National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040; Impact Factor: RJIF 5.22
Received: 07-01-2019; Accepted: 11-02-2019
www.nationaljournals.com
Volume 4; Issue 2; April 2019; Page No. 09-14

Secure key exchange using RSA in extended Playfair cipher technique

Pawan Tiwari[1], Dr. Rohit Kumar Singhal[2]
[1] M.Tech Research Scholar, I.E.T Alwar, Rajasthan, India
[3] Professor and H.O.D, Department of CSE, I.E.T, Alwar, Rajasthan, India

Abstract
In time of internet when we are sending and receiving information over network in presence of third-party n it is very necessary to protect our data from assaulter's, in series to protect data we are using cryptography algorithms. Day to day new cryptography algorithms are found and re is modification in previous algorithm also. According to key encryption algorithm are of two types. First is symmetric key algorithm and second are asymmetric key algorithms.
The proposed work is an example of symmetric key with asymmetric key together. In work I done improvement in play fair matrix technique. I used all rules of basic play fair algorithm with some changes (changes in matrix).
The objective of thesis is to secure key of play fair procedure of new extended size16x16 using RSA algorithm. It is a two-stage algorithm. In first stage at sender end, I used rules of matrix 5x5 for making matrix and making cipher text. It makes use of alphabets both lower case and upper-case characters, number and special characters for constructing contents of matrix and after this we use shifting value to rotate matrix.
In second stage, RSA public key encryption technique is used for sending key of play fair ciphers securely and by this key we make play fair matrix at receiver end.

Keywords: internet, RSA, Playfair cipher technique

Introduction

In era of digital world, security of 'information' has very important to both organization and individuals. When information 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 unwanted 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 passwords, ATM cards, and electronic commerce. present research focuses on trying to being enhance basic Playfair technique (5x5 matrix) 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 5 X 5 matrix of letters constructed using a keyword. This algorithm can only allow text that contains alphabets only. For this in this paper an enhancement to existing algorithm, that a 6 X 6 matrix can be constructed. re is total 36 character, where all 10-decimal numbers (0-9) and 26-alphabets of English language in upper case. V. Umakanta Sastry *et al* in [3] this paper, it generalized and modified Playfair cipher into a block cipher. There use of ASCII values in playfair. He uses of 7-bit ASCII values rises character support to 128 characters. In this paper uses a key matrix of size 8×8 in which key K consists of 64 distinct numbers, denoted by K_i, where i = 1-64 and each number lies between ASCII limit of 0-127. It was found to be breakable with some amount of computation, as structure of plaintext is not that much dissipated in corresponding cipher text. Lt. Ravindra Babu Kallam *et al*. In [4] this paper, its speeches problem in a absolutely dissimilar way by producing a Block Cipher using Color Replacement. Binary values of 7-bit ASCII codes are used accompanied by consistent colors of ARGB color model. In this paper "Play Color Cipher" replacements each letter of plaintext with the shade block from 18 decillions of colors. Color limit of ARGB color model is N = 256×256×256×256 = 4294967296. With this we have following problems: It is a time taken process for both encryption as well as decryption, It is challenging for crypt analyzer to explore problem. Also suffers with problems in current system. Mohamed Hashem *et al*. in [5] this paper, it modifies Play fair cipher considerably by presenting DNA-based amino acid structures to core of ciphering process. A binary form of info, such as plaintext, or images are changed into orders of DNA nucleotides. Then, these nucleotides go through a Play fair encryption procedure based on amino-acids structure. Principal idea in arrears this encryption technique is to impose or conventional cryptographic algorithms which showed to be broken, and also to open door for put on DNA and Amino Acids

concepts to more conservative cryptographic algorithms to enhance their security structures. But they were incapable to obviously handlebar problem of doubt as achieved by our algorithm. Subhajit Bhattacharyya *et al.* [6] in this paper which contains a rectangular matrix taking 10 columns and 9 rows and 6 repetition steps for encryption along with decryption purpose. This 10 x 9 rectangular matrix take in all alphanumeric characters and some special characters. In this modified play fair cipher 6 dissimilar keys and six repetition steps used to make encrypted data stronger than 5x5 playfair cipher. Packirisamy Murali *et al.* [7] in this paper have tried to implement improved Play fair cipher using Linear Feedback Shift Register. Classical Play fair cipher is not safe because it have only 676 structures. With mapping of random orders to 5x5 play fair cipher, escalations security of communication by many folds. It is comparatively easy to break because it still leaves much of structure and a few hundreds of letters of cipher text are sufficient. Fauzan Saeed, Sriram Ramanujam, Shiv Shakti Srivastava *et al.* In [9-10] concentrated on well-known 5x5 aim was to induce some strong point to 5x5 play fair encryptions for that purpose blended classical encryption with structure of current methods like DES and SDES. Advantages of classical or ancient cryptography as well as clubbed it with significant features of modern cryptographic algorithms. Permissible to understand idea of Avalanche Effect and comparison purposes, taken some algorithms like Playfair Cipher, Vigenere Cipher, Caesar Cipher, Data Encryption Standard (DES) and Blowfish.

Playfair Algorithm

In the Play fair cipher, the alphabets are arranged in a 5×5 key matrix based on secret key. Though there are 26-alphabets in English language but PF cipher can handle only 25-alphabets. So, any one of i/j is used. To fill-in the key matrix table of size 5X5, the letters of the keyword (dropping all duplicate letters) are put in serially, and then remaining spaces are filled with rest of the letters of the alphabet in order.

Key: PASSWORDSRAS

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 message, the message is broke into groups of 2 letters such that, for example, "Hello How Are You" is to be treated as "HE LL OH OW AR EY OU", and then mapped them out on the key table. Then these 4 rules are applied, in order, to each pair of letters in the plaintext:

Rules for making the CT using PF Matrix

1. Add an "X" letter after the first letter, if both letters are the same (or only one letter is left). Encrypt the new pair and continue doing this. Some variants of play fair use "Q" instead of "X", but any uncommon monograph will do.
2. If both alphabets appear on the same row in play fair matrix table, replace them with the letters to their immediate right side respectively (wrapping around to the left side of the row if a letter in the original plain text pair was on the right side of the row).
3. If both the alphabets appear on the same column in play fair matrix table, replace them with the letters immediately below side respectively (wrapping around to the top side of the column if a letter in the original plain text pair was on the bottom side of the column).
4. If both alphabets are not on the same column or row, replace them with the letters on same row respectively but at other pair of corners of the rectangle defined by the original pair. The order is important first letter of encrypted pair is one that lies on the same row as the first letter of the PT pair.

The decryption process (DP), use the INVERSE (opposite) of the last 3 (2, 3, 4) rules, and the first as-is (dropping any extra "X"s (or "Q"s) that do not make any sense in the final result message when finished).

Motivation

Reason behind take in cryptography and trying to being improve basic Playfair technique (5x5 matrix) to 16x16 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, confidentiality, Integrity and Authentication 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.

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 (symmetric 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 modified cipher which will be stronger than traditional Playfair cipher.

There are some limitations of 5X5 playfair matrix.

1. 5×5 PLAY FAIR Matrix considers character set ‘I’ as well as alphabet ‘J’ as single character.
2. Only 26 character set of upper case in English can take as key devoid of replicas.
3. Blank space in the middle of two words in plain text is not considered as a character.
4. Special characters can’t proceed in this matrix.
5. In 5X5 playfair algorithm only capital letters are used.
6. 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 misperception because ‘X’ could be a part of PT, so we cannot basically eliminate X in DP.
7. ‘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.

Objectives of work

Objectives of work include following main issues:

1. Study and analysis popular symmetric key cryptosystem Play fair matrix.
2. Study and analysis asymmetric key cryptosystems like RSA cryptographic method.
3. Use properties of both symmetric and asymmetric key to make such type of algorithm which provide better security and previous Play fair algorithm in cryptography.
4. Implementation of play fair matrix.
5. Implementation of RSA with Turbo C++.
6. Performance analysis of RSA encryption algorithm and playfair matrix of a text.

Symmetric key cryptography

If encryption and decryption individually are complete with similar key then it is called private key or Symmetric cryptography. Symmetric-key cryptography is where individually senders and receivers sharing similar key. These keys are castoff for equally encryption and decryption. Examples are AES and DES.

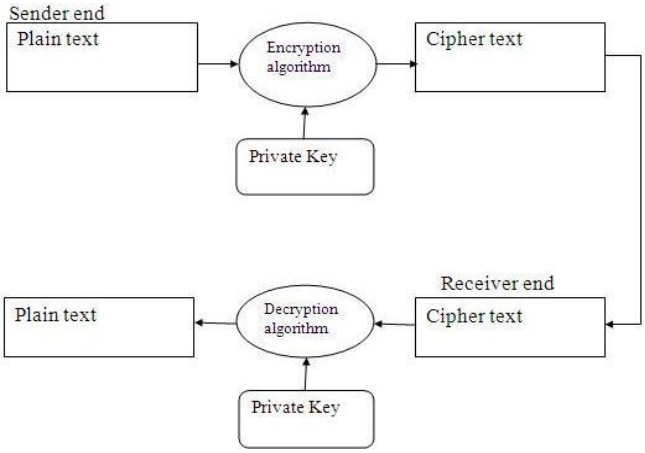


Fig 1: Private Key cryptography

Play fair Algorithm

In Play fair algorithm, letters are organized in a 5×5 key matrix based on top-secret key. Still there are 26-characters in English but PLAY FAIR algorithm can hold only 25-alphabets. So, any one of i/j is used. To stand-in key matrix of size 5X5, 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.

Key: PASSWORDS

Table 2: 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 "HE LL OH OW AR EY OU", and then recorded them out on key table. After that, these 4 rules are functional, in order, to every pair of characters in plaintext:

Rules for 5x5 Play Fair Matrix

1. 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.
2. If both alphabets seem on similar row in play fair matrix table, interchange them with letters to their immediate right side character correspondingly.
3. If both characters seem on similar column in play fair matrix table, change them with characters immediately lower than correspondingly.
4. If both characters are not on similar column or row, exchange them with letters on same row correspondingly 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.

Asymmetric key cryptography

In this technique public key is known to everybody, those are in communication. So supposing there are two parties Party 1st and Party 2nd. If 2nd (sender) party wants to send a data or info to 1st party (receiver), he encrypts info with 1st party public key and 1st party decrypts it with its private key, which is well-known just to him only. It takes additional time but added security features. Examples are RSA algorithm, Diffe Hellman and ECC.

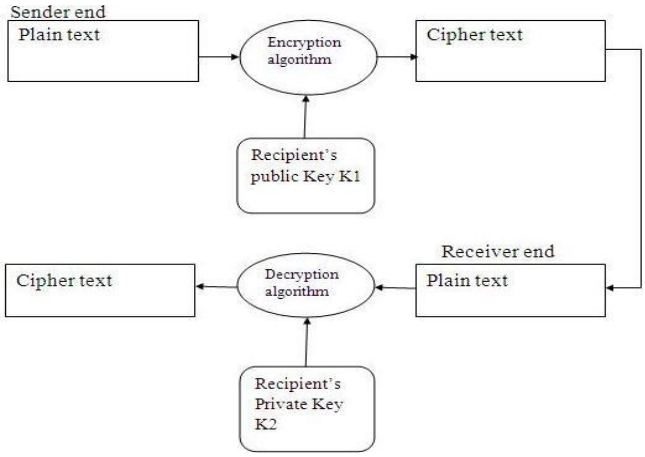


Fig 2: Public key cryptography

Implementation

Tools Used

In this dissertation, Turbo C/ C++ is use for simulate the algorithm.

Execution Process

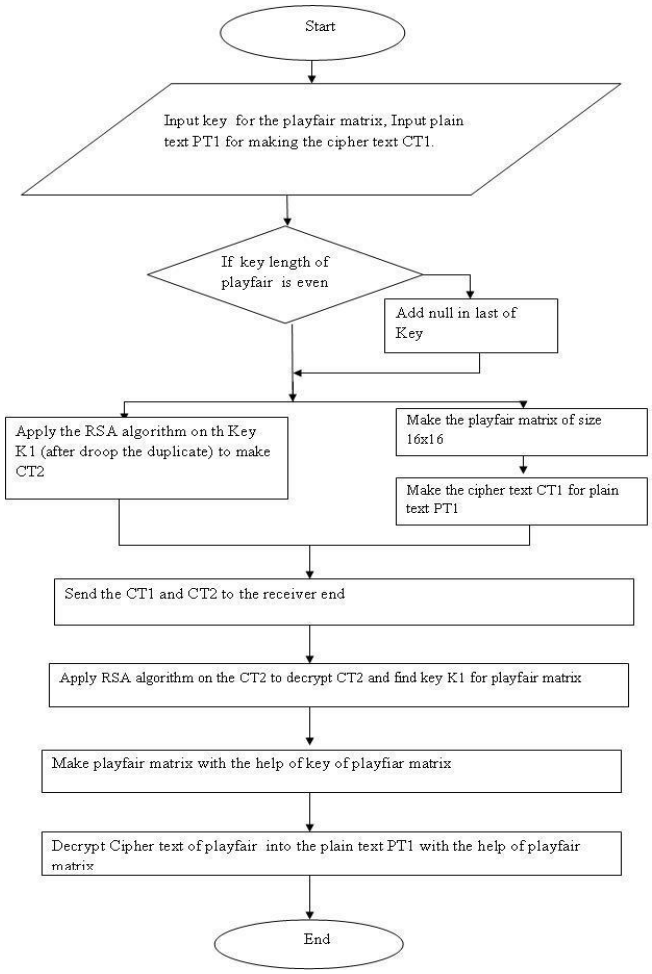


Fig 3: shows the diagram of the complete methodology followed in this dissertation

The proposed work consists of the following these steps:

At the Sender ends.

Step 1: construct a modified table of Playfair cipher technique of size 16X16, which contain all the alphabets form A to Z upper case and a to z in lower case, all the special characters which are on the keyboard and all numeric values (from 0 to 9). The PF encryption technique is divide into two phases:

1. First phase is creation and population of Matrix (by using the key and rotate the matrix with rotation factor after insert the key without duplicate).
2. The second phase is encryption process of the plain text message with the help of the Matrix. Make the Cipher text (CT1) of the plain text.

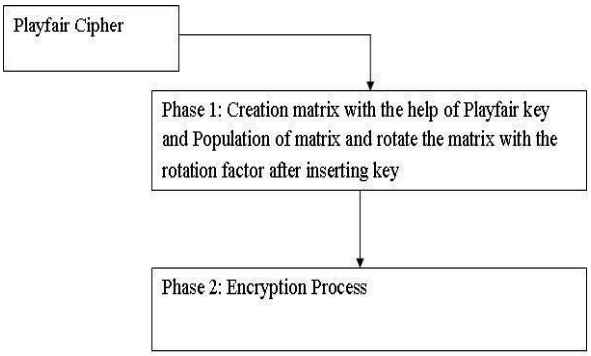


Fig 4: Play fair cipher encryption steps [32]

Step 2: use the key of Playfair technique as a Plain Text in RSA algorithm to make the Cipher text (CT2) of the key and send to the receiver.

At the Receiver ends.

Step 3: decrypt the Cipher Text (CT2) into Plain Text (Playfair matrix key).

Step 4: construct a modified table of Playfair cipher technique of size 16X16, which contain all
the alphabets form A to Z upper case and a to z in lower case, all the special characters which are on the keyboard and all numeric values (from 0 to 9). The PF decryption technique is divided into two phases:

1. First phase is creation and population of Matrix (by using the key).
2. The second phase is decryption process of the cipher text (CT1) message with the help of the matrix and makes the plain text.

Experimental Result

The proposed work is dividing in two phases: 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 (I and 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.

Table 3: 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 4: 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 6: List of numeric values

0	1	2	3	4
5	6	7	8	9

Table 7: List of operators

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

Table 8: List of Special characters

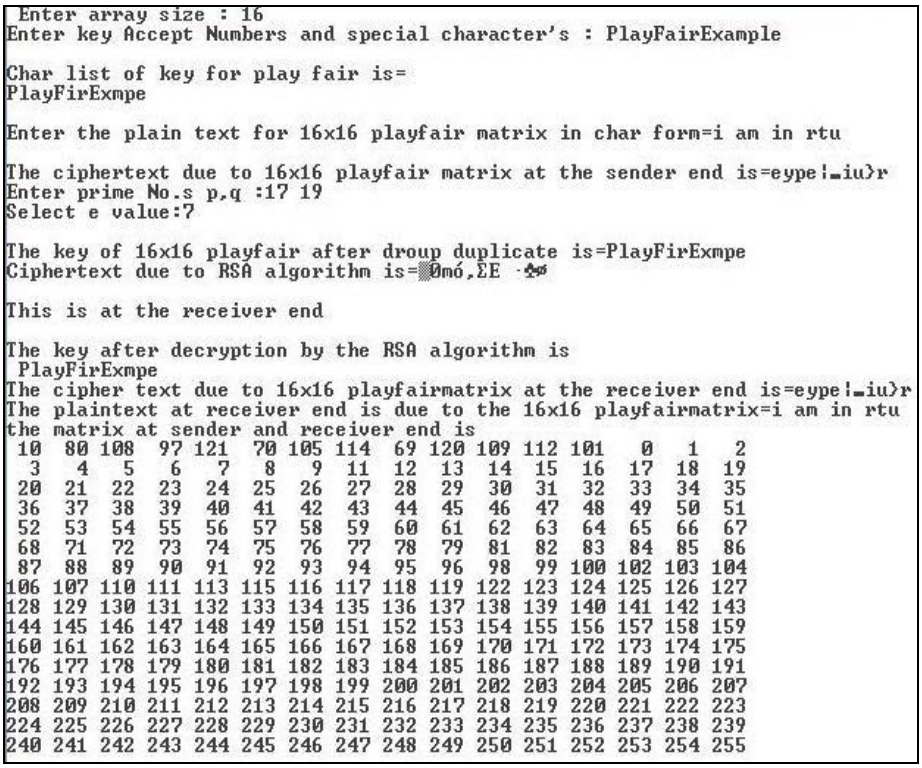
Space	Null	"	#	$	'	,	`
:	;	@	_	.	?	~	\

1. 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.
2. This algorithm can't separate a repeating PT letters with a filter letter.

Output Snapshot of Example 1with 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=ÆØmf,Σø

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
 10 112 108  97 121 102 105 114 101 120 109   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  69
 70  71  72  73  74  75  76  77  78  79  80  81  82  83  84  85
 86  87  88  89  90  91  92  93  94  95  96  98  99 100 103 104
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 5: Output Snapshot of Example 1, rotation 0 with P=17, Q=19 and E=7 Example 2, 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=▒Ømó,ΣE ·♣ø

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 6: Output Snapshot of Example 2, with P=17, Q=19 and E=7

Conclusions and Future work

Conclusions

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 PLAY FAIR algorithm. In order to overcome demerits, I 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 algorithm used the public key encryption algorithm RSA to secure the key of symmetric algorithm.

Future work

In future we have to concentrate on these things.

1. We can use image, audio, video as object for encryption and decrytion.
2. We can use an algorithm for solving the key distribution problem more efficiently.
3. We can use some idea to decrease decryption time of RSA algorithm.

References

1. Aftab Alam, B Shah Khalid, Muhammad Salam C. "A Modified Version of Playfair Cipher Using 7×4 Matrix". International Journal of Computer Theory and Engineering, 2013, 5(4).
2. Ravindra babu, Udaya Kumar, Vinaya babu. "An Extension to Traditional Play Fair Cipher Cryptographic Substitution Method". 2011; 17(5):IJCA,0975-8887.
3. Umakanta Sastry V, Ravi Shankar N, Durga Bhavani S. A Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering. 2009; 1(5):1793-8201
4. Lt. Ravindra Babu Kallam, Udaya Kumar S, Vinaya Babu A, Thirupathi Reddy M. A Block Cipher Generation Using Color Substitution, ©2010 International Journal of Computer Applications, 1(28), 0975-8887.
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, 2010, 8(3).
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, 2014, 3(2).
7. Packirisamy Murali, Gandhidoss Senthil kumar. "Modified Version of Playfair Cipher using Linear Feedback Shift Register", 2009 International Conference on Information Management and Engineering, 2009, 488-490.
8. Fauzan Saeed, Mustafa Rashid. "Integrating Classical Encryption with Modern Technique", IJCSNS International Journal of Computer 280 Science and Network Security. 2010; 10(5):280-285.
9. Sriram Ramanujam, Marimuthu Karuppiaj. "Designing an algorithm with High Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security. 2011; 11(1):106-111.
10. Shiv Shakti Srivastava, Nitin Gupta. "A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications. 2011; 20(6):0975-8887.
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. 2011; 1(3):10-16.