International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

IMPROVED PLAYFAIR WITH MULTISTAGE ENCRYPTION AND DECRYPTION

K. Banupriya[1], Dr.G.Arutchelvan[2]
[1]Research Scholar, Dept. of Computer Science, [2]Director & Head/CSA
[1,2]Adhiparasakthi College of Arts and Science (Autonomous), Kalavai.
Vellore, Tamil Nadu, India

Abstract: Secured communication is essential for all communication system. Cryptography is an study of art and science which converts original message into a non-readable form of message. which contains number of techniques which used for encryption process. Encryption is the process of converting an plaintext into ciphertext. Usually there are two basic building blocks of encryption techniques are available. That are substitution and the transposition. Various limitations that will occur on each kind of an substitution and the transposition techniques. So in this paper i have focused to solve such a kind of limitations and problems by combining both substitution and the transposition techniques. This will provide a better security. Hence in this paper we have proposed a method to improve a playfair cipher with ascii value generation also with taking of an two key values. Taking an first key value as a seed value for the entire process that can be done based on the length of the message that we are used for communication. On the second stage of an encryption taking of a columnar transposition from the second stage of an value. On the third stage taking of an another secret key value performing multilevel columnar transposition for multiple stages using the same secret key value. The columnar transposition has been done on two stages before using of an second secret key and while during the usage of an that has done. To make it more secure i have used single level row transposition also combining with multi-level columnar transposition cipher with two kind of an key value and encryption with different level.

Index Terms: Cryptography, encryption, plaintext, cipher text, ascii values, transposition

I. INTRODUCTION

Network security plays a vital role in data communication system. In today's information exchange it is impossible to imagine without internet. Because there is a great need of inter exchanging of data through internet. Especially while sending any kind of sensitive information through internet we need lot of security. For providing network security various encryption techniques are to be used. Encryption is an process of converting an plaintext to cipher text.

II. RELATED TECHNIQUES

A. CRYPTOGRAPHY:

[1]Cryptography is an art and science of study about those encryption techniques which are used for converting an plaintext into ciphertext so that only the intended person able to read. Encryption is the process of converting an plaintext into ciphertext. Plaintext is the intended original message and ciphertext is the converted or coded form of message.

B. CONVENTIONAL CRYPTOGRAPHY:

In conventional cryptography there will be a usage of an single key value for both the encryption and decryption process. Also termed as symmetric key cryptography. Both encryption and decryption algorithm are inverse of each other. Further this conventional cryptography can be divided into classical and modern techniques.

C. SUBSTITUTION TECHNIQUE:

In the substitution technique in which the letters of plaintext that it is replaced by using any kind of an letters, or by symbols or numbers. Some other examples of substitution techniques are caesar cipher, play fair cipher, hill cipher etc.. A very different kind of an approach which it is used for mapping that can be done through some sort of permutation on the plaintext can be achieved that is named as transposition technique.

D. TRANSPOSITION TECHNIQUE:

The transposition along with the ciphertext in matrix that can be done along with column transposition. This transposition technique is more secure by performing more than one stage of transposition. Then the resultant matrix will becomes more complex permutation. Number of classical encryption techniques which are available. But in this paper we particularly using one of the substitution technique called playfair cipher also with the combining form of transposition technique with additional changes can be done through it.

E. PLAYFAIR CIPHER:

Playfair is one of the substitution technique. Play fair cipher is based on the 5*5 matrix of alphabetic letters arranged in an appropriate manner. We can sellect a keyword place it in the matrix one by one with the remaining missing alphabets sequentially. Plain text is broken into pairs and if the pair having same alphabet then they are separated by filling the letter 'X'. Otherwise with different alphabet that resides in the same row of matrix. If the pair of matrix in the same column then it is replaced by the letter below it. This technique has a great advantage over simple mono alphabetic ciphers. There are only 26 letters but 26*26=676 diagrams. So identification of an individual diagram is very difficult.

III. EXISTING TECHNIQUE

In existing play fair all alphabets that are must to be used also there must be limited amount of code words are to be able to use. Also in transposition technique only column transposition can be achieved. There will be a possibility easy to trace.

IV. PROPOSED TECHNIQUE

In this paper play fair cipher 5* 5 matrix can be used for implementing the message without any changes with repeated alphabets. If the space is available after filling the message that can be filled by the alphabets which are not used under the message in order A to Z. In this paper both row and column transposition can be achieved. Initially before performing row and column transposition for to increase security two secret key values are to be calculated. Multilevel column transposition can be achieved for enhancing the security. There will be a chance in play fair for easy to break few hundreds letters are generally sufficient. For to avoid those things in this paper we are implementing a statement with the repeated alphabet's whatever there is we are presenting as it is with some changes made through some calculation based on the length of the statement what we are using.

HOW IT WORKS

ENCRYPTION ALGORITHM:

- Read the plaintext message
- Replace the plaintext character one by one in 5*5 matrix
- After filling of an character can be achieved if it is space is available that can be filled by the remaining alphabets.
- Apply ascii values for the filling alphabets in the 1st level of encryption.
- Generate a first secret key value by keyvalue1 = (length of the message/2-remaining alphabets that u are added). When nothing is added as an additional alphabet then the remaining value is considered as zero.
- Using the secret keyvalue1 make less from all those ascii value what we are used in matrixM1.
- From the getting matrix M2 row transposition can be achieved to get the matrix M3.
- Based on another secret keyvalue2 performing multilevel columnar transposition for up to getting an matrix M6.
- Getting cipher text matrix M6.

FOR EXAMPLE:

Considered a plain text a plaintext that can be encrypted using the proposed algorithm. Now take a message "Research is new invention". Arrange this message in a 5*5 matrix. After the message get filled then the remaining space is filled by the remaining unused alphabets in sequential manner.

PLAINTEXT:

R	E	S	E	A
R	C	H	I	S
N	E	W	I	N
V	E	N	T	I
O	N	B	D	F

Applying ASCII value for the alphabets that are in 5*5 matrix. The matrix of the ascii value for the above plaintext matrix is represented below.

1st LEVEL OF ENCRYPTION:

82	69	83	69	65
82	67	72	73	83
78	69	87	73	78
86	69	78	84	73
79	78	88	89	90

The secret keyvalue1 has been calculated by Secret keyvalue1= ((length of the message/2) - number of additional alphabets added). No more alphabets are added take the value as zero. After finding of an secret key value1 make it less from all previous value what we are using in previous matrix through the secret key.

2nd LEVEL OF ENCRYPTION:

72	59	73	59	55
72	57	62	63	73
68	59	77	63	68
76	59	68	74	63
69	68	78	79	80

3rd LEVEL OF ENCRYPTION:

After getting such a value the rows are transmitted into columns from top to bottom. Such a row transmission is done from the previous getting matrix value.

72	72	68	76	69
59	57	59	59	68
73	62	77	68	78
59	63	63	74	79
55	73	68	63	80

4th LEVEL OF ENCRYPTION:

Taking another secret key value 2 (31452) and perform the columnar transposition.

68	72	76	69	72
59	59	59	68	57
77	73	68	78	62
63	59	74	79	63
68	55	63	80	73

5th LEVEL OF ENCRYPTION:

Again perform the columnar transposition based on the same secret keyvalue2.

76	68	69	72	72
59	59	68	57	59
68	77	78	62	73
74	63	79	63	59
63	68	80	73	55

6th LEVEL OF ENCRYPTION:

From the getting matrix again perform the columnar transposition. Now the cipher text is generated. The generated ciphertext is very secure and it cannot easily reconstruct the plain text.

69	76	72	72	68
68	59	57	59	59
78	68	62	73	77
79	74	63	59	63
80	63	73	55	68

DECRYPTION ALGORITHM:

1. Read the cipher text message.
2. By using secret keyvalue2 perform columnar transposition from top to bottom upto repeated the same process getting matrix value from 3rd level.
3. From the 3rd level of decryption perform the column into row transposition for to getting the 4th level.
4. By taking an first secret key value1 add those value with all the matrix value that are available in 4th level getting an 5th level of value .
5. From the 5th level perform the reverse ascii value substitution.
6. Get the plaintext.

FOR EXAMPLE:

Read the cipher text message.

69	76	72	72	68
68	59	57	59	59
78	68	62	73	77
79	74	63	59	63
80	63	73	55	68

1st LEVEL OF DECRYPTION:

By taking an secret keyvalue2 (31452) perform the columnar transposition upto the 2nd level of decryption. Then the multi-level columnar transposition is maintained for two levels using the same secret keyvalue2.

69	76	72	72	68
68	59	57	59	59
78	68	62	73	77
79	74	63	59	63
80	63	73	55	68

2nd LEVEL OF DECRYPTION:

72	69	72	68	76
57	68	59	59	59
62	78	73	77	68
63	79	59	63	74
73	80	55	68	63

3rd LEVEL OF DECRYPTION:

72	72	68	76	69
59	57	59	59	68
73	62	77	68	78
59	63	63	74	79
55	73	68	63	80

After getting this matrix column transposition into row transposition has been done. And in the order of sequential form of one, two, three, four and five columns into row from top to bottom.

4th LEVEL OF DECRYPTION:

72	59	73	59	55
72	57	62	63	73
68	59	77	63	68
76	59	68	74	63
69	68	78	79	80

5th LEVEL OF DECRYPTION:

From the getting matrix add with each of the matrix value using the secret keyvalue1. Then the getting matrix is, all these values are to be in the form of ascii values.

82	69	83	69	65
82	67	72	73	83
78	69	87	73	78
86	69	78	84	73
79	78	88	89	90

6th LEVEL OF DECRYPTION:

From the getting matrix value write alphabets for each of the ascii values that are in the previous getting matrix. Now retaining of the plaintext message will be done.

R	E	S	E	A
R	C	H	I	S
N	E	W	I	N
V	E	N	T	I
O	N	B	D	F

V. CONCLUSION

A combination of playfair cipher with transposition has giving various advantages over the Caesar cipher. It will be a lot of scope for enhancing more security while making transactions. Easy for implementing and secure. Also practically helpful for secure communication from client to server through implementation of combining techniques.

REFERENCES

[1] S G Srikanthaswamy and Dr.H D Phaneendra ” Improved Caesar cipher with random number generation technique and multistage encryption”-International journal on Cryptography and Information Security(IJCIS)vol.2,No.4,December 2012

[2] OchocheAbraham, Ganiyu O.Shefiu ”An improved Caesarcipher algorithm”-n[IJESAT]International journal of engineering science & advance technology.volume-2,issue-5,1198-1202

[3] Programmer Enas Ismael Imran ,Programmer Farah abdulameerabdulkareem ”Enhancement Caesar cipher for better security” IOSR journal of Computer Engineering(IOSR-JCE)e-issn:2278,p-issn:2278-8727volume 16,issue 3,ver.v(may-jun2014),pp 01-05

[4] Anupama Mishra “Enhancing security of caesar cipher using different methods” IJRET: Internation journal of research in engineering and technology eissn:2319

