An Improved Version of Playfair Technique

Manish Dhingra, Gulista Khan, Kamal Kumar Gola

Abstract: Encryption which is defined as a process which converts plain text into a coded form i.e. which is in an unreadable form, so that no one can extract it or read it. It is very important to keep our data safe. There are a lot of techniques which are used for this purpose. Playfair technique is one of them. Playfair technique is used for the encryption of data. Playfair technique allows the existence of alphabets (upper case and lower case both), integer value and special symbol. In many algorithms only alphabets is used, most of the algorithm used alphabets as well as integer value and so on. Playfair techniques consider the plain text as single unit and convert the plain text into cipher text. The use of this technique is a challenge to the attack to understand the text and then decrypt it. Some time it may be possible for the attacker to understand the plaintext due to their weak matrix and key. To overcome this problem, this work proposes a technique that enhances the security of play fair technique using rectangular and substitution matrix. This work uses 8*8 matrices that contain alphabets, integers and special symbols. The objective of this work is to provide security for the data that contain alphabets, integer value as well as special symbols during transmission.

Index Terms: Rectangular Matrix, Substitution Matrix, Gray Coder, Encryption and Decryption and Key Compression.

I. INTRODUCTION

The network security and cryptography are the two very important in terms of cyber world because without these two things our data is not secure. There are mainly two types of data the one is authenticated and the other is confidential data. If we talk about the symmetric cryptography then it includes confidential data but not authentication while on the other hand the “digital signature” includes authenticated data and not confidential one [1].

Cryptography is the science of secret writing known as ancient art. This is the technique with which we can convert the message into secret text which is not easily to use to ensure that the contents of message are confidential transmitted and would be not altered. It is the technique for hiding data and information from unauthorized user. When we send a simple message from one location to another then we use one of the cryptography method for conversion of plain text into cipher text [2] [3]. Data security is required because of the large number of cybercrimes [4]. It is called the encryption technique where plaintext is randomized using a key to be ciphertext [5] [6].

Mathematical and computer science are the major parts of the cryptography. For the proper knowledge of public key of cryptosystem, number theory should be known properly. The public key algorithm is more reliable on mathematics than on permutation, the public key cryptosystem is based on mathematical function more than substitution method. As we know that public key cryptosystem is based on the method of cryptography that is asymmetric rather than symmetric cryptography [7].

Play fair cipher is widely used and quite useful in its era. Play fair cipher is a classical cryptographic algorithm that belongs to a Polygram cipher where play index is con-verted to a Polygram form and a decryption encryption process perform for the poly-graph. The playfair cipher is not more protective because it provides only 676 structures. We use Playfair cipher to encrypt and decrypt the data. We use rows and columns as a sequence using alphabets. This method creates security while we transfer the data because we use 6*6 matrix and 8*8 matrix. Our work on focus on increase the matrix size by using special characters, numbers, and so on.

II. RELATED WORK

In [8] the authors have proposed a 6*6 matrix which includes alphabets in uppercase and integer value. This work uses the loop process to generate the keywords. Four keywords are used for encryption and decryption process. In [9] the authors have used a 6*6 matrix which consist the alphabets as well as integer value. This work uses the excess 3-code to provide the more security. A method is also proposed here to generate the rectangular matrix. Key encryption process is also done for more security which is done by Caesar Cipher technique.in [10] the authors have used a 12*8 matrix which consist the alphabets, integer value as well as special symbol. The author divided his work into two parts. In the first part he extended the size of matrix and in the second part converted into ASCII code (American Standard Code for Information Interchange). Further this work uses RSA public key encryption for the encryption of key. In [11] the author used a RSA digital signature algorithm. Digital signature algorithm provided the data services. In this work, key is encrypted during transmission. In [12] the author used in his research a 10*8 matrix which consist the alphabets (in uppercase and in lowercase both), integer value from 0 to 9, list of operators as well as list of brackets. This work has divided into two parts. In the first part the key encrypted with the help of ASCII code and in the second part the concept of digital signature used [13]. A great deal of research has been done on various characters of Playfair ciphers. In [14] the authors have modified a 5*5 matrix to a 7*4 matrix. In [15] Playfair cipher is very strong for use in a wireless and mobile communications. This potential of Playfair cipher lies in a simple way which uses less power; consume less power such as algorithm RSA,

Revised Manuscript Received on July 10, 2019.

Manish Dhingra, Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, 244001, India.

Gulista Khan, Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, 244001, India.

Kamal Kumar Gola, Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, 244001, India.

DES, and AES. This paper represents a various sizes of matrices like 9*9, 10*10 and 11*11. Hence it depends on Playfair cipher where it depends on us which types of symbols and letters be used.

III. PROPOSED WORK

A. *Generation of Rectangular Matrix*

i) First place all the alphabets of key in a given matrix of from left to right and top to bottom with no repeating alphabets, integer value and special symbol.

ii) Now fill all the remaining entries of matrix 8*8 with remaining alpha-bets, integer value and special symbol according to Table 1.

Table 1. Symbols Table

Symbols			
a	**q**	**6**	**[**
b	**r**	**7**	**]**
c	**s**	**8**	**{**
d	**t**	**9**	**}**
e	**u**	**BS (Blank Space)**	**@**
f	**v**	**-**	**$**
g	**w**	**_**	*****
h	**x**	**,**	\
i	**y**	**?**	**&**
j	**z**	**/**	**#**
k	**0**	**.**	**%**
l	**1**	**^**	**+**
m	**2**	**'**	**<**
n	**3**	**"**	**=**
o	**4**	**(**	**>**
p	**5**	**)**	**|**

iii) Convert all the entries into its equivalent integer value according to the given **Table 2.**

iv)Table 2. Symbol Representation

Symbols	Value	Symbols	Value	Symbols	Value	Symbols	Value
0	0	g	16	w	32	[	48
1	1	h	17	x	33	]	49
2	2	i	18	y	34	{	50
3	3	j	19	z	35	}	51
4	4	k	20	BS	36	@	52
5	5	l	21	-	37	$	53
6	6	m	22	_	38	*	54
7	7	n	23	,	39	\\	55
8	8	o	24	?	40	&	56
9	9	p	25	/	41	#	57
a	10	q	26	.	42	%	58
b	11	r	27	^	43	+	59
c	12	s	28	'	44	<	60
d	13	t	29	"	45	=	61
e	14	u	30	(	46	>	62
f	15	v	31	)	47	|	63

iv) Converts all the entries into its equivalent binary number of 6 bits.

v) Find the gray code for each value of table that comes from **step (iv).**

vi) Now convert that code into its integer value.

vii) If the value is greater than 64 then take a mode of that value with 64.

viii) Now convert the values according to the Table 2.This matrix will be used for encryption purpose.

B. *Key Encryption Process*

Encrypt the key using caeser cipher technique.

The formula which will be used for the encryption of key.

K1=E (k+n) mod64

Where n takes on a value in the range 0 to 63.But in our case the value of n=34 according to the values in table 2.

n= (e+n+g+i+r) mod64

Now with the help of this technique we will get an integer value for each letter of key.

For the dual level of security we will again encrypt the key with the help of substitution matrix Table 3.

For the same purpose, first we will convert the integer value (Get from Caeser Cipher Technique) of each letter of key into its binary number of 6 bits.

We will take the first and last bit same and the middle four bits except first and last will be equal integer value (I) and first and last bit will be equal to integer value (II).

Now will the help of I and II we will get integer value(III) by using **Table 3** substitution matrix and the value (III) will be converted into binary no of 4 bits and place between first and last bit.

Thus the total no of bits will be equal to 6.

C. *Key Compression Process*

Now we will use the data compression technique for compressing the key. This technique will reduce the size of key than the original size. So that it will consume less space in memory and also take less time to transmit.

Key compression can be done by eliminating the repetitive bits and replacing a smaller bit. For ex: If one is used nine times in a text then it will write as 91 which means one is repeated nine times.

If the same bits are used more than nine times in the expression then it will be categorized into some parts. For ex: If there are 18 same bits repeated in an expression then it will be divided into a pair of nine (divided into two parts), if there are 27 same bits repeated in an expression then it will be divided into a pair of nine (divided into three parts) and so on.

Key compression will be done if the key have more than two repeating bits.

Table 3. Substitution Matrix

Middle Six Bits																	
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Outer Bits	0	0	1	3	5	7	9	11	13	15	2	4	6	8	10	12	14
	1	2	4	6	8	10	12	14	0	1	3	5	7	9	11	13	15
	2	14	12	10	8	6	4	2	15	13	11	9	7	5	3	1	0
	3	15	13	11	9	7	5	3	1	0	14	12	10	8	6	4	2

IV. IMPLEMENTATION

A. *Generation of Rectangular Matrix and Encryption*

Suppose we have 8*8 rectangular matrix. In a given example key is engineering and plain text is real estate

i) First place all the alphabets of key in a given matrix of from left to right and top to bottom with no repeating alphabets, integer value and special symbol.

ii) Now fill all the remaining entries of matrix 8*8 with remaining alphabets, integer value and special symbol.

e	n	g	i	r	a	b	c
d	f	h	j	k	l	m	o
p	q	s	t	u	v	w	x
y	z	0	1	2	3	4	5
6	7	8	9		-	_	,
?	/	.	^	‘	“	(	)
[	]	{	}	@	$	*	\
&	#	%	+	<	=	>	|

iii) Convert all the entries into its equivalent integer value according to the given table 2.

14	23	16	18	27	10	11	12
13	15	17	19	20	21	22	24
25	26	28	29	30	31	32	33
34	35	0	1	2	3	4	5
6	7	8	9	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

iv) Now convert all the entries into its equivalent binary number.

001110	010111	010000	010010	011011	001010	001011	001100
001101	001111	010001	010011	010100	010101	010110	011000
011001	011010	011100	011101	011110	011111	100000	100001
100010	100011	000000	000001	000010	000011	000100	000101
000110	000111	001000	001001	100100	100101	100110	100111
101000	101001	101010	101011	101100	101101	101110	101111
110000	110001	110010	110011	110100	110101	110110	110111
111000	111001	111010	111011	111100	111101	111110	111111

v) Find the gray code for each value of the above table.

001001	011100	011000	011011	010110	001111	001110	001010
001011	001000	011001	011010	011110	011111	011101	010100
010101	010111	010010	010011	010001	010000	110000	110001
110011	110010	000000	000001	000011	000010	000110	000111
000101	000100	001100	001101	110110	110111	110101	110100
111100	111101	111111	111110	111010	111011	111001	111000
101000	101001	101011	101010	101110	101111	101101	101100
100100	100101	100111	100110	100010	100011	100001	100000

vi) Now convert that code into its integer value.

9	28	24	27	22	15	14	10
11	8	25	26	30	31	29	20
21	23	18	19	17	16	48	49
51	50	0	1	3	2	6	7
5	4	12	13	54	55	53	52
60	61	63	62	58	59	57	56
40	41	43	42	46	47	45	44
36	37	39	38	34	35	33	32

vii) If the value is greater than 64 then take a mode of that value with 64.

9	28	24	27	22	15	14	10
11	8	25	26	30	31	29	20
21	23	18	19	17	16	48	49
51	50	0	1	3	2	6	7
5	4	12	13	54	55	53	52
60	61	63	62	58	59	57	56

40	41	43	42	46	47	45	44
36	37	39	38	34	35	33	32

viii) Now convert the values according to the **Table 2**.This matrix will be used for encryption purpose.

9	**s**	**o**	**r**	**m**	**f**	**e**	**a**
b	**8**	**p**	**q**	**u**	**v**	**t**	**k**
l	**n**	**i**	**j**	**h**	**g**	**[**	**]**
}	**{**	**0**	**1**	**3**	**2**	**6**	**7**
5	**4**	**c**	**d**	*****	\	**$**	**@**
<	=	|	>	**%**	+	**#**	**&**
?	/	^	**.**	**(**	**)**	**“**	**‘**
BS	**-**	**,**	**_**	**y**	**z**	**x**	**w**

Now encrypt the message **real estate.**
*First break the message into groups of two.
re al e st at ex
***re** encrypt by **ma**, **al** encrypt by **9]**, **blank space e** encrypt by **9x**, **st** encrypt by **e8**, **at** encrypt by **ek** and **ex** encrypt by **te**.
Thus the encrypted message is **ma9]9xe8ekte**.

B. *Key Encryption Process*

Now encrypt the key using ceaser cipher technique.
General additive cipher algorithm can be expressed as follows. For each alphanumeric value of key.
K1=E (k+n) mod64
Where n takes on a value in the range 0 to 63.But in our case the value of n=34.
n= (e+n+g+i+r) mod64
= (14+23+16+18+27) mod64
= (98) mod64
= 34
For example. Key is **engineering.**
K1=E (e+34) mod 64
=E (14+34) mod64
=58
K2=E (n+34) mod64
=E (23+34) mod64
=57
K3=E (g+34) mod64
=E (16+34) mod64
=50
K4=E (i+34) mod64
=E (18+34) mod64
=52
K5=E(r+34) mod64
=E (27+34) mod64
=61
Thus encrypted key is **58 57 50 52 57 58 58 61 52 57 50**
Now first we will convert the integer value 58 into binary number of 6 bits.
58=111010
We will take the first and last bit same and the middle four bits except first and last will be equal integer value 13 and first and last bit will be equal to integer value 2.
111010
Now will the help of 2 and 13 we will get integer value 3 by using substitution matrix and the value 3 will be converted into binary no of 4 bits.
3=0011
Now we place this binary no between first and last bit.
58=100110
Thus the total no of bits will be equal to 6.
Similarly we will repeat this process for the other integer values.
57=111001
8=1000
57=110001
50=110010
11=1011
50=110110
52=110100
9=1001
52=110010
61=111101
4=0100
61=101001
Hence the final encrypted key is
10011011000111011011001011000110011010011010 1001 110010110001110110

C. *Key Compression Process*

We will eliminate the repetitive bits and replacing a smaller bit to minimize the transmission time and save the space in the memory.
100110110001110110110010110001100110100110101001 110010110001110110
It will be written as:-
12021021303102102120102130212021012021010120312 0102130310210

IV. RESULTS AND COMPARISION

A comparison has been done with the baseline algorithm [9] where the authors have used the rectangular matrix which includes the alphabets in lower case and integer (0-9) only and the size of matrix is 6*6. In [9] the authors have also encrypted the key using caesar cipher while in the proposed algorithm 8*8 matrix is used which includes alphabets in lower case only, integers (0-9) and special symbols. A new rectangular matrix is used here to provide the more security during encryption process. Key encryption is also done with substitution matrix in the proposed algorithm to provide the more security during key transmission. Key compression process is also used that reduces the size of key than the original size. So that it will consume less space in memory and also takes less time to transmit while in [9] the authors simply transfer the key which lessens the security. To sum up, proposed algorithm is more secure as compared to baseline algorithm [9].

Table 6. Comparison with Baseline Algorithm [9]

Parameters	Proposed Algorithm	Baseline Algorithm [9]
Size of Matrix	8*8	6*6
Input Parameters	Alphabets in lower case, integers (0-9) and special symbols.	Alphabets in lower case and integers (0-9) only
Substitution matrix and ASCII	Substitution matrix and ASCII are used to provide the more security	Not available
Key Encryption	Key encryption is performed using modified Caesar cipher.	Key encryption is performed using Caesar cipher where the value of n is taken randomly.
Key Compression Process	Key Compression Process is used to reduce the memory size	Not Available

V. CONCLUSIONS

The conclusion of this work is that the use of Playfair technique is very useful. The requirement of the security can be done by using this technique. The encryption of key is very useful for more security. For the encryption of key this work uses Ceaser Cipher and Substitution matrix so that no one can understand it. Further this work uses Data Compression technique. Many authors used Playfair technique in the research but the transmission time is very huge due to large size of key and data consumes very large space in the memory. Hence the advantage of this work is that data will consume a very less space in memory and transmission time will very less as compared to others.

REFERENCES

1. Babita and Gurjeet Kaur, "network security based on cryptography and steganography techniques", International journal of advanced research in computer science. VOL 8, NO. 4, May 2017(special issue), pp-161-165.
2. Prerna Mahajan and Abhishek Sachdeva, "A Study of encryption algorithms AES, DES and RSA for security", Global journal of CS and technology network, web and security. Vol 13, issue 15 version 1.0, year- 2013. Pp-15-22.
3. N.A.Putri,A.P.U.Siahaan. F.Wadly and Muslim "Image Similarly Test Using Eigen face Calculation," Int.J.Sci.Technol.,vol.3,no.6,pp.510-515,2018.
4. A.P.U.Siahaan, "High Complexity Bit-Plane Security Enhancement in BPCS Steganography," Int.J.Comput.appl,vol.148,no.3,pp.17-22,2018.
5. A.P.U.Siahaan, "Pelanggaran Cybercrime dankekuatanYuridikshi di Indonesia,"J.Tek.Daninformvol.5, no.1, pp.6-9, 2018.
6. Hariyanto,A.P.U.Siahaan,R.Rahim and Mesran, "Internet protocol security as the network CryptographySystem," Int. J. Sci. Res.Sci.Technol.,vol.3,no.6,pp.223-226,2018.
7. Hariyanto and A.P.U.Siahaan, "Intrusion detection system in Network forensic analysis and," IOSR J.Comput. Sci.Enginee,vol.18,no.6,pp.115-121,2018.
8. Nisarga Chand and subhajit Bhattacharya "A novel approach for Encryption of Text messages Using PLAYFAIR Cipher 6*6 Matrix with four Iteration Steps", International Journal of Engineering Science and Innovative Technology , vol 3,Issue 1, Jan 2014.
9. Zubair Iqbal, Bhumika Gupta, Kamal Kumar Gola and Prachigupta, "Enhanced the Security of Playfair Technique using Excess 3 code (XS3) and Ceaser Cipher",IJCA (0975-8887)vol 103,no 13, October 2014.
10. Surendra Singh Chauhan,Hawa Singh and Ram NiwasGurjar, " Secure Key Exchange using RSA in extended Playfair Cipher Technique", International journal of Computer Applications (0975-8887) vol 104,no-15, Oct 2014.
11. Kamal Kumar Gola , Zubair Iqbal and Bhumika Gupta, " Modified RSA digital signature scheme for data confidentially", IJCA(0975-8887), vol 106, no 13, Nov 2014.
12. Kamal Kumar Gola, Zubair Iqbal and Bhumika Gupta, " Dual Level Security for key Exchange using Modified RSA Public Key Encryption in Playfair Technique", IJCA(0975-8887) vol 106, no 13, Nov 2014.
13. P.Murli and G. Senthilkumar, and J. Palchodhury, "A Framework for the Development of a New Approach of Playfair Cipher", in Porceedings of India Com 2008, pages 1 -2, Feb 2008.
14. H. Obayes, "Suggested Approach to Embedded Playfair Cipher Message in Digital Image", Int. Journal of Engineering Research and Applications, Vol.3, Issue 5, pp.710-714,2013
15. Salman A. Khan "Design and Analysis of Playfair Ciphers with Different Matrix Sizes", Computer Engineering Dept. , College of Information Technology, University of Bahrain, Bahrain, 25 May,10 Aug, 20 Aug. 1,Sept, 2015.

AUTHORS PROFILE

Manish Dhingra is an engineer and management professional with more than 18 years of experience in industry and academics. He has done BE (Production) from Nagpur University in 1996, Master in Business Administration degree from Kurukshetra University in the year 2003 and secured M.Tech. (Manufacturing Systems) degree in 2015. He started his career as an engineer and served into many companies of International repute and then switched to academics after obtaining his MBA. Presently, he is working as Associate Professor in Faculty of Engineering, Teerthanker Mahaveer University, Moradabad. He has published number of papers in National & International Journals.

Gulista Khan has completed B.Tech. in Information technology from Kurukshetra university in 2006. She completed Post Graduation (M. Tech.) from MMEC, Mullana in 2009. She is pursuing Ph.D. in Computer Science and Engineering from Teerthanker Mahaveer University Moradabad. Also working as Assistant Professor in Computer Science and Engineering department, Teerthanker Mahaveer University since 2011. Her Area of research is wireless sensor networks. Published more than 26 papers in International conferences mostly have preceding in Scopus. Published 24 paper in International Journals including mostly Scopus, Elsevier, Springer, and Thomson Reuter's indexed journals.

Kamal Kumar Gola is working as Assistant Professor in Faculty of Engineering, Teerthanker Mahaveer University, and Moradabad. He received his B.Tech. Degree from Moradabad Institute of Technology in Computer Science and Engineering and M.Tech. Degree from Uttarakhand Technical University in Computer Science and Engineering. His main research interests are Wireless Sensor Networks, Algorithms and Security.