An Impregnable Block Cipher Generation using Modern Transposition and Substitution Algorithms with a large Key, Modular Arithmetic and Integral Functions

Ravindra Babu Kallam
Research Scholar,
J.N.T.U, Hyderabad
A.P, India

S.Udaya Kumar
Principal,
M.V.S.R Engineering College
Hyderabad, A. P, India

A.Vinaya Babu
Principal, JNTUCE
J.N.T.U.H, Hyderabad
A.P, India

ABSTRACT
In this research, we have invented a method to generate the secure block cipher using modern transposition and substitution with 128bit key, modular and integral functions. This method supports an input in the form of ASCII, extended ASCII characters, images and diagrams etc. Initially, the algorithm converts the given input in to ANSI characters using rich text format, then it performs 16rounds of permutations with internal functions and finally it carryout color substitution.

The functions used in this algorithm alter the plain text in various ways before it takes the shape of cipher text. A brief introduction about the tree data structures and its traversal methods has explained. The process of encryption, decryption and the sub key generation algorithms are explained with example. The avalanche effect and the cryptanalysis inspected in this investigation evidently indicate that the cipher is potential one.

General Terms
Binary Trees, Inorder, Preorder, Postorder, Cryptanalysis, Block cipher, Play color cipher, Encryption, Decryption, Decillions, Security and Algorithm.

Keywords
Symmetric block cipher, Play color cipher (PCC), Substitution, Permutation, RSA algorithm, Rich text format (RTF), PUb: Public key of user B, PRa: Private Key of user A, PUa: Public key of user A, PRb: Private key of user B.

1. INTRODUCTION
The area of cryptography is growing at present at a rapid rate as a number of researchers are engrossed in developing new ciphers which are highly suitable for security of information either in the personal system or in transmission through channel. Some of the ciphers suitable for data base security and web security are also attracting researchers.

To fulfill the current necessities in the field of cryptography and network security, a number of encryption algorithms have been developed and updated in the recent past[1-10], which can be found in the literature. In his investigation, Vinaya et al. have implemented a contemporary cryptographic algorithm in several variations, by name it is Play Color Cipher [11-17]. These algorithms are proven to be very strong and the generated ciphers are highly potential.

In the present investigation, we have updated the play color cipher algorithm, for this, we have involved the tree traversal methods to generate the cipher text in first phase and then we did permutation based on the key for 15 rounds.

Form the literature [18-19] we can learn that a tree is a non linear data structure primarily used to represent the hierarchical association between the data. Many software developers use these structures in organizing and designing software's into modules. Principally these structures are very useful in developing system software's.

Tress can be either general trees or binary trees. A general tree is a finite non empty set of nodes and can have any number of nodes. A binary tree is a finite set of elements that is either empty or is partitioned into three disjoint subsets. The first subset contains a single element called the root of the tree. The other two subsets themselves are binary trees, called the left sub tree and right sub tree of the original tree.

A binary tree is very useful data structure when bi directional decisions must be made at each point in a process. The advantage of a binary tree is that the item can be placed in the tree in a sorted manner. In a complete and strict binary tree the numbering is given from top to bottom and left to right and nodes must be filled from left to right[18].

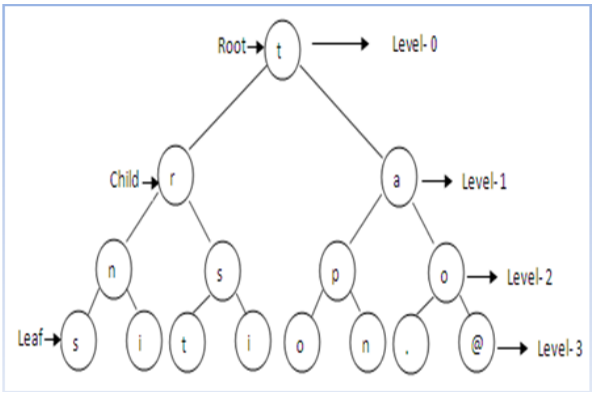


Figure 1: A Binary Tree Structure with depth four

In this no node can have more then two children and the maximum degree of a binary tree is only 2. The top most node in tree is called root node, each node (except the root) has exactly one node above it, which is called its parent and the nodes directly below a node are called its children. Node with no children is sometimes called leaves, or terminal as shown in figure -1. If it is having 'n' nodes then it contains 'n-1' edges. The maximum number of nodes of a binary tree of depth K or height H is 2^K -1or 2^H -1, (K >0).

This structure we have used in our proposed encryption algorithm for transposition and the detailed explanation is presented in section.

2. MATHEMATICAL METHODS AND OPERATIONS INVOLVED

The process of enhancing the "Play Color Cipher Algorithm" has been divided in to 4 modules for encryption:

Module1: Key selection, distribution and sub key generation algorithm.

Module2: Converting the plain text in the form of alphanumeric characters, diagrams and images etc in to rich text format.

Module3: Perform 16 rounds of transpositions on the output of module2 based on the keys generated in module1.

Module4: Carry out the color substitution on the ultimate cipher generated after last transposition. The output of this stage is the final cipher intended for the secure transmission.

Note: Reverse of this process is called the decryption

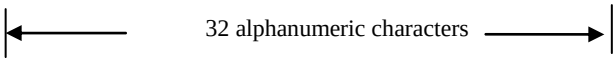
The brief explanation and the methods used in each module are explained below:

2.1 Key Selection & Distribution

In this we have used a 32 characters alphanumeric key. The key format is shown in the figure 2 and Steps involved in sub key generation algorithm is as follows:.

- Select key 'K', should be 32 alphanumeric characters, for our convenience from know on the word "alphanumeric characters" will be called as a "characters" in this paper.
- In the entered 32 characters: from LHS to RHS, the sub key generation algorithm considers out put of the first 15 characters as parameter 1 (K1), next 7 characters as parameter 2 (K2), the out put of 23rd characters (K3) will be used to select integral function and also used to select the tree traversal method for first transposition in each round of first 15 rounds. The out put of last 9 characters (K4) will be used as a key for 2nd transposition in first 15 rounds.
- There is one more key K5 will be generated by the sub key generation algorithm based on the sum of the ANSI values of the final cipher after 15th rounds, it is used as a transposition key in the final (16th) round of the encryption process.
- Keys, K1 and K2 will be passed as parameters to the function selected by K3 and the output will be the starting address K1' and Increment value K2'. These two values are used to performing color substitution on the final cipher generated after transposition.

For distributing the key from the source to destination, we have used our enhanced RSA algorithm [10] in which we have used one prime and one non negative integer.



15 Char (K1) Parameter-1 (1 to 15 char)	7 Char (K2) Parameter-2 (16 to 22 char)	1Char to select the function (K3) (23rd char)	Transposition key in 9 char (K4) (24th to 32 char)

Figure 2: Key format in 32 alphanumeric characters

Sequence of events in key distribution is:

- Encrypt K using senders (Source A) private key (PRa) for authentication ---------- 2.1
- Encrypt the result of 2.1 using receivers (User B) public key (PUb) for confidentiality. ---------- 2.2
- Send the result of 2.2 to the receiver----------2.3
- Decrypt 2.3 by using PRb ---------- 2.4
- Decrypt 2.4 by using PUa ---------- 2.5

Hence with the both authentication and confidentiality we have distributed the keys between User A and User B.

2.2 Converting the Plain Text in to Rich Text Format:

RTF is a file format standardized by Microsoft for creating formatted text files. It provides a format for text and graphics interchange that can be used with different output devices, operating environments, and operating systems. Unlike a basic text file, an RTF file can include information such as text style, size, and color. The nice thing about the RTF format is that it is a universal format, meaning it can be read by nearly all word processors.

In our research, we have used this in the first phase to convert the plain text (input) in the form of alphanumeric characters, symbols, images and diagrams, etc in to rich text format. Considered the input as shown in the figure 5, then the corresponding output is Cipher 1 as shown in the figure 7.

```
string strin = richTextBox1.Rtf;
```

2.3 Perform 16 Rounds of Transpositions:

The encryption algorithms invented so far are based on two general principles: substitution and the transposition, in this section we are mainly focusing on the transposition

The elements in the plaintext are rearranged in the transposition. These are block ciphers that change the position of the characters or bits of the input blocks. To encipher, the plaintext is broken into *n* symbols and a key specifies one of (n!—1) possible permutations. Deciphering is accomplished by using an inverse permutation which restores the original sequence. Transposition ciphers preserve the frequency distribution of single letters but destroy the diagram. These ciphers are often combined with other ciphers to produce a more secure product cipher [3].

The simplest such cipher is the **rail fence technique**, in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows.

A more complex scheme is to write the message in a rectangle, row by row and read the message column by column. But permute the order of the columns. The order of the columns then becomes the key to the algorithm. If the plain text have less number of characters in the last row to form the rectangle, then the remaining positions are filled with filler letters .Dot with @ symbol, is '.@'. This method we have used in our 16th round of the algorithm as a function F3.

In recent past, Udaya et al [17] have proven that the complete binary tree traversal methods are very useful in converting plain text in to cipher texts, if the depth of the tree is more, we can have more complicated cipher text.

Hence to involve new methods in the cryptography, we have used the tree traversal methods in our algorithm in first part of function F2 and the selection of the traversal method is based on the key K3. The tree traversal methods we have are; inorder, pre order and post order [18-19].

In our algorithm we have considered the tree with the depth – 9; thus, we can place total 511 characters in the tree. Hence the block size is 511 characters. To aid in understanding we have shown all these steps in the figures 3 and 4.

In the figure 3: L – Length of the cipher text, N- Number of blocks, Z – Is block size = 511, P – Number of Padding characters, Q – total length after padding.

To calculate the above, need to perform the following functions:

- The given input in the form of alphanumeric characters, diagrams, images, etc, is initially converted into RTF format using function F1 and considered it as Cipher 1.
- Calculate the length of the Cipher 1, consider it as –L.
- Calculate P = L % Z, if the result is zero, go to next step, else pad the cipher 1 with P digits to make the Cipher1 into desired length. For padding, use '.' (dot) with continues @ symbols.
- Calculate N= L / Z, gives us number of blocks.
- Apply tree traversal method based on K3' as a first part of F2.

  If the value of K3 is 1 - select inorder, 2- select pre order, 3 or any other number– select post order.

  In inorder, traverse the left subtree in inorder, process the root node and then traverse the right subtree in inorder.

  In preorder, traverse the root first, traverse the left subtree in preorder and then traverse the right subtree in preorder.

  In postorder, traverse the left subtree in postorder, traverse the right subtree in postorder and finally traverse the root.

- Perform permutation based on K4' as a second part of F2.

  For this permutation assign the key value, a 9digit decimal number form left to right to the tree levels from top to bottom. Read the message row by row based on the key in ascending order.

  Execute the function F2 for 15 rounds to generate more complicated cipher text to enhance the strength, as shown in figure 4.Process each block of 511 characters separately and append the outputs of each stage in sequential order. Consider the output of this stage as Cipher 2. The resultant cipher for the given input is shown in the figure 8.

- Write the Cipher 2 in a rectangle, row by row and read the message column by column based on the key K5 in ascending order. This we have considered as a function F3 as shown in the figure 4. The output of this stage is named as a cipher3 and shown in the figure 9 for the given input text shown in the figure 5
- Finally, perform the color substitution on the cipher 3. It is explained in the next sub section.

2.4 Perform the Color Substitution on the out put of Previous Step:

Substitution technique is the one in which the elements in the plaintext are replaced by other letters or by the numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

In our thesis we have performed color substitution in place of each character in the plain text. From the literature survey [3] [11] we learnt that, a computer can display 18 decillions of colors. This is why; we have chosen color substitution for encrypting the plain text in to cipher text. Because we have massive number of colors in the computer world, the length of the key can be extended as much as we need.

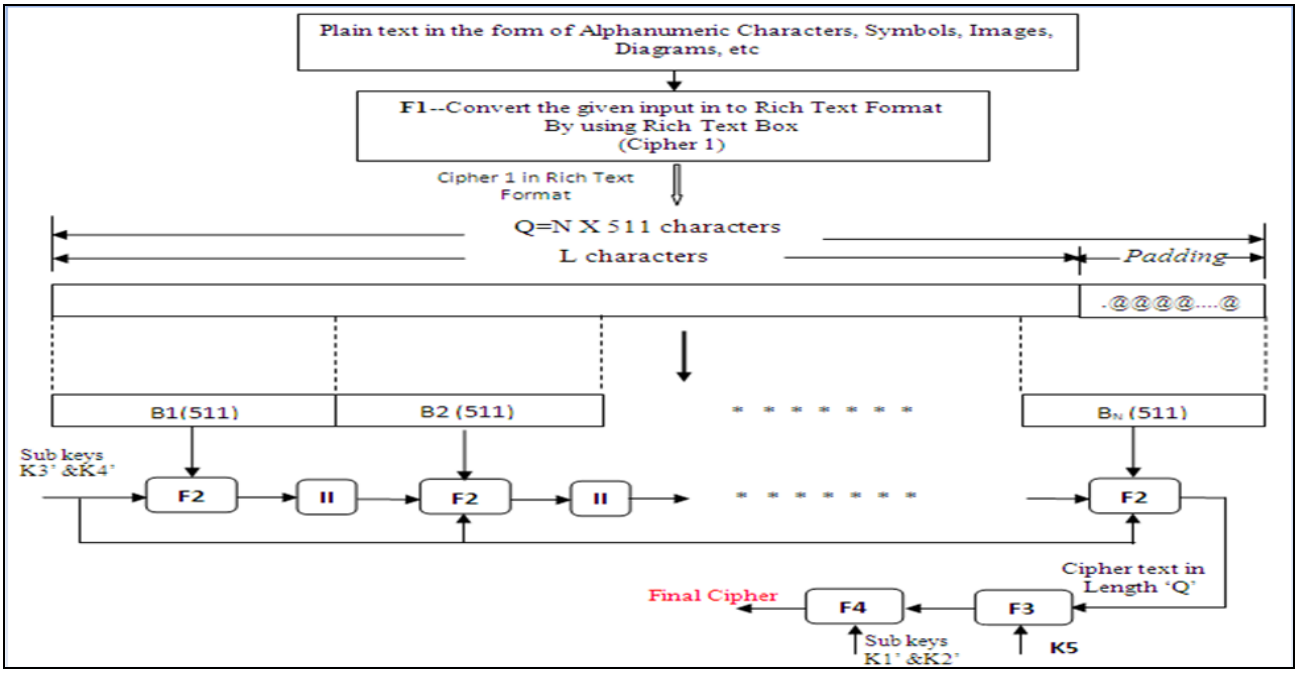


Figure 3: Block Cipher Generation Using an Enhanced Play Color Cipher Algorithm

To make the stronger cipher, instead of continues color assignment, we have involved the modular and integral functions to generate starting address and a random increment value. The selection of modular or integral function is based on the value of K3' and the color substitution is based on the keys K1', K2'. These keys are generated by the sub key generation algorithm. The steps involved in color substitution algorithm are:

- Using starting address (K1') and increment value(K2') prepare the color array.
- Assign colors to the characters

-Create the Font object for the image text drawing.

-Create a graphics object to measure the text's width and height.

Create the bmpImage again with the correct size for the text and font.

-Add the colors to the new bitmap, Set Background color and draw the text. The resultant cipher for the given input is shown in the figure 11.

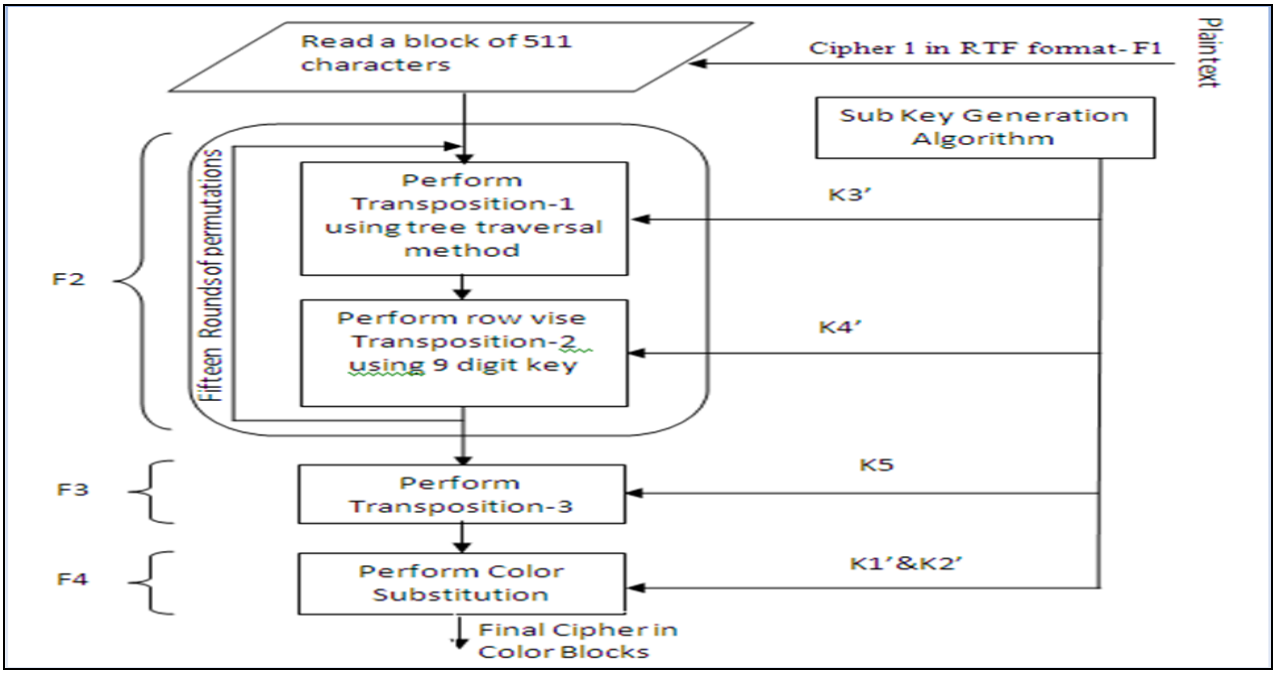


Figure 4: A Flow Chart for Encryption Process Using an Enhanced Play Color Cipher Algorithm

3. DEVELOPMENT OF THE CIPHER

In this we have considered a plain in the form of alphanumeric characters, symbols, images and diagrams, etc as shown in the figure 5. For the development of the cipher we have several phases in this algorithm as shown in the figure 4.

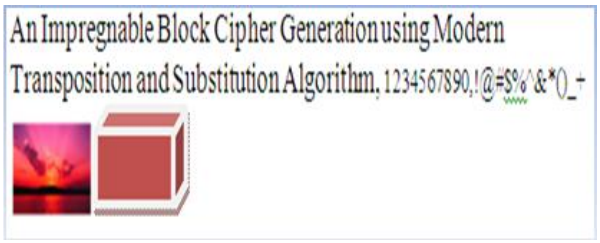


Figure 5: Plain text 1 considered for encryption

To exhibit and prove a strong avalanche effect we have considered another plain text in which we have changed a single character in the first plain text as shown figure 6. It is to be noted that only the first character in the plain text is differ in figure 5 & 6, which is character A is changed to I.

A desirable property of any encryption algorithm is that a small change in either the key or the plain text should produce a significant change in the cipher. In particular, a change in one bit / character of the plain text or key should produce a change in many bits / characters of the cipher text. The same we have proven in this algorithm. The resultant output after changing a single character in the first input is as shown in the figures 10 and 12.

Figure 6: Plain text 2 considered for encryption

Figure 7: a snap shot of converted Cipher text in Rich text format C1, out of 20 pages of out put

Figure 8: a snap shot of the output after 15th transposition of C1 to C2, out of 20 pages of out put

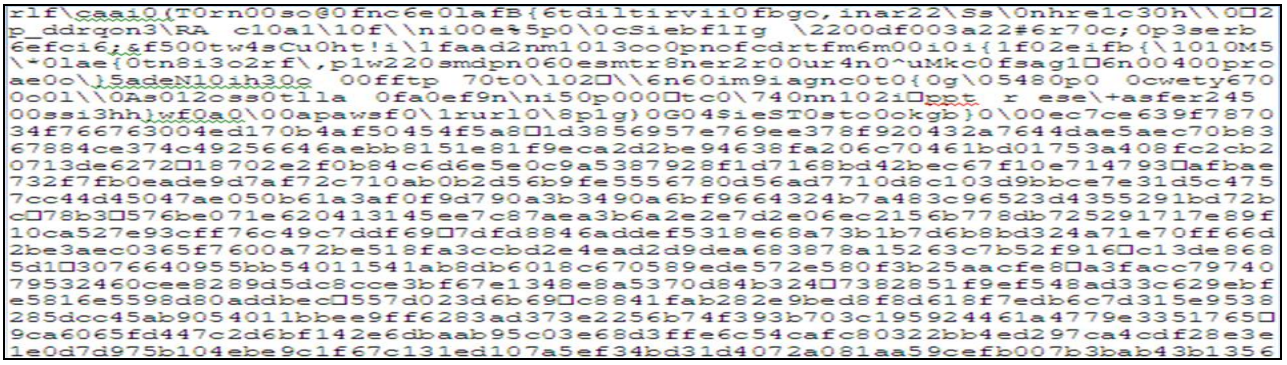


Figure 9: a snap shot of 16th transposition (C2 to C3), out of 20 pages of out put

Figure 10: a snap shot of 16th transposition (C2 to C3) out of 20 pages of out put after changing one character in the plain text input shown in figure 6.

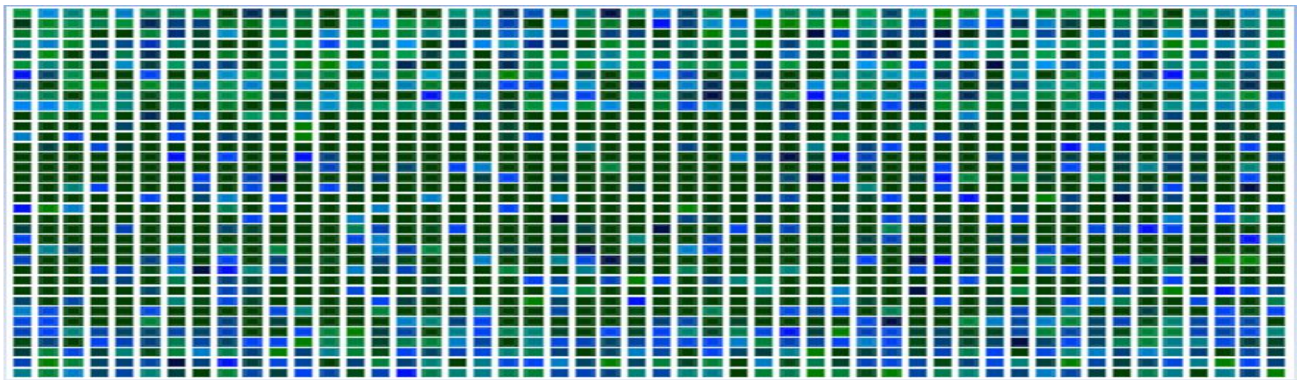


Figure 11: a snap shot of color substitution on C3 to produce final cipher C4 using play color cipher

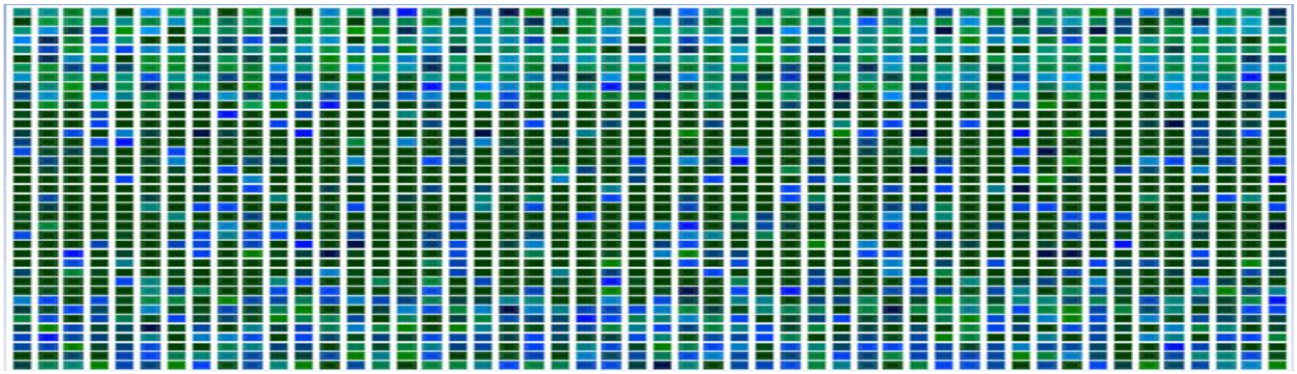


Figure 12: a snap shot of color substitution on C3 to produce final cipher C4 using play color cipher After change a single character in the plain text input shown in figure 6.

4. CRYPTANALYSIS

The cryptanalyst assails which are usually measured in the literature of Cryptography are:

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

In this investigation the key 'K' is a 32 digits alphanumeric character. From the Left hand side first 22 characters (15 + 7) are used to compute the starting address and increment value for color substitution, next character (23^{rd}) is used to select integral function and tree traversal method, and the remaining 9 characters (24^{th} to 32 positions) are used as a key for permutation. In this we have three possibilities:--

Case 1: key can be only characters: Because, the alphabets are only 26, to enter 32 characters in the key, obviously some characters will be repeated. In these circumstances:

Maximum number of Keys = $(26)^{32} = 1.9 \text{ X } 10^{45}$ Keys

If the time required for resolving of the plain text for one value of the key in the key space is taken as 10^{-3} seconds, then time required for obtaining the plain text by considering all the possible keys in the key space is $1.9X10^{45}X10^{-3}$

If we perform one encryption per micro second it takes

$$\frac{1.9 \text{ X } 10^{45} \text{ X } 10^{-3}}{365 \text{ X } 24 \text{ X } 60 \text{ X } 60} = 6 \text{ X } 10^{35} \text{ Years}$$

Case 2: Out of 32 characters, first 26 can be characters and the remaining 6 can be numbers between '0 to 9'. In this situation:

Maximum number of Keys = $(26)^{26} + (10)^6 = 6 \text{ X } 10^{36}$ Keys. If we perform one encryption per micro second it takes

$$\frac{6 \text{ X } 10^{36} \text{ X } 10^{-3}}{365 \text{ X } 24 \text{ X } 60 \text{ X } 60} = 1.9 \text{ X } 10^{27} \text{ Years}$$

Case 3: key can be only numbers: Because the key length is 32 and the numbers can be any decimal number between '0 to 9', naturally the numbers will be repeated in the key. In this condition:

Maximum number of keys= $(10)^{32}$.

if we perform one encryption per microsecond it takes:

$$\frac{10^{32} \text{ X } 10^{-3}}{365 \text{ X } 24 \text{ X } 60 \text{ X } 60} = 3.1 \text{ X } 10^{29} \text{ Years}$$

In all three cases the number of possible keys was large, and the time required to try all probable keys is too high. Brut force attack is not possible and 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 texts. Moreover

the input to the color substitution algorithm is not the actual plaintext rather it was permuted 16 rounds in the process.

With 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. Other then all these, to prove that the cipher is potential one, it is mandatory that the cipher should confirm a strong avalanche. To reveal and confirm a strong avalanche effect we have considered one more plain text in which we have changed a single character in the first plain text as explained in section 3 and it is shown figure 6.

It is noticeable that the only first character in the plain text is differed in figure 5 & 6. We have also encrypted the new plain text with the same key 'K', with the same procedure and experimentally more then 90% of the cipher in the second experiment is differ from the first experiment. A snap shot of the 16^{th} transposition and the color substitution of both the experiments were shown in the figures 9, 10, 11and 12. In view of the above conversation, we conclude that the Cipher is a potential one.

5. RESULTS

The enhanced play color cipher algorithm works with 32 alphanumeric key and it is confirmed that it is comfortably converting all kinds of text, symbols, diagrams and images as shown in the figure 13 and 14.

The greatness of this algorithm is that it works in 16 rounds, and supports a block size of 511 characters, is 2044bits in binary. In this, we have used three types of permutations and it's a new dimension in the cryptography. To improve the

secrecy we can even increase the block size to 1023 characters. The process of conversion with examples was explained. The strength of the any algorithm depends on key rather then the algorithm, in this the length of the key is 32 characters and proven that it is far from crypt analysis attacks and especially it gives a strong avalanche effect.

6. CONCLUSION

In this paper we have developed an enhanced play color cipher algorithm i.e. a symmetric block cipher generation algorithm using multiple transformation and color substitution. In this we have used three types of transposition algorithms to improve the complexity and have 16 rounds of permutations. We have involved 32 alphanumeric characters as a dynamically permuted key with integral functions. We have proven that it can encrypt / decrypt all kinds of text, numbers, symbols, images and diagrams with example as shown in figure 13 and 14. For performing one encryption per micro second it takes minimum 1.9 X 10^{27} years.

For transferring key from sender to receiver we have used an enhanced RSA algorithm. Especially we have concentrated on the sub key generation algorithm, explained the three possible cases and its time complexity. The brief explanation and the advantages of RTF were given; production of cipher text in all the phases was explained with example.

Lastly, we conclude that, with the 32 characters alphanumeric key, the cipher is very strong and the algorithm is potential one.

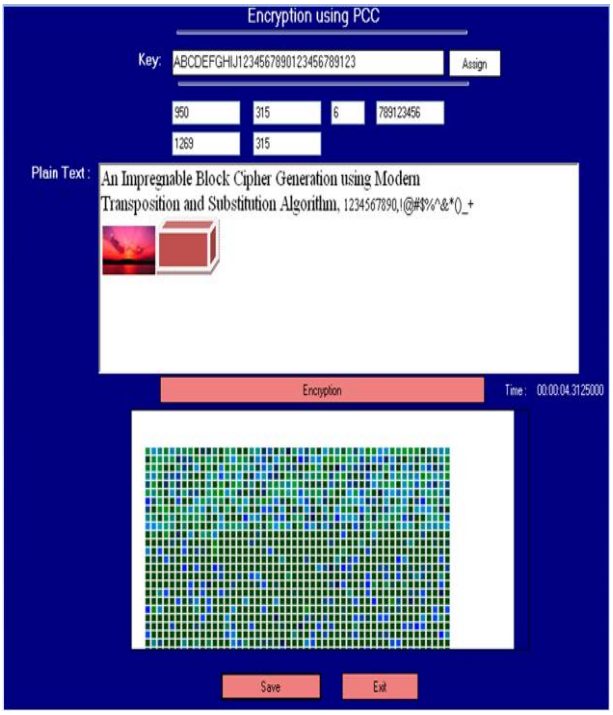


Figure 13: Encryption using an enhanced PCC with 32 alphanumeric key

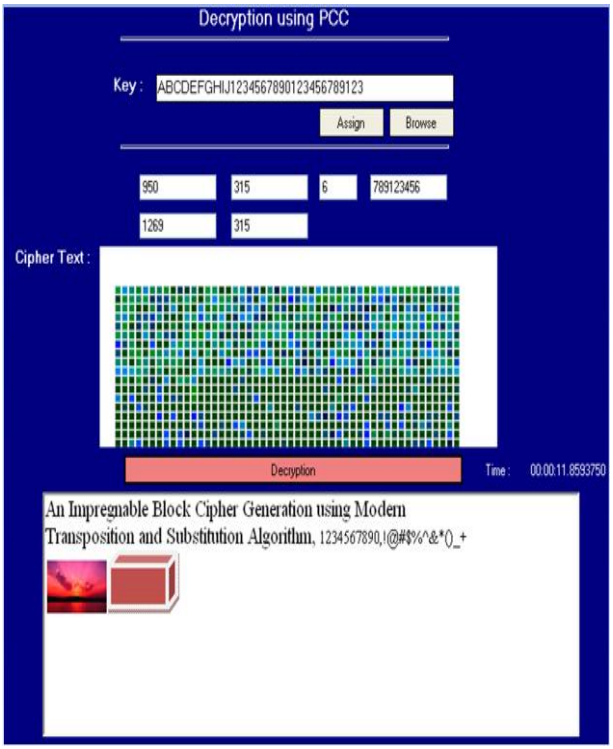


Figure 14: Decryption using an enhanced PCC with 32 alphanumeric key

7. ACKNOWLEDGMENTS

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

He also likes to thank the principal, management of AZCET and JNTUH for providing all the facilities.

It is great pleasure and privilege to convey my deep regards to all my family members for their overwhelming support all along. Special thanks to IJCA for allowing us to use its template.

8. REFERENCES

[1] Denning, D., F. Ayoub , " Cryptographic techniques and network security", IEEE proceedings, Vol 131, 684-694,Dec 1984.

[2] Stalling, " Cryptography and network security", Fourth edition, LPE, 81-7758-774-9.

[3] Ravindra babu, Udayakumar and Vinaya babu " A Survey on Cryptography and Steganography Methods for Infromation Security", IJCA, 0975-8887, Vol 12, No-2, Nov2010.

[4] Ravindra, Udaya and Vinaya babu, An Improved Playfair Cipher Cryptographic Substitution Algorithm, JARCS, (0976-5697), Volume 2, No-1, Jan-Feb 2011.

[5] Ravindra, Udaya and Vinaya babu, An Extension to traditional Playfair Cipher Cryptographic Substitution Method, IJCA, (0975 – 8887), Volume 17, No-5, March 2011.

[6] Ravindra Babu, Udaya Kumar and Vinaya babu, An Enhanced Poly alphabetic Cipher using Extended Vigenere Table, IJARCS, (0976-5697),Volume 2, No.2, Mar-April 2011.

[7] Ravindra Babu, Udaya Kumar and Vinaya babu, An Enhanced and Efficient Cryptographic Substitution Method for Information Security, IJMA, Archive-2 (10), 2078-2083, Oct 2011.

[8] Ravindra, Udaya Kumar and Vinaya babu, A Contemporary Poly alphabetic Cipher using Comprehensive Vigenere Table, WCSIT,(2221-0741), Vol.1,No 4, 167-171,2011

[9] Alaa, Bilal, A fast approach for braking RSA cryptosystem, WCSIT,2221-0741,Vol 1,No 6, 260-263, 2011.

[10] Ravindra Babu, Udaya Kumar and Vinaya babu, An Enhanced RSA public key cryptographic algorithm, communicated to IJARCS, 0976-5697, Vol-2, No 5, 497-499, Sep-Oct 2011.

[11] Ravindra, Udaya and Vinaya babu, A Paper on "a block cipher generation using Color Substitution" is published in International Journal of Computer Applications, (0975 – 8887), Volume 1- No-28, US, @2010.

[12] Ravindra Babu, Udaya Kumar and 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.

[13] Ravindra Babu, Udaya Kumar and Vinaya babu, A More secure block cipher generation involving multiple transposition and substitution with a large key, IJARCS, (0976-5697), Vol 2, No 2, Mar-April 2011.

[14] Ravindra Babu, Udaya Kumar and Vinaya babu, A Modern Play color cipher involving dynamic permutated key with iterative and modular arithmetic functions, IJARCS, (0976-5697), Vol 2, No 3, May-June 2011.

[15] Ravindra Babu, Udaya Kumar and Vinaya babu, A Variable length block cipher generation using modern play color cipher algorithm with alphanumeric key and iterative functions, published in the proceedings of ICNICT-11, ISBN 978-93-81126-21-1, No 56, 288-293.

[16] Ravindra Babu, Udaya Kumar and Vinaya babu, An Unassailable Block Cipher generation with an extended play color cipher, concerning a large alphanumeric key, modular arithmetic and integral functions, (0975-8887),IJCA, Volume 28-no.9, August 2011.

[17] Ravindra Babu, Udaya Kumar and Vinaya Babu, A Block Cipher Generation Using an Innovative Permutation Algorithm, Communicated to International Journal of Mathematical Archive, ISSN-2229-5046.

[18]Yedidyah, Moshe J. Augenstein, M.Tenebaum, Data Structures Using C and C++, 2nd Edition, 249-319, ISBN-81-203-1177-9, Jan 2000.

[19]Ashok N. Kamthane, C and Data Structures, Pearson Education, ISBN 81-297-0261-4, pages:572-576, First edition, 2004.