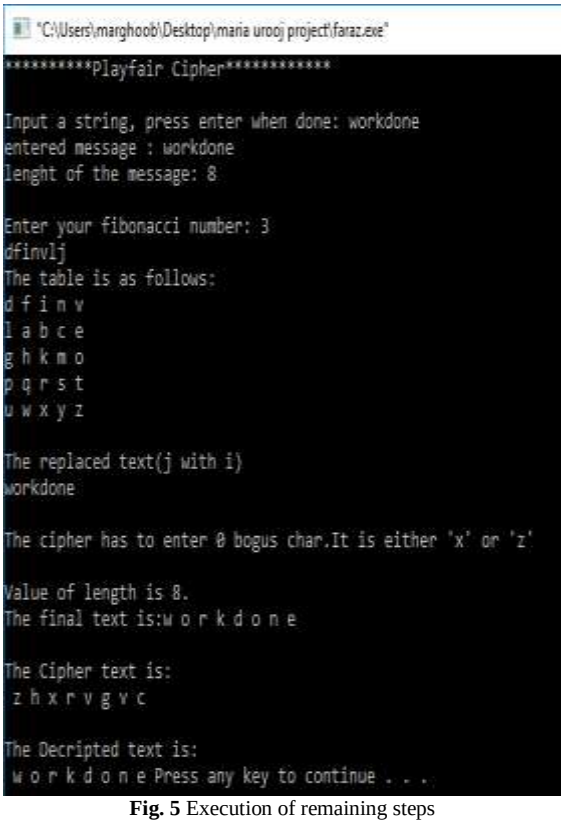


Fig. 5 Execution of remaining steps

6. Conclusion

To achieve, what we have promised in our problem statement, we have implemented the modified Playfair encryption algorithm using Fibonacci term. The modified algorithm starts with generating the random key of fixed length (in this case, it is seven) by generating the next six terms of the input Fibonacci term. After that these terms are converted into ASCII characters to form a key. The randomly generated key is then placed into 5x5 grid. The remaining alphabets are then placed in their orders. Duplicate letters are omitted and I & J shares the same cell in the grid. Then, the plaintext letters are arranged in the form of digraphs (combination of two letters). In the case, if the last digraphs ends with only single letter, append Z to it. After that, we have applied the encryption rules of Playfair cipher to transform the input plaintext digraphs into cipher text digraphs. To decrypt the message, we used the encryption algorithm in reverse order.

References

[1] Nadeem Akhtar, Mohd Vasim Ahamad, "Graph Tools for Social Network Analysis". In N. Meghanathan (Ed.), Graph Theoretic Approaches for Analyzing Large-Scale Social Networks (pp. 18-33). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2814-2.ch002.

[2] A. Sinkov, Elementary Cryptanalysis: A Mathematical Approach, Mathematical Association of America, 1966.

[3] Shiv Shakti Srivastava, Nitin Gupta "A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.

[4] S.S.Dhenakaran, M. Ilayaraja, "Extension of Playfair Cipher using 16X16 Matrix", International Journal of Computer Applications (0975 – 888) Volume 48– No.7, June 2012.

[5] Md.Atiullah Khan, Kailash Kr.Mishra, N.Santhi, J.Jayakumari, "A New Hybrid Technique for Data Encryption", Proceedings of 2015 Global Conference on Communication Technologies (GCCT 2015), 978-1-4799-8553-1/15.

[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 (IJARCET) Volume 3, Issue 2, February 2014.

[7] https://en.wikipedia.org/wiki/Playfair_cipher, visited on June, 2017.

[8] https://www.tutorialspoint.com/cryptography/traditional_ciphers.htm, visited on June, 2017

[9] Asia Mashkoor, Mohd Vasim Ahamad, "Visualization, Security and Privacy Challenges of Big Data", *International Journal of Advanced Technology in Engineering and Science*, 5 (6), June 2017, 394 - 400, ISSN No. 2348-7550