International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 1, Jan-Feb-2021, ISSN (Online): 2395-566X

Enhanced the Security through Asymmetric Based RSA Algorithm

Mahendra Kumar Choudhary, Ravinder Singh
Department of Computer science and Engineering
Govt. Engg. College Ajmer, Rajasthan,India

***Abstract*- In the last some decades we are using the internet in our daily communication. We are sending our non-secret as well as secret data using internet. So there is a chance that our data can be leaked of hacked by someone or some unauthorized person or party. So we can try to secure our data with the help of cryptography.The proposed work is using an old symmetric algorithm that is play fair with some modification and RSA that is asymmetric algorithm also. As we know the symmetric key algorithm is using the same time for encryption and decryption.The problem of key exchange problem I used here RSA algorithm.**

***Keywords*- RSA, encryption and decryption etc.**

I. INTRODUCTION

In era of digital world, security of 'information' has very important to both organization and individuals. When info rmation is sending and receiving by a message or packets of messages by some channel, there should be some method to save from harm that information from hacking. So we need to hide data in such a way that no any un wanted person can't hack message. Hence Cryptography plays an important role in data communication in today's digital world or in internet. Modern cryptography is part of mathematics and technology of computer science. Applications of cryptography include all computer passw ords, ATM cards, and electronic commerce [29].

Present research focuses on trying to being enhance basic Playfair technique(5x5matrix) to 16x16 size of rectangular matrix with help of RSA algorithm (asymmetric key cryptography), attacks possible on information and tackle m with right types of counter measures. and to secure key of playfair technique is need to ensure security of a given message by some kind of mechanism and increase security, confidentiality, integrity and availability.

Aftab Alam et al. in [1] this paper original 5×5 matrix playfair cipher is modified to 7×4 matrix playfair cipher. symbols "*"and "#" are included in matrix which create one-to-one correspondence between plaintext and cipher text. So encryption and decryption process is unambiguous and easy. text is more unreadable when se symbols appear in resulting cipher text. Also this method can be extended to encrypt and decrypt messages of any language by taking a proper size matrix. Ravindra babu et al. In [2] existing playfair algorithm, its merits and demerits. existing play fair algorithm is based on use of a 5X5 matrix of letters constructed using a keyword. producing a Block Cipher using Color Replacement. Binary values of 7-bit ASCII codes are used accompanied by consistent colors of ARGB color model.

1. Motivation:
Reason behind take in cryptography and trying to being improve basic Playfair technique (5x5 matrix) to16x16 sizes of rectangular matrix and to secure key of playfair technique is need to make sure safety of a given message by some kind of mechanism. There is Availability, confide ntiality, Integrity andAuntication four main goals of safety that at all times need to be taken care of and make sure these was my incentive for taking up sis.

2. Problem Statement:
Problem statement of this algorithm is to ensuring these goals of security, confidentiality, integrity and availability and secure key of playfair matrix cipher technique (symm etric key cryptography) and provide secure channel to send key of Playfair cipher to receiver end with help of RSA algorithm (asymmetric key cryptography), attacks possible on info and tackle them with correct types of poker chip measures and look at several variants proposed by different authors and then to come up with a new modi fied cipher which will be stronger than traditional Playfair cipher.

There are some limitations of 5X5 playfair matrix.

- 5×5 PLAY FAIR Matrix considers character set 'I' as well as alphabet 'J' as single character.
- Only 26 character set of upper case in English can take as key devoid of replicas.
- Blank space in the middle of two words in plain text is not considered as a character.
- Special characters can't proceed in this matrix.
- In 5X5 playfair algorithm only capital letters are used.
- An additional symbol'X' is added when PT word contains of odd total of letterings. In DP this 'X' is overlooked. 'X' is a effective character and it makes

© 2021 IJSRET

misperception because 'X' could be a part of PT, so we cannot basically eliminate X in DP.
- 'X' is castoff a filler letter whereas reiterating letter falls in similar pair are detached.

To design an efficient algorithm by such type of method to overcome se limitation of 5X5 playfair matrix and provide secure method to send key.

3. Objectives:

Objectives of work include following main issues:
- Study and analysis popular symmetric key crypto system Playfair matrix.
- Study and analysis asymmetric key cryptosystems like RSA cryptographic method.
- Use properties of both symmetric and asymmetric key to make such type of algorithm which provide better security and previous Playfair algorithm in crypto graphy.
- Implementation of playfair matrix.
- Implementation of RSA with Turbo C++.
- Performance analysis of RSA encryption algorithm and playfair matrix of a text.

4. Symmetric Key Cryptography:

If encryption and decryption individually are complete with similar key then it is called private key or Symmetric cryptography.

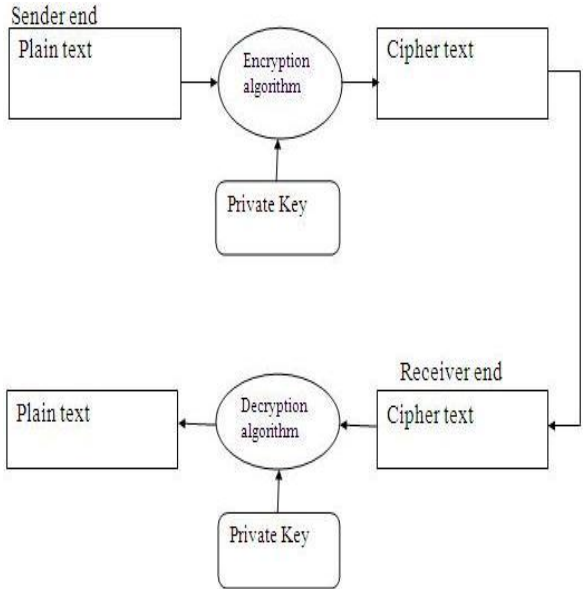

Fig 1. Private Key cryptography.

5. Playfair Algorithm:

In Playfair algorithm, letters are organized in a 5×5 key matrix based on top-secret key.Still there are 26-characters in English but PLAYFAIR algorithm can hold only 25-alphabets.So, any one of i/j is used. To stand-in key matrix of size5X5,letters of keyword (reducing all replica letters) are put in serially, and then left over spaces are filled with rest of characters of in order. [31], [32], [33]

5.1 Key: Passwords

Table 1. Key Matrix.

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

To encrypt a data, it is broken into groups of 2 characters set, for example, "Hello How Are You" is to be treated as "HELLO HOW ARE YOU", and then recorded them out on key table. After that, these 4 rules are functional, in order, to every pair of characters in plaintext:

5.2 Rules for 5x5 Play Fair Matrix:
- Supplement an "X" character afterward first character, if there are both character are alike (or only one character is leftward). Encrypt new pair and carry on this up to end.
- If both alphabets seem on similar row in play fair matrix table, interchange them with letters to their immediate right side character correspondingly.
- If both characters seem on similar column in play fair matrix table, change them with characters immedia tely lower than correspondingly.
- If both characters are not on similar column or row, exchange them with letters on same row correspondi ngly but at or pair of corners of rectangle well-defined by unique pair. Order is significant first letter of encoded pair is one that lies on similar row as first letter of PT pair.

Decryption process, use reverse of last 3 rules, dropping any extra "X"s that do not make any logic in last outcome message when ended). [31], [32], [33]

5.3 RSA Cryptosystem:

RSA cryptosystem was invented by, Ronald Rivest, Adi Shamir and Leonard Adleman in the year 1978. It has grown into a standard public- key cryptography algorithm used to encrypt info, and it was first put out public key system. High level of security of RSA depends on diffic ulty of factoring large numbers which are products of two large primes. [29],[31], [32], [33], [34], [35], [36], [38]

6. Process in RSA Algorithm:

RSA procedure is a public key cryptographic system that is used to help ensure data (information) communication security. It is simply based on two main processes.

In first process, using a public key it translates an input data (plain text) into cipher text this is called encryption process, such that it is very difficult to recover original PT without encryption key in a sort amount of time.

© 2021 IJSRET

In second process, using a secrete key, RSA algorithm then translates encrypted data back to its original form, this is decryption process.

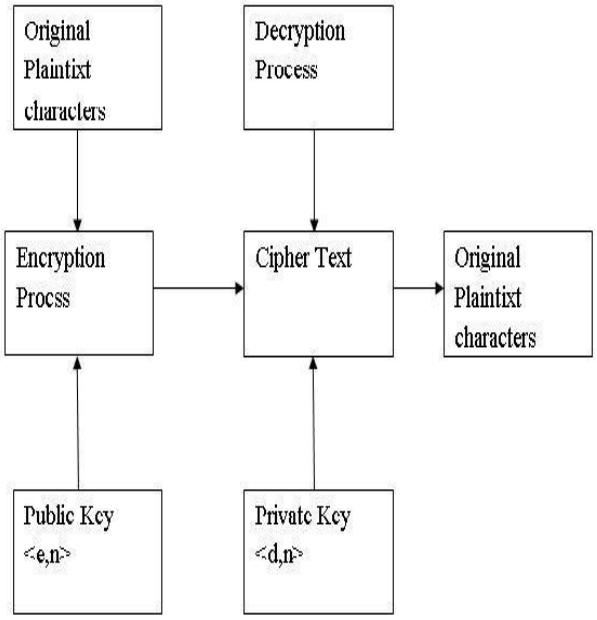

Fig 2. RSA Model

This process is based on one-way function. As name suggests, function is only one-way i.e. there given some input values it is relatively easy to compute result. Thou gh, it is really hard, nearly impossible to determine input values given result . [29], [31], [32], [33], [34], [35], [36], [38]

6.1 RSA Algorithm:

- Select2 prime numbers which are very large, P, Q and Calculate N=P*Q.
- Select public key E, such that it is not a factor of (P-1) and (Q-1).
- Select private key D, such that following equation fulfill this condition; (D*E) mod (P-1)*(Q-1)=1
- For encryption, calculate cipher text (CT) by this equation, CT =PT E mod N
- Send this cipher text CT to receiver.
- For decryption, calculate plain text PT from received cipher text CT as follows:PT=CTD mod N. [29],[31], [32], [33], [34], [35], [36],[38]

II. LITERATURE REVIEW

The main limitation of playfair algorithm is that it supports only 25-characters of English language. Over years quite a lot of efforts have been made to rise limit of its dataset a number of of these are discussed here.

According to**Aftab Alam,Shah Khalid, and Muhammad Salam, et al [1]** has discussed in this paper, a key is use to create 7x4 playfair matrix using characters and symbols, "#"and"*"two special symbols aswell as upper case letters are base for this Playfair method.7x4 playfiar matrix is made by filling key without repeating (duplicate) letters. There is I and J are in different cells.

According to **Ravindra babu, Udaya Kumar, Vinaya babu, et al [2]** has discussed in this paper proposed a 6×6 size of matrix use of a larger key. re is total 36 character, where all 10-decimal numbers (0-9) and 26-alphabets of English language in upper case. But its requirement more letters support satisfactory to be able to work over a large choice of text file. They also projected use of exchange ciphers to reserve rate of recurrence distribution of single letters to finish diagram and higher order distribution.

According to **V.Umakanta Sastry,N.Ravi Shankar, and S.Durga Bhavani, et al [3]** has discussed in this paper, it generalized and improved Playfair cipher into a block cipher. In this paper,he focuses on use of ASCII values in playfair. use of 7-bit ASCII values rises character increasing to 128 characters. Work uses a matrix 8×8 size in which key K consists of 64 distinct numbers, denoted by Ki, where i= 1-64 and each number lies between ASCII limit of 0-127. remaining locations of matrix are filled by remaining numbers Ri, where i=1-64. Initially, and every plaintext P is read 2n characters at a time, andusing ASCII code,P is represent in form of a table given by-P=Pij,i = 1-n and j = 1-2. This extended playfair key matrix is used to encrypt / decrypt plaintext matrix row wise, using same rules of Playfair ciphertext and the cipher text P1 is gotten. In adding to this extended matrix, idea of linking is presented, which

According **to Lt. Ravindra Babu Kallam, Dr. S. Udaya Kumar, Dr.A.Vinaya Babu3 and Dr.M. Thirupathi Re ddy,et al [4]** has discussed in this paper, it reports problem in a totally different way by producing a Block Cipher using Color Substitution.Binary values of 7-bitASCII cod es are used accompanied by consistent colors of ARGB color model. Projected "Play Color Cipher" replac ements each character of plaintext with a color block from an 18 decillions of colors. Color limit of ARGB color model is N=256×256×256×256=4294967296.

To use maximum color limit some futher candidness are made before selec ting next color of cipher constructed on key. From given key,starting addressK1 and increment valueK2 are chosen in such a way that (K1+(C×K2))<N , where C= Numbers of characters in plain text. K1 and K2 are exchanged using RSA. se keys can be of variable lengths and hence more secure. This projected effort uses ARGB color model with 256 color shades for each one, thus limiting extreme color address to 294967296.But still,this projected proce dure with 8-but ASCII support focus on encryption of a character set to equivalent color, limiting scope to English only. Though some small alterations in planned process can also make it compatible to multilingual characters.

© 2021 IJSRET

International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 1, Jan-Feb-2021, ISSN (Online): 2395-566X

III. EXPERIMENT ANALYSIS

The proposed work is dividing in two phases:

1. first phase for Matrix construction uses all rules of traditional Play fair matrix with se changes:

- Two I and J letters in upper case and lower case are considered as two different letters (Iand J are different and i and j are different).
- It allows more than 26 (up to 256 characters without any duplicate) characters as key and it supports these are shown in these tables.
- Key length is very large in comparison with previous algorithms, here, so it is very difficult to find plain text from CT without knowing a key.
- This algorithm can't separate a repeating PT letters with a filter letter.

Table 2. List of Upper Case Letters.

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

Table 3. List of Lower Case Letter.

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

Table 4. List of Numeric Values.

0	1	2	3	4
5	6	7	8	9

Table 5. List of Operators.

^	*	/	%	+	-
<	=	>	!	|	&

Table 6. List Of Brackets.

(	)	{
}	[	]

Table 7. List of Special Characters.

Space	Null	"	#	$	'	,	`
:	;	@	_	.	?	~	\

2. Example , with P=17, Q=19 and E=7

```
 Enter array size : 16
Enter key Accept Numbers and special character's : PlayFairExample

Char list of key for play fair is=
PlayFirExmpe

Enter the plain text for 16x16 playfair matrix in char form=i am in rtu

The ciphertext due to 16x16 playfair matrix at the sender end is=eype!_iu)r
Enter prime No.s p,q :17 19
Select e value:7

The key of 16x16 playfair after droup duplicate is=PlayFirExmpe
Ciphertext due to RSA algorithm is=▒0mó,ΣE ·≤≈

This is at the receiver end

The key after decryption by the RSA algorithm is
 PlayFirExmpe
The cipher text due to 16x16 playfairmatrix at the receiver end is=eype!_iu)r
The plaintext at receiver end is due to the 16x16 playfairmatrix=i am in rtu
the matrix at sender and receiver end is
 10  80 108  97 121  70 105 114  69 120 109 112 101   0   1   2
  3   4   5   6   7   8   9  11  12  13  14  15  16  17  18  19
 20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35
 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  64  65  66  67
 68  71  72  73  74  75  76  77  78  79  81  82  83  84  85  86
 87  88  89  90  91  92  93  94  95  96  98  99 100 102 103 104
106 107 110 111 113 115 116 117 118 119 122 123 124 125 126 127
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
208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223
224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239
240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255
```

Fig 3. Output Snapshot of Example , with P=17, Q=19 and E=7.

3. Example , with P=17, Q=19 and E=7

```
 Enter array size : 16
Enter key Accept Numbers and special character's : PLAYFAIREXAMPLE

Char list of key for play fair is=
PLAYFIREXM

Enter the plain text for 16x16 playfair matrix in char form=I AM RAM

The ciphertext due to 16x16 playfair matrix at the sender end is=M└Y ╪MY
Enter prime No.s p,q :17 19
Select e value:7

The key of 16x16 playfair after droup duplicate is=PLAYFIREXM
Ciphertext due to RSA algorithm is=▒08└ópÄEñ¼

This is at the receiver end

The key after decryption by the RSA algorithm is
 PLAYFIREXM
The cipher text due to 16x16 playfairmatrix at the receiver end is=M└Y ╪MY
The plaintext at receiver end is due to the 16x16 playfairmatrix=I AM RAM
the matrix at sender and receiver end is
 10  80  76  65  89  70  73  82  69  88  77   0   1   2   3   4
  5   6   7   8   9  11  12  13  14  15  16  17  18  19  20  21
 22  23  24  25  26  27  28  29  30  31  32  33  34  35  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  64  66  67  68  71  72
 74  75  78  79  81  83  84  85  86  87  90  91  92  93  94  95
 96  97  98  99 100 101 102 103 104 105 106 107 108 109 110 111
112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127
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
208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223
224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239
240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255
```

Fig 4. Output Snapshot of Example, with P=17, Q=19 and E=7.

IV. EXPERIMENTAL RESULT ANALYSIS

1. Performance Analysis:

This chapter delineates techniques applied in keeping content secret through character supported, frequency anal ysis, and required matrix for brute force attack.

1.1 Character Supported:

From the discussed examples, we can see that there is no any two results of cipher text1 and cipher text 2 are same. So we can say that this algorithm is enough safe from attacks. With comparison with existence algorithm this

© 2021 IJSRET

proposes algorithm takes advantage on m in number of character supported. Fig 6.1 shows this comparison.
Para meters5x5 matrix 7x4 matrix 6x6 matrix12x8 matrix 16x16 matrix Diffi Hellman Proposed algorithm.

Table 8. Comparison of proposed algorithm with different algorithm.

Parameters	5x5 matrix	7x4 matrix	6x6 matrix	12x8 matrix	16x16 matrix	Diffi Hellman Proposed algorithm
Character supported	26	28	36	96	256	256
Frequency analysis	0.0384	0.0357	0.0277	0.0104	0.0039	0.0039
Brute Force Attack	625	784	1296	9216	65536	65536
Security	Less security	More than 5x5	More than 7x4	More than 6x6	More than 12x8	Highest security
Man in middle attack	possible	possible	Possible	Not possible due to RSA	possible	Not possible due to RSA algorithm

V. CONCLUSION AND FUTURE WORK

1. Conclusion:
In this work the concept of playfair matrix 5x5 and make some changes in that, extension in its size for calculating cipher text. We have point out demerits of traditional PLAYFAIR algorithm. In order to overcome demerits,we have proposed an extension in traditional PLAY FAIR cipher algorithm; which can be used more efficiently even for Plain Text containing ASCII 8 values.
In this algorithmI used the public keyencryption algorithm RSA to secure the key of symmetric algorithm.

2. Future Work:

- In future we have to concentrate on these things.
- We can use image,audio,videoas object for encryption and decrytion .
- We can use an algorithm for solving the key distrib ution problem more efficiently.
- We can use some idea to decrease decryption time of RSA algorithm.

REFERENCES

[1] Charles Edge, William Barker & Zack Smith A brief history of cryptography, Foundation of MacOSX Sec urity, October 23 2007.
[2] WilliamStallings,"CryptographyandNetwork Security: Principlesand Practice",4thedition,PrenticeHall, 2006.
[3] Atul Kahate,"Cryptography and Network Security", 2nd edition, McGraw-Hill, 2010.
[4] BehrouzA.Forouzan,CryptographyandNetwork Secur ity.Special Indian Edition 2007,Tata McGraw-Hill Publishing Company Limited, New Delhi.s
[5] David Terr History of cryptography, http://ww w.davi dterr.com/sciencearticles/cryptography.html
[6] Michael Calderbank The RSA cryptosystem: History, Algorithm, Primes, August 20, 2007.
[7] Abrief history:The origins of public-key cryptography and ECC,http://www.certicom.com/index.php/a-brief-history.
[8] Diffie,Whitfield;Hellman,Martin(8June1976). "Multi-user cryptographic techniques".AFIPS Proceedings. 45:109–112.
[9] Rivest, Ronald L.;Shamir, A.; Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. Association for Computing Machinery. 21 (2):120–126.doi:10.1145/359340.359342. Archived November 16,2001,at the Wayback Machine. Previously released as an MIT "Technical Memo" in April 1977, and published in Martin Gardner's Scientific American Mathematical recreations column.
[10] Koblitz N. (1987). "Elliptic curve cryptosystems". Ma thematics of Computation. 48(177):203–209. doi:10.2 307/2007884. JSTOR 2007884. 52
[11] Miller, V.(1985)."Use of elliptic curves in cryptograp hy".CRYPTO.Lecture Notes in Computer Science. 85:417–426. doi:10.1007/3-540-39799-X_31. ISBN 978-3-540-16463-0.

© 2021 IJSRET