Generation of A Novel Cryptographic Algorithm for Implementation "Play Color Cipher" Substitution Technique with Unicode Transformation Format-8

[1]Pritha Johar
Student of ME in IT, MITM Indore, MP, India.

[2] Mohsin Sheikh,
Assistant Professor in Department of Computer Science & Engineering, MITM Indore, MP, India.

[3]Santhosh Easo,
Associate Professor in Department of Computer Science & Engineering, MITM Indore, MP, India.

[4]K K Johar
Professor & Head, Department of Physics Computer Science, Govt PG College, Khargone, MP, India.

Abstract

In this paper a novel block cipher is developed with play color cipher algorithm. In it a alphanumeric key of 32 character is used with transposition and substitutions. These mutate the plain text by many ways before cipher text takes the shape. The encryption, decryption, key generation is explained with suitable example. The cipher is very strong as it is indicated by examining the cryptanalysis.

General Terms-
Decillions, Block cipher, Play color cipher, Encryption, Decryption, Cryptanalysis, Algorithm.

Key words-
Symmetric block cipher, PCC-Play Color Cipher, Substitution, Permutation, PUA-Public key of User A, PUB-Public key of User B,PRA-Private key of User A,PRB-Private key of user B,RSA algorithm.

1. Introduction

In literature number of cryptographic algorithms have been reported[1,2] Uday et al. developed play color cipher [3],[4,5,6].Permutation,iteratioin,transposition, substitution are used to strengthen the cipher. In present paper we have used a 32 character alphanumeric key with UTF-8 to exhibit language independent cipher & proven that it is safe from known cryptanalytic attack.

2. Selection & Distribution Of Key

The sub key generation algorithm at al Key format are given in Table 1 & flow charts figure-5.Key transfer from source to destination is represented by figure 2.

(i) Select "32 character alphanumeric key", K.

(ii) Sub key K1, considered first 15 characters, K2 has characters from 16 to 23,K3 has characters from 23rd to last 10 characters.

(iii) 15 characters of key K1 are parameters to generate color matrix, 7 characters of key K2 for increment the color value & key K3 is used for color substitution.

(iv) Use RSA public key encryption algorithm for key distribution as shown in figure -2.

(v) Encrypt K using private key PRA of source A for authentication-2.1.

(vi) Encrypt the result of 2.1 using public key of receiver PUB for confidentiality-2.2.

(vii) Send the result of 2.2 to the receiver-2.3.

(viii) Decrypt 2.3 by using PRB----------2.4.

(ix) Decrypt 2.4 by using PUA---2.5.

Table 1- Key format in 32 alphanumeric characters

K-32 character long alphanumeric key		
K1 1 to 15 character 15 character long	K2 16 to 22 character 7 character long	K3 23 to 32 character 10 character long

3. Development Of Cipher & Results

We have considered a block of plaintext in the form of alphanumeric characters & special symbols as shown in figure 1[7].

ABCDabcd1234!@#$

Figure-1 plaintext in alphanumeric form

- **3.1.-Conversion of plain text into UTF-8-**

All types of characters, numbers, and symbols converted into an UTF-8(Unified text format -8) character format. The plain text shown in figure 1 is a combination of characters, numbers and special symbols is converted into cipher text and snap shot of which is shown in figure 5 named C1.

- **3.2-Character matrix-**
Utf-8 characters are changed into a matrix in square form. These characters are useful for any known language of the world. Here we are using only English language character set, show in Figure 5.

- **3.3-Color matrix-**
[8,9]From the character matrix of 3.2 by using key K1 and its ASCII value, key K2 for increment of color with its ASCII value a color matrix in created shown in figure 5.

3.4-Play Fair Cipher-
Key K3 is used in play fair algorithm for transposition of characters in Character matrix. We apply play fair cipher on C1 and output will be C2.

- **3.5-Transposition-**
Transposition is process in which order of the characters is changed so that it spells out in the different way and makes the cipher strong. Key K3 is generated from last 10 character of main key K.K3 operates on C2 and produces C3.

- **3.6-Color substitution-**
In PCC4 each character,(symbols, numbers(0-9)) ,small and capital letters, different types of letters is substituted by a color block from 18 decillions colors[5] formed in the computer world. To make cipher strong we have used ARGB with 256x256x256x256=4228256625 colors. Substitution is more complicated with key K1 & key K2 (15+7=22 characters). Snap shots of color substitution on C3 to produce final cipher C4 is shown in figure 7.Here we put color value at a place of particular character.

We have developed the separate algorithm for images & diagrams also in which these are used as text.

4. Cryptanalysis

Normally the cryptographic attack in literature is focused as below:
Cipher text attack only
Known plain text attack

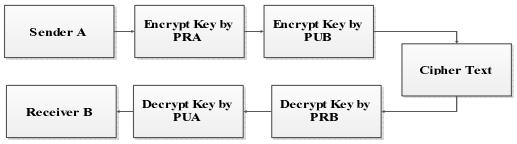

Figure 2-Key Transmission by RSA

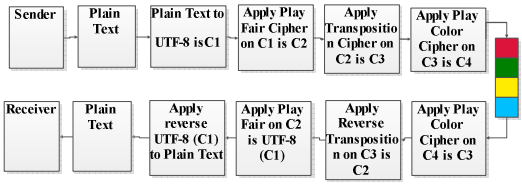

Figure 3- Block Diagram of Play Color Cipher Using UTF-8

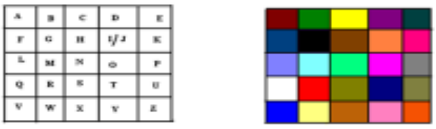

Figure 4- Charater & Color Matrix

Chosen plain text attack
Chosen cipher text attack
In this paper a 32 character long key K is sub divided into K1, K2 & K3 key with 15,7 & 10 characters respectively. We have the following two different possibilities.

Case 1: [5,6]In English language 26 characters and 10 numbers, where in Hindi language or Devnagri it includes it's all symbol for grammar have 117 character and 10 number. In English maximum number of key= $(26)^{32}=1.9X10^{45}$In Devnagri maximum number of key= $(117)^{32}=1.5X10^{66}$.

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

In English maximum number of key= $(26)^{32}=1.9X10^{45}X10^{-3}$ second
In Devnagri maximum number of key= $(117)^{32}X10^{-3}=1.5X10^{66}X10^{-3}$

If we perform one encryption per second it takes

$$\frac{1.9X10^{45}X10\text{-}3}{365X24X60X60} = 6X10^{35} \text{ years in English}$$

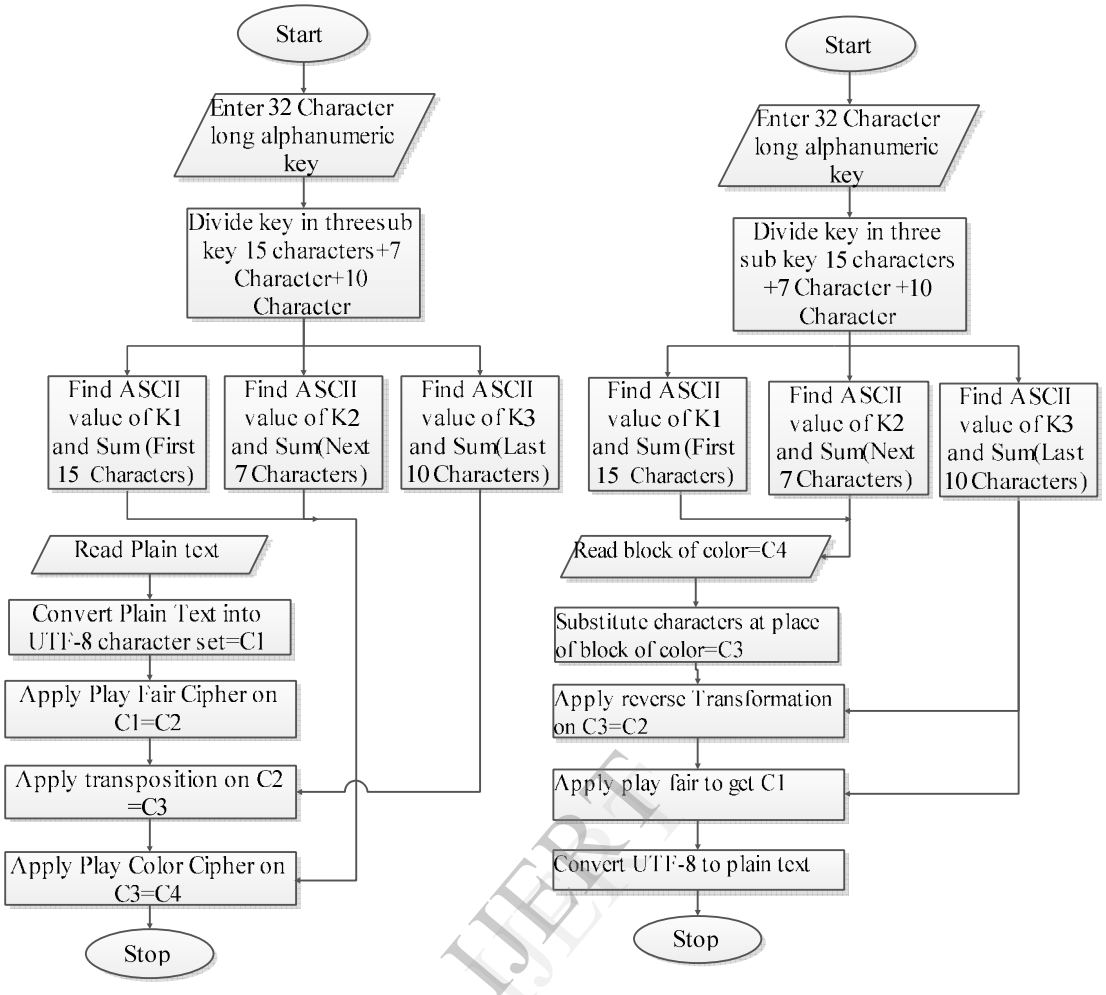

Figure-5 Encryption Decryption Algorithm

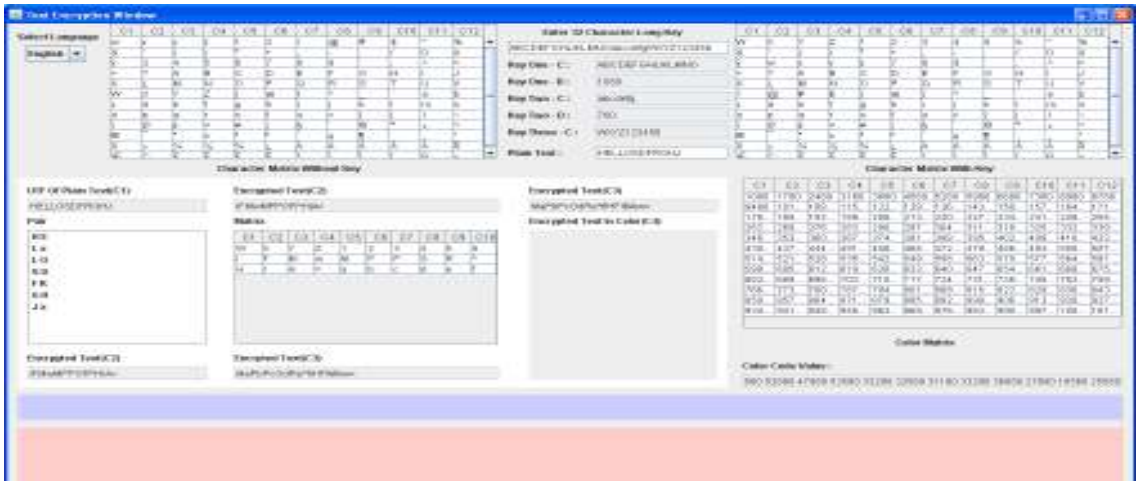

Figure 6- Text encryption window with C1,C2,C3

Figure 7-Encrypted text in block of color C4

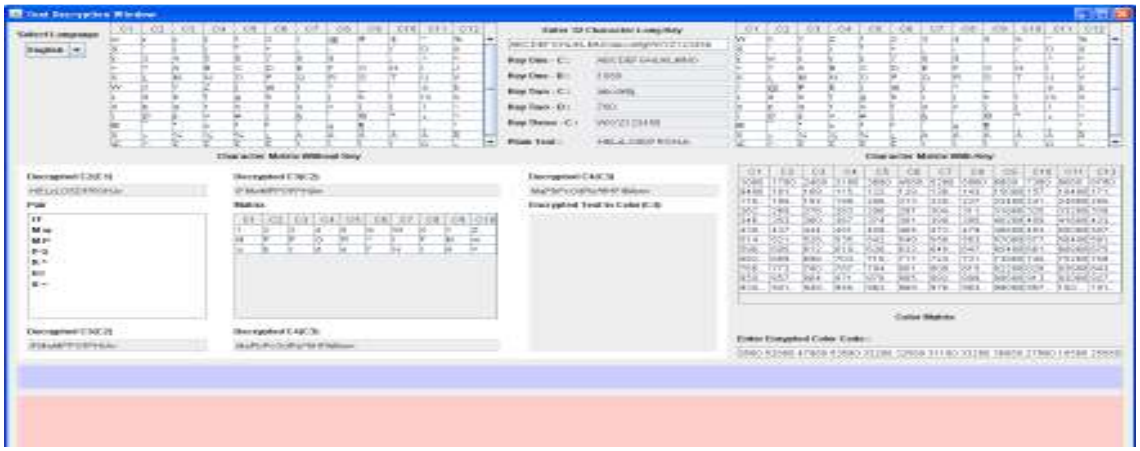

Figure 8-Text decryption window with C3,C2 and C1

Figure 9-Image used for encryption

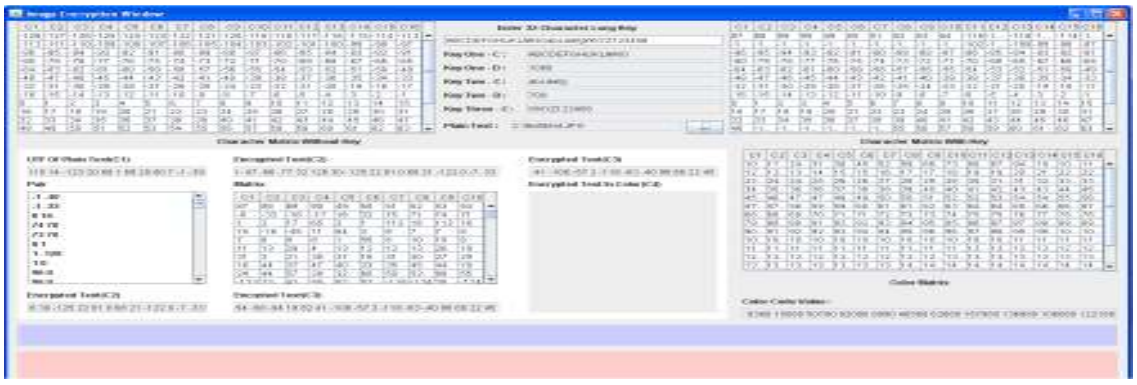

Figure 10-Image encryption window with C1,C2,C3

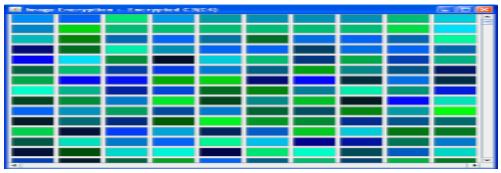

Figure 11-Encrypted image in block of color C4

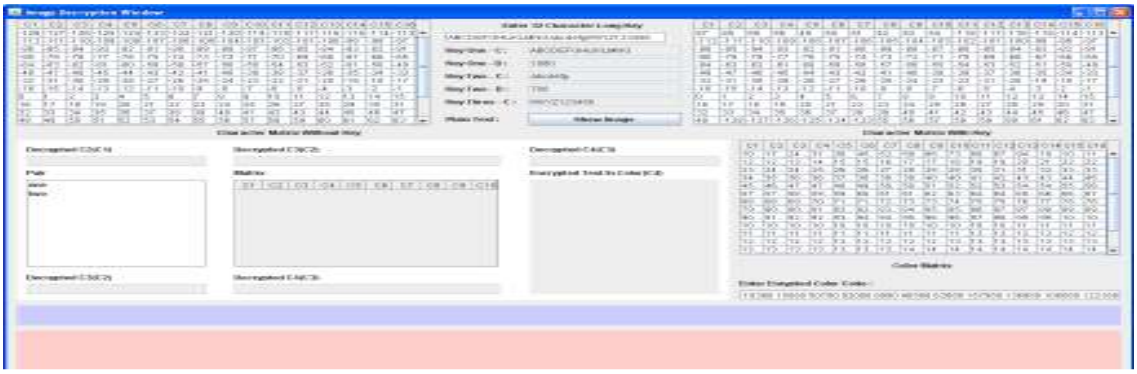

Figure 12-Image decryption window with C3,C2,C1

Figure 13-Original image after decryption

$1.5X10^{66}X10\text{-}3$
$\_\_\_\_\_ = 4.75X10^{55}$ year in Hindi

365X24X60X60

Case 2- Out of 32 character it may be that all character are number than maximum number of key=$(10)^{32}$.If we perform one encryption per microsecond it takes

$10^{32}X10^{-3}$
$\_\_\_\_\_ = 3.1X10^{29}$ years

365X24X60X60

In both cases number of key is large so it require time to try all possible key is too high. Brute force attack is difficult in this situation.
In case plain text attacks we have to know as many pair of plaintext and cipher text as we require. The numbers of color in the computer are more than [7]18 decillions, with minor difference in color. We are permuting once so it is difficult to know. In all discussion we got that it is strong cipher. [8]If we apply this substitution in DES it will create strong DES.

5. Conclusion

The paper presents algorithm for encryption & decryption using UTF-8, play fair cipher, transposition & color substitution. We have proved that the algorithm can encrypt /decrypt all kinds of text including characters, number and symbols. We have also proved that text may be purely image, diagram for encryption/decryption algorithm has three sub key K1, k2 & K3 generated from same key K.UTF-8 is measure allocation of this algorithm.RSA algorithm is used for transferring text.

Combination of UTF-8,play fair cipher, transposition & color substitution made stronger to algorithm.UTF-8 is explained in brief. Cipher generation in 4 steps in explained.128 bit key cipher is strong analysis & beyond the range of cryptanalyst attacks. In last we conclude that algorithm is quite strong & potential one.

6. Acknowledgements

We are thankful to all my mentors Mrs. Usha Johar, Professor K K Johar, Associate Professor Santhosh Easo and Assistant Professor Mohsin Sheikh for giving me guideline and advice for my research work .We are specially thankful professor Ravindra Babu Kallam ,Dr. S. Uday Kumar and Dr. A. Vinaya Babu for inventing this algorithm and giving substitution technique a new way.

7. References

[1] William Stallings, Cryptography and Network Security, principle and practice .5th edition,2008.

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

[3] A Block Cipher Generation using Color Substitution ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 28.

[4] A New Framework for Scalable Secure Block Cipher Generation using Color Substitution and Permutation on Characters, Numbers, Images and Diagrams International Journal of Computer Applications (0975 – 8887) Volume 20– No.5, April 2011.

[5] An Unassailable Block Cipher Generation with an Extended PCC, Concerning a Large Alphanumeric Kay, Modular Arithmetic and Integral Functions International Journal of Computer Applications (0975 – 8887) Volume 28– No.9, August 2011.

[6] A Survey On Recently Modernized Cryptographic Algorithms And analysis On The Block Cipher Generation Using Play Color Cipher Algorithm International Journal of Mathematical Archive - 2(10),2011 page:2084-2089 IISN 2229-5046.

[7] A Novel Approach to Substitution "Play Color Cipher" International Journal Of Next Generation Computer Applications ISSN 2319-524x.

[8] RGBA color space http:// en. wikipedia. org/wiki/ RGBA_ color_ space

[9] " for number of colors in the world" www.whyiscolor.org,