International Journal of Mathematical Archive-3(4), 2012, Page: 1443-1447

IJMA Available online through www.ijma.info ISSN 2229 – 5046

A BLOCK CIPHER GENERATION USING AN INNOVATIVE PERMUTATION ALGORITHM

Kallam Ravindra Babu[1*], Dr .S. Udaya Kumar[2] and Dr. A. Vinaya Babu[3]

[1]Research Scholar (JNTUH), HOD CSE&IT, AZCET, Mancherail, (A.P), India

[2]Principal, M. V. S. R. Engineering College, Hyderabad, (A.P.), India

[3]Principal, JNTU College of Engineering, JNTUH, Hyderabad, (A.P), India

E-mail: rbkallam2510@gmail.com, uksusarla@rediffmail.com, avb1222@gmail.com

(Received on: 27-03-12; Accepted on: 17-04-12)

ABSTRACT

The aim of our research is to develop a new transposition algorithm for generating a block cipher. The plaintext considered in this method can be the combination of any ASCII characters. A brief explanation about the transposition algorithms was given. The results shown at the end of the presentation will prove scope and strength of the algorithm. Some of the cryptanalysis attacks were discussed and proven that the cipher is potential one.

Keywords: *Cryptanalysis, block cipher, encryption, decryption, algorithm, transposition, permutation, binary tree, inorder, preorder, postorder, DES, EFT, substitution.*

1. INTRODUCTION

The most customary and common approach to counter the threats to information security is encryption. Even though it is very powerful, the cryptanalysts are very intelligent and they were working day and night to break the ciphers. The threat to the information can be either it is in the transmission through communication channel or in the system.

Many Scientist were doing research on the existing methods to make more stronger and unbreakable ciphers by enhancing them [4-16]. 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 [3]. All encryption algorithms invented so far are based on two general principles: the transposition, in which elements in the plaintext are rearrange and the substitution in which the element in the plain text is mapped into another element. 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 [4-10].

To fulfill the present necessities and to face the cryptanalyst in the field of the communication and data security, we need stronger Cryptographic algorithms. For this it is must and should that to invent new Cryptographic algorithms rather then updating the existing one all the time. Part of it we have chosen tree structures for performing transposition. Form the history [17] we can learn that a tree is a non linear data structure mainly used to represent the hierarchical relationship between data. In real time it has been used by the developers to organize and design software into a modular fashion. Especially these structures play a vital role in compiler constructions, database design, operating systems and other system software's.

Tress are classified into two types, they are General trees and Binary trees. A general tree is a finite non empty set of nodes and can contain 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 two-way 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.

Corresponding author: Kallam Ravindra Babu[1*], *E-mail: rbkallam2510@gmail.com

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 3.

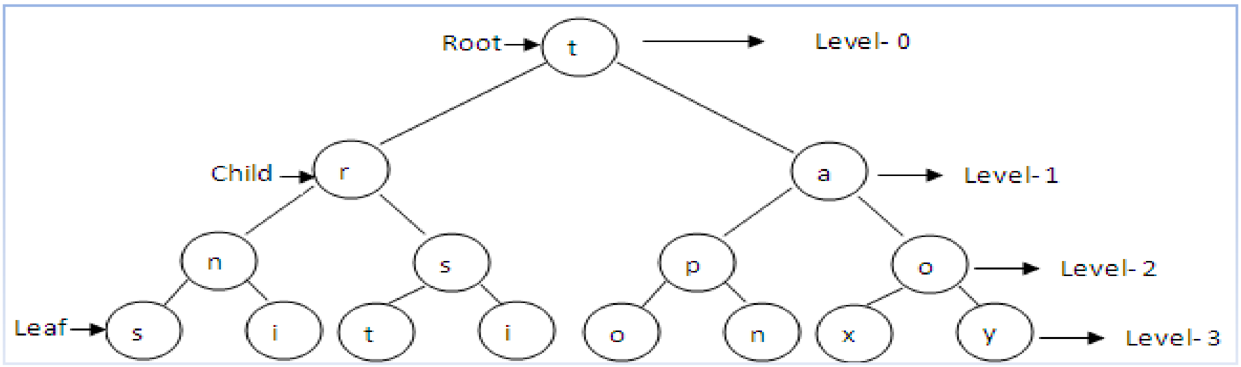
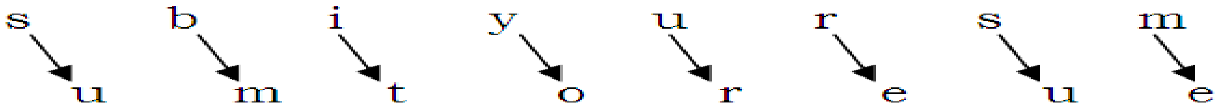


Figure: 1 A Complete Binary Tree with four levels

2. EXISTING TRANSPOSITION METHODS

It Transposition ciphers are block ciphers that change the position (or the sequence) 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.

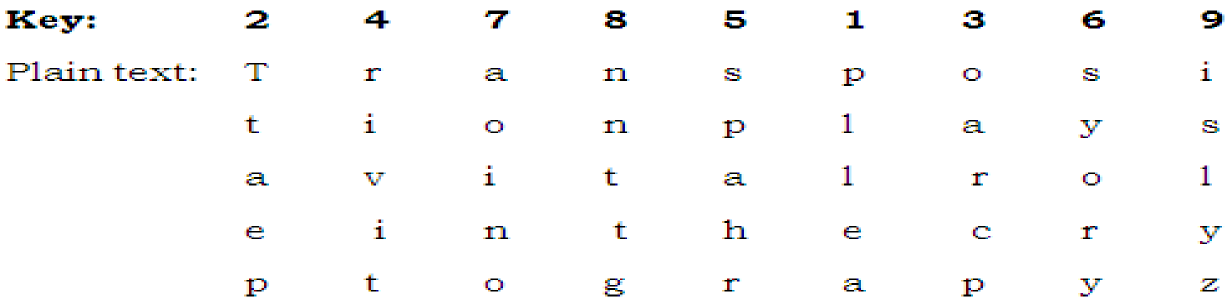
The simplest such cipher is the **rail fence technique**, in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message "*submit your resume*" with a rail fence of depth 2, we can write it as mentioned below:



The encrypted message is: SBIYURSMUMTOREUE

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 has less number of characters in the last row to form the rectangle, then the remaining positions are filled with filler letter 'z'

A plain text considered in the example is *"Transposition plays a vital role in the cryptography"*, it has been placed in the table as shown below, and to make it in to desired length the last position in the last row is filled with the character 'z'. The secret key and the corresponding cipher text are shown below:



Key:	**2**	**4**	**7**	**8**	**5**	**1**	**3**	**6**	**9**
Plain text:	T	r	a	n	s	p	o	s	i
	t	i	o	n	p	l	a	y	s
	a	v	i	t	a	l	r	o	l
	e	i	n	t	h	e	c	r	y
	p	t	o	g	r	a	p	y	z

Cipher text: plleaTtaepoarcprivietspahrsyoryaoinonnttgislyz

By performing more then one stage of permutation we can enhance the strength of the cipher, the result is more complex permutation that is not easily reconstructed.

3. PROPOSED TRANSPOSITION ALGORITHM

To give the new dimension to the cryptographic algorithms, we have used Binary tree structure and its traversal methods along with some modifications for transposing plain text into cipher text. On the trees we can perform some of the operations like, displaying the elements, search for a given key, inserting, deleting an element and copying a tree, etc by using tree traversal methods. Visiting each node exactly once in systematic way is known as traversing. Binary trees can be traversed in three different ways: Inorder, Preorder and 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.

To aid in understanding, considered a plaintext “transposition” as shown in the figure 1. To make the complete binary tree of level 4, we need 15 elements, but in our plaintext we have only 13 elements, hence, we propose to pad the characters at the end of the plain text to make it to desired length and thus the last two characters are padded with the filler letter ’x’. By applying the tree traversal techniques the result is as shown below:

Plain text:	transposition
Plaintext after padding:	transpositionxx
Inorder:	snirtsitopnaxox
Preorder:	trnsistiaponoxx
Postorder:	sintisronpxxoat

From the above results we can notice that, without any loss the plain text is permuted in to an unintelligible text and by reversing it we can get back our plain text. Even though these are tree traversal methods, they work like converting plain text in to cipher text by permutation (encryption) and the reverse of it is called decryption.

By executing more then one stage of transposition we can extend the strength of the cipher, the result is more complex permutation that is not easily breakable. Keeping this in view, initially, we propose to use the tree traversal method based on first digit in the key and consider this as first transposition (T1) and then perform second transposition based on remaining 9 digits in the key (T2). If we consider this as a single round, we can perform ‘n’ number of rounds to extend the strength of the cipher with number of variations in algorithm.

4. DEVELOPMENT OF THE CIPHER

In our proposed algorithm, we have considered a complete binary tree with the depth of 9 levels, hence, maximum number of characters / elements we can place in the tree are 2^n -1 that is 2^9-1= 511. For increasing the confusion level in cipher we have also used a 10 digit decimal key. In this the first digit selects one of the three traversing techniques and the remaining 9 digits are assigned to the tree levels from top to bottom. Because it can support at max 511 elements we can say that the block size of the plain text is 511. If the length of the plain text is more then 511characters, then the plain text will be divided in to the number of blocks with the length of 511 characters. If the length of the last block is less then 511 then it will be padded to make it to the desired length.

Sequence of events in our algorithm is:
Step 1: Read the plain text in the form of ASCII characters

Step 2: Divide the plain text in to the blocks of 511 characters and process one block at a time

Step 3: If the number of characters in the block are less then 511, pad the plaintext with the filler latter ’x’ to make it to the desired length.

Step 4: Read the key in 10 digit decimal numbers

Example: 1456738291

Step 5: Select the tree traversal method based on first digit in the key

If the number is 1- Inorder, 2- Pre order and 3 or any other number select Post order

In the example it is Number-1 and hence Inorder will be selected

Step 6: Perform transposition based on the tree traversal method, consider this as **Cipher 1**

Step 7: Fill the tree with the characters in Cipher-1 from top to bottom and left to right in sequential order

Step 8: Assign the remaining key elements to the tree levels from top to bottom in the sequence order

In the example it is "456738291" and 9 levels in the tree ate "123456789"

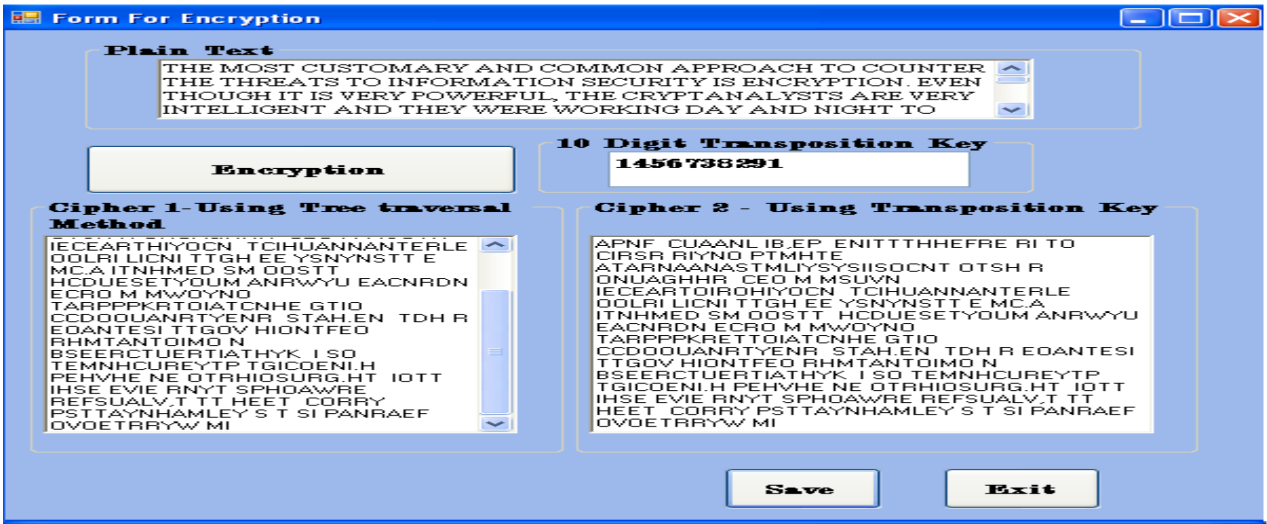
Hence, the assignment is as follows: 1-4, 2-5, 3-6, 4-7, 5-3, 6-8, 7-2, 8-9, 9-1

Step 9: Read and print the elements in the rows based on the above 9 digit transposition key, consider this as **Cipher 2** To read the elements, select the rows based on the transposition key in ascending order and read the complete elements in that row, in the above example the sequence of rows selected are: 9,7,5,1,2,3,4,6,8. In this way, the algorithm encrypts the plaintext twice by using tree traversal method and the transposition key. By exact reverse of it we can again get the plain text.

5 RESULTS AND CONCLUSION

It is observed that the algorithm is successfully working, it could able to encrypt and decrypt the plain text in the form of alphanumeric characters, symbols, or any ASCII character. To prove that it is working well we have considered plain text and a 10 digit key and the corresponding screen shots has shown in the figures2 and 3. It is also noticed that the conversion has taken place without any loss of information.

Figure: 2 A Screen Shot of Encryption Process using Tree Transposition Algorithm



Plain Text

```
THE MOST CUSTOMARY AND COMMON APPROACH TO COUNTER
THE THREATS TO INFORMATION SECURITY IS ENCRYPTION. EVEN
THOUGH IT IS VERY POWERFUL, THE CRYPTANALYSTS ARE VERY
INTELLIGENT AND THEY WERE WORKING DAY AND NIGHT TO
```

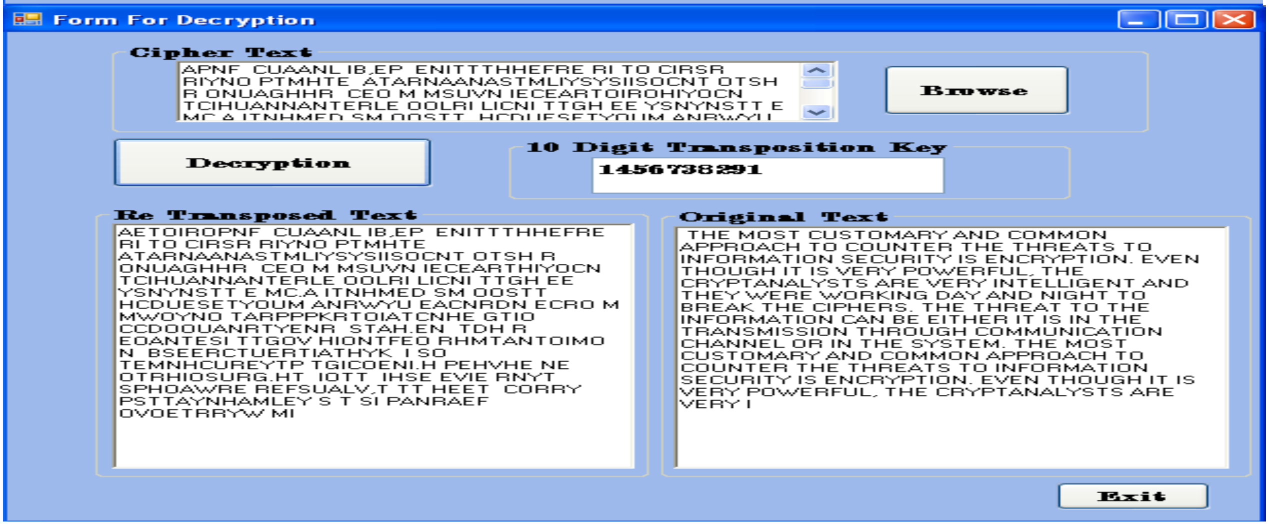
10 Digit Transposition Key: 1456738291

Cipher 1-Using Tree traversal Method

```
IECEARTHIYOCN  TCIHUANNANTERLE
OOLRI LICNI TTGH EE YSNYNSTT E
MC.A ITNHMED SM OOSTT
HCDUESETYOUM ANRWYU EACNRDN
ECRO M MWOYNO
TARPPPKRTOIATCNHE GTIO
CCDOOUANRTYENR  STAH.EN  TDH R
EOANTESI TTGOV HIONTFEO
RHMTANTOIMO N
BSEERCTUERTIATHYK  I SO
TEMNHCUREYTP TGICOENI.H
PEHVHE NE OTRHIOSURG.HT  IOTT
IHSE EVIE RNYT SPHOAWRE
REFSUALV,T TT HEET  CORRY
PSTTAYNHAMLEY S T SI PANRAEF
OVOETRRYW MI
```

Cipher 2 - Using Transposition Key

```
APNF  CUAANL IB,EP  ENITTTHHEFRE RI TO
CIRSR RIYNO PTMHTE
ATARNAANASTMLIYSYSIISOCNT OTSH R
ONUAGHHR  CEO M MSUVN
IECEARTOIROHIYOCN  TCIHUANNANTERLE
OOLRI LICNI TTGH EE YSNYNSTT E MC.A
ITNHMED SM OOSTT  HCDUESETYOUM ANRWYU
EACNRDN ECRO M MWOYNO
TARPPPKRETTOIATCNHE GTIO
CCDOOUANRTYENR  STAH.EN  TDH R EOANTESI
TTGOV HIONTFEO RHMTANTOIMO N
BSEERCTUERTIATHYK  I SO TEMNHCUREYTP
TGICOENI.H PEHVHE NE OTRHIOSURG.HT  IOTT
IHSE EVIE RNYT SPHOAWRE REFSUALV,T TT
HEET  CORRY PSTTAYNHAMLEY S T SI PANRAEF
OVOETRRYW MI
```



Cipher Text

```
APNF  CUAANL IB,EP  ENITTTHHEFRE RI TO CIRSR
RIYNO PTMHTE  ATARNAANASTMLIYSYSIISOCNT OTSH
R ONUAGHHR  CEO M MSUVN IECEARTOIROHIYOCN
TCIHUANNANTERLE OOLRI LICNI TTGH EE YSNYNSTT E
MC.A ITNHMED SM OOSTT  HCDUESETYOUM ANRWYU
```

10 Digit Transposition Key: 1456738291

Re Transposed Text

```
AETOIROPNF  CUAANL IB,EP  ENITTTHHEFRE
RI TO CIRSR RIYNO PTMHTE
ATARNAANASTMLIYSYSIISOCNT OTSH R
ONUAGHHR  CEO M MSUVN IECEARTHIYOCN
TCIHUANNANTERLE OOLRI LICNI TTGH EE
YSNYNSTT E MC.A ITNHMED SM OOSTT
HCDUESETYOUM ANRWYU EACNRDN ECRO M
MWOYNO TARPPPKRTOIATCNHE GTIO
CCDOOUANRTYENR  STAH.EN  TDH R
EOANTESI TTGOV HIONTFEO RHMTANTOIMO
N  BSEERCTUERTIATHYK  I SO
TEMNHCUREYTP TGICOENI.H PEHVHE NE
OTRHIOSURG.HT  IOTT  IHSE EVIE RNYT
SPHOAWRE REFSUALV,T TT HEET  CORRY
PSTTAYNHAMLEY S T SI PANRAEF
OVOETRRYW MI
```

Original Text

```
 THE MOST CUSTOMARY AND COMMON
APPROACH TO COUNTER THE THREATS TO
INFORMATION SECURITY IS ENCRYPTION. EVEN
THOUGH IT IS VERY POWERFUL, THE
CRYPTANALYSTS ARE VERY INTELLIGENT AND
THEY WERE WORKING DAY AND NIGHT TO
BREAK THE CIPHERS. THE THREAT TO THE
INFORMATION CAN BE EITHER IT IS IN THE
TRANSMISSION THROUGH COMMUNICATION
CHANNEL OR IN THE SYSTEM. THE MOST
CUSTOMARY AND COMMON APPROACH TO
COUNTER THE THREATS TO INFORMATION
SECURITY IS ENCRYPTION. EVEN THOUGH IT IS
VERY POWERFUL, THE CRYPTANALYSTS ARE
VERY I
```

Figure: 3 A Screen Shot of Decryption Process using Tree Transposition Algorithm

To enhance the strength of the cipher we can have, more number of rounds with different keys at each round, length of the block can be extended to 1023 or more, length of the key can be improved to avoid brut force attack. When the plaintext block is less then the desired length of 511characters, we did padding with the filler letter 'x', it provides partial traffic flow confidentiality by concealing the actual length of payload when the data is under transmission through communication channel. With all this we can conclude that the algorithm is potential one and have lot of scope in cryptography and network security.

6 ACKNOWLEDGMENTS

The first authors like to thank the management and Principal of AZCET and JNTU for providing all the resources and also like to thank the editor and review committee of IJMA for their valuable suggestions.

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

****