A New Framework for Scalable Secure Block Cipher Generation using Color Substitution and Permutation on Characters, Numbers, Images and Diagrams

Ravindra Babu Kallam
Research Scholar, JNTUH
AZCET, Mancherial
A.P, India

Dr. S.Udaya Kumar
Deputy Director, SNIST
Ghatkesar, A.P
India

Dr. A.Vinaya Babu
Director, Admissions
J.N.T.U.H, Hyderabad
A.P, India

ABSTRACT

The aim of our research is to develop a new framework for secure block cipher generation using color substitution and permutations on alphanumeric letters, symbols, images, diagrams or any kind of text. To transfer the keys from source to destination we have used RSA public key algorithm and for encryption / decryption of the information, we have used our invented 'play color substitution' algorithm. Importance of RTF will be explained, Cryptanalysis attacks were discussed and shown that the cipher cannot be broken by any cryptanalysis attacks.

General Terms

Crypt analysis, block cipher, play color cipher, decillions, encryption / decryption algorithm.

Keywords

RSA, ETF: Electronic Frontier Foundation, PUB: Public key of user B, PRA: Private Key of user A, PUA: Public key of user A, PRB: Private key of user B, PCC: Play color cipher, RTF: Rich text format, LHS: Left hand side, RHS: Right hand side.

1. INTRODUCTION

The most prevailing and universal approach to countering the threats to network / data security is encryption. Even though it is very influential, the cryptanalysts are very intellectual and they were working round the clock to break the ciphers.

Many Scholars and Scientist were investigating day and night on the existing algorithms to make more stronger and unbreakable ciphers by enhancing them[1,2,3,4,5,6,7,8,9,10]. But still most of the algorithms were vulnerable to attack. One of the most widely used cryptographic algorithm is DES, is also broken and announced by the Electronic Frontier Foundation in July 1998 [16], many substitution algorithms like Caesar Cipher, Mono alphabetic Cipher, Play fair Cipher and Poly alphabetic Ciphers are proven to be not stronger and even they only support for limited applications.

To meet the current requirements and to fight with the cryptanalyst in the battle of the network and information security , we need stronger Cryptographic algorithms.

It is mandatory that to sharp our brain and invent new Cryptographic algorithms rather then updating the existing one all the time. In lieu of this and to bring the revolution in the field of network and Information security; have invented a new cryptographic algorithm by using 'Color substitution technique' and named it as 'Play color Cipher' in our previous paper [15].

In the present paper we have used 92 bit key and extended the algorithm to the wide range of applications, where it allows to encrypt / decrepit all types of characters, numbers, symbols, diagrams and images, etc.,. To create stronger cipher we did permutations/ transposition on the out put of R.T.F and before applying color substitution. Finally, we have proven that the cipher is very stronger and resistant to the cryptanalysis attacks.

2. KEY SELECTION & DISTRIBUTION

Sequence of steps involved in *selecting a key and procedure for transferring key from source to the destination* as shown in the Figure 1and Figure 2:

- Select key 'K', should be 23 decimal numbers between 0 to 9 (having 3 sub keys)
  The first 14 digits in the Key can be between 0000000000 0001 (Min) to 9999999999 9999 (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.
- In the above 23 decimal numbers:, from LHS to RHS, algorithm considers first 10 numbers as staring address (K1), next 4 numbers as increment value(K2) and the last 9 numbers as key (K3)for transposition / permutation..
- 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.

3. METHODOLOGY

Sequence of steps in our 'Play color cipher' algorithm for encryption and decryption:

Procedure for encrypting the plaintext at the sender as shown in Figure 3,4,6 and 7:

- Use Windows XP and Microsoft Visual Studio for executing "*Play Color Cipher Algorithm*".
- Debug the algorithm to get the '*Form for Encryption'*

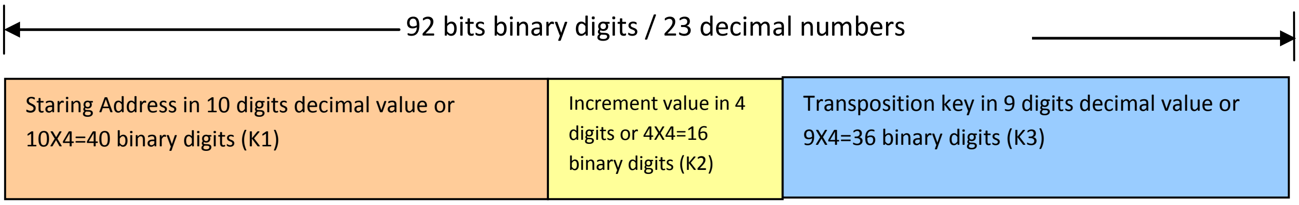

92 bits binary digits / 23 decimal numbers
Staring Address in 10 digits decimal value or 10X4=40 binary digits (K1)
Increment value in 4 digits or 4X4=16 binary digits (K2)
Transposition key in 9 digits decimal value or 9X4=36 binary digits (K3)

Figure 1: Key format in 92 binary bits

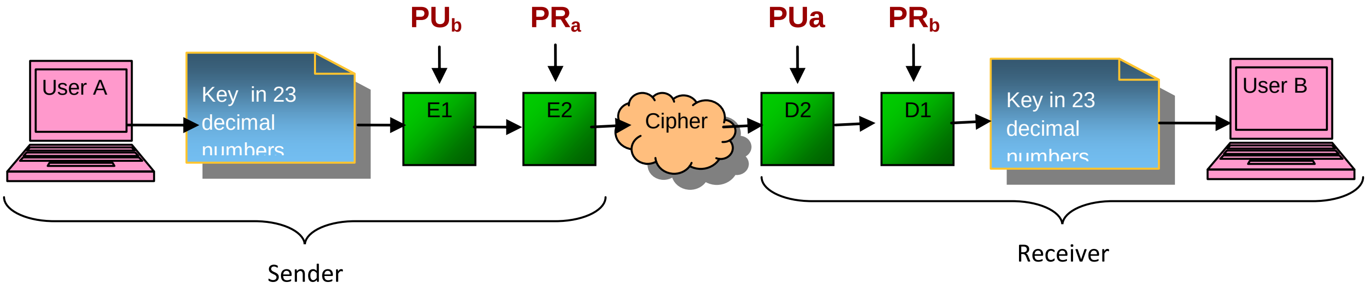


Figure 2: Secure Transmission of Key using RSA

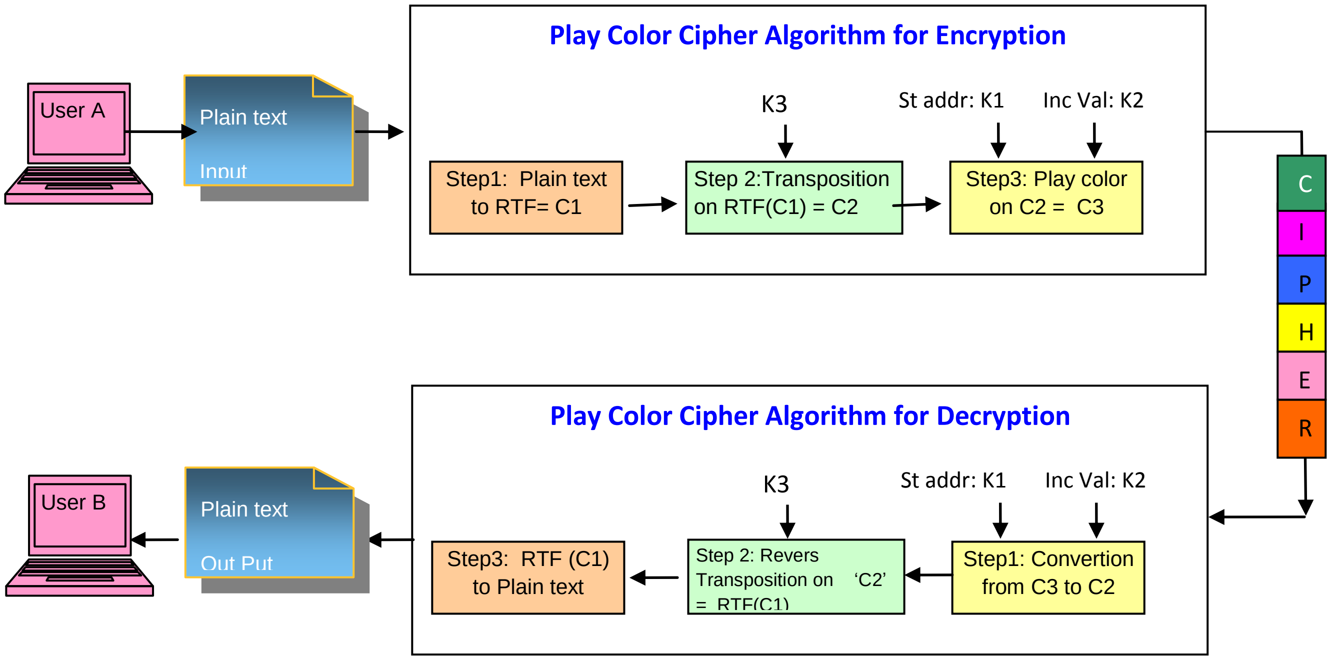

User A
Plain text Input
Play Color Cipher Algorithm for Encryption
K3
St addr: K1
Inc Val: K2
Step1: Plain text to RTF= C1
Step 2:Transposition on RTF(C1) = C2
Step3: Play color on C2 = C3
C
I
P
H
E
R
Play Color Cipher Algorithm for Decryption
K3
St addr: K1
Inc Val: K2
Step1: Convertion from C3 to C2
Step 2: Revers Transposition on 'C2' = RTF(C1)
Step3: RTF (C1) to Plain text
Plain text Out Put
User B

Figure 3: Process of Encryption & Decryption using Play Color Cipher

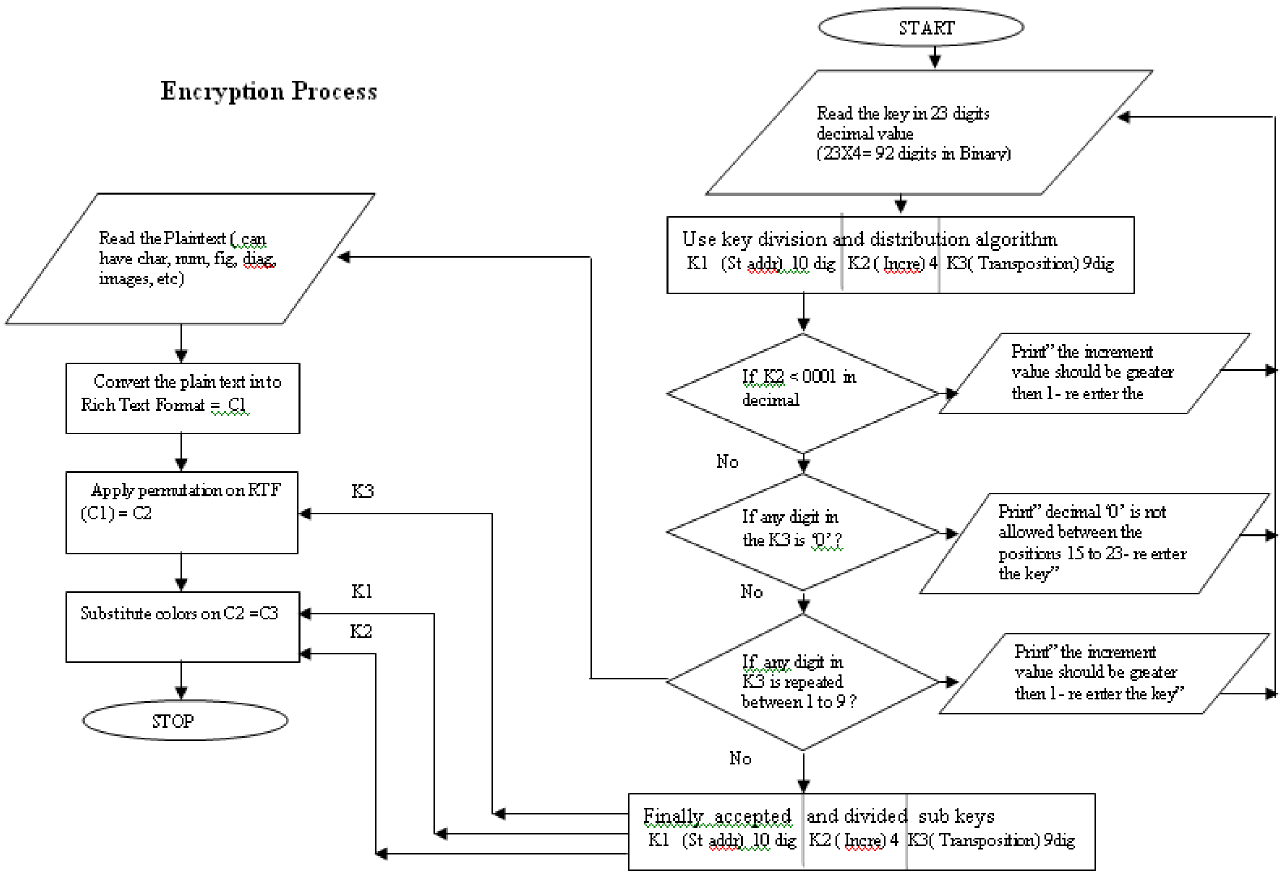

Encryption Process
START
Read the key in 23 digits decimal value (23X4= 92 digits in Binary)
Use key division and distribution algorithm
K1 (St addr) 10 dig K2 (Incre) 4 K3(Transposition) 9dig
If K2 < 0001 in decimal
Print" the increment value should be greater then 1- re enter the
No
If any digit in the K3 is '0' ?
Print" decimal '0' is not allowed between the positions 15 to 23- re enter the key"
No
If any digit in K3 is repeated between 1 to 9 ?
Print" the increment value should be greater then 1- re enter the key"
No
Finally accepted and divided sub keys
K1 (St addr) 10 dig K2 (Incre) 4 K3(Transposition) 9dig
Read the Plaintext (can have char, num, fig, diag, images, etc)
Convert the plain text into Rich Text Format = C1
Apply permutation on RTF (C1) = C2
K3
Substitute colors on C2 =C3
K1
K2
STOP

Figure 4: Flow chart for encryption process

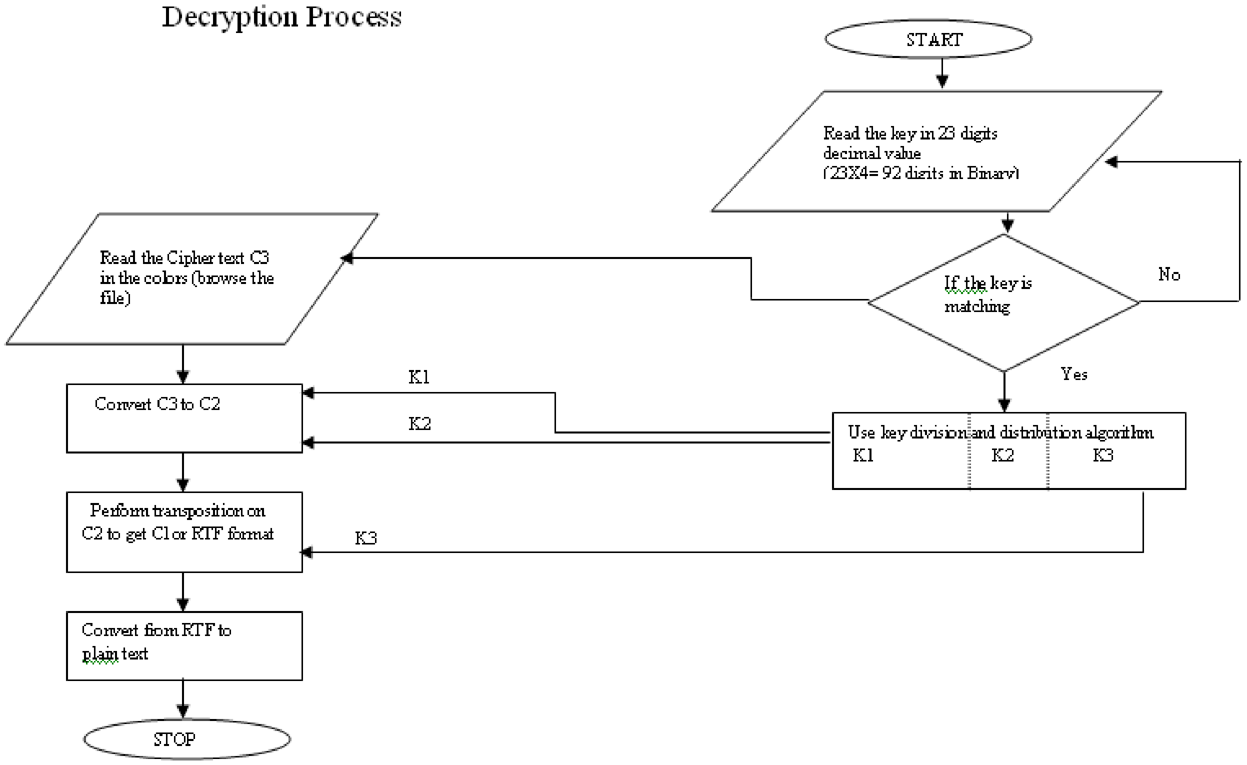

Decryption Process
START
Read the key in 23 digits decimal value (23X4= 92 digits in Binary)
If the key is matching
No
Yes
Use key division and distribution algorithm
K1 K2 K3
Read the Cipher text C3 in the colors (browse the file)
Convert C3 to C2
K1
K2
Perform transposition on C2 to get C1 or RTF format
K3
Convert from RTF to plain text
STOP

Figure 5: Flow chart for Decryption Process

- Enter the values of key 'K' in the box given and click on 'assign button'
- Enter the plain text in the box given (can use any characters, numbers, symbols, figures, diagrams or any kind of text.
- Click on *'Encryption Button'*
- 'Save' the result as a file with the extinction of .tif and 'exit' from encryption form.
- Now the cipher is ready for transferring from source to destination.

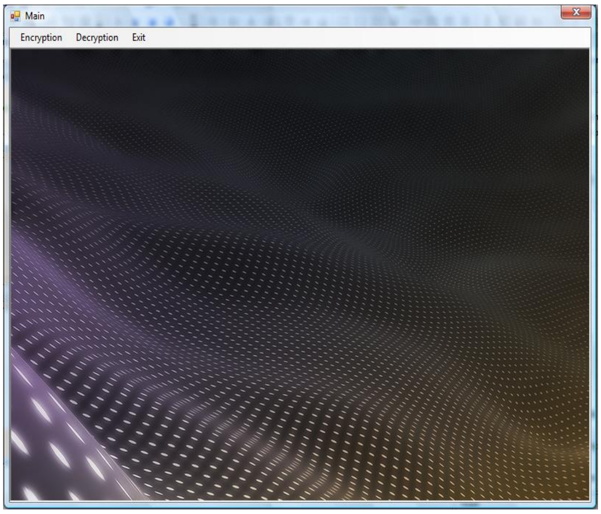
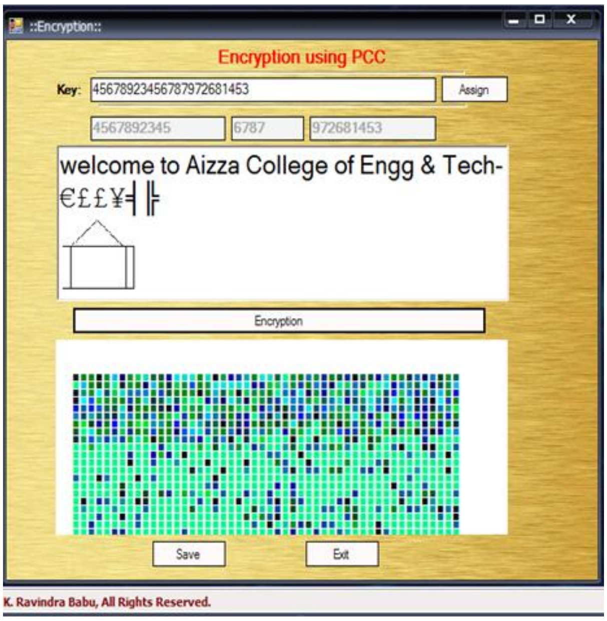


Figure 6: Main form of 'play color cipher algorithm'



Key: 4567892345678797268145З

4567892345 | 6787 | 972681453

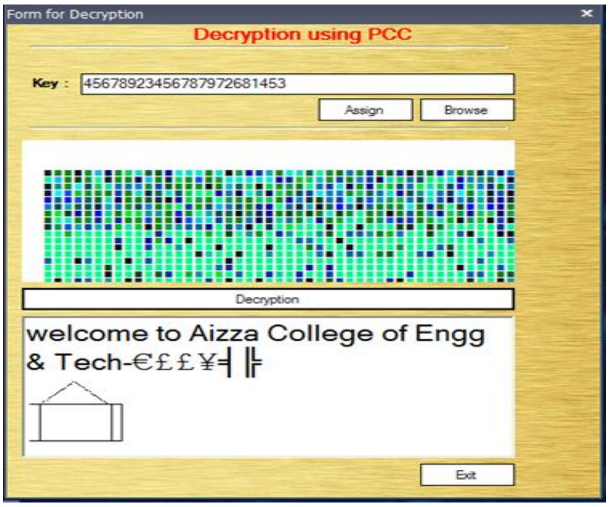
welcome to Aizza College of Engg & Tech-€££¥╡╟

K. Ravindra Babu, All Rights Reserved.

Figure 7: Form for Encryption

Procedure for Decrypting the cipher text at the receiving end as shown in Figure 3,5 and 8:

- Use Windows XP and Microsoft Visual Studio for executing "*Play Color Cipher Algorithm*".
- Debug the algorithm to get the '*Form for Decryption'*
- Open the '*Form for Decryption*' and enter the 'K'
- Browse for the received and saved cipher file
- Click on '*Decryption Button*'
- Observe the converted '*plain text*'.



Key : 45678923456787972681453

welcome to Aizza College of Engg & Tech-€££¥╡╟

Figure 8: Form for Decryption

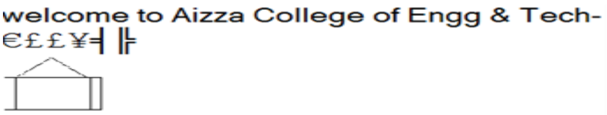
4. DEVELOPMENT OF THE CIPHER

4.1 About RTF and Converting a Plain text in to the RTF format:

About Rich Text Format (RTF): The 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. The Rich Textbox control 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. The output of this step we name it as Cipher text C1.

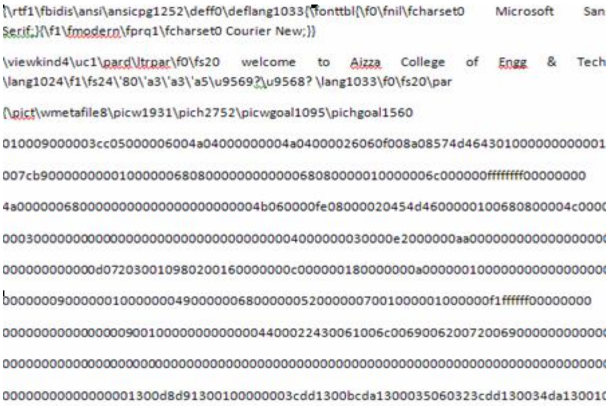
Consider the plain text as shown below, it may contain characters, numbers, symbols, diagrams, images e.t.c., by using rich text box it is converted in to an un intelligible form as shown below; it is noticeable that the diagrams or the images in the plain text is also got converted into numbers and symbols.

Plain text:



welcome to Aizza College of Engg & Tech-€££¥╡╟

Rich text / Cipher text 'C1'for the above plain text:

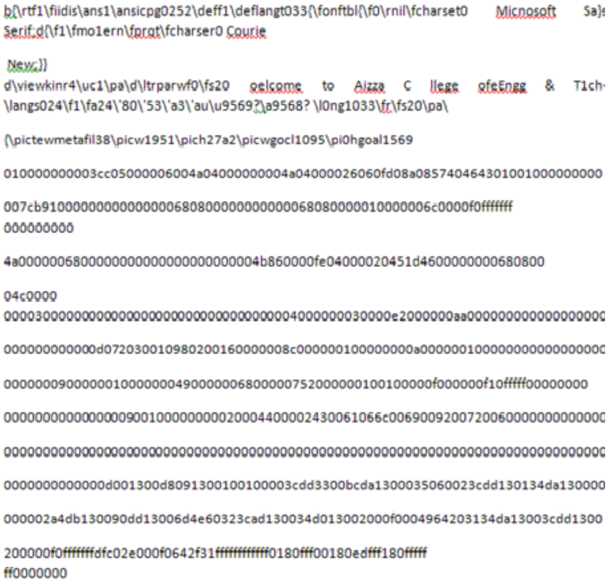


```
{\rtf1\fbidis\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fnil\fcharset0    Microsoft    San
Serif;}{\f1\fmodern\fprq1\fcharset0 Courier New;}}

\viewkind4\uc1\pard\ltrpar\f0\fs20   welcome   to   Aizza   College   of   Engg   &   Tech
\lang1024\f1\fs24\'80\'a3\'a3\'a5\u9569?\u9568? \lang1033\f0\fs20\par

{\pict\wmetafile8\picw1931\pich2752\picwgoal1095\pichgoal1560

010009000003cc05000006004a04000000004a04000026060f008a08574d4643010000000000001

007cb900000000010000006808000000000000006808000000100000006c000000ffffffff00000000

4a000000680000000000000000000000000004b060000fe08000020454d460000001006808000004c000

000300000000000000000000000000000000000004000000030000e2000000aa0000000000000000000

0000000000000d07203001098020016000000000c000000180000000a00000010000000000000000000

b00000009000000100000004900000068000000520000007001000001000000f1ffffff00000000

00000000000000000900100000000000000044000224300610 06c00690062007200690000000000000

0000000000000000000000000000000000000000000000000000000000000000000000000000000000

00000000000000001300d8d9130010000003cdd1300bcda1300035060323cdd130034da130010
```

4.2 Performing Permutation on the output of Previous step (4.1) using K3

To make stronger cipher from the previous step 4.1, we have performed permutation on C1 by using key K3. The sub key K3 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 below, the key- K3 is *'972681453'* used for performing transposition on the cipher C1, the out put is as follows and named it as Cipher C2:

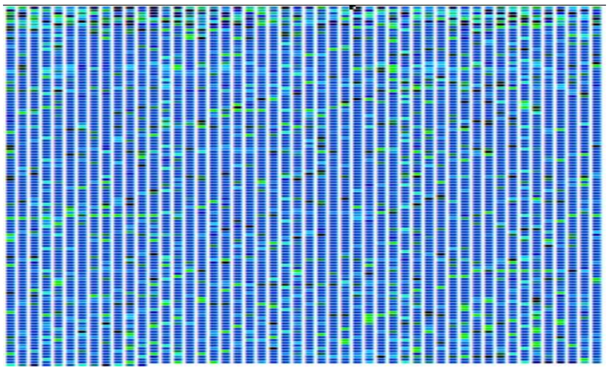


```
b{\rtf1\fiidis\ans1\ansicpg0252\deff1\deflangt033{\fonftbl{\f0\rnil\fcharset0     Micnosoft     Sa}s
Serif;d{\f1\fmo1ern\fprqt\fcharser0 Courie

 New;}}
d\viewkinr4\uc1\pa\d\ltrparwf0\fs20   oelcome   to   Aizza   C   llege   ofeEngg   &   T1ch
\langs024\f1\fa24\'80\'53\'a3\'au\u9569?\a9568? \l0ng1033\fr\fs20\pa\

{\pictewmetafil38\picw1951\pich27a2\picwgocl1095\pi0hgoal1569

010000000003cc05000006004a04000000004a04000026060fd08a0857404643010010000000000

007cb91000000000000000006808000000000000006808000001000000 6c0000f0fffffff
000000000

4a000000680000000000000000000000004b860000fe04000020451d460000000000680800

04c0000
0000300000000000000000000000000000000004000000030000e2000000aa00000000000000000

000000000000d07203001098020016000000 8c000000100000000a00000010000000000000000

00000009000000100000004900000068000007520000001001000 00f000000f10fffff00000000

0000000000000000900100000000002000440000243006106 6c006900920072006000000000000

0000000000000000000000000000000000000000000000000000000000000000000000000000000

000000000000d001300d809130010010000 3cdd3300bcda130003506002 3cdd130134da130000

000002a4db130090dd13006d4e60323cad130034d013002000f0004964203134da13003cdd1300

200000f0fffffffdfc02e000f0642f31ffffffffffff0180fff00180edfff180fffff
ff0000000
```

4.3 Applying play color cipher on the out put of previous step(4.2) using K1and 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 more stronger we have used staring address of the color K1 in 10 digits decimal number from 0000000000 to 9999999999 and increment value K2 in 4 digits decimal number with the range 0001 to 9999. It is to be noted that increment value should not be 0000 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 '4567892345' and the Increment value K2 is ' 6787', by applying this on the out put Cipher(C2) in previous step, we got the color code as shown below. This is the final cipher C3 generated by the source/ sender intended for destination/ receiver.



5. CRYPTANALYSIS

The cryptanalyst attacks which are generally considered in the literature of Cryptography are

1. Cipher text only attach (Brute force attack)
2. Known plaintext attack
3. Chosen plaintext attack
4. Chosen cipher text attack

In this analysis the key K is consisting of 23 decimal numbers, where in each number can be represented in the form of 4 binary bits. Hence the length of the key is 92 bits and the size of the key space is

$$2^{92} = 5.0 \text{ X } 10^{27} \text{ Keys}$$

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

$$\frac{5.0 \text{ X } 10^{27} \text{ X } 10^{-3}}{365 \text{ X } 24 \text{ X } 60 \text{ X } 60} = 1585 \text{ X } 10^{14} \text{ Years}$$

If we perform one encryption per micro second it takes 2.4 X 10^{16} years, and for 10^{6} encryptions per micro second it leads to 1842.6 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.

6. RESULTS

The invented play color cipher algorithm works with 92 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 23 decimal digits and proven that it is far from crypt analysis attacks.

7. CONCLUSION

In this paper we have presented a conventional encryption scheme using color substitution and permutations with symmetric key. The length of the block is variable in size. we have proven that it can encrypt / decrypt all kinds of text, numbers, symbols, images and diagrams with example. Algorithm have three functions, works with three sub keys K1, K2 and K3 generated from the main key K. Using the existing 'Rich text box' feature from Microsoft Visual studio is the center of attraction of this algorithm. For transferring key from source to destination we have used RSA algorithm and the procedure was explained with neat diagram.

Applying the combination of permutation and substitution enhanced the strength of the algorithm to the great extent. This algorithm is implemented by using C#.net. The brief explanation and the advantages of RTF were given; Generation of cipher text in three stages was explained with example. With the 92 bit key the cipher is very strong and far from cryptanalyst attacks. For performing 10^6 encryptions per micro second it takes 1842.6 years. Finally we conclude that the algorithm is potential one.

8. ACKNOWLEDGMENTS

The first author likes to thank Dr. S. Udaya kumar and Dr. A.Vinaya Babu for their valuable suggestions and guidance given round the clock to complete the task successfully.

He also likes to thank his parents and family members for their overwhelming support all along. Special thanks to IJCA for allowing us to use its template.

9. 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, Volume-12, No-2, November 2010

[8] Ravindra Babu K, Dr. Udaya kumar, Dr. A.Vinaya Babu, 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.