Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Modern Play Color Cipher Involving Dynamic Permuted key with Iterative and Modular Arithmetic Functions

Prof. Ravindra Babu Kallam*
Department of Computer Science Engineering
Vivekananda Institute of Technology & Science SET
Kareemnagar, A.P, India
rb_kallam@yahoo.com

Dr. S.Udaya Kumar
Principal
MVSR Engineering College,
Hyderabad, India
uksusarla@rediffmail.com

Dr.A.Vinaya Babu
Director, Admissions
Jawaharlal Nehru Technological University, Hyderabad
A.P, India
avb1222@gmail.com

Abstract: In this paper, we have developed a block cipher involving permutation, color substitution with iterative and modular arithmetic functions. For this development we have used a large symmetric key of 128bits. By using sub key generation algorithm the 128bit key in turn divided into four parts as K_1, K_2, K_3 and K_4. Among these K_1, K_2 were used as a parameters to the function, and the function is selected based on K_3 out available 10 functions. The output of the function will be treated as a starting address and increment value for selecting the color in our previously invented " Play color cipher algorithm". K_4 is used as a key for transposition. The process of encryption and decryption were explained with example. From the cryptanalysis carried out in this paper, we conclude that the cipher cannot be broken by any cryptanalysis attack.

Keywords: Symmetric block cipher, Cryptanalysis, Play color cipher (PCC), substitution, permutation, RSA algorithm

I. INTRODUCTION

Cryptography is a principle enabler of many secure computing systems. Using cryptographic techniques such as encryption and secure hashing, we can gratify several crucial security requirements for networks, computers, data and information against a diverse set of threats[1-4].

A number of block ciphers [5-10][12-15] have been developed in the recent past, which can be observed in the literature [11]. Feistal [8][9] has used the concept of Hill cipher and developed the Feistal cipher. However subsequently he found that his approach is vulnerable for cryptanalytic attacks.

In the current exploration, Udaya et al, have invented a modern symmetric block cipher [16-18] by using a Color substitution and permutations with 128 bit key [17]. Form their presentation it is observed that the plain text including alphanumeric characters, symbols, diagrams and image are first converted into rich text format, then to inculcate confusion the cipher was transposed twice by using 36 bit key and at the end each character was substituted with a color from the available 18 decillions of colors in the computer world[11]. Finally they have proven that the cipher they have developed is cryptographically stronger.

Since the security provided by cryptographic processing depends on the secrecy and integrity of the cryptographic keys, in this paper we have devoted our attention towards keys, involved iterative and modular arithmetic function to generate sub keys and hence to develop more stronger cipher.

II. KEY LAYOUT AND IT'S ORGANIZATION

The key layout and its organization among the participants in communication is as follows:

In this we have used a 128 bit key. By using sub key generation algorithm it is divided in to 4 sub keys for encryption and decryption purpose. Among these from the LHS the first two keys K_1 (60 bits), K_2 (28bits) were used as a parameters to the function selected by using K_3 (4bits) out available 10 functions. The output of the function will give two values and they were the starting address and the increment value for color substitution and the last 36 bits in the main key is K4 used for the transposition of the cipher in the rich text format. The range of the keys and its detailed explanation is given below.

- Choose a key 'K', should be 32 decimal numbers between '0 to 9' (having 4 sub keys), from LHS the first 15 digits in the Key can be between 0000 0000 0000 001 (Min) to 9999 9999 9999 999 (Max). Next 7 digits in the key can be 0000 001 (Min) to 9999 999 (Max), these two are the parameters passed to the iterative and modular arithmetic function selected by K_3 out of the available 10 functions. The value of K_3 should be between 0 to 9. The next 9 digits in the main key will be the key K_4 for transposition. The key should be the numbers between '1 to 9', and the number once used should not be repeated.

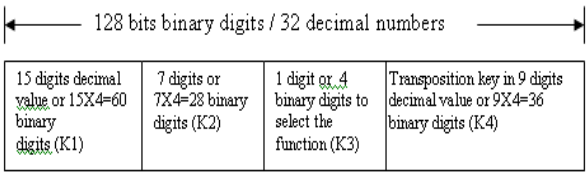


Figure 1. Key layout for 128 binary bits

- Use RSA [19] Public key encryption algorithm for key distribution as shown in Figure 2:

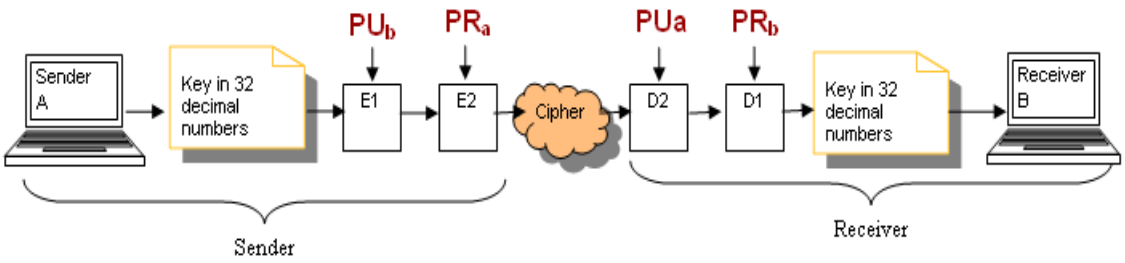


Figure 2. Secure transmission of key using RSA algorithm

- Encrypt K using receivers (User B) Public key (PUB) for confidentiality ---------- 2.1
- Encrypt the result of 2.1 using senders (User A) Private key (PRA) for Authentication.-------- 2.2
- Send the result of 2.2 to the receiver----------2.3
- Decrypt 2.3 by using PUA ---------- 2.4
- Decrypt 2.4 by using PRB ---------- 2.5

Hence with both validation and secrecy we have dispersed the keys between User A and User B.

III. DEVELOPMENT OF THE CIPHER

In this we have developed the cipher in four phases, in first phase: the plain text in alphanumeric characters, diagrams, symbols and images were converted in to Rich text format; named it as C1, in second phase the C1 is transposed in to C2 by using the key K3, in third phase the C2 is again permuted in to C3 by using K3 and in fourth phase the color substitution is applied on C3 to produce C4, it is the final cipher and can be treated as very strong. The process of input and the output of each phase were explained in brief in beneath:

A. Brief on RTF and Converting plain text in to rich text format (RTF) :

The Rich Text Format (RTF) is a method of encoding formatted text and graphics for use within applications and for transfer between applications. Users often depend on special translation software to move word-processing documents between various applications developed by different companies. RTF serves as both a standard of data transfer between word processing software, document formatting, and a means of migrating content from one operating system to another. RTF allows documents to migrate forward and backward in time. As with the Textbox control, the text displayed is set by the Text property. The rich textbox control does everything the Text Box control does, but it can also display fonts, colors, and links; load text and embedded images from a file; and find specified characters. It has numerous properties to format text. We can convert all types of characters, numbers, symbols and diagrams by using rich text box in to Rich text format. By using this we can convert the plaintext into an unintelligible text.

In our paper, we have used it in the first phase to convert the plain text contain characters, numbers, symbols, diagrams, images e.t.c., in to an un comprehensible form as shown below; it is noticeable that the diagrams or the images in the plain text is also got converted into numbers and symbols. We have named the output of this step as Cipher text C1.

Plain text considered for encryption:

AN INVENTION OF A NEW
CRYPTOGRAPHIC ALGORITHM
DEV BY RAVINDRA
1111111@@@@@@@@@@
^&***((()))555599999999

Converted Cipher text in Rich text format C1:

```
{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f
\viewkind4\uc1\pard\f0\fs20 AN INVENTION OF A NEW\par
CRYPTOGRAPHIC ALGORITHM\par
DEV BY RAVINDRA\par
1111111@@@@@@@@@@\par
^&***((()))555599999999\par
{\pict\wmetafile8\picw2091\pich995\picwgoal1185\pichg
0100090000039c01000008001c0000000000040000000301080000
000c02f400f601040000002e0118001c000000fb0210000700000
53797374656d0000f601000057ec0000c4e9120026e2823910b01
0004000000020101001c000000fb029cff000000000000090010000
4e657720526f6d616e000000000000000000000000000000000000
02000000020d000000320a5400fdff01000400fdfffafff101ee0
0000fc02000000ccff000000040000002d01020008000000fa020
002d0103000e000000240305000c0051000c00e700d801e700d80
0000000000000000000040000002d0104000700000fc020000f
0008000000fa020000060000000000000040000002d010600070
040000002d0107000c000000240304000c0051000c00e700d801e
0004000000 2d01050004000000f001060004000000 2701ffff040
07000000fc020000808000000000040000002d0102000400000000
0000002403030 0f70006001600540 0d80154000400000 2d01040
2d01050008000000fa020000060000000000000040000002d010
0024030300f70006001600540 0d80154000400000 2d0104000040
0600040000002701ffff04000000f001020003000000 1e0007000
0000002d0102000400000 2d0103000e000000240305 00ac004f0
ac004f00040000002d0104000400000 2d01050008000000fa020
002d0106000400000 2d0107000c000000240304 00ac004f00ac0
00002d0104000400000 2d01050004000000f001060004000000 2
0000000000
}\par
}
```

B. First Transposition on the output of previous step Cipher1(C1).

For this we have used a 36bit key, which is the sub key (K4) of the 128bit key (K). It is a 9 digits decimal number as shown in the Figure 1. The numbers in the K4 can be between 1 to 9, zero is not allowed to use and the number once used should not be repeated.

For performing transposition message should be written in the rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes key to the algorithm. In the example shown, we have considered the key- K4 is '456789123' used for performing transposition on the cipher C1, the out put is as follows and named it as Cipher C2:

Output of the first transposition C2:

```
tf1\an{\ransicpsi\52\defg12deflanf0\33{\fog10bl{\f0ntt
Scro Serifans
\vie;}}nd4\ucwkiard\f01\p20 AN \fsENTIONINV A NEW OFr
CRY\paGRAPHIPTOLGORITC Apar
DHM\BY RAVEV RA\parIND111111
1@@@@@@@@@ar
^&@\p(((()5***999999555par
(99\ct\wme\piile8\ptaf2091\picw995\piichoal118cwgichgo
011569000000000101000039c01c000080000004000000030000000 5
000000f400f6c02400000001001180002e00000f1c0100007b02000
53792224656d0737f601000007ec000005e912000c428239126e1b
000400000020100001c000010fb029c000000000ff000900100000
e65770
26f6d620500000016e000000000000000000000000000000000004
00d000000220a540003ff01000fd0fdfff040f101eeaff0672d000
00000ccf000000004f000002d000000080010020fa0200000000005
004d0103000200000000e30500024051000cc00700d8000e00d801
000f000000000000000000000000000041040002d00000fc700000ff
00d0100000f080000006a020000000000004000000 2d0100000700
040000002d0100000c0000702403040000c0051000000e70000c1e7
00041040002d0000000400105 0f0010000040000600701fff00200
0700000fc020000008000000800040000002d0100000400002006 0
00000a
30300f2400600167004 00d8000500040015402d010000040000400
2000000008200000fa0000000600000040000002d0100004000 06
0070006000f00540001615400 0d8000002d400400040010002d010
000004000602701ff000400000ff00102000f000000103007000 0
0000002d0100000400002 02d0103000e000000000305000 2404f00
ac14ff00040004002d0100000400004 02d0105000800000000200
002000060004d010002d0000000c00107024030000ac004f400c00
```

C. Ssecond Transposition on the out put of previous step (C2)

Same operation is performed on C2 with the same key- (K4) '456789123', with this multiple transpositions, we can extend the strength of the cipher, so that it is not easily breakable

Output of the second transposition C3:

```
1\rtfb\f{adis\insicansi1pg\e52\d0ff2adefl1ng\f33{\tonOfbl{\f0\
qit0 TsmeeRNew aom f;}{\f1\ncil\frhanMet0 rics softnSaoi Ser}1
\vkew}und4\\c1ilard\ptrp\r\f04fsa2\u87\1?4?87258\uuu30?\595751
\fs12 □734560892
par□a\p\rd\ltrpar fs32 . \uhe qkicTnbrowf \
0\fs2p{\1mct\waeti\ile8cpif\5114cpiw\1617cpih2goal989wgpichlo
17
0019009003000030000000e0001c000700000004000000130058000000000
c000128400c000040000048e011100200000b0fc021000070000000000c0
57792674650d0341c00000008ca0000024e91200c3e28209b60f16000cd00
000c00b000f90200ff00000c0000009000000000010440051206696d35745
6e0000□000000000000000000000000000000000040000002d0101000400000
0200000
020d000005320a07001fff0000ff00ffdff44fbc0081f2200b0d0103000100
0ec000f0020f00fffff000000004020001d00820000000000fa52000000
002d0103000e0002000003053004000400030b7a0143003a01b0047000034
000000000000000000000400020000010440 0d0000002d0002000801a000f
000000000004000102d0005000700000001c020000f000000000000400000
03
0404430000000000 7a31b3147a00b30004000404d0002001000004000410
0005f004000000f701f0ff200000d024010000030000000000a
}\p
r1
.0423)
```

D. Implementing color substitution on pevious step(C3):

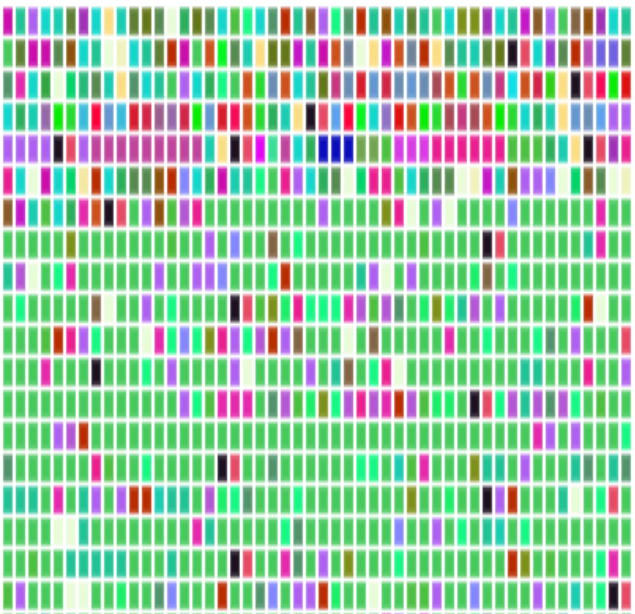
By using our invented 'Play Color Cipher' [16-18] algorithm, each Character (Capital, Small letters, any kind of text, Numbers (0-9), Symbols) in the plain text is substituted with a color block from a 18 decillions of colors[11] available in the computer world. In this we have considered only ARGB with the maximum number of 255 X 255 X 255 X 255 = 4228250625 colors.

In this paper, to strengthen the algorithm and to make the stronger cipher, we have used iterative and modular arithmetic functions. By using the key 'K3' we have an option to select any one of the function out of available 10 functions.

Based on the chosen function, the value of K1 and K2 were passed as parameters to the function and the out put of the function will give us the staring address and the increment values to select the color for substitution. The value of K1 can be any 15 digits decimal number from 000000000000001 to 999999999999999 and the value of K2 can be any 7 digits decimal number from 0000001 to 9999999. It is to be noted that all zeros are not accepted as shown in Figure 3.

In the example shown below the value of the K1 is '123456789012345', K2 is ' 6789012' and the K3 is 3. By passing these two parameters in to the function 3, it produces the starting address and the increment values, applying these on the out put Cipher (C3) in previous step; we got the color code as shown below. This is the final cipher C4 generated by the sender intended for the receiver. The decryption process is the reveres of the encryption process as shown in the Figure 4.

The Play color substitution on C3 and its resultant cipher C4 can be observed:



The flow charts for the encryption and decryption process of 'Play color cipher algorithm' were given below.

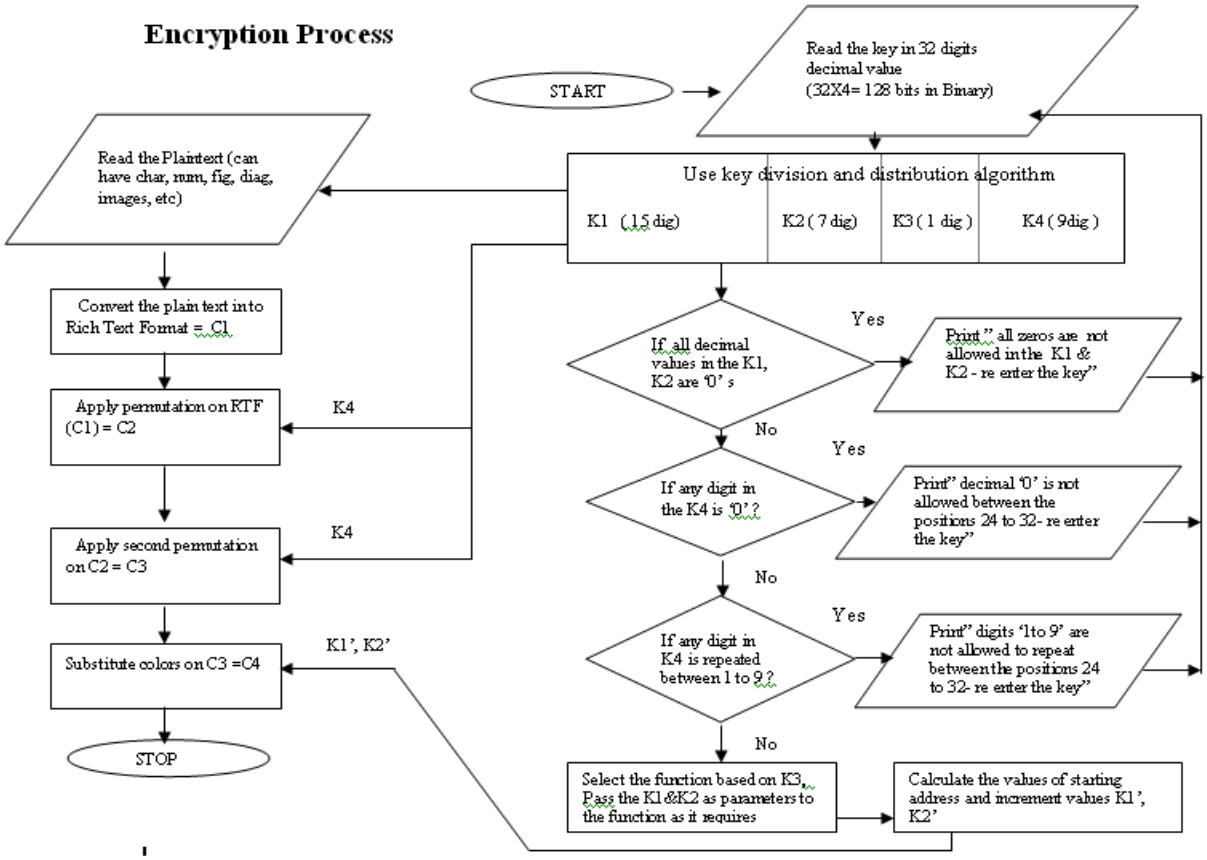


Figure 3. Flow chart for encryption process

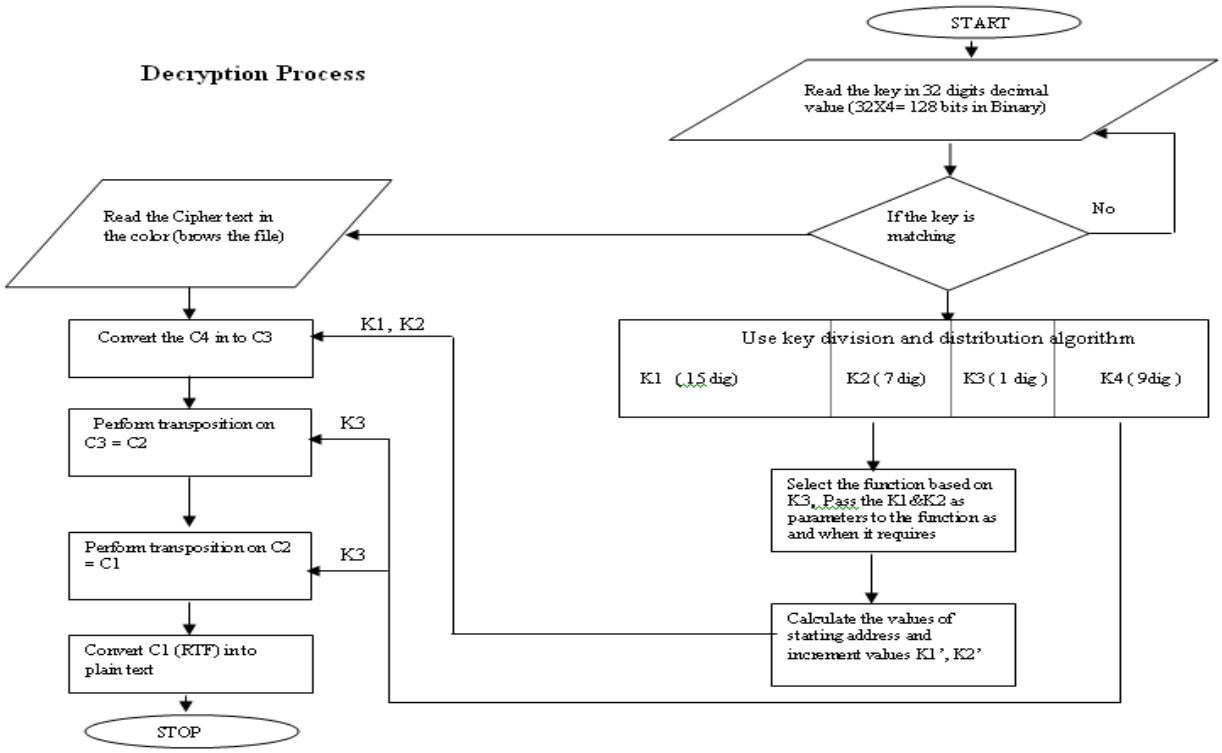


Figure 4. Flow chart for decryption process

IV. CRYPTANALYSIS

The cryptanalyst attacks which are commonly measured in the field of Cryptography and network security are:

Cipher text only attack (Brute force attack)
Known plaintext attack
Chosen plaintext attack
Chosen cipher text attack

In this analysis the key 'K' consisting of 32 decimal numbers, where in each number can be represented in the form of 4 binary bits. Hence the length of the key is 128 bits and the size of the key space is

$2^{128} = 3.4 \text{ X } 10^{38}$ Keys

If the time required for the determination of the plain text for one value of the key in the key space is taken as 10^{-3} seconds, then the time required for obtaining the plain text by considering all the possible keys in the key space is

$$\frac{3.4 \text{ X } 10^{38} \text{ X } 10^{-3}}{365 \text{ X } 24 \text{ X } 60 \text{ X } 60} = 1078 \text{ X } 10^{28} \text{ Years}$$

If we perform one encryption per micro second it takes $5.4 \text{ X } 10^{24}$ years, and for 10^6 encryptions per micro second it leads to $5.4 \text{ X } 10^{18}$ years. This number is very large; hence, it is impossible to break the cipher.

In the case of known plain text attack, we have to know as many pairs of plaintext and cipher text as we require. The number of colors in the computer world is more then 18 decillions, with minor difference we have thousands of shades in the same color, by looking at the colors it is impossible to obtain the plain text, even if you have number of plain text and the corresponding cipher text, the plain text is not the exact plain text of the color cipher because in step one we have converted the plain text in to RTF format, considered the result as C1, then in the second step we have performed trans position on the C1 and the result in this step is C2, in third step we again permuted with the same key and the result is C3 and finally we did color substitution on the C3 and the result is C4.

Hence, the plain text for final cipher C4 is another cipher C3, but not the exact plain text. With this permutations and substitutions in different stages we can conclude that knowing plain text does not work.

In the last two cases of the cryptanalysis attack, no scope is found for breaking the cipher. In view of the above discussion, we conclude that the Cipher is a very strong.

V. EXPERIMENTAL RESULTS

The invented play color cipher algorithm works with 128 bit key and it is proven that it is comfortably converting all kinds of text, symbols, diagrams and images.

The process of conversion with example was explained in section - III. The strength of the any algorithm depends on key rather then the algorithm, in this the length of the key is 32 decimal digits and proven that it is far from crypt analysis attacks.

In this paper especially we have used dynamic permuted key with iterative and modular arithmetic functions to set hurdles in the algorithm and hence to strengthen the cipher.

The execution of encryption and decryption of the 'play color cipher algorithm' with example is shown below

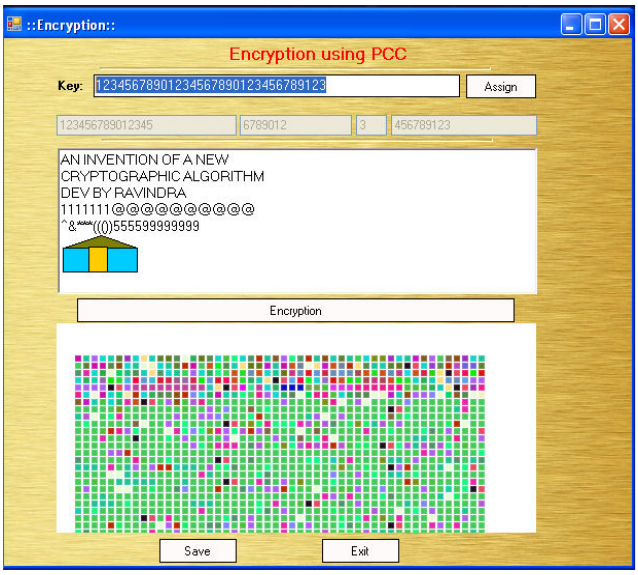


Figure 5. Encryption using PCC with 128 bit key

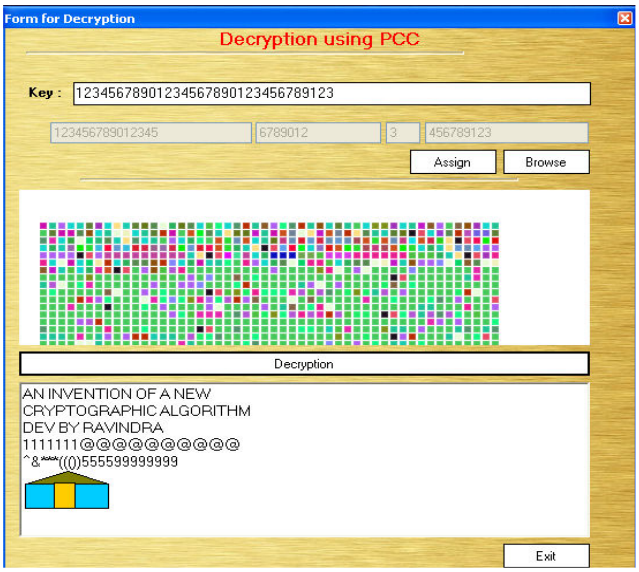


Figure 6. Decryption using PCC with 128 bit key

VI. CONCLUSION

In this paper we have presented a symetric encryption scheme using color substitution and permutations involving dynamic permuted key with iterative and modular arithmetic functions. We have proven that it can encrypt / decrypt all kinds of text, numbers, symbols, images and diagrams with example. For sending the key from source to destination we have used RSA algorithm and the procedure was explained with neat diagram. The brief explanation and the advantages of RTF were given; Generation of cipher text in four stages was explained with example. With the 128 bit key the cipher is very strong and far from cryptanalyst attacks. For performing 10^6 encryptions per micro second it takes $5.4 \text{ X } 10^{18}$ years. Finally we conclude that the algorithm is potential one.

VII. ACKNOWLEDGMENT

The first author likes to thank Dr. S. Udaya Kumar and Dr. A.Vinaya Babu for their precious suggestions and supervision all along to complete the task successfully. He also likes to thank his parents and family members for their overwhelming support. Special thanks to IJARCS for allowing us to use its template.

VIII. REFERENCES

[1] Sastry V.U.K, S. Udaya Kumar and A. Vinaya babu, 2006, A large block cipher using modular arithmetic inverse of a key matrix and mixing of the key matrix and the plain text. J.Comput. Sci., 2: 698-703.

[2] S. Udaya Kumar, A.Vinaya Babu, 2006, A Large block cipher using an iterative method and the modular arithmetic inverse of a key matrix. IAENG Int. J. Comput. Sci., 32: 395-401.

[3] S. Udaya kumar, Sastry and A.Vinaya Babu, 2007. A block cipher involving interlacing and decomposition. Inform. Technol. J., 6: 396 – 404

[4] V.U.K.Sastry, Aruna, S.Udaya Kumar, A Modern Hill Cipher Involving a Permuted key and Modular arithmetic Addition Operation, IJARCS, Vol 2, No 1, Jan-Feb 2011.

[5] Adams, C.M., 1997. The CAST-128 encryption algorithm. RFC 2144, May 1997.

[6] Daemen J and V.Rijmen, 2001. Rijndel, the advanced encryption standard (AES). Dr. Dobb's J., 26: 137- 139.

[7] Daemen J, S. Borg and V. Rijmen, 2002. The Design of Rijndael: AES-the Advanced Encryption Standard. Springer- Verlag, ISBN 3-540-42580-2.

[8] Feistel, H. 1973, Cryptography and Computer privacy. Sci. Am., 288: 15-23.

[9] Feistel, H., W. Notz and Smith, 1975. Some Cryptographic techniques for machine to machine data communications. Proceedings of the IEEE, 63: 1545-1554

[10] Rivest, R.L., 1995. The RC5 encryption algorithm. Dr. Dobbs J., 20: 146-148.

[11] Ravindra Babu K, Dr.S. Udaya Kumar, A Survey on Cryptography and Steganography Methods for Information Security, IJCA, Vol-12, No-2, Nov 2010

[12] Ravindra Babu K, Dr. Udaya kumar, An Improved Playfair Cipher Cryptographic Substitution Algorithm, IJARCS, Volume 2, No-1, Jan-Feb 2011.

[13] Ravindra Babu K, Dr. S.Udaya Kumar, Dr.A.Vinaya Babu, An enhanced and efficient cryptographic substitution method for information security, IJNS, (in press)

[14] Ravindra Babu K, Dr.S. Udaya Kumar, Dr.A.Vinaya Babu, An Extension to traditional Playfair Cipher Cryptographic Substitution Method, IJCA, Volume 17, No-5, March 2011.

[15] Ravindra Babu K, Dr.S. Udaya Kumar, Dr.A.Vinaya Babu, An Enhanced Poly alphabetic Cipher using Extended Vigenere Table, IJARCS, Volume 2, No.2, Mar-April 2011.

[16] Prof. Ravindra Babu Kallam, Dr. S.Udaya Kumar, A Block Cipher generation using Color Substitution, IJCA, 2010 Vol 1, No-28.

[17] Ravindra Babu K, Dr.S. Udaya Kumar, Dr.A.Vinaya Babu, A More secure block cipher generation involving multiple transpositions and substitution with a large key, IJARCS, Vol 2, No 2, Mar-April 2011.

[18] Ravindra Babu K, Dr.S. Udaya Kumar, Dr.A.Vinaya Babu, A New frame work for scalable secure block cipher generation using color substitution and permutation on characters, numbers, images and diagrams, IJCA, Volume 20-no.5, April 2011.

[19] William Stallings, Cryptography and Network Security, Principles and practice, 5th edition, 2008.