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

A More Secure Block Cipher Generation Involving Multiple Transpositions and Substitution with a large key

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
Deputy Director
Department of Computer Science Engineering, SNIST
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 devoted our attention to the study of a symmetric block cipher generation by involving multilevel transpositions and substitution with 128 bit key. For substitution we have used our previously invented "Play color substitution algorithm", by which we can encrypt all types of text, numbers, symbols, images and diagrams, e.t.c. To strengthen the cipher, we have performed multiple transpositions before substitution by using a 36bit key. In this analysis the length of the key and the permutations is playing a vital role in strengthening the cipher. Using a sub key generation algorithm, we have divided the 128bit key into three sub keys for better performance. For secure exchange of the key between the sender and receiver we have used RSA algorithm. The cryptanalysis thoroughly indicate the strength of the cipher.

Keywords: Cryptanalysis, symmetric block cipher, avalanche effect, play color cipher, substitution, permutation, RSA algorithm

I. INTRODUCTION

In a recent investigation, Kallam et al, have developed a modern symmetric block cipher [15] by using a Color substitution and permutations with 92 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 it was permuted by using 36 bit key and finally each character was substituted with a color from the available 4228250625 (ARGB) colors.

It is also noticeable that, we have hug numbers of colors in the world. If we have 10-million colors, times 10-million lighting types, times 10-million lighting levels, times 10-million surrounding colors, times 6-billion people in the world, times 3 modes of viewing we get around 18-decillions of colors. With color substitution, from the available massive number of colors, the cipher is far from cryptanalyst attacks.

For performing substitution we have to use a key which act as a staring address of the color in sequence. To strengthen the key, the authors have proposed an increment value along with the starting address of the color [17]. By using sub key generation algorithm, the authors have divided the available 92 bit key into three sub keys., from LHS first 40 bits shows the starting address, next 16 bits shows the increment value and the remaining 36 bits were used as a key for transposition.

Even though the generated cipher with 92bit key is stronger, the cryptanalyst were working round the clock to break the ciphers. Hence to meet the current requirement in the field of network and information security, it is mandatory that to enhance the strength of the existing algorithms or to invent new algorithms, many scientist were working towards it and got successes [1,2,3,4,5,6,7,8,9,10,11,12,13,14].

In this paper the multi level transposition and the 128bit key is playing a very prominent role in strengthening the cipher.

II. KEY FORMAT AND IT'S MANAGEMENT

The key format and its distribution among the users is as follows:

- Select key 'K', should be 32 decimal numbers between '0 to 9' (having 3 sub keys), the first 23 digits in the Key can be between 0000 0000 0000 0000 0000 001 (Min) to 9999 9999 9999 9999 9999 999 (Max). Remaining 9 digits (RHS) of the key should be the numbers between '1 to 9', and the number once used should not be repeated.

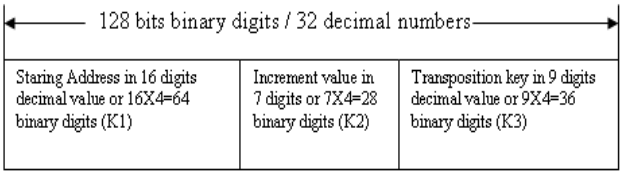


Figure 1. Key format for 128 binary bits

- In the above 32 decimal numbers:, from LHS to RHS, algorithm considers first 16 numbers as staring address (K1), next 7 numbers as increment value(K2) and the last 9 numbers as key (K3)for transposition. Use RSA [16] Public key encryption algorithm for key distribution as shown in Figure 2:
- 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 authentication and confidentiality we have distributed the keys between User A and User B.

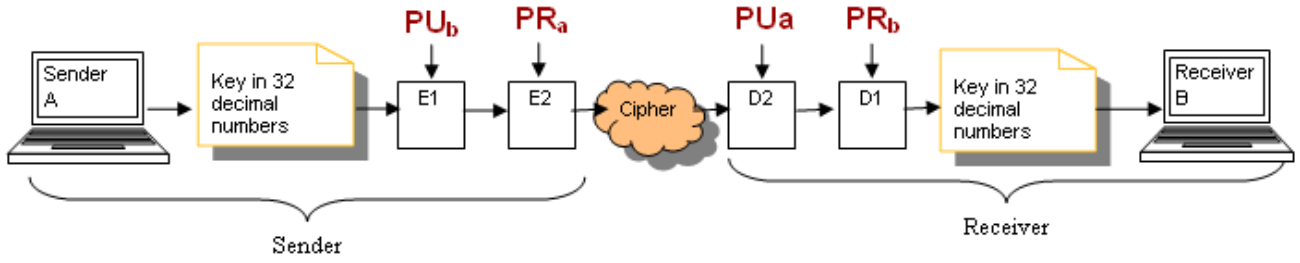


Figure 2. Secure transmission of key using RSA algorithm

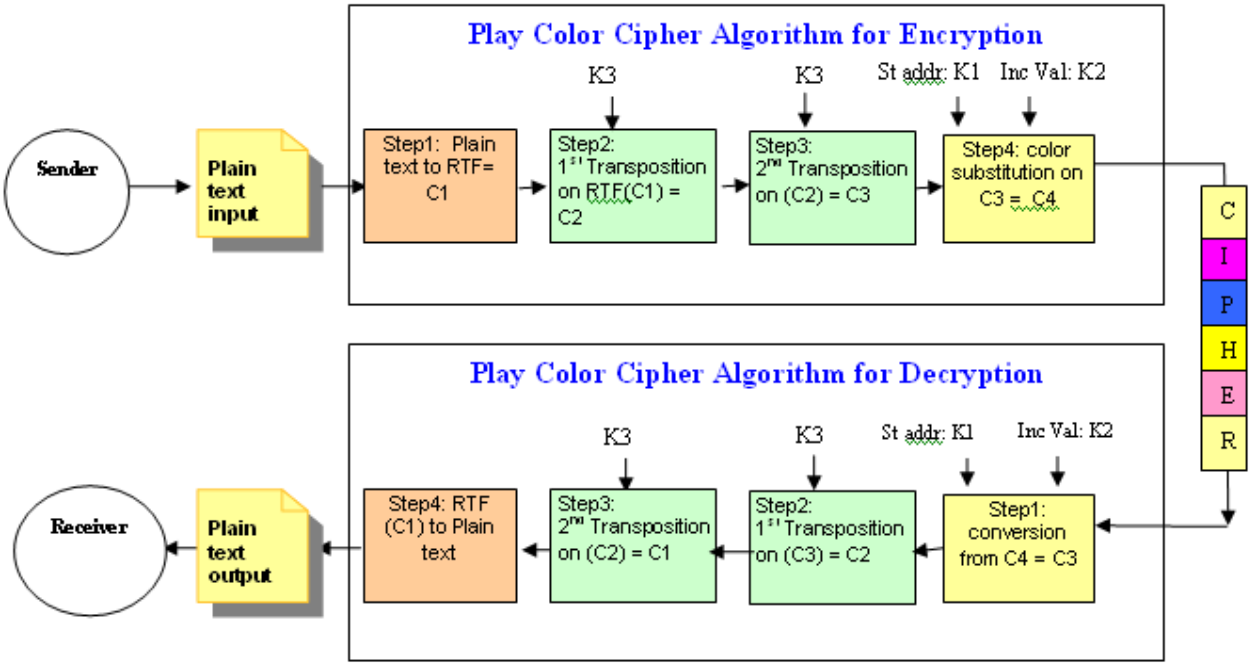


Figure 3. Procedure of encryption and decryption using transposition and play color cipher

III. DEVELOPMENT OF THE CIPHER

In this we have developed the cipher in four phases as shown in Figure 3, 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 input and the output of each phase we have explained below:

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

As with the Textbox control, the text displayed is set by the Text property. Windows Forms Rich Text Box control is used for displaying, entering, and manipulating text with formatting. 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. It is typically used to provide text manipulation and display features similar to word processing applications such as Microsoft Word. 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 algorithm, 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 intelligible 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:

I AM GOING TO COLLEGE
11111111222222222333
77777777777777777777
#####@@@@@@@&&&&

Apply second permutation on C2 = C3

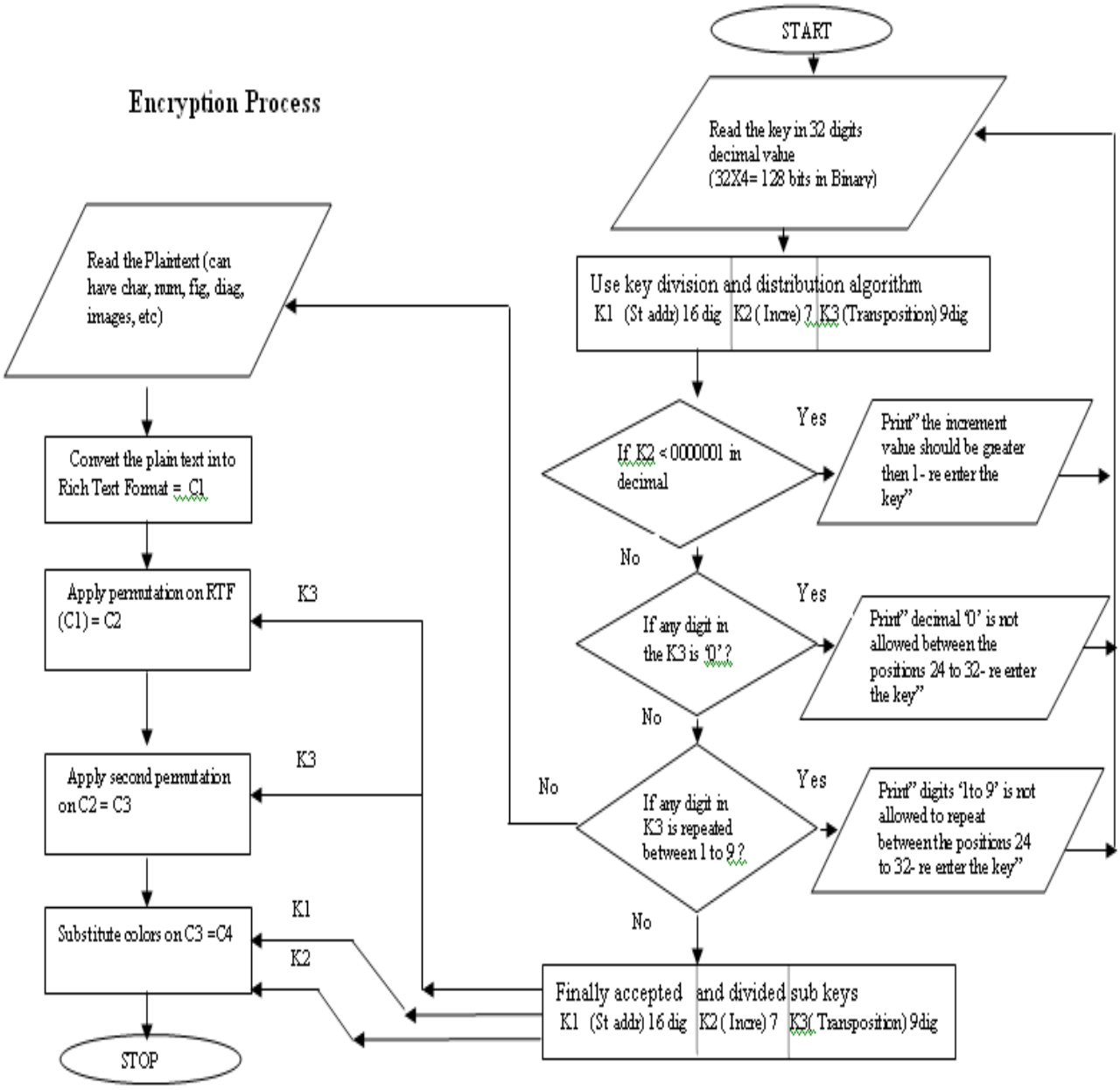


Figure 4. Flow chart for encryption process

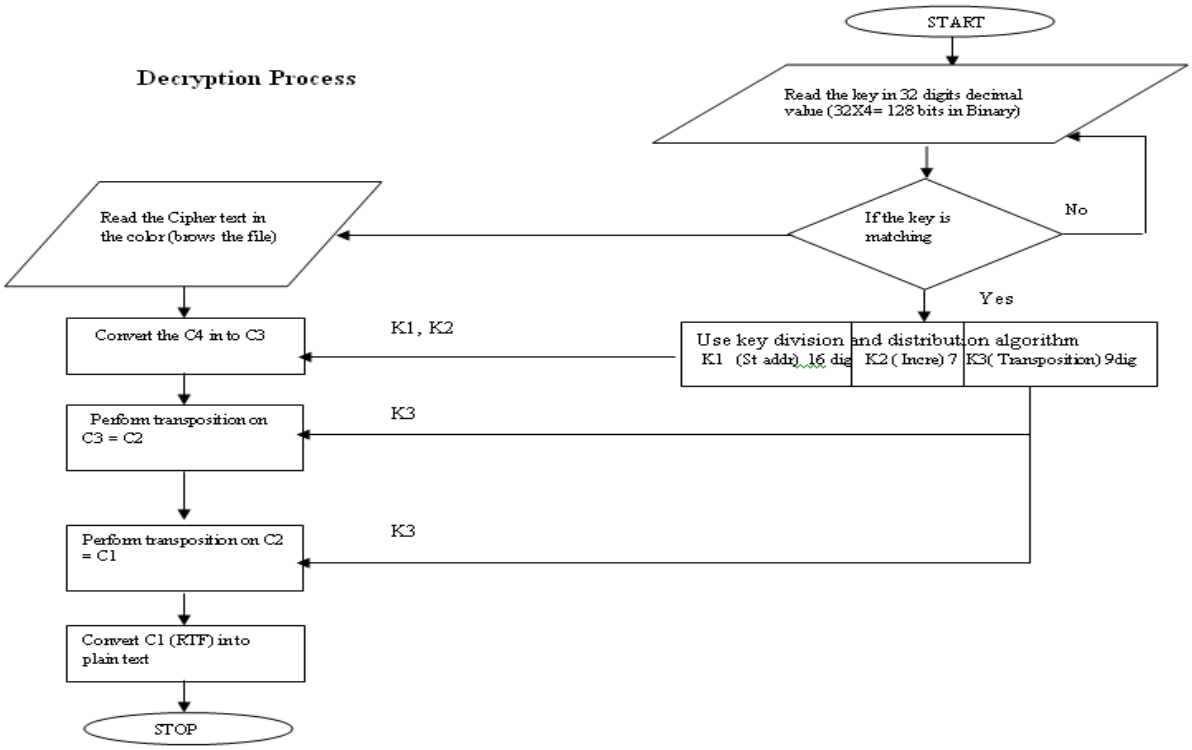


Figure 5. Flow chart for decryption process

Converted Cipher text in Rich text format C1:


```
{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fnil\
\viewkind4\uc1\pard\f0\fs20 I AM GOING TO COLLEGE\par
11111111222222222223333\par
77777777777777777777\par
##########&&&&\par
{\pict\wmetafile8\picw3814\pich1325\picwgoal2162\pichgoal75
010009000003a801000007002600000000000400000003010800050000
000c0239018d03040000002e0118001c000000fb029cff00000000000
54696d6573204e657720526f6d616e0000000000000000000000000000
000400000002010100050000000902000000020d000000320a5a00fdff
390120cf2d00030000001e0007000000fc020000ffffff0000000400000
020500000000000ffffff00040000002d0102000e0000002403050002000
800303000200030008000000fa020000000000000000000040000002d0
0008000000fa020000060000000000000040000002d0104000700000f
040000002d0105000c000000240304000200030002003401800334018000
000400000002d01010004000000f00104000400000027 01ffff030000001
7e03250006001c000000fb02bdff0000000000009001000000000440001
20526f6d616e0000000000000000000000000000000000040000002d010
0e000000320a6100420002000400060025007e03140120201100110014
000400060025007e0314014170706c79202f00220022001200200011002
1200040006002 5007e0314017365636f6e64207065726d75746174696f6
00220011002 2001d00160034002100130 01d00130013002100210 00d000
0400060025007e03140120cf1000040000000201010010000000320aaf0
007e0314016f6e2002210022001100110000003 20aaf00960004000400
203d2c00220010002600100000000320aaf001a0103000400060025007e0
0022000d000000320aaf007901010004000600 25007e03140120cf1d000
0000fb02100007000000000bc020000000001020222537973746 56d000
971b00f8b11b00b0951b0024d98239040000002d01060003000000000
}\par
}
```


B. Performing permutation on the output of previous step Cipher1(C1).

For this we have used a 36bit key, which is the sub key (K3) of the 128bit key (K). It is a 9 digits decimal number as shown in the Figure 1,4. The numbers in the K3 can be between 1 to 9, zero is not allowed to use and the number once used should not be repeated.

For performing transposition write the message 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- K3 is '912345678' 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:


```
n(\rtf1\apsi\ansicfg1252\denf0\deflaog1033(\fOnttbl(\fh\fnil\fciarset0 MScrosof
fans Serie;})
\vicwkind4\u01\pard\fA\fs20 I TM GOING EO COLLEG1\par
1121111122232222223373\par
7777777777777777777#77\par
@#########r@&&&&\pa\
(\pictewmetafil18\picw3824\pich13a5\picwgocl2162\pi hgoal7510
010009100003a8020000070006000000000040000000301080005000000b0200000000500009
000c0230018d03041000002e0018001c00c000fb0290ff000000100009000000000
44000127546966573204e657620526f6d016e0000000000000000000000000000000000400000
2d0100
000400000002010100950000000002000000020d00000f320a5a004dff01000000fdff00908703
300120cf2d00030000001e0007000000fc020000ffffff0000000400000002d01010008000000fa
020500000000000ffffff00040000002d0102004e0000002003050002000300020334018003340 1
800003000200030008000000fa020000000000000000000d400000020010300041000002d0001
0008200000fa0000000600000000000000040000002d01040f070000000c020100000000000000
040000002d0105000c000000240304002200030000003401803334018000030004003000 2d0100
000400100002d0100000400000f00104020400000003701ffff000000001e000700000 160414010
7e03250006001c00d000fb02b0ff000000100000900000000000444000125269 6d6573
04e6577620526f6d016e0000000000000000000000000000000000000040000002d0104002400000000
010100
2e000000300a6100420002000407060025000e03140120201100110014000006320a6100040006
0204000600450 07e0316014170700c79202f0122002200120022000100026000000320a61001a01
1200040006012500 7e0334017365676f6e64205065726d7674617469df6e1a0010001e00212022
00200011002200 1d00160134002100330 01d00100130021002 1000d060000320a1100270300000
0400e60025007c031401200f1000040000000201010010000000320aaf0042000302040006003 5
007e0214016f6e2002210022000110011a000003200af00960064000400000025007e2314014330
203d2c00220010002600100 0f000320aa0001a0103000400060125007e0334012043 30211002cd
```


C. Performing second permutation on the out put of previous step (C2)

Same operation is performed on C2 with the same key-(K3) '912345678', 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:

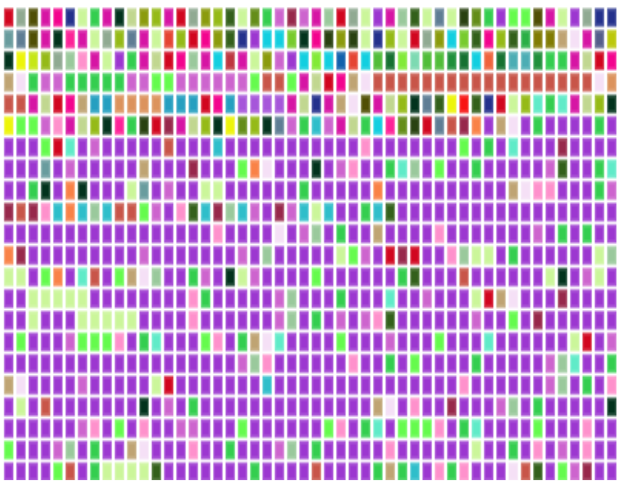
```
1\rtfb\f{adis\insicansi1pg\e52\d0ff2adefl1ng\f33{\tonOfbl{\f0\
qitO TsmeeRNew aom f;}{\f1\ncil\frhanMetO rics softnSaoi Ser}:
\vkew}und4\\c1ilard\ptrp\r\f04fsa2\u87\1?4?87258\uuu30?\595757
\fs12 □734560892
par□a\p\rd\ltrpar fs32 . \uhe qkicTnbrowf \
0\fs2p{\1mct\waeti\ile8cpif\5114cpiw\1617cpih2goal989wgpichlo
17
0019009003000003000000e0001c000700000004000000130058000000000
c000128400c000040000048e011100200000b0fc021000070000000000c0
57792674650d0341c00000008ca0000024e91200c3e28209b60f16000cd00
000c00b000f90200ff00000c0000009000000000010440051206696d35745
6e0000□0000000000000000000000000000000040000002d0101000400000
0200000
020d000005320a07001fff0000ff00ffdff44fbc0081f2200b0d0103000100
0ec000f0020f00fffff000000004020000 1d00820000000000fa5200000000
002d0103000e000200000305300400040003 0b7a0143003a01b00470000340
0000000000000000000040002000001044 00d0000002d0002000801a000f0
000000000040000102d0005000700000 1c020000f000000000000400000
03
0404430000000000 7a31b3147a00b30004000404d000200100000400041020
0005f0040000000f701f0ff200000d024010000030000000000a
}\p
r1
.0423}
```

D. Implementing color substitution on pevious step(C3) with the keys K1 and K2:

Play Color Cipher: 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[15] 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, to make the cipher stronger we have used staring address of the color K1 in 16 digits decimal number from 0000000000000000 to 9999999999999999 and increment value K2 in 7 digits decimal number with the range 0000001 to 9999999. It is to be noted that increment value should not be 0000000 as shown in the Figure 4, because all the characters will get the same color, which is not acceptable in algorithm.

In the example shown below the value of the starting address K1 is '9999999999999999' and the Increment value K2 is ' 9999999', by 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 source/ sender intended for destination/ receiver. The decryption process is the reveres of the encryption process as shown in the Figure 5.

Play color substitution on C3 and its output C4:



IV. CRYPTANALYSIS

The cryptanalyst attacks which are generally considered in the literature of Cryptography 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 mıcro second ıt 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 impracticable to break the cipher.

In the case of known plain text attack, we 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 did color substitution on the C2 and the result is C3. Hence, the plain text for final cipher C3 is another cipher C2, 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. 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 previous section. 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.

VI. CONCLUSION

In this paper we have presented a conventional encryption scheme using color substitution and permutations with symmetric key. We have proven that it can encrypt / decrypt all kinds of text, numbers, symbols, images and diagrams with example. For transferring 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 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 valuable suggestions and guidance all along to complete the task successfully. He likes to be grateful to his parents and family members for their overwhelming support all the time. He also like to thank the Management and the Principal of VITS SET, Kareemnagar, for providing all the resources to fulfill the task. Special thanks to IJARCS for allowing us to use its template.

VIII. REFERENCES

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

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

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

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

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

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

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

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

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

[10] Schneier B, 1994. The blowfish encryption algorithm. Dr. Dobbs J., 19: 38-40

[11] 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

[12] 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.

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

[14] 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.

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

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

[17] 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, (paper sent for publication).

