Advance Cryptography using Color Code based Substitution with Multi-Language Support

Monica Kanchan
B.E Computer Engineering, Viva Institute of technology

Avinash Shah
B.E Computer Engineering, Viva Institute of technology

Jayesh Gupta
B.E Computer Engineering, Viva Institute of technology

Sunita Naik
Prof of Computer Engineering Department Viva Institute of Technology

ABSTRACT
The threats to information security have been incrementing at an astounding rate. The most influential approach used for countering such threats is encryption. Various encryption techniques are classified into substitution and transposition techniques. In all conventional substitution techniques; the numbers, characters and special symbols are substituted with other numbers, characters and special symbols. An unprecedented cryptographic substitution method is proposed to generate a stronger cipher than the existing substitution algorithms. This algorithm of substitution is based on Play Color Cipher. Furthermore, asymmetric RSA algorithm is used to make the PCC key more secure and robust. The system will prove that the cipher is strong. A translator is used to enable multiple language input as plain text.

Keywords
Language translator, Play color cipher (PCC), Color substitution, color block, RSA algorithm.

1. INTRODUCTION
Security is the main concern regarding data transfer. Integrity of the data is an important factor for both the sender as well as the receiver. In today's times, many techniques are used to ensure the same; one of those techniques is cryptography. In the substitution techniques frequently used till date; numbers, characters and special symbols are substituted with other numbers, characters and special symbols. Like an alphabet would be substituted with another alphabet itself, or a number would be substituted with a number itself. In this system, an unprecedented cryptographic substitution method is proposed to generate a stronger cipher than the existing substitution algorithms. This system emphasizes on the substitution of characters, numbers and special symbols with color blocks. Color code substitution will be used in the project for encryption and decryption of the data using the algorithm play color cipher. This is known as color code substitution. The cryptanalysis done will prove that the cipher is strong.

2. PROBLEM DEFINITION
Sending data over a shared medium using symmetric key is vulnerable for attack. In Symmetric-key ciphers, the sender sends the plaintext which is encrypted using a shared secret key. The Asymmetric key cryptography system is based on personal secrecy. Unlike symmetric key cryptography, this has distinctive keys: a public key and a private key. Public key of the receiver is used for encryption while the private key of sender is used for decryption. In existing system, play color code technique is only applicable for single language. The data accepted can only be in the English language. This puts restrictions on the data that can be encrypted using play color cipher. Thus, limiting the play code substitution cryptography. The block size which forms a major part in the color code cipher is fixed, that is the block size is pre-defined. This is another vulnerability to the existing systems being used.

On a basic level, Translator performs simple substitution of words in one language for words in another, improving output by limiting the scope of allowable substitutions. This technique is particularly effective in domains where formal language is used the process of language translation in the system which takes the source text and convert it into required language if needed. Analysis is done on the source text to obtain the Interlingua language which is then used to generate the target text.

3. LITERATURE REVIEW
Cryptography based on Color Substitution for plain text was done for English Language. In Symmetric-key ciphers, the sender sends the plain text which is encrypted using a shared secret key. The receiver decrypts it using the same shared key. These ciphers consist of Substitution and Transposition ciphers.

Devyani Patil et al [1], has proposed that the symmetric key for cryptography in play color cipher was carried out on the ASCII values of the plain text. This could be carried out for encrypting login or password. This was done for single Language for English. In Symmetric-key ciphers, the sender sends the plaintext which is encrypted using a shared secret key. The receiver decrypts it using the same shared key.

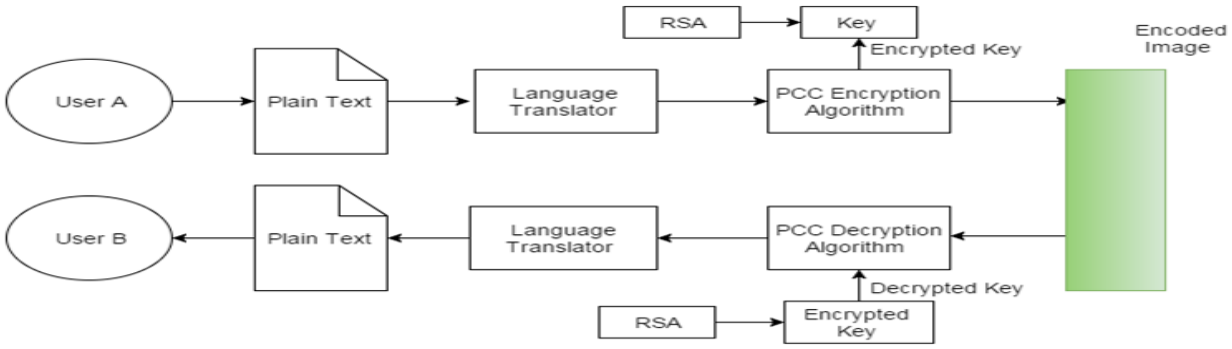

Fig 1: System Overview

A Substitution cipher replaces one symbol with another. This formed the basis for color code cryptography.

Prasanna Raghaw Mishra et al [2], has explained that the input text given in Hindi language will be converted to English and Cryptanalysis will be performed using translator.

4. SYSTEM DESCRIPTION

4.1 Diagrammatic Representation

System has proposed advance cryptographic technique with Multilanguage support which consist of various techniques that are clubbed together to develop the system as depicted in figure1. The system uses play color cipher to encrypt and decrypt the plain text. The key which is the backbone of any cryptographic technique is symmetric for PCC. In order to make this more robust, the key is encrypted using RSA algorithm which is an asymmetric cryptography technique. The google translator is used for Multi-language support. The translator is used to convert Hindi language into English language when the input is in Hindi rather than English. Figure1 shows the pictorial representation of the system.

4.2 Advantages of the system

In order to increase the security of the data and making it more robust, asymmetric encryption technique is used on the data for multiple language.

The character or letter is substituted with a color and then passed through the asymmetric algorithm to obtain the cipher text.

For language support, a translator is used. This way instead of just taking data which is in English language as an input, we can take Hindi as the input text, translate it into English using the translator then accept that translated data for the play color cipher. The cipher is also stronger being an asymmetric key.

To make the system more robust the block size used is made variable. This makes the key used for decryption more secure. Variable block size gives a better chance of security to the system.
After decryption the plain text obtained is again passed through the translator to obtain the original language if the input text was in Hindi. Thus, the decrypted data obtained would be in the language it was originally encrypted in.

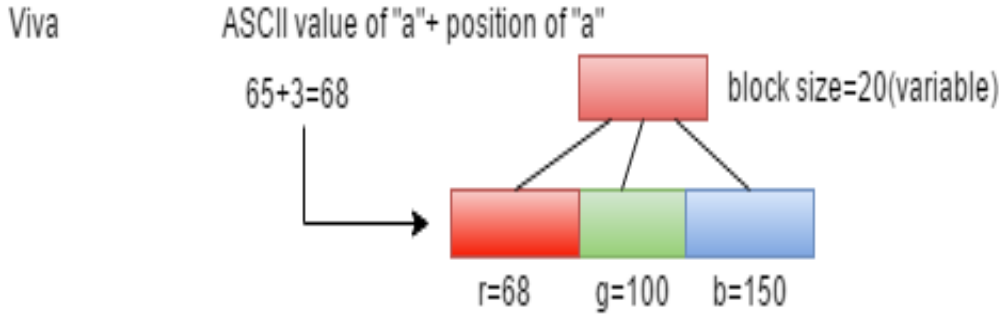

Fig 2: Example of PCC

Figure 2 is the example of the system in which character “a” is taken whose ASCII value and the position is calculated and accordingly color block is selected.

5. DESIGN AND IMPLEMENTATION

5.1 At Encryption Side

1. Accept the input text file in English/Hindi.
2. If input is in Hindi, it is translated into English with the help of a translator.
3. Input the color-channel (R/G/B) and color value (RGB value).
4. Define the block-size (say n), depending on the block size, picture is divided into grid of blocks, each of size n.
5. Input text is separated into individual characters.
6. ASCII value of each character is added with its position and color block of every character is formed accordingly.
7. The cipher image is then generated from the inputted data using PCC algorithm.
8. RSA algorithm is applied on the key generated by PCC algorithm which generates Asymmetric key.

9. Cipher image and keys value is sent to receiver via mail.

5.2 At Decryption side

1. Image will be received at the receiver side.
2. RSA decryption algorithm is applied in order to obtain the PCC key.
3. PCC decryption key is applied to cipher image.
4. The block size, color channel and the starting position of color block are extracted from the PCC key.
5. From each block, the pixel value of the central pixel is extracted and ASCII character are obtained. This is done for all blocks and the corresponding characters are extracted.
6. Characters are obtained back by using ASCII values.
7. Original text are obtained with the help of a translator.

5.3 Flow of the system

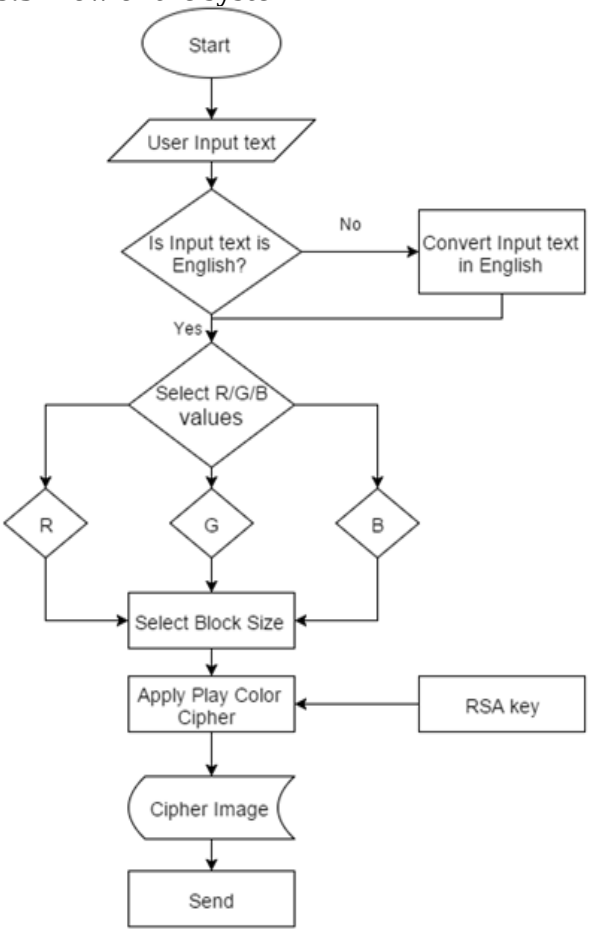

Fig 3: sender side system flow

Above figure 3 describes the working of the system. The input given by the user is first determined whether it's in English or not. If the language is used for encryption is determined to be in English, PCC algorithm is applied. One color channel from RGB is chosen. The next step is that the block size for encryption in PCC is chosen. The play color cipher algorithm is applied on this to obtain the cipher image. RSA algorithm is then applied on the key obtained after PCC encryption. The cipher image and the encrypted key is then sent to the receiver side via mail thus completing encryption.

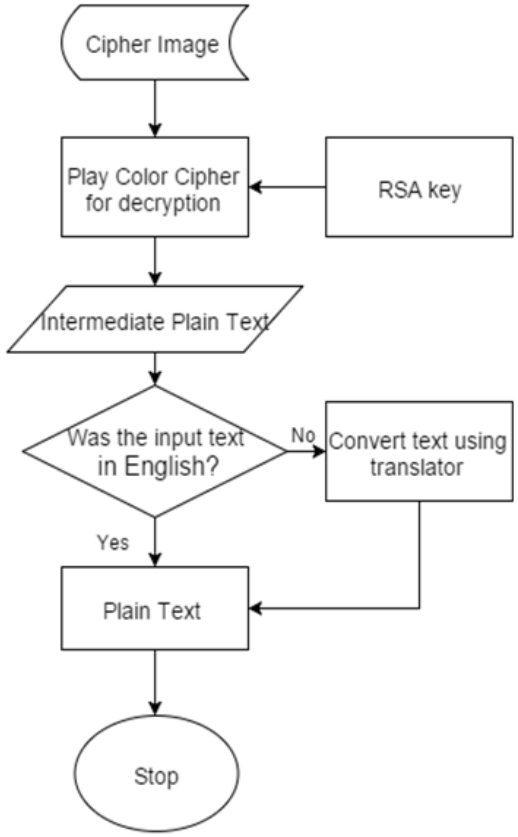

Fig 4: receiver side system flow

In above figure 4, the RSA algorithm for decryption is applied on the encrypted key to obtain the PCC decryption key. The next step is to apply the PCC decryption algorithm. The intermediate plain text is thus obtained. If this is needed in the English language then it is sent forth, otherwise translated and then sent as the plain text needed.

6. RESULTS

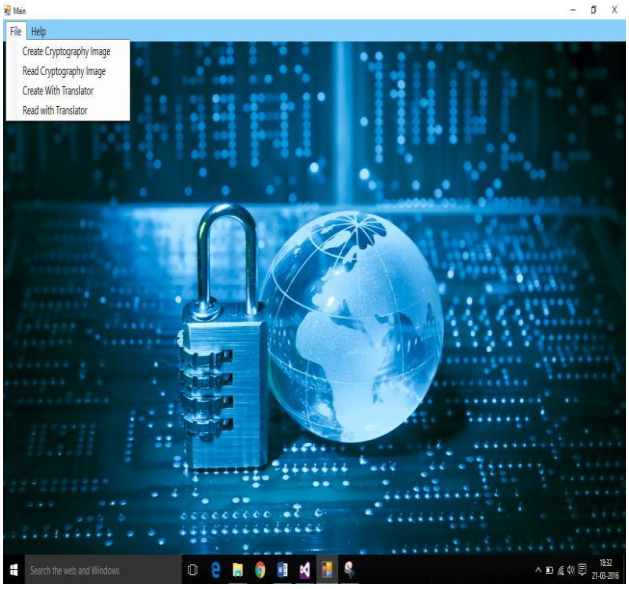

Fig 5: Main page

In above figure 5 the main page of the system is seen where all the options provided by the system is displayed. The user can choose any option based on his choice.

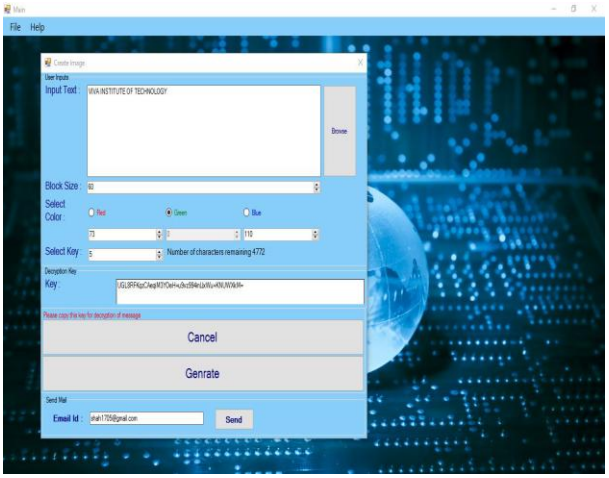

Fig 6: Encryption window

In above figure 6**,** the encryption window is displayed; where the input text can be entered by the user in order to encrypt it.

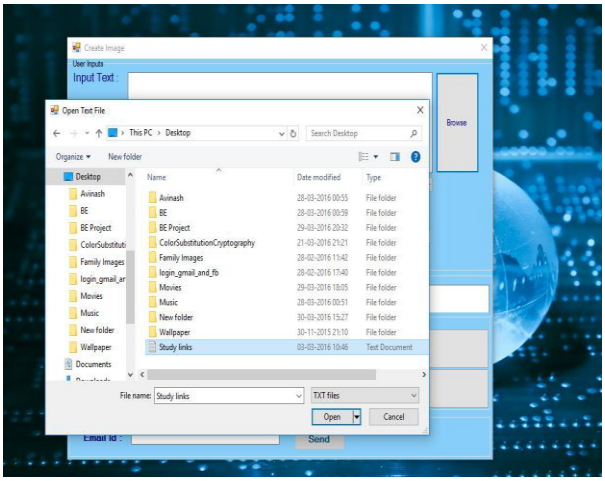

Fig 7: Browse Window

Browse window is used to save the cipher text obtained after encryption in a particular place; as shown in above figure7.

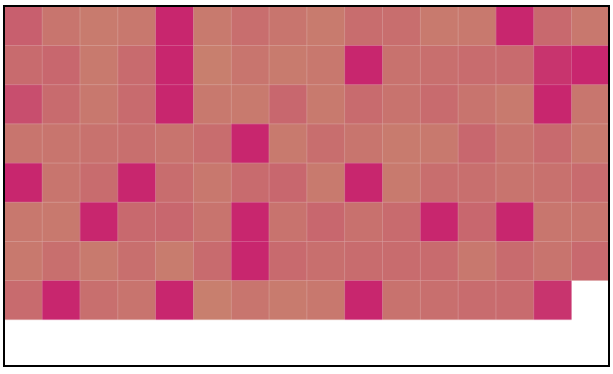

Fig 8: Cipher image

In above figure 8, the cipher image is obtained which is majorly in the shade of red. This is due to the color channel selected is red.

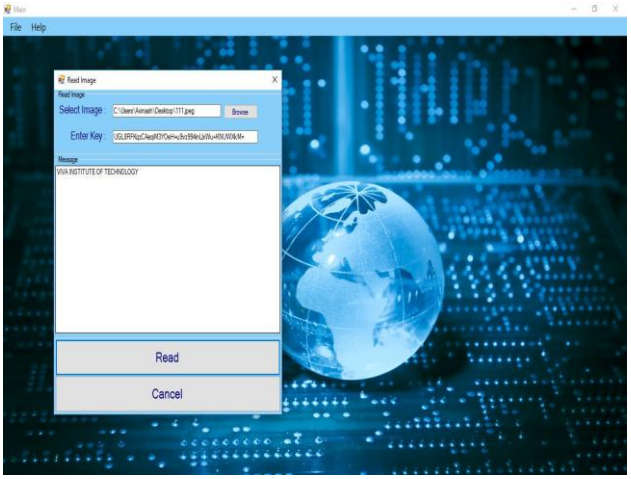

Fig 9: Decryption window

The decryption window can be seen as seen in figure 9; where the receiver can obtain the original data sent to him by using the cipher image and the key sent by the sender.

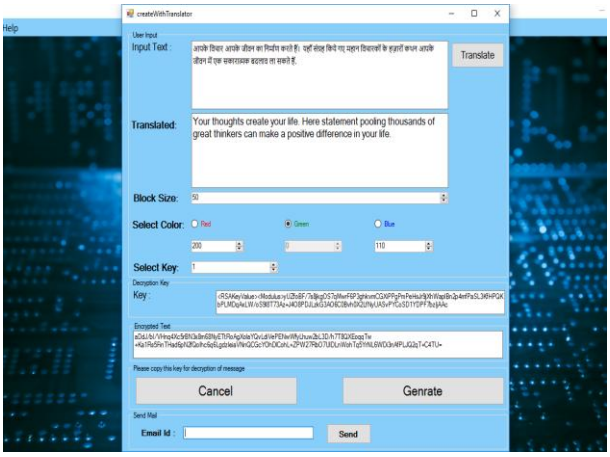

Fig 10: Encryption using Translator

In figure 10 Encryption using a translator is displayed. Here the sender can send data which is originally in Hindi by using a translator. The translated data is then encrypted.

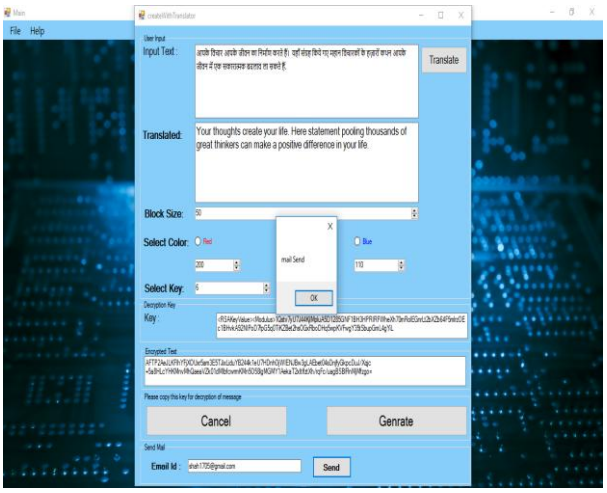

Fig 11: Automated E-mail generation

In figure 11, the automated mail generation shows that once the cipher image is generated, it can be sent to receiver via email.

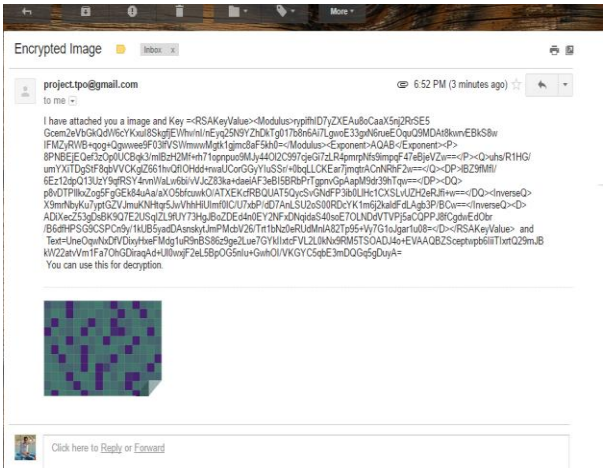

Fig 12: Receiver side email

In above figure 12, the mail of the receiver is seen. The receiver obtains the cipher image and the key used for decryption

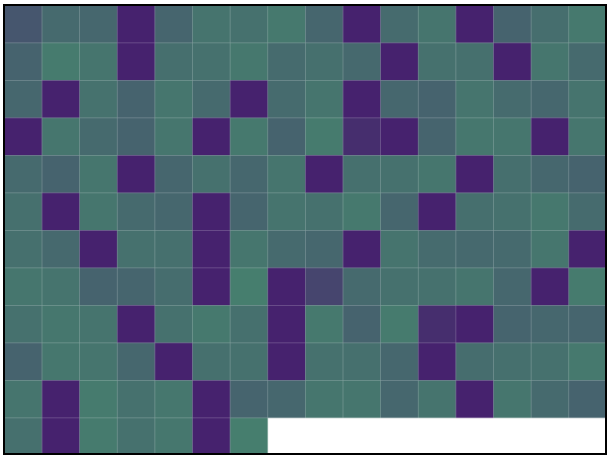

Fig 13: Cipher image

The cipher image obtained after encrypting the input data can be seen in above figure 13

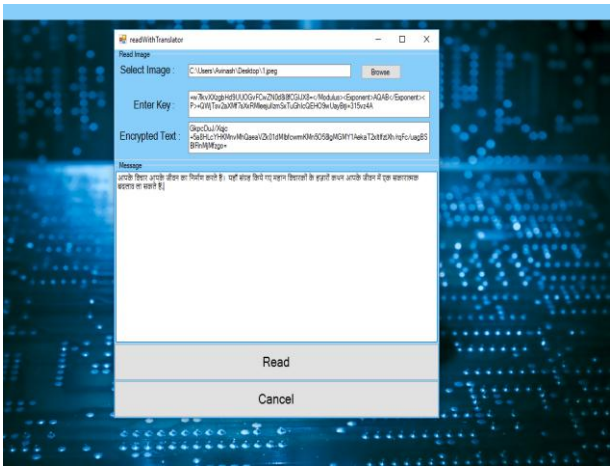

Fig 14: Receiver side decryption

In figure 14, the receiver side decryption is seen where the data is obtained using the cipher image and the encrypted text and the key used for decryption.

7. CONCLUSION

The system carries out the cryptanalysis in such a way that it will show that the cipher has great potential as it eliminates major attacks like brute force, man in the middle, known plain text and known cipher text attacks. In this system, implementation of encryption-decryption scheme is done using symmetric and asymmetric techniques for securing the transmission of data for multiple language support using variable block. The data which is encrypted uses color blocks for encryption instead of normal substitution of characters.

In future, the figures, tables, pictures, and so forth can be incorporated into the plaintext for transformation and consequently the extent of the calculation can be expanded. To create a stronger cipher text the quantity of parameters (such as alpha, gamma adjustment and so on.) can be expanded for producing the color to get 18 decillions of color combinations

8. REFERENCES

[1] Devyani Patil, Vishakha Nayak, Akshaya Sanghavi, Aparna Bannore. "Cryptography based on Color Substitution" published in IJCA(0975-8887) volume 91-No.16,April 2014.

[2] Prasanna Raghaw Mishra, Indivar Gupta and Navneet Gaba. "Cryptanalysis of Multilanguage Encryption Technique"; published in IJCA(1275-8847) volume 87-No.12,April 2012.

[3] Ravindra Babu Kallam, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu. "Scalable Secure Block Cipher Generation using Color Substitution", published in IJCA(0975-8887) volume 20-No.5,April 2012.

[4] Aditya Gaitonde 2012. Color Coded Cryptography, International Journal of Scientific & Engineering Research, Volume 3, Issue 7.

[5] Prof. K. Ravindra Babu, Dr.S.Udaya Kumar, Dr.A.Vinaya Babu and Dr.Thirupathi Reddy, 2010. "A block cipher generation using color substitution", International Journal of Computer Applications Volume 1 – No. 28.

[6] Pritha Johar, Santosh Easo and K K Johar, 2012. "A Novel Approach to Substitution Play Color Cipher", International Journal of Next Generation Computer Application Volume 1- Issue 2.

[7] Johan Hastad, 1986. "On using RSA with low exponent in a public key network", Advances in Cryptology-CRYPTO "85, LNCS 218, pp. 403-408.

[8] B.A.Forouzan, Cryptography and Network Security, 4th edition, 2008.

[9] Christian Gross, Beginning C# 2008 From Novice to Professional 2nd edition, 2008.

[10] "http://cdn.bitbucket.org/mvngu/numtheory", last accessed on 29/09/2015.

[11] "http://crypto.com/downloads/numtheory-crypto.pdf.", last accessed on 25/09/2015.

[12] "http://csrc.nist.gov/publications/fips/fips46-3.pdf", last accessed on 26/09/2015