IMPROVEMENT IN SECURITY MEASUREMENT IN CRYPTOGRAPHIC ALGORITHM WITH PLAYFAIR EXAMPLE

Chhotu Ram Jat[1], Shalini[2]
[2]AP, [1,2]Jaipur Institute of Technology Group of Institution, Jaipur

Abstract: In the time of internet when we are sending and receiving the information over the network in the presence of the third party then it is very necessary to protect our data from the attacker's, in the series to protect the data we are using the cryptography algorithms. Day to day the new cryptography algorithms are found and there is modification in the previous algorithm also. According to the key the encryption algorithm are of two types. First is symmetric key algorithm and second is asymmetric key algorithms. The proposed work is an example of the symmetric key algorithm. In the work I done the improvement in the playfair matrix technique. I used the all the rules of the basic playfair algorithm with some changes (changes in matrix). This work is divided into two parts. In Ist part the basic 5X5 playfair cipher table improve in size of matrix, so that limitations of earlier works of playfair cipher can remove. In this projected system, i used two matrix of size 12×8 , that contain many alphabetic, numeric as well as special character (total 96) use as input and after this we use the shifting value to shift the matrix. In IInd spart of making the cipher text, we check the position of plain text in first matrix and according to the playfair matrix rules replace these characters with the characters from the second matrix (this is the improvement in this work) make cipher text by it. This cipher text is sent to receiver end, at receiver end receiver check the position of this cipher text in second matrix and saves theses position and gets the plain text by seeing these positions in this first matrix. By these matrixes we can encrypt as well as the messages finally, safety strength of entire system has been analyze as well as tried to perform requisite of security. In last, dissertation present scope for concludes the dissertation as well as further work.

I. INTRODUCTION

1.1 Introduction on the subject of cryptography:-

In the era of digital world, security of 'information' has extremely important to both organization as well as individuals. When information is stored or transmit by a message or packets of messages by some channel there, be supposed to be some system or method to protect the information from interruption and hacking. If information hacked by the wrong one there might occur various problems. Therefore, we need to secrete data in such a way that no any third person or party can't hack that exact communication. The present research focuses on the annoying to being enhance the basic Playfair technique (5x5 matrix) to two matrix of size 12x18 size of rectangular matrix, attacks probable on data and tackle these attacks by means of right types of contradict measures. In addition, to secure the key of the playfair technique is need to make sure the safety measures of a given data by some kind of mechanism and increase the security, confidentiality, integrity as well as availability.

1.2 Cryptographic algorithms

The cryptography algorithms are those algorithms that can convert the data readable form to unreadable form as well as unreadable from to readable form. According to key, cryptography algorithms are of two types first is symmetric key algorithm and other is asymmetric key algorithm.

1.3 Symmetric key cryptography

If the encryption and decryption both are done using the same key then it is called the private key or Symmetric cryptography. Symmetric-key cryptography is where senders and receivers share the same keys. So those keys are used for encryption and decryption. They are used mainly with block ciphers and stream ciphers. [30],[34].Examples are AES and DES.

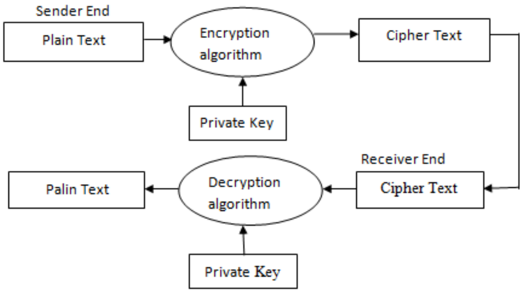


Fig 1 Private key cryptography

II. MOTIVATION

2.1 Existing work

The existing work is on play fair algorithm is done on 5x5, 7x4, 6x6, 12x8 and 16x16 on single matrix. It dose not any matter that these matrixes are rectangular or squares in size. These algorithms are not sufficient according to the security levels in present scenario. There are some drawbacks of these algorithms that some of these are very easy to break, and other breaks with some hard work, but these are not secure perfectly. There is a day to day enhancement in these algorithms to enhance the security of data by different algorithm. There are different types of attack on these algorithm some of these are present by the experimental result. So it is required to enhance the security levels by different parameters as characters supported of an algorithm, frequency analysis on a algorithm and brute force attack on an algorithm. Security is the most significant aspect of recants trends. So provide the security we study cryptography and application of cryptography techniques.

What is cryptography and how it works. Cryptography is the art or it is the science so how we can accomplish the security or encoded the plain test to cipher test. Cryptography is the well-defined or systematic technique while in the cryptanalysis we can finding the non-readable message to readable message and it is hit and trial based technique. Therefore, there are many cryptography techniques.

In this follow a line of research, I have study the play fair procedure. In play fair techniques it is symmetric key cryptography in this cryptography techniques only solo key is used to perform encryption as well as decryption .We have study how the uses and work of play fair techniques so we can do encrypted and decrypted message . In the encryption as well as decryption process we have augment the basic Playfair technique (5x5 matrix) to two 12x8 sizes of rectangular matrix is needed to ensure security of a given data by some kind of mechanism. There are four main important goals in providing security following are:

- Availability that means ease of use or accessibility.
- Confidentiality that means privacy or secrecy.
- Integrity.
- Authentication that means verification or confirmation.

Therefore, we need to fulfill the security according to these goals and send or receive the data in better manner in comparison of previous algorithms.

2.2 Problem Statement

The main problem is that the 5X5 matrix cannot use in present scenario because of its limitations this algorithm is invented in 1854 so it is less secure in present scenario the reason is limitations of the 5X5 playfair matrix.

- The 5×5 PF Matrix judge the alphabet 'I' as well as alphabet 'J' as one character.
- Only 26 letters of upper case in English can take as the key.
- The Space is not considered as one character.
- The special characters as well as numbers can't use..
- In 5X5 playfair matrix only uppercase English letters are only used in 5x5 Matrix.
- The 'X' is used a filler letter while repeating letter falls in the same pair are separated.

To design an efficient algorithm by such type of method to overcome these limitation of the 5X5 playfair matrix.

2.3 Objectives of the Dissertation

The Objectives of the dissertation include the following main issues:

- Study and analysis the popular symmetric key cryptosystem Playfair matrix.
- Use the properties of symmetric key algorithm, which provide the better security, then the previous Playfair algorithm in cryptography.
- Implementation of playfair matrix with Turbo C++.
- Performance analysis of playfair encryption algorithm on some text.

III. METHODOLOGY & IMPLEMENTATION

3.1 Proposed work

The proposed algorithm remove the disadvantage of previous algorithms by taking 192 characters in two tables, in first table 96 characters of ASCII 7 code and in table 2, 96 characters of ASCII 8 characters. The size of first and second table or matrix is 12x8. I fill up the key of play fiar algorithm in first table and make he table with the help of play fair rules. The second table is ideal there is no any change in any situation. I apply the rotation on the first table from value 0 to 7. So by this i can change the first matrix 8 times for a single key and a single input plain text. So the output of first table is change according to input key, plain text and shifting value s. The positions of output of first table are save and according to this I create the output by second table. At the receiver end the reveres process of this process is apply.

3.2 Proposed System

The proposed work consists of the following these steps:

At The Sender Ends.

Step 1: Build a customized matrix of Playfair cipher technique method of size 12X8, which include all alphabets from A to Z upper case and a to z in lower case, all the special characters as well as all numeric values (from 0 to 9). Construct second matrix of same size 12X8 with ASCII code 8 values from 128 to 223.

The encryption method is alienated in these two phases:

- Ist phase is making as well as population the Matrix process.
- The IInd phase is encryption method by help of playfair matrix of plain text message. Make the Cipher text of the plain text.

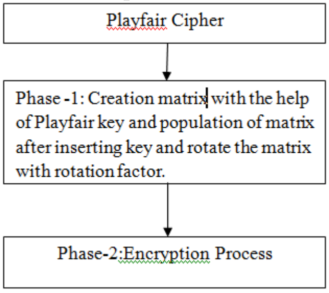

Playfair Cipher
Phase -1: Creation matrix with the help of Playfair key and population of matrix after inserting key and rotate the matrix with rotation factor.
Phase-2:Encryption Process

Fig 2 Playfair cipher encryption steps [32]

At The Receiver Ends.

Step 2: Create second matrix of same size 12X8 with ASCII code 8 values from 128 to 223. Take the CT in pair of two characters and check its positions in the second matrix.

Step 4: Create a customized table of Playfair matrix technique of size 12X8, which include all alphabets from A to Z upper case and a to z in lower case, all special letters which are on the keyboard and all numeric values (from 0 to 9). The PF decryption technique is divided into these two phases:

- First phase is regarding the creation as well as population of Matrix by help key).
- The second phase is regarding the decryption process method of the cipher text (CT1) by the position in the second matrix with the help of the first matrix and makes the plain text.

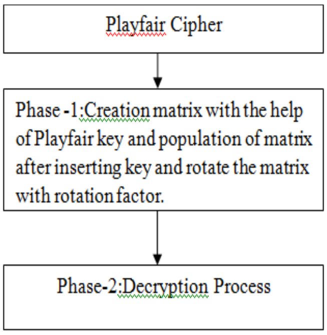
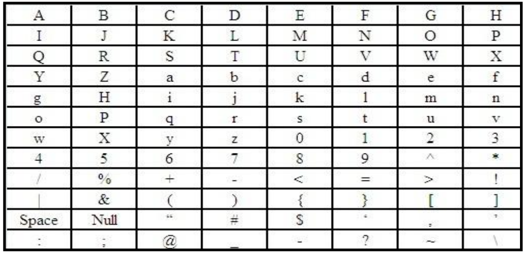

Playfair Cipher
Phase -1:Creation matrix with the help of Playfair key and population of matrix after inserting key and rotate the matrix with rotation factor.
Phase-2:Decryption Process

Fig 3 Playfair cipher decryption steps

3.3 Experiment Analysis

- The proposed algorithm work is dividing in these two phases:
- Ist phase for Matrix making uses all rules of Play fair matrix with these given changes:
- Both I and J letters in upper case as well as lower case are considered as two different letters (all four I, J, i and j are different).
- It allows 256 characters without any duplicate as key.
- It is case sensitive; it uses the upper case A-Z as well as lower case a-z characters. Mixture of numbers efficiently can easily encrypted and decrypted efficiently by user.
- Combination of operators, brackets, special characters, can easily encrypted and decrypted efficiently by user.
- This proposed algorithm adds Null character to complete pair, because “Null” character can’t affect PT at end of word or sentence.
- Space among two words or sentences’ in PT measured as one character.

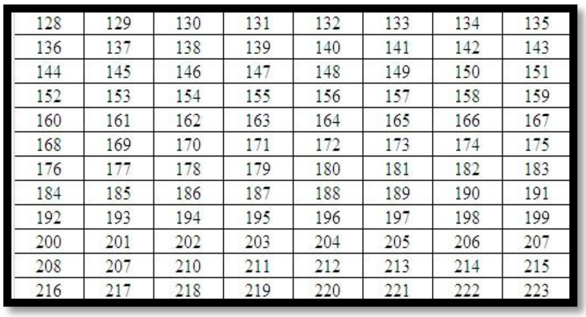
Table 1 List Of Upper Case Letters, Lower Case Letter, Numeric Values, Operators, Brackets and Special Characters.



A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X
Y	Z	a	b	c	d	e	f
g	H	i	j	k	1	m	n
o	P	q	r	s	t	u	v
w	X	y	z	0	1	2	3
4	5	6	7	8	9	^	*
/	%	+	-	<	=	>	!
|	&	(	)	{	}	[	]
Space	Null	“	#	$	‘	,	’
:	;	@	_	-	?	~	\

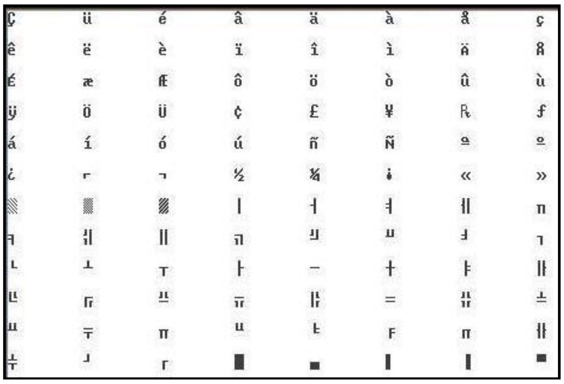
In second matrix, we use the ASCII code from value 128 to 223.

Table 2 ASCII code use in second table.



128	129	130	131	132	133	134	135
136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151
152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167
168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183
184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199
200	201	202	203	204	205	206	207
208	207	210	211	212	213	214	215
216	217	218	219	220	221	222	223

Table 3 Char form of the table



Ç	ü	é	â	ä	à	å	ç
ê	ë	è	ï	î	ì	Ä	Å
É	æ	Æ	ô	ö	ò	û	ù
ÿ	Ö	Ü	¢	£	¥	₧	ƒ
á	í	ó	ú	ñ	Ñ	ª	º
¿	⌐	¬	½	¼	¡	«	»
░	▒	▓	│	┤	╡	╢	╖
╕	╣	║	╗	╝	╜	╛	┐
└	┴	┬	├	─	┼	╞	╟
╚	╔	╩	╦	╠	═	╬	╧
╨	╤	╥	╙	╘	╒	╓	╫
╪	┘	┌	█	▄	▌	▐	▀

- The key length is very large in comparison with the previous algorithms, here, so it is very difficult to find the plain text from CT without knowing a key.
- This algorithm can’t separate a repeating PT letters with a filter letter.

3.4 Algorithm

At The Sender Ends.

Step 1: In the first phase:

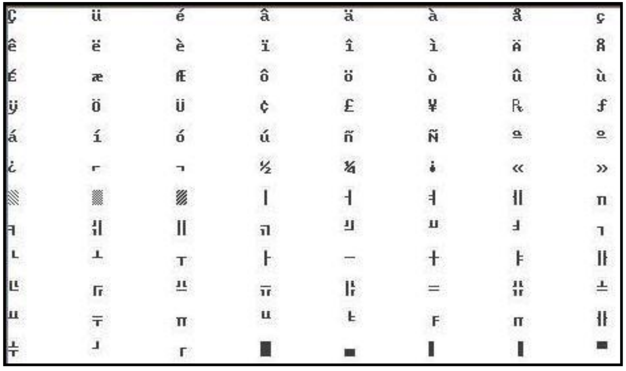
- If in plaintext if there is odd number of character then add the Null character in the last of the key.
- Use two PF matrix size of 12×8.
- In First matrix we insert the key without duplicate and fill up the key in the PF matrix without any duplicate from left side to right side and from top to bottom of the PF matrix side, then fill the remaining cells with the upper given tables and rotate the matrix with shifting value .
- In second matrix we use the ASCII code from 128 to 223.
- If both letters come into view in same row in PF matrix table, change them with the letters to their instant right side equally (wrapping just about to left side of row if a character in the original PT pair was on right side of the row).
- If both letters come into view in same column in play fair table, change them with alphabets to their instant below side correspondingly (wrapping just about to top side of column if a letter in original PT pair was on bottom side of the column).
- If both letters are not on same column as well as row, change them with letters on same row equally but at other pair of corners of rectangle defined by PT.
- By this make the cipher text (CT1) of the plain text.

At The Receiver Ends.

- Apply deception process on CT using matrix 2 to get the position of the character and save these position.
- Construct matrix 1 at receiver side; first insert the key without duplicate and after this insert the remaining characters in upper given tables and rotate the matrix with shifting value .
- According the position of the CT characters (in pair of 2 characters until end of cipher text) decrypt it using matrix 1 and get the original plain text.
- Decrypt the cipher text to get PT by this PF Matrix.

IV. INPUTS

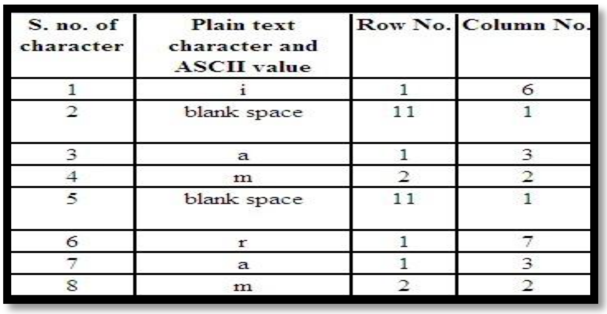
Table 4 second matrix table for all input



Ç	ü	é	â	ä	à	å	ç
ê	ë	è	ï	î	ì	Ä	Å
É	æ	Æ	ô	ö	ò	û	ù
ÿ	Ö	Ü	¢	£	¥	₧	ƒ
á	í	ó	ú	ñ	Ñ	ª	º
¿	⌐	¬	½	¼	¡	«	»
░	▒	▓	│	┤	╡	╢	╖
╕	╣	║	╗	╝	╜	╛	┐
└	┴	┬	├	─	┼	╞	╟
╚	╔	╩	╦	╠	═	╬	╧
╨	╤	╥	╙	╘	╒	╓	╫
╪	┘	┌	█	▄	▌	▐	▀

Inputs in different examples Key=playfairexample and plain text is= i am ram for all examples After remove duplicate = playfire , Plain text= i am ram

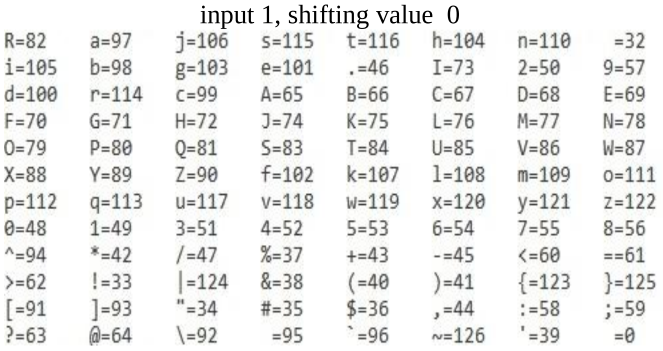
Table 5 of plain text i am ram



S. no. of character	Plain text character and ASCII value	Row No.	Column No.
1	i	1	6
2	blank space	11	1
3	a	1	3
4	m	2	2
5	blank space	11	1
6	r	1	7
7	a	1	3
8	m	2	2

Input 1 with shifting value 0

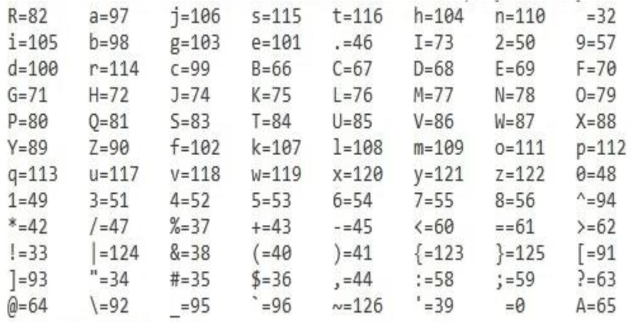
TABLE 6 matrix at sender end as well as receiver side for input 1, shifting value 0



R=82	a=97	j=106	s=115	t=116	h=104	n=110	=32
i=105	b=98	g=103	e=101	.=46	I=73	2=50	9=57
d=100	r=114	c=99	A=65	B=66	C=67	D=68	E=69
F=70	G=71	H=72	J=74	K=75	L=76	M=77	N=78
O=79	P=80	Q=81	S=83	T=84	U=85	V=86	W=87
X=88	Y=89	Z=90	f=102	k=107	l=108	m=109	o=111
p=112	q=113	u=117	v=118	w=119	x=120	y=121	z=122
0=48	1=49	3=51	4=52	5=53	6=54	7=55	8=56
^=94	*=42	/=47	%=37	+=43	-=45	<=60	==61
>=62	!=33	|=124	&=38	(=40	)=41	{=123	}=125
[=91	]=93	"=34	#=35	$=36	,=44	:=58	;=59
?=63	@=64	\=92	=95	`=96	~=126	'=39	=0

Input 1 with shifting value 1

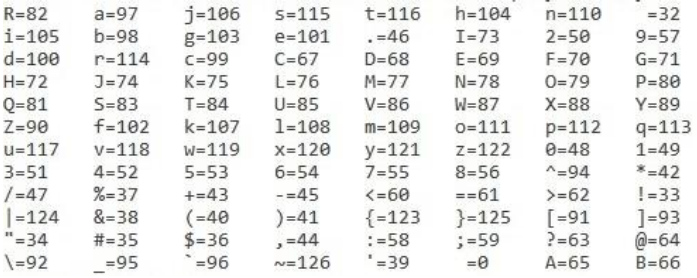
TABLE 7 playfair matrix at sender as well as receiver side for input 1, shifting value 1



R=82	a=97	j=106	s=115	t=116	h=104	n=110	=32
i=105	b=98	g=103	e=101	.=46	I=73	2=50	9=57
d=100	r=114	c=99	B=66	C=67	D=68	E=69	F=70
G=71	H=72	J=74	K=75	L=76	M=77	N=78	O=79
P=80	Q=81	S=83	T=84	U=85	V=86	W=87	X=88
Y=89	Z=90	f=102	k=107	l=108	m=109	o=111	p=112
q=113	u=117	v=118	w=119	x=120	y=121	z=122	0=48
1=49	3=51	4=52	5=53	6=54	7=55	8=56	^=94
*=42	/=47	%=37	+=43	-=45	<=60	==61	>=62
!=33	|=124	&=38	(=40	)=41	{=123	}=125	[=91
]=93	"=34	#=35	$=36	,=44	:=58	;=59	?=63
@=64	\=92	_=95	`=96	~=126	'=39	=0	A=65

Input 1 with shifting value 2

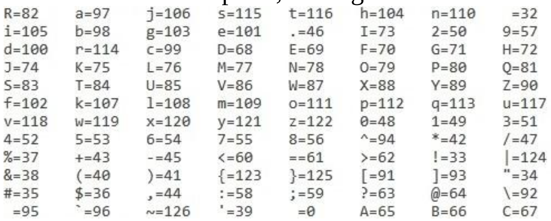
TABLE 8 matrix at sender as well as receiver side for input 1, shifting value 2



R=82	a=97	j=106	s=115	t=116	h=104	n=110	=32
i=105	b=98	g=103	e=101	.=46	I=73	2=50	9=57
d=100	r=114	c=99	C=67	D=68	E=69	F=70	G=71
H=72	J=74	K=75	L=76	M=77	N=78	O=79	P=80
Q=81	S=83	T=84	U=85	V=86	W=87	X=88	Y=89
Z=90	f=102	k=107	l=108	m=109	o=111	p=112	q=113
u=117	v=118	w=119	x=120	y=121	z=122	0=48	1=49
3=51	4=52	5=53	6=54	7=55	8=56	^=94	*=42
/=47	%=37	+=43	-=45	<=60	==61	>=62	!=33
|=124	&=38	(=40	)=41	{=123	}=125	[=91	]=93
"=34	#=35	$=36	,=44	:=58	;=59	?=63	@=64
\=92	_=95	`=96	~=126	'=39	=0	A=65	B=66

Input 1 with shifting value 3

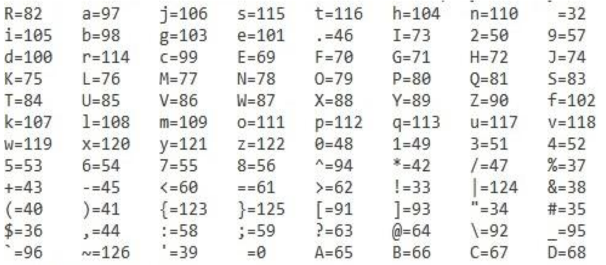
TABLE 9 First matrix at sender as well as receiver sidefor input 1,shifting value 3



R=82	a=97	j=106	s=115	t=116	h=104	n=110	=32
i=105	b=98	g=103	e=101	.=46	I=73	2=50	9=57
d=100	r=114	c=99	D=68	E=69	F=70	G=71	H=72
J=74	K=75	L=76	M=77	N=78	O=79	P=80	Q=81
S=83	T=84	U=85	V=86	W=87	X=88	Y=89	Z=90
f=102	k=107	l=108	m=109	o=111	p=112	q=113	u=117
v=118	w=119	x=120	y=121	z=122	0=48	1=49	3=51
4=52	5=53	6=54	7=55	8=56	^=94	*=42	/=47
%=37	+=43	-=45	<=60	==61	>=62	!=33	|=124
&=38	(=40	)=41	{=123	}=125	[=91	]=93	"=34
#=35	$=36	,=44	:=58	;=59	?=63	@=64	\=92
=95	`=96	~=126	'=39	=0	A=65	B=66	C=67

Input 1 with shifting value 4

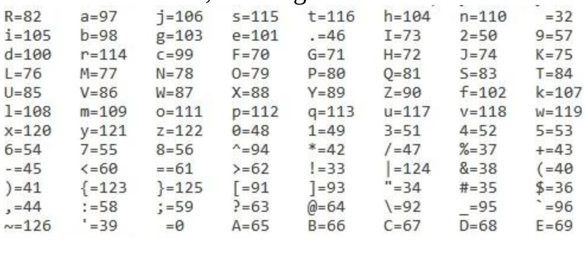
TABLE 10 matrix at sender as well as receiver side for input 1, shifting value 4



R=82	a=97	j=106	s=115	t=116	h=104	n=110	=32
i=105	b=98	g=103	e=101	.=46	I=73	2=50	9=57
d=100	r=114	c=99	E=69	F=70	G=71	H=72	J=74
K=75	L=76	M=77	N=78	O=79	P=80	Q=81	S=83
T=84	U=85	V=86	W=87	X=88	Y=89	Z=90	f=102
k=107	l=108	m=109	o=111	p=112	q=113	u=117	v=118
w=119	x=120	y=121	z=122	0=48	1=49	3=51	4=52
5=53	6=54	7=55	8=56	^=94	*=42	/=47	%=37
+=43	-=45	<=60	==61	>=62	!=33	|=124	&=38
(=40	)=41	{=123	}=125	[=91	]=93	"=34	#=35
$=36	,=44	:=58	;=59	?=63	@=64	\=92	_=95
`=96	~=126	'=39	=0	A=65	B=66	C=67	D=68

Input 1 with shifting value 5

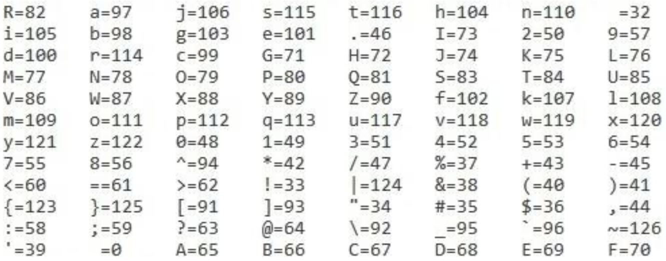
TABLE 11 matrix at sender as well as receiver side for input 1, shifting value 5



R=82	a=97	j=106	s=115	t=116	h=104	n=110	=32
i=105	b=98	g=103	e=101	.=46	I=73	2=50	9=57
d=100	r=114	c=99	F=70	G=71	H=72	J=74	K=75
L=76	M=77	N=78	O=79	P=80	Q=81	S=83	T=84
U=85	V=86	W=87	X=88	Y=89	Z=90	f=102	k=107
l=108	m=109	o=111	p=112	q=113	u=117	v=118	w=119
x=120	y=121	z=122	0=48	1=49	3=51	4=52	5=53
6=54	7=55	8=56	^=94	*=42	/=47	%=37	+=43
-=45	<=60	==61	>=62	!=33	|=124	&=38	(=40
)=41	{=123	}=125	[=91	]=93	"=34	#=35	$=36
,=44	:=58	;=59	?=63	@=64	\=92	_=95	`=96
~=126	'=39	=0	A=65	B=66	C=67	D=68	E=69

Input 1 with shifting value 6

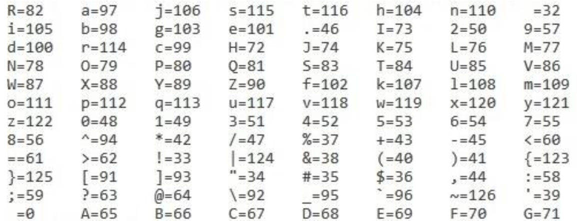
TABLE 12 First matrix at sender as well as receiver side for input 1,shifting value 6



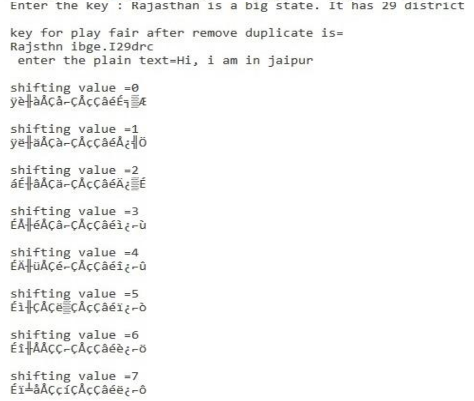
R=82	a=97	j=106	s=115	t=116	h=104	n=110	=32
i=105	b=98	g=103	e=101	.=46	I=73	2=50	9=57
d=100	r=114	c=99	G=71	H=72	J=74	K=75	L=76
M=77	N=78	O=79	P=80	Q=81	S=83	T=84	U=85
V=86	W=87	X=88	Y=89	Z=90	f=102	k=107	l=108
m=109	o=111	p=112	q=113	u=117	v=118	w=119	x=120
y=121	z=122	0=48	1=49	3=51	4=52	5=53	6=54
7=55	8=56	^=94	*=42	/=47	%=37	+=43	-=45
<=60	==61	>=62	!=33	|=124	&=38	(=40	)=41
{=123	}=125	[=91	]=93	"=34	#=35	$=36	,=44
:=58	;=59	?=63	@=64	\=92	_=95	`=96	~=126
'=39	=0	A=65	B=66	C=67	D=68	E=69	F=70

Input 1 with shifting value 7

TABLE 13 matrix at sender as well as receiver side for input 1, shifting value 7



```
R=82    a=97    j=106   s=115   t=116   h=104   n=110    =32
i=105   b=98    g=103   e=101   .=46    I=73    2=50    9=57
d=100   r=114   c=99    H=72    J=74    K=75    L=76    M=77
N=78    O=79    P=80    Q=81    S=83    T=84    U=85    V=86
W=87    X=88    Y=89    Z=90    f=102   k=107   l=108   m=109
o=111   p=112   q=113   u=117   v=118   w=119   x=120   y=121
z=122   0=48    1=49    3=51    4=52    5=53    6=54    7=55
8=56    ^=94    *=42    /=47    %=37    +=43    -=45    <=60
==61    >=62    !=33    |=124   &=38    (=40    )=41    {=123
}=125   [=91    ]=93    "=34    #=35    $=36    ,=44    :=58
;=59    ?=63    @=64    \=92    _=95    `=96    ~=126   '=39
 =0     A=65    B=66    C=67    D=68    E=69    F=70    G=71
```

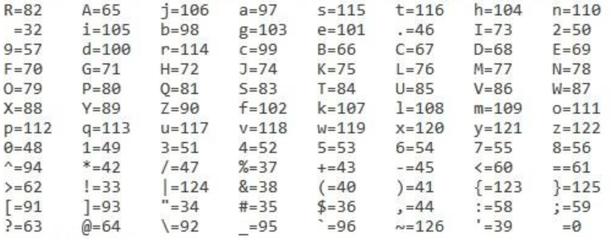


```
Enter the key : Rajasthan is a big state. It has 29 district

key for play fair after remove duplicate is=
Rajsthn ibge.I29drc
 enter the plain text=Hi, i am in jaipur

shifting value =0
ÿè╫àÅÇå-ÇÅçÇâéÉ┐▒Æ

shifting value =1
ÿë╫äÅÇà-ÇÅçÇâéÅ¿╢Ö

shifting value =2
áÉ╫âÅÇä-ÇÅçÇâéÄ¿▒É

shifting value =3
ÉÅ╫éÅÇâ-ÇÅçÇâéì¿-ù

shifting value =4
ÉÄ╫üÅÇé-ÇÅçÇâéî¿-û

shifting value =5
Éì╫ÇÅÇë▒ÇÅçÇâéï¿-ò

shifting value =6
Éî╫ÅÅÇÇ-ÇÅçÇâéè¿-ö

shifting value =7
Éï╧åÅÇçíÇÅçÇâéë¿-ô
```

Fig. 4.Output of input 1 with shifting value 1 to 7

Input 2 shifting value 0

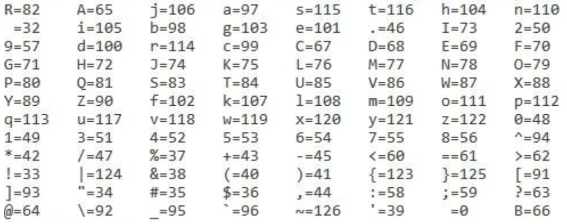
TABLE 14 matrixes at sender as well as receiver side for input 2, shifting value 0



```
R=82    A=65    j=106   a=97    s=115   t=116   h=104   n=110
 =32    i=105   b=98    g=103   e=101   .=46    I=73    2=50
9=57    d=100   r=114   c=99    B=66    C=67    D=68    E=69
F=70    G=71    H=72    J=74    K=75    L=76    M=77    N=78
O=79    P=80    Q=81    S=83    T=84    U=85    V=86    W=87
X=88    Y=89    Z=90    f=102   k=107   l=108   m=109   o=111
p=112   q=113   u=117   v=118   w=119   x=120   y=121   z=122
0=48    1=49    3=51    4=52    5=53    6=54    7=55    8=56
^=94    *=42    /=47    %=37    +=43    -=45    <=60    ==61
>=62    !=33    |=124   &=38    (=40    )=41    {=123   }=125
[=91    ]=93    "=34    #=35    $=36    ,=44    :=58    ;=59
?=63    @=64    \=92    _=95    `=96    ~=126   '=39     =0
```

Input 2 shifting value 1

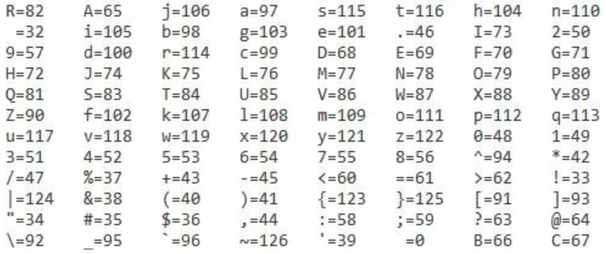
TABLE 15 matrix at sender as well as receiver side for input 2, shifting value 1



```
R=82    A=65    j=106   a=97    s=115   t=116   h=104   n=110
 =32    i=105   b=98    g=103   e=101   .=46    I=73    2=50
9=57    d=100   r=114   c=99    C=67    D=68    E=69    F=70
G=71    H=72    J=74    K=75    L=76    M=77    N=78    O=79
P=80    Q=81    S=83    T=84    U=85    V=86    W=87    X=88
Y=89    Z=90    f=102   k=107   l=108   m=109   o=111   p=112
q=113   u=117   v=118   w=119   x=120   y=121   z=122   0=48
1=49    3=51    4=52    5=53    6=54    7=55    8=56    ^=94
*=42    /=47    %=37    +=43    -=45    <=60    ==61    >=62
!=33    |=124   &=38    (=40    )=41    {=123   }=125   [=91
]=93    "=34    #=35    $=36    ,=44    :=58    ;=59    ?=63
@=64    \=92    _=95    `=96    ~=126   '=39     =0     B=66
```

Input 2 shifting value 2

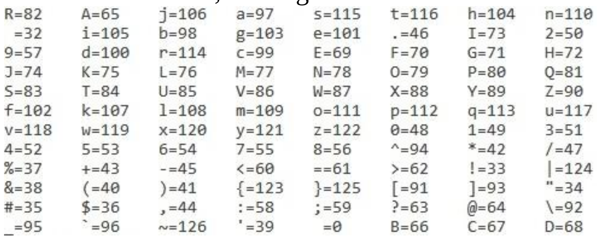
TABLE 16 matrix at sender as well as receiver side for input 2, shifting value 2



```
R=82    A=65    j=106   a=97    s=115   t=116   h=104   n=110
 =32    i=105   b=98    g=103   e=101   .=46    I=73    2=50
9=57    d=100   r=114   c=99    D=68    E=69    F=70    G=71
H=72    J=74    K=75    L=76    M=77    N=78    O=79    P=80
Q=81    S=83    T=84    U=85    V=86    W=87    X=88    Y=89
Z=90    f=102   k=107   l=108   m=109   o=111   p=112   q=113
u=117   v=118   w=119   x=120   y=121   z=122   0=48    1=49
3=51    4=52    5=53    6=54    7=55    8=56    ^=94    *=42
/=47    %=37    +=43    -=45    <=60    ==61    >=62    !=33
|=124   &=38    (=40    )=41    {=123   }=125   [=91    ]=93
"=34    #=35    $=36    ,=44    :=58    ;=59    ?=63    @=64
\=92    _=95    `=96    ~=126   '=39     =0     B=66    C=67
```

Input 2 shifting value 3

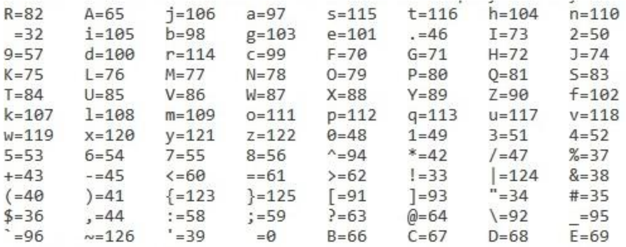
TABLE 17 matrix at sender as well as receiver side for input 2, shifting value 3



```
R=82    A=65    j=106   a=97    s=115   t=116   h=104   n=110
 =32    i=105   b=98    g=103   e=101   .=46    I=73    2=50
9=57    d=100   r=114   c=99    E=69    F=70    G=71    H=72
J=74    K=75    L=76    M=77    N=78    O=79    P=80    Q=81
S=83    T=84    U=85    V=86    W=87    X=88    Y=89    Z=90
f=102   k=107   l=108   m=109   o=111   p=112   q=113   u=117
v=118   w=119   x=120   y=121   z=122   0=48    1=49    3=51
4=52    5=53    6=54    7=55    8=56    ^=94    *=42    /=47
%=37    +=43    -=45    <=60    ==61    >=62    !=33    |=124
&=38    (=40    )=41    {=123   }=125   [=91    ]=93    "=34
#=35    $=36    ,=44    :=58    ;=59    ?=63    @=64    \=92
_=95    `=96    ~=126   '=39     =0     B=66    C=67    D=68
```

Input 2 shifting value 4

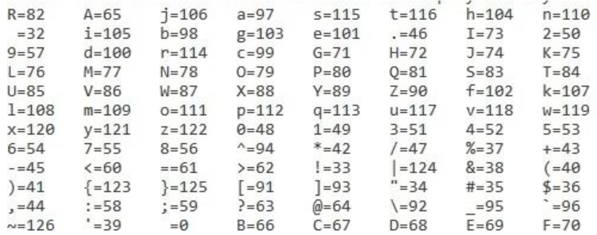
TABLE 18 matrix at sender as well as receiver side for input 2, shifting value 4



```
R=82    A=65    j=106   a=97    s=115   t=116   h=104   n=110
 =32    i=105   b=98    g=103   e=101   .=46    I=73    2=50
9=57    d=100   r=114   c=99    F=70    G=71    H=72    J=74
K=75    L=76    M=77    N=78    O=79    P=80    Q=81    S=83
T=84    U=85    V=86    W=87    X=88    Y=89    Z=90    f=102
k=107   l=108   m=109   o=111   p=112   q=113   u=117   v=118
w=119   x=120   y=121   z=122   0=48    1=49    3=51    4=52
5=53    6=54    7=55    8=56    ^=94    *=42    /=47    %=37
+=43    -=45    <=60    ==61    >=62    !=33    |=124   &=38
(=40    )=41    {=123   }=125   [=91    ]=93    "=34    #=35
$=36    ,=44    :=58    ;=59    ?=63    @=64    \=92    _=95
`=96    ~=126   '=39     =0     B=66    C=67    D=68    E=69
```

Input 2 shifting value 5

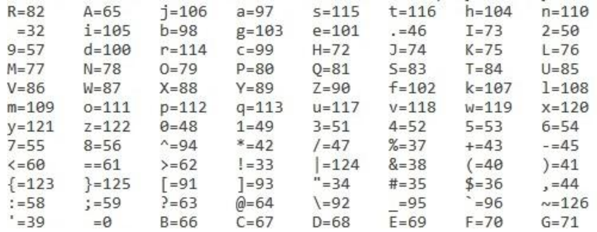
TABLE 19 matrix at sender as well as receiver side for input 2, shifting value 5



```
R=82    A=65    j=106   a=97    s=115   t=116   h=104   n=110
 =32    i=105   b=98    g=103   e=101   .=46    I=73    2=50
9=57    d=100   r=114   c=99    G=71    H=72    J=74    K=75
L=76    M=77    N=78    O=79    P=80    Q=81    S=83    T=84
U=85    V=86    W=87    X=88    Y=89    Z=90    f=102   k=107
l=108   m=109   o=111   p=112   q=113   u=117   v=118   w=119
x=120   y=121   z=122   0=48    1=49    3=51    4=52    5=53
6=54    7=55    8=56    ^=94    *=42    /=47    %=37    +=43
-=45    <=60    ==61    >=62    !=33    |=124   &=38    (=40
)=41    {=123   }=125   [=91    ]=93    "=34    #=35    $=36
,=44    :=58    ;=59    ?=63    @=64    \=92    _=95    `=96
~=126   '=39     =0     B=66    C=67    D=68    E=69    F=70
```

Input 2 shifting value 6

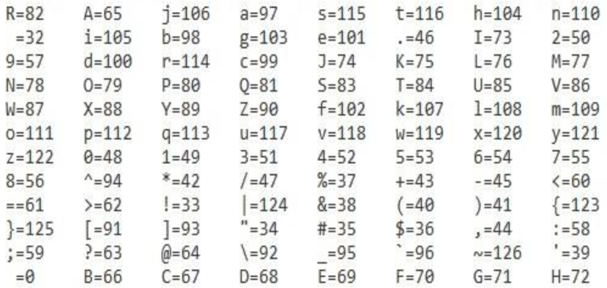
TABLE 20 matrix at sender as well as receiver side for input 2, shifting value 6



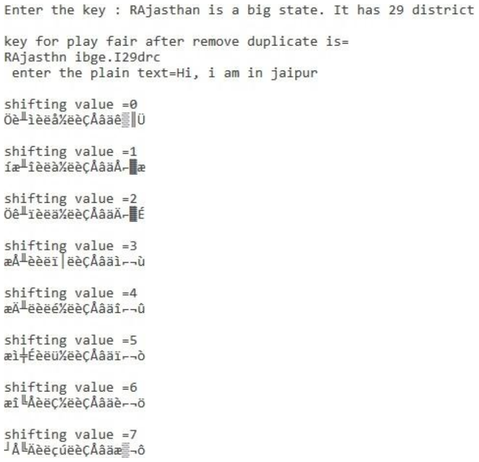
```
R=82    A=65    j=106   a=97    s=115   t=116   h=104   n=110
 =32    i=105   b=98    g=103   e=101   .=46    I=73    2=50
9=57    d=100   r=114   c=99    H=72    J=74    K=75    L=76
M=77    N=78    O=79    P=80    Q=81    S=83    T=84    U=85
V=86    W=87    X=88    Y=89    Z=90    f=102   k=107   l=108
m=109   o=111   p=112   q=113   u=117   v=118   w=119   x=120
y=121   z=122   0=48    1=49    3=51    4=52    5=53    6=54
7=55    8=56    ^=94    *=42    /=47    %=37    +=43    -=45
<=60    ==61    >=62    !=33    |=124   &=38    (=40    )=41
{=123   }=125   [=91    ]=93    "=34    #=35    $=36    ,=44
:=58    ;=59    ?=63    @=64    \=92    _=95    `=96    ~=126
'=39     =0     B=66    C=67    D=68    E=69    F=70    G=71
```

Input 2 shifting value 7

TABLE 21 matrix at sender as well as receiver side for input 2, shifting value 7



```
R=82    A=65    j=106   a=97    s=115   t=116   h=104   n=110
 =32    i=105   b=98    g=103   e=101   .=46    I=73    2=50
9=57    d=100   r=114   c=99    J=74    K=75    L=76    M=77
N=78    O=79    P=80    Q=81    S=83    T=84    U=85    V=86
W=87    X=88    Y=89    Z=90    f=102   k=107   l=108   m=109
o=111   p=112   q=113   u=117   v=118   w=119   x=120   y=121
z=122   0=48    1=49    3=51    4=52    5=53    6=54    7=55
8=56    ^=94    *=42    /=47    %=37    +=43    -=45    <=60
==61    >=62    !=33    |=124   &=38    (=40    )=41    {=123
}=125   [=91    ]=93    "=34    #=35    $=36    ,=44    :=58
;=59    ?=63    @=64    \=92    _=95    `=96    ~=126   '=39
 =0     B=66    C=67    D=68    E=69    F=70    G=71    H=72
```



```
Enter the key : RAjasthan is a big state. It has 29 district

key for play fair after remove duplicate is=
RAjasthn ibge.I29drc
 enter the plain text=Hi, i am in jaipur

shifting value =0
Öè╨ìèëå½ëèÇÅâäê▒║Ü

shifting value =1
íæ╨îèëà½ëèÇÅâäÅ⌐█æ

shifting value =2
Öê╨ïèëä½ëèÇÅâäÄ⌐█É

shifting value =3
æÅ╨èèëï│ëèÇÅâäì⌐¬ù

shifting value =4
æÄ╨ëèëé½ëèÇÅâäî⌐¬û

shifting value =5
æì╪Éèëü½ëèÇÅâäï⌐¬ò

shifting value =6
æî╙ÅèëÇ½ëèÇÅâäè⌐¬ö

shifting value =7
┘Å╙ÄèëçúëèÇÅâäæ▒¬ô
```

Fig. 5 output of input 2 with shifting value 7

V. EXPERIMENTAL RESULT

5.1 Performance Analysis

This chapter delineates the techniques applied in keeping the content secret through character supported, frequency analysis, and required matrix for brute force attack with the help of different examples 1, 2, 3 and 4 with keys and plaintext produce different cipher text with different rotations.

5.1.1 Character Supported

From the above example, we can see that there is no any two results of cipher text 1 and cipher text 2 are same. So we can say that this algorithm is enough safe from the attacks. With the comparison with existence algorithm this proposes algorithm takes the advantage on them in number of character supported. Fig 6 shows this comparison.

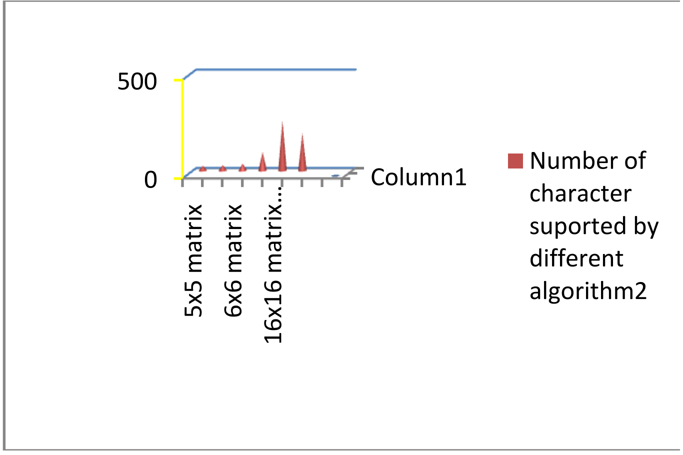


Fig. 6 Graph number of character supported by different algorithm.

This algorithm supports the 192 characters, these are greater than the 5x5 matrix that uses 26 characters, 7x4 matrix that uses 28 characters, 6x6 matrix that uses 36 characters, 12x8 matrix that support 96 characters but only a 16x16 matrix that uses the 256 characters so according to supports the characters that is below than 16x16 matrix but 16x16 matrix that uses many non printable characters those are not on the keyboard. But two 12x8 matrix use two matrix one in front and one in back. The front matrix use the ASCII 7 characters and back matrix use the 96 characters those are of ASCII 8. So this take more advantage on the 16x16 matrix also.

5.1.2 Frequency Analysis

Now, with the comparison with existence algorithm this proposes algorithm takes the advantage on them in frequency analysis attack. Fig 7 shows this comparison.

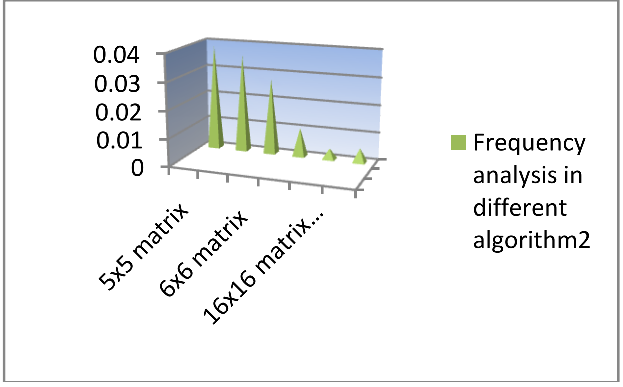


Fig. 7 Graph of frequency analysis attack by different algorithm.

Frequency analysis = 1/ (total no of characters that are supported by the algorithm)

So according to this the frequency analysis of 5x5 matrix=0.038, the frequency analysis of 7x4 matrix=0.035, frequency analysis of 6x6 matrix=0.027, frequency analysis of 12x8 matrix=0.0104,frequency analysis of 16x16 matrix=0.00390 and frequency analysis of two 12x8 matrix=0.00520 for a single rotation if we change the rotation number then we can calculate these different values for 8 rotation.

5.1.3 Brute Force Attack

In the last comparison with existence algorithm this proposes algorithm takes the advantage on them in Brute Force Attack. Fig 8 shows this comparison.

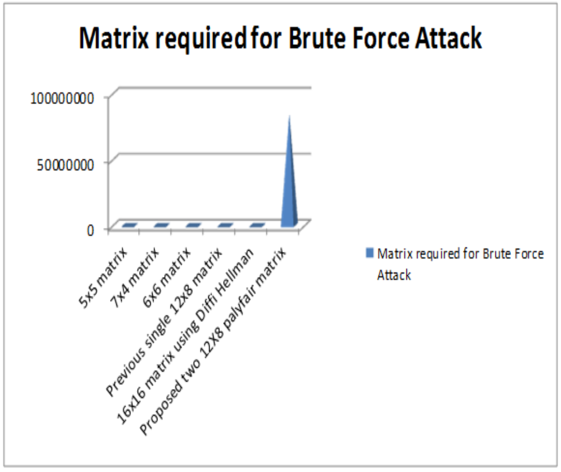
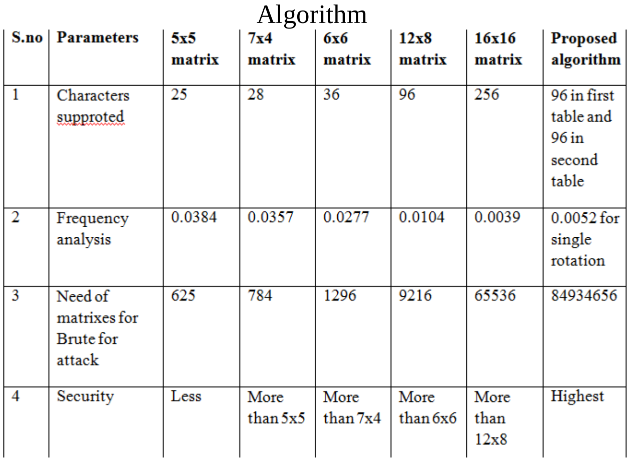


Fig. 8 Graph of required matrix for Brute Force Attack on different algorithm.

An attack on a cipher text message, wherein the attacker attempts to use all possible permutation and combinations, it is called Brute force attack. [4]

The size of key area in this dissertation the modified two 12X8 playfair cipher is 96!X96! (Factorial 96X Factorial 96). As the key area is very large it will be very hard for modified cipher. Thus the modified two 12x8 play fair cipher algorithm is stronger than traditional cipher. There are 5X5 playfair cipher is 25! (Factorial 25) combination of matrix, 7X4 playfair cipher is 28! (Factorial 28) combination of matrix, 6X6 playfair cipher is 36! (Factorial 36) combination of matrix, 12X8 playfair cipher is 96! (Factorial 96) combination of matrix, and 16X16 playfair cipher is 256! (Factorial 256) combination of matrix. So the two 12X8 matrix is more efficient than other these matrix.

Table 22 Comparison Of Proposed Algorithm With Different Algorithm



S.no	Parameters	5x5 matrix	7x4 matrix	6x6 matrix	12x8 matrix	16x16 matrix	Proposed algorithm
1	Characters supproted	25	28	36	96	256	96 in first table and 96 in second table
2	Frequency analysis	0.0384	0.0357	0.0277	0.0104	0.0039	0.0052 for single rotation
3	Need of matrixes for Brute for attack	625	784	1296	9216	65536	84934656
4	Security	Less	More than 5x5	More than 7x4	More than 6x6	More than 12x8	Highest

So by the experiment I create this table according to experiment results this algorithm takes advantage over other given algorithms. I tested this algorithm with my proposed algorithm with these algorithms with these parameters.

IV. CONCLUSION AND FUTURE SCOPE

Conclusion

As far as this, the encryption system take on idea of playfair matrix has been simulated for calculating the Cipher Text. To end with, we have showed qualities as well as demerits of conventional PF algorithm method. To overcome limitation, presented algorithm of two 12X8 playfair cipher algorithm; which can be used more professionally even for the plaintext contain 96 in first matrix and 96 characters in second matrix. Absolute mathematical source is given to show correct result at sender as well as receiver sides. After finishing point of thesis, the potency of this technique has been checked.

Future Scope

In the future when new technology of cryptanalysis will come in to prevent the data form that kind of attack, enhance this work in such type that it will be save our data from that kind of attack on data. There are some suggestions for the future work.

- Work on the method for encryption as well as decryption of the image, audio, video.
- Make easy key distribution, if there is more than on receiver.
- There are 192 letters are used so it is better than 5x5 matrix which take only 26 letters.
- The proposed two 12×8 Playfair cipher is safe from Brute Force Attack, because attacker needs to find in a 96x96x96x96 = 84934656 digraphs.
- Rising key size, also reduce probability to break cipher by Frequency Analysis. The prospect of occurrence of a characters in original (PF) matrix table of size 5×5 was 1/26 = 0.0384, whereas in proposed two 12×8 Playfair matrix probability is 1/192 =0.0052, which is far less when compare as well as it makes frequency analysis a tougher job.
- The 'I' as well as 'J' letters are in two different cells. Blank Space in between two words in PT is consider as one letter. Special characters are used in this algorithm.

REFERENCES

[1] A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam, "A Modified Version of Playfair Cipher Using 7×4 Matrix". International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.

[2] Ravindra babu, Udaya Kumar, Vinaya babu, "An Extension to Traditional Play Fair Cipher Cryptographic Substitution Method", IJCA,0975-8887, Vol. 17, No 5, March 2011.

[3] V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani," A Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering, Vol. 1, No. 5, 1793-8201 December, 2009.

[4] Lt. Ravindra Babu Kallam, Dr. S. Udaya Kumar, Dr. A.Vinaya Babu3 and Dr. M. Thirupathi Reddy, "A Block Cipher Generation Using Color Substitution", © International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 28 2010.

[5] Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa, "A DNA and Amino Acids-Based Implementation of Playfair Cipher" , (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 3, 2010.

[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 Volume 3, Issue 2, February 2014.

[7] Packirisamy Murali and Gandhidoss Senthil kumar, "Modified Version of Playfair Cipher using Linear Feedback Shift Register", International Conference on Information Management and Engineering, , Page 488-490 2009.

[8] Fauzan Saeed and Mustafa Rashid, "Integrating Classical Encryption with Modern Technique", IJCSNS International Journal of Computer 280 Science and Network Security, Vol.10, No.5, , Page 280-285 May 2010.

[9] Sriram Ramanujam and Marimuthu Karuppiaj, "Designing an algorithm with High Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, Vol. 11, No. 1, Page 106-111 January 2011.

[10] 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.

[11] Gaurav Agrawal, Saurabh Singh, Manu Agarwal, "An Enhanced and Secure Playfair Cipher by Introducing the Frequency of Letters in any Plain text", Journal of Current Computer Science and Technology Vol. 1 Issue 3 10-16 2011.

[12] Packirisamy Murali and Gandhidoss Senthilkumar, "Modified Version of Playfair Cipher using Linear Feedback Shift Register", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

[13] Harinandan Tunga, Soumen Mukherjee, "A New Modified Playfair Algorithm Based On Frequency Analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1, January 2012.

[14] Monika Arora, Anish Sandiliya, and Jawad Ahmad Dar," Modified Encryption Technique by Triple Substitution on Playfair Square Cipher Using 6 By 6 Matrix with Five Iteration Steps" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 4, 2015.

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

[16] Sanjay Basu, and Utpal Kumar Ray, "Modified Playfair Cipher using Rectangular Matrix", International Journal of Computer Applications (0975 – 8887) Volume 46– No.9, May 2012.

[17] Sagar Gurnani, Nitish Mhalgi, Samyukta Iyer, and Deepika Dixit," Modified 3-D Playfair Stream Cipher", International Journal of Computer Applications (0975 – 8887) Volume 84 – No 15, December 2013.

[18] Ali Mir Arif Mir Asif, and Shaikh Abdul Hannan," A Review on Classical and Modern Encryption Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 12 Number 4 - Jun 2014.

[19] Ayushi Kansal, Shruti Sneha, and Manish Kumar Patel," Modifying Playfair Cipher by Using DNA and Amino Acids", International Journal of Education and Science Research Review , E-ISSN 2348-6457, Volume-3, Issue-2,. www.ijesrr.org April- 2016.

[20] Nisarga Chand, and Subhajit Bhattacharyya, "A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 1, January 2014.

[21] Arv ind Kumar, Pawan Singh Mehra, Gagan Gupta, and Manika Sharma, "Enhanced Block Playfair Cipher", International Conference on Heterogeneous Networking for Quality , Reliability , Security and Robustness. QShine 201 3: Quality , Reliability , Security and Robustness in Heterogeneous Networks pp 689-695.

[22] Hadab Khalid Obayes, "Suggested Approach to Embedded Playfair Cipher Message in Digital Image", Hadab Khalid Obayes . Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 3, Issue, pp.710-714 5, Sep-Oct 2013.

[23] Muhammad Salam, Nasir Rashid, Shah Khalid, and Muhammad Raees Khan, "A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:5, No:1, 2011.

[24] Robbi Rahim, and Ali Ikhwan, "Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher", © IJSRST | Volume 2 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X Themed Section: Science and Technology 2016.

[25] Bhagyashree Bodkhe, and D. C. Jain, "An Enhanced Play-fair Cipher Cryptographic Substitution Algorithm with 6X6 Matrix", Journal of Current Engineering Research, 2 (3), 1-4 , May-June 2012.

[26] Chandan Kumar, Sandip Dutta, and Soubhik Chakraborty, "A Hybrid Polybius-Playfair Music Cipher", International Journal of Multimedia and Ubiquitous Engineering Vol.10, No.8 (), pp.187-198 http://dx.doi.org/10.14257/ijmue.2015.10.8.19 2015.

[27] Priyanka Goyal, Gaurav Sharma and Shivpratap Singh Kushwah, "Network Security: A Survey Paper on Playfair Cipher and its Variants", International Journal of Urban Design for Ubiquitous Computing Vol. 3, No. 1, pp.1-8 ttp://dx.doi.org/10.21742/ijuduc.2015.3.1.01 2015

[28] Cryptography, Cryptography portal, http://en.wikipedia.org/wiki/Cryptography.

[29] Charles Edge, William Barker & Zack Smith A brief history of cryptography, Foundation of Mac OS X Security, October 23 2007.

[30] William Stallings, "Cryptography and Network Security: Principles and Practice", 4th edition, Prentice Hall, 2006.

[31] Atul Kahate, "Cryptography and Network Security", 2nd edition, McGraw-Hill, 2010.

[32] Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition, Tata McGraw- Hill Publishing Company Limited, New Delhi.s 2007.

[33] David Terr History of cryptography,http://www.davidterr.com/science-articles/cryptography.html.

[34] Michael Calderbank The RSA cryptosystem: History, Algorithm, Primes, August 20, 2007.

[35] A brief history: The origins of public-key cryptography and ECC,

http://www.certicom.com/index.php/a-brief-history.

[36] Diffie, Whitfield; Hellman, Martin . "Multi-user cryptographic techniques". AFIPS Proceedings. 45: 109–112 8 June 1976.