ISSN 2319-524X

A Novel Approach to Substitution “Play Color Cipher”

[1]Pritha Johar, [2]Santosh Easo,[3] K K Johar

[1]Student, Master of Engineering,Medicaps Institute of Technology & Management, Indore, India.
[2]Assistant Professor CS & IT Department, Medicaps Institute of Technology & Management, Indore, India.
[3]Professor & Head, Department of Physics &Computer Science, Government PG College Khargone, MP, India.
[1]prithajohar@yahoo.co.in
[2]san.easo@gmail.com
[3]kishorekumarjohar@gmail.com

***Abstract-* In world of computer network if we want to secure any type of data then we have various ways like, encryption algorithm, digital signature and authentication protocol. Traditional encryption techniques use substitution and transposition.**

[1]Substitution technique map plaintext into cipher text. In all traditional substitution technique, it substitutes character, number and special symbol with character, number and special symbol. But we are emphasis on substitution of character, number and special symbol with color block. [2]This algorithm of substitution is Play Color Cipher.

***Keywords-* Play Color Cipher, RSA algorithm, Substitution, Permutation, PUS-public key of Sender, PRS-Private key of sender, PUR-Public key of Receiver, PRR-Private key of receiver, Decillion, RTF-Rich Text Format, Unicode.**

I. Introduction

We know that encryption techniques are used widely in security of data. Malicious users are also ready to break encryption algorithm security. Different types of attack apply on the algorithm, but when an algorithm develops it s also ready to avoid attack. Encryption algorithm is based on number of substitution and transposition. When a substitution algorithm is developed strong then it normally uses number of substitution and transposition, but it is easy to break.

When for encryption an algorithm process on data then it uses one of the approach- block cipher or stream cipher. In block cipher it uses a block of plaintext for encryption and gives a block of cipher text in return. Where in stream cipher it continuously takes plaintext character one by one and gives cipher text.

Play color cipher is a new substitution technique. Each character (capital and small letter, number (0-9), symbol on keyboard) in plaintext is substituted with a block of color from 18 decillion of color. At the receiving end the cipher text block (in color) is decrypted in to plaintext block.

In play color cipher we need to transmit key for security of algorithm. It use RSA algorithm for key transmission which is a public key algorithm. Play color cipher uses same way for encryption as we use in the play fair cipher. First we select a key like monarchy put it in our matrix, encrypt it in same way as we encrypt in play fair cipher, get the encrypted output of text , check that what color value is at the encrypted text, substitute it and get cipher text in form of block of color, transmit this block of color to receiver .Key which is used in matrix is transmitted by using RSA algorithm. [2]It uses [3]2 character alphanumeric key. This 32 character long key included 4 key in itself.k1,k2,k3 and k4.

K1- initial color value.
K2- increment value for color. K3- select language.
K4- key for encryption.

II. Process of Encryption and Decryption -

Encryption-

1. Read plain text, it may be in any language like English, Hindi, Tamil etc.
2. Convert it into [4]UTF.
3. Create block of plaintext it will be C1.
4. Apply permutation on C1 by key k4.this cipher text will be C2.
5. Again apply permutation on C2 by keyk4 it will be C3.
6. Now substitute color value for particular character according to color matrix position with character matrix.
7. Send cipher text to receiver and key also by encrypting with RSA algorithm.

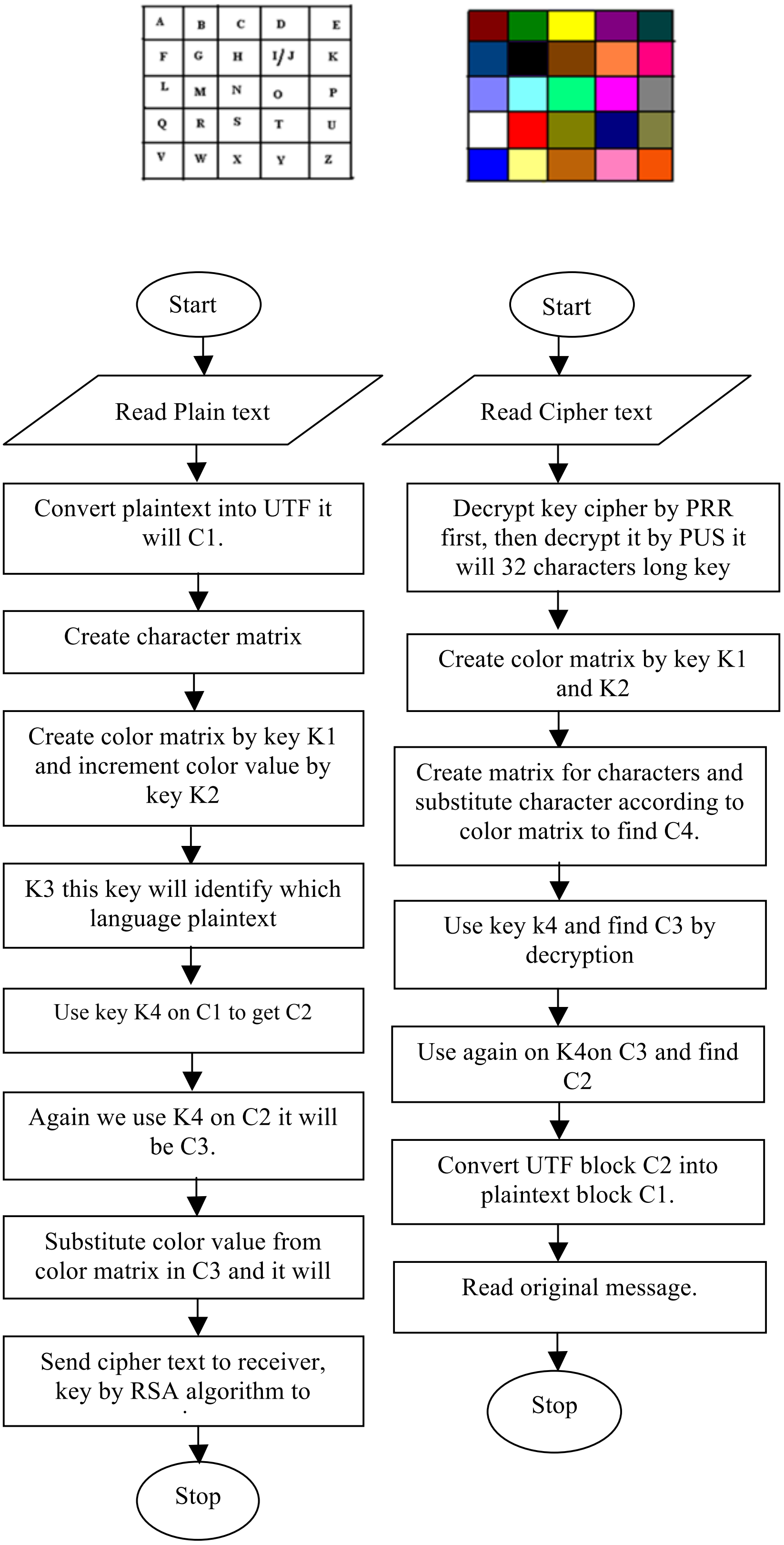
Decryption-

1. Receiver receives encrypted key.
2. Decrypts it by PRR.
3. Decrypts it by PUS.
4. Then he gets what is the key.
5. Key length will 32 character long.
6. 1-15 character is k1,16-22 character for k2,23rd character is k3 and 24 to 32 is k4.
7. it will create matrix according to the value of k1 and K2.
8. Put character according to the color matrix at place of color to get C3.
9. Use k4 in matrix and find C2.
10. Again use k4 in matrix and find c1.
11. Now change UTF to plaintext.

I. Cryptanalysis

Cryptanalyst is a person who doesn’t know about encryption algorithm and key but by the possible way of attack he finds the Algorithm to key and break security.
We are considering here 4 type of attack-
Only Cipher text attack
Known plain text attack
Chosen plaintext attack
Chosen cipher text attack
As we know that we are using 32 character long alphanumeric key. It has three possibility of attack. Key can be character of any chosen language.

ISSN 2319-524X



A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Start
Read Plain text
Convert plaintext into UTF it will C1.
Create character matrix
Create color matrix by key K1 and increment color value by key K2
K3 this key will identify which language plaintext
Use key K4 on C1 to get C2
Again we use K4 on C2 it will be C3.
Substitute color value from color matrix in C3 and it will
Send cipher text to receiver, key by RSA algorithm to
Stop
Start
Read Cipher text
Decrypt key cipher by PRR first, then decrypt it by PUS it will 32 characters long key
Create color matrix by key K1 and K2
Create matrix for characters and substitute character according to color matrix to find C4.
Use key k4 and find C3 by decryption
Use again on K4on C3 and find C2
Convert UTF block C2 into plaintext block C1.
Read original message.
Stop

Figure1-character matrix and color matrix with Play Color Cipher algorithm

Case 1- [5,6]In English language 26 characters and 10 number 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 for 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

1.9X1045X10-3
_______________ =6X10^{35} years in English

365X24X60X60

1.5X1066X10-3
_____________=4.75X1055 year in Hindi

365X24X60X60

Case 2- Out of 32 character it may that all character are number than maximum number of key=(10)32

If we perform one encryption per microsecond it takes
1032X10-3
_____________ =3.1X1029 years

365X24X60X60

In both case 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 decillion, with minor difference in color. We are permuting twice so it is difficult to know. We have strong avalanche effect because we are changing first character position in pervious so it is really difficult to know what is plain text. In all discussion we got that it is strong cipher. [8]If we apply this substitution in DES it will create strong DES.

III. CONCLUSION

R=We have developed a Play Color Cipher algorithm by using color substitution method.32charater long key has been used for encryption and decryption.RSA algorithm is used to transmit key. Use of UTF in Play Color Cipher makes it possible to be independent of any language. It's a better algorithm as compared to RTF. We can conclude that it will be a strong symmetric key algorithm for any data transmission.

IV. ACKNOWLADGMENTS

We are thankful to all my mentor Assistant Professor Santosh Easo and Professor K K Johar 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.

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 Infromation Security",IJCA, 0975-8887, Vol 12, No-2, Nov2010.

[3] An Unassailable Block Cipher Generation with an Extended PCC, Concerning a Large Alphanumeric Kay, Modular Arithmetic and Integral Functions.

[4] Unicode standard 6.1.0 http://www.unicode.org/versions/Unicode6.1.0/

[5] "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 IJMA available online through www.ijma.info ISSN 2229-5046

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

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

[8] National Bureau of Standards" Data Encryption Standard" FIPS-PUB, 46, Washington, D.C., Jan 1977. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf