A Block Cipher Generation using Color Substitution

Prof. K. Ravindra Babu[1], Dr .S.Udaya Kumar[2], Dr. A.Vinaya Babu[3] and Dr. Thirupathi Reddy[4]
[1] Research Scholar (JNTUH),HOD CSE&IT, Aizza College of Engineering &Technology, Mancherail, A.P, India
[2] Deputy Director, Sreenidhi Institute of Science and Technology, Hyderabad, Andhra Pradesh, India
[3] Director, Admissions, JNTUH, Hyderabad, A.P, India, [4] Principal, AZCET, Mancherial, A.P, India

ABSTRACT
The most influential and universal approach to countering the threats to network / information security is encryption. Even though it is very authoritative, the cryptanalysts are very intelligent and they were working day and night to break the ciphers. To make a stronger cipher it is recommended that to use: More stronger and complicated encryption algorithms, Keys with more number of bits (Longer keys), larger block size as input to process, use authentication and confidentiality and secure transmission of keys.

It is certain that, if we follow all the mentioned principles, can make a very stronger cipher. With this we have the following problems: It is a time consuming process for both encryption and decryption, It is difficult for the crypt analyzer to analyze the problem. Also suffers with the problems in the existing system.

The main intention of this paper is to present an innovative cryptographic Substitution method, can generate stronger cipher then the existing substitution algorithms. We are sure that concept is new and the cryptanalysis did on this will prove that the cipher is strong.

Categories and Subject Descriptors
C#.net is used for coding and design of front end; it a simple modern object oriented and type safe programming language. C# combines the high productivity of rapid application development languages and the raw power of c++. It includes an interactive development environment, visual designers for building windows and web applications, a compiler and a debugger. Even though c# is a new language it has complete access to the same rich class libraries that are used by session tools such as visual basic.net and visual c++.net.[14][15]

General Terms
Block cipher, Play color, Cryptography, encryption, decryption Decillions, Substitution, Transposition, Color.

Keywords
RSA, EFF, PUB, PRA, PUA, PRB, PCC.

1. INTRODUCTION
In his research F.Ayoub [2][5] mentioned that, Cryptographic systems are used to provide privacy and authentication in computer and communication systems. Encryption algorithms encipher the Plaintext, into unintelligible cipher text or cryptograms using a key[1]. Deception algorithm is used for decipherment in order to restore the original information. In

general, the enciphering and deciphering keys need not be identical. Eavesdropping is the interception of messages by a third party monitoring a Communication channel. Anyone trying to break (solve) a cipher is called a cryptanalyst. According to William Stallings [1], Cryptographic systems are generally classified along three independent dimensions:

- The type of operations used for transforming plaintext to cipher text: all the encryption algorithms are based on two general principles: Substitution, in this each element in the plaintext (bit, letter, group of bits are letters) is mapped in to another element and the transposition in which elements in the plain text are rearranged. Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

- The number of keys used: If both sender and receiver use the same key, the system is referred to as symmetric, single key, secret key, or conventional encryption. If the sender and receiver each uses a different key, the system is referred to as asymmetric, two – key, or public key encryption [1], [4].

- The way in which the plain text is processed: A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing out put one element at a time, as it goes along.

Augmented intimidation / Intruder activities in recent times and a doubt about existing security algorithms [3][7][8] have created a need for inventing stronger secure algorithms. In recent past many researches have modified the existing algorithms [6][7][8][9][10] to fulfill the need in the current market, but still the ciphers are vulnerable to attacks.

On of the most extensively used cryptographic method is DES, is also broken and announced by electronic Frontier Foundation in July 1986[1][3].

Another prevailing public key algorithm is RSA, is based on mathematical functions rather then on simple operations on bit patterns. Hastad [6] made an attack on RSA with small key by sending an encryption of more than $e(e+1)/2$ linearly related messages of the type (ai * m + bi), where ai and bi are known; allowing an adversary to decrypt the messages provided that the Modulus ni satisfy $ni > 2^{(e+1)(e+2)/4} * (e+1)^{(e+1)}$. Wiener [7] proposed an attack hinges about find the d value directly with

special case of *d*, the RSA secret exponent *d* is chosen to be small compared to the RSA modulus *N*. A well-known attack on RSA mentioned that he can break the RSA in 953 milliseconds of length 'n' with 180 digits, where n is the product of two unequal prime numbers. Many more scientists were working day and night to break the RSA in fewer times.

In Cryptography, Substitution plays key role in many algorithms. In the existing Substitution technique[1] like Caesar Cipher, Mono alphabetic Cipher, Play fair Cipher and Poly alphabetic Ciphers are not strong enough and even they only support Capital and small letters.

The challenge is to implement stronger, scalable, substitution algorithms without any burden on the existing system. With the survey on Cryptography and Information Security, we came to the conclusion to implement a new algorithm rather then up dating the existing methods. With this, have invented a new with low secret-exponent *d* was given by Wiener about 15 years ago. In the recent past Prof. Alaa invented a new method, and substitution technique, 'color substitution' and named as a "Play Color Cipher (PCC)".

Play Color Cipher: Each Character (Capital, Small letters, Numbers (0-9), Symbols on the keyboard) in the plain text is substituted with a color block from the available 18 Decillions of colors in the world [11][12][13] and at the receiving end the cipher text block (in color) is decrypted in to plain text block. It overcomes the problems like "Meet in the middle attack, Birthday attack and Brute force attacks [1]".

It also reduces the size of the plain text when it is encrypted in to cipher text by 4 times, with out any loss of content. Cipher text occupies very less buffer space; hence transmitting through channel is very fast. With this the transportation cost through channel comes down.

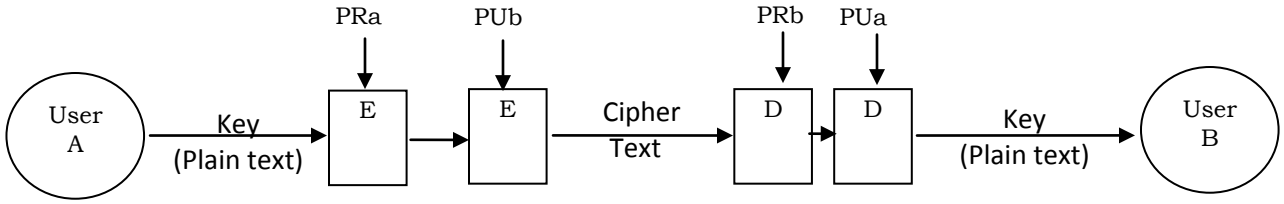

Figure1. Secure transmission of key using RSA

2. KEY SELECTION AND DISTRIBUTION

The number of colors in the computer world is, more then 18 Decillions, or the best answer we can say that, it is infinity [x]. According to the psychophysicists, we can see about 1000 levels of light-dark, 100 levels of red-green, and 100 levels of yellow-blue for a single viewing condition in laboratory.

For our convenience, in this algorithm, we have considered only ARGB colors combinations for color substitution, with each color ranges from 0 to 255.

Because, Play color cipher algorithm is a symmetric key algorithm both the sender and receiver has to use the same key for encryption and decryption. Hence, initially the key has to be communicated through secure communication channel between sender and receiver. It has the following steps:

- Select Starting address K1 such that K1< N
  Where: N =256X256X256X256 = **4,29,49,67,296,) (ARGB)**

.

- Select Increment value K2 such that (K1 + (C X K2)) < N,
  Where: K1 - Session key 1, K2 - Session key 2, C - Number of characters in the plain text, N- Maximum Number of colors
- Use RSA [1] Public key encryption algorithm for key distribution as shown in the figure1:
- Encrypt K1 and K2 using senders (User 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 both authentication and confidentiality we have distributed the keys between User A and User B

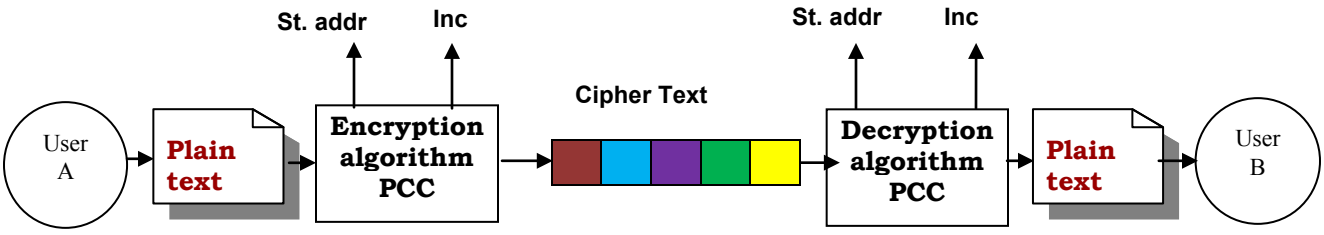

Figure 2: A Block Diagram of Encryption and decryption using Play Color Cipher

3. DEVELOPMENT OF THE CIPHER

Use Play color cipher algorithm for encryption and decryption: as shown in the figure 2, 4 and 5, Sequence of events are:

1. Use Windows 2000 and Microsoft Visual Studio for executing "*Play Color Cipher Algorithm*".
2. Debug the algorithm to get the '*Main Form' and then click on encryption for 'form for Encryption'*. As shown in figure 3 and 4
3. Enter the values of K1 and K2 in the box given and click on 'assign button'
4. Enter the plain text in the box given (can use Alphabets (Small & Big), Numbers (0 – 9), All symbols available on key board)
5. Click on '*Encryption Button'*
6. 'Save' the result as a file and 'exit' from encryption form.
7. Open the '*Form for Decryption*' and enter the K1 and K2
8. Browse for the saved cipher file
9. Click on '*Decryption Button*'
10. Observe the converted '*plain text*'.

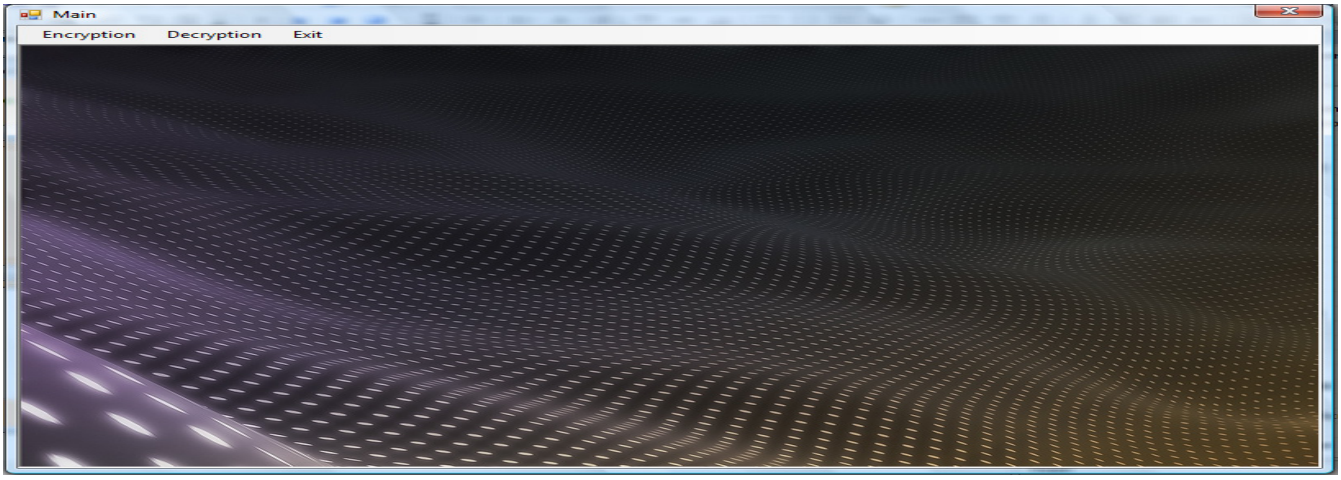

Figure 3: A Screen shot of Main form appears for encryption/decryption

3.1 Algorithm for Encryption

Step 1: Declare the array which contains alphanumeric special symbols

```
private string[] a = new string[96];
a[0] = "a";  a[1] = "b";    a[2] = "c";  a[3] = "d";
---------  a[93] = "/"; a[94] = "\n";  a[95] = "\"";
```

Step 2: Fetch the input from the user as K1(Starting address) , K2(Increment value)

Step 3: Declare and prepare the color Array based on starting address and increment value

- static private Color[] cl = new Color[96];
- for (int variable = 0; variable < 96; variable++)
  {
  ko = Color.FromArgb(255, Color.FromArgb(startingaddress));
  cl[variable] = ko;
  incrementvalue += startingaddress;
  }

Step 4: Read the data from the user Declare bitmap image

- public Bitmap objBmpImage=new Bitmap(1,1);
- Create graphics to draw the image
- Graphics objGraphics = Graphics.FromImage(objBmpImage);
- for (int variable = 0; varaible < inputdatalength; i++)
  {
- Fetch one character from the inputdata
- temp = inputdata.Substring(variable, 1);
- for (int j = 0; j < 96; j++)
- compare with predefined array

Step 5. Assign color to particular character and Draw the image

- Color FontColor = cl[j];
- SolidBrush objBrushForeColor = new SolidBrush(FontColor);
  objPoint.X += 8;
  a1 = FontColor.A;
  r1 = FontColor.R;
  g1 = FontColor.G;
  b1 = FontColor.B;
  objGraphics.DrawString(".", objFont, new SolidBrush (Color.FromArgb(a1, r1, g1, b1)), objPoint);cp = cp = cp + 1 } }

Decryption process is a reveres of encryption process

4. RESULTS

While execution it is observed that, play color cipher is comfortably converting plaintext into cipher text and then cipher to plain text with out any loss of contents with in limitations as shown in figure 5 and 6.

It uses two session keys for each session, in the example Starting address is 50000 and the increment value is 2000, the plain text considered for encryption is given below and its corresponding cipher text is shown in the figures 4.

The plaintext considered for encryption includes characters, numbers and symbols is:

AIZZA COLLEGE OF ENGINEERING AND TECH
MANCHERIAL
ADILABAD 1234567890 !@#$%^&*()_+

Figure 4 Plain text after Convertion using Color Substitution

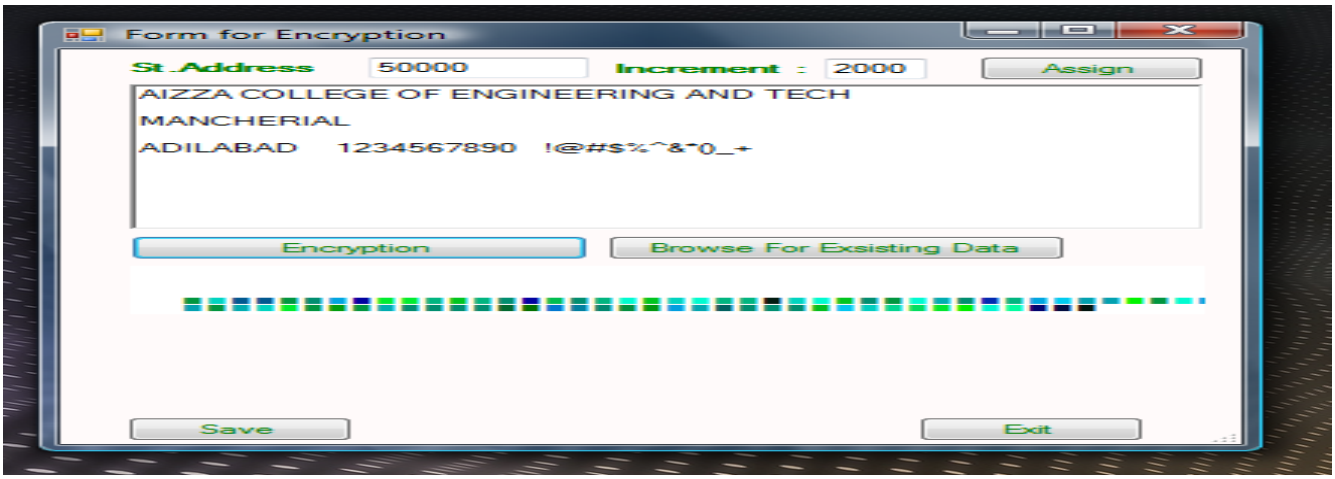

Figure 5: A Screen Shot of Encryption Process

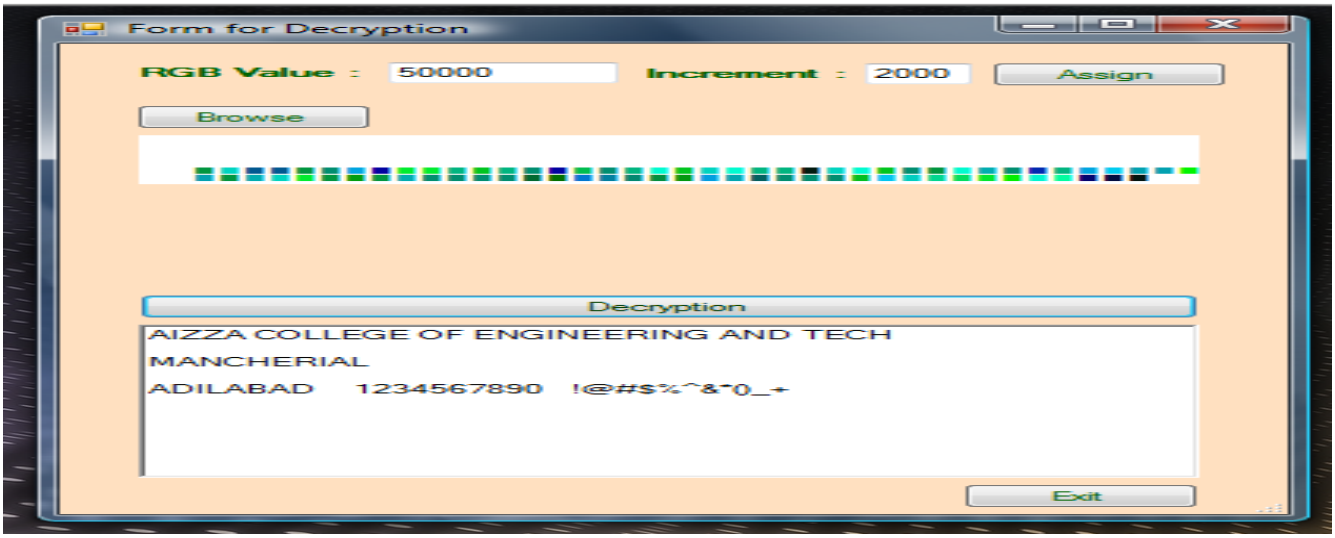

Figure 6: A Screen Shot of Decryption Process

5. CRYPTANALYSIS

In the algorithm we have considered the plain text with only ASCII and extended Characters. For color substitution, we have used only 4 parameters (ARGB)[10][11] each one is of 256 color shades. Maximum number of color combinations is 4,29,49,67,296 in decimal.

The length of the key is 10 digit decimal numbers and if we assume that the key can be any combination of 0 to 9 numbers then the maximum number of keys can be $(10)^{10}$, if we perform one encryption per micro second it takes:

$$\frac{10^{10}X10^{-3}}{365X24X60X60} = 3.1 \text{ years}$$

In the algorithm, maximum number of colors considered is 4,29,49,67,296, even though the value is less then $(10)^{10}$, it takes more then 2years for trying all possible combinations. Hence we can conclude that the brut force attack is not possible. If we look at the man in the middle, known plain text, known cipher text attacks, we have 18 dissilience of colors in the computer world, hence by looking at the color image it is not possible to gees or decrypt the plain text.

5. CONCLUSION

In this paper we have presented the basic model of innovative concept that is color substitution on characters for encryption. In the results section we have presented all the screen shots of converting plaintext in to cipher text and vice versa. The cryptanalysis carried out on this experiment shows that the cipher is potential one.

In future, we can include the figures, tables and images, etc in the plaintext for conversion and hence we can increase the scope of the algorithm. To generate the stronger cipher, we can increase the number of parameters for generating the color to get 18 Decillions of color combinations.

We can use integral and mathematical functions for generating the starting address and increment value to strengthen the algorithm. With small changes we can use the same algorithm for other then English language. Moreover we can implement multiple permutations and substitutions for enhancing security with confusion and diffusion.

6. ACKNOWLEDGEMENTS

The first author likes to thank to Trylogic Soft Solutions P.v.t, Hyd, for their support in code implementation. Our sincere thanks to IJCA for allowing us to modify the templates they had developed.

6. REFERENCES

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

[2] F. Ayoub, The Design of Complete Encryption Networks Using Cryptographically equivalent Permutations, ESP, 1883, 261-267.

[3] National Bureau of Standards" Data Encryption Standard" FIPS-PUB, 46, Washington, D.C., Jan 1977.

[4] R.L.Rivest, Shamir and Adleman," A Method of Obtaining Digital Signatures and Public Key Cryptosystems Laboratory for Computer Science, MIT Cambridge, 1978, Original RSA papers@ http://people.csail.mit.edu/rivest/Rsapaper.pdf,p6-8.

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

[6] Hastad, J. "On Using RSA with low exponent in a public key Network", Advances in Cryptology –CRYPTO '85, Springer-Velag LNCS 218, pp. 403-408, 1986.

[7] Nguyen, H. Number Theory and the RSA Public Key Cryptosystem. http://cdn.bitbucket.org/mvngu/numtheory-crypto/downloads/numtheory-crypto.pdf. Accessed on 25/9/2009.

[8] 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.

[9] 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.

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

[11] "Community reference for ARGB color", www. Blitzbasic. Com.

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

[13] " for number of colors in the world" www.jimloy.com

[14] Microsoft visual studio 2008 programming by Jamie, Tata Mc Graw Hill, 2009.

[15] .Net frame work programmers reference by Dan Rahmel, Tata Mc Graw Hill, 2002,