

# Information Security Using Play Color Cipher

## Computer Security Chiefs

Presented By:

Vinay Kumar Reddy Donda( Team Lead)

Lakshmi Pravallika Somisetty


N V Ravi Kishor Mokkapati

Sai Madhav Kilaru

Shiva Charan Gona



## OVERVIEW


- Abstract
  - Play color cipher
  - Why RSA is used?
  - RSA Algorithm
  - Algorithm used
  - Advantages & Disadvantages
  - Conclusion
- 



## ABSTRACT

In this paper, we are studying about a new encryption technique Play color cipher using RSA algorithm for key transmission. This method is used to prevent Brute-force attacks, Birthday attacks and Man-in-Middle attacks.

We use substitution method to convert plain text into cipher text. All the characters in plain text is converted into colors which is impossible by the hacker to find out the correct text among 18 decillion permutations of colors.



## PLAY COLOR CIPHER

It is much similar to play fair cipher. It uses a  $5 \times 5$  matrix and fits keyword in the first and remaining are placed next. And sequence of 0-25 is allotted.

**Encryption:-**First convert a letter into number between 0 to 25 and then multiply it with scaling factor after adding the numbers.

**Decryption:-**Take first letters of cipher text and key and subtract them both and then divide them by scaling factor. If after subtraction the value is negative add 26 to get the result. Result will be between 0 to 25 i.e., a to z.

## Why RSA is used?

DES algorithm in general uses a 64 bit-key in which 8 bits are used for parity checking, hence only 56 bits are being used and gives  $2^{56}$  permutations. AES algorithm depends on rounds of encryption hence provides few permutations only.

For example if we take three colors namely yellow, green and orange, RSA provides 1,67,77,216 permutations due to the color range and scaling factor.

## RSA Algorithm

Using RSA algorithm we generate a public key by multiplying two random large prime numbers. Also, private key is generated using same prime numbers. Here encryption is done using public key and decryption is done using private key.

It uses four steps Key generation, Key distribution, Encryption, Decryption. Now the scenario is information is being transmitted from user A and user B.

### **Key generation:**

Compute  $\lambda(n)$ ,  $\lambda(p)$ ,  $\lambda(q)$  where  $p$  and  $q$  are two prime numbers

Then,  $d \equiv e^{-1} \pmod{\lambda(n)}$



## Key distrubution:

User B transmits his public key  $(n, e)$  to user A via a reliable, but not necessarily secret, route. User B private key  $(d)$  is never distributed.


## Encryption:

After user A obtains user B public key, he can send a message  $M$  to user B.

$$C = (m^e) \pmod{n}$$

## Decryption:

User B can recover  $m$  from  $C$  by using his private key exponent  $d$  by computing

$$C^d = (m^e)^d = m \pmod{n}$$


## Algorithm used

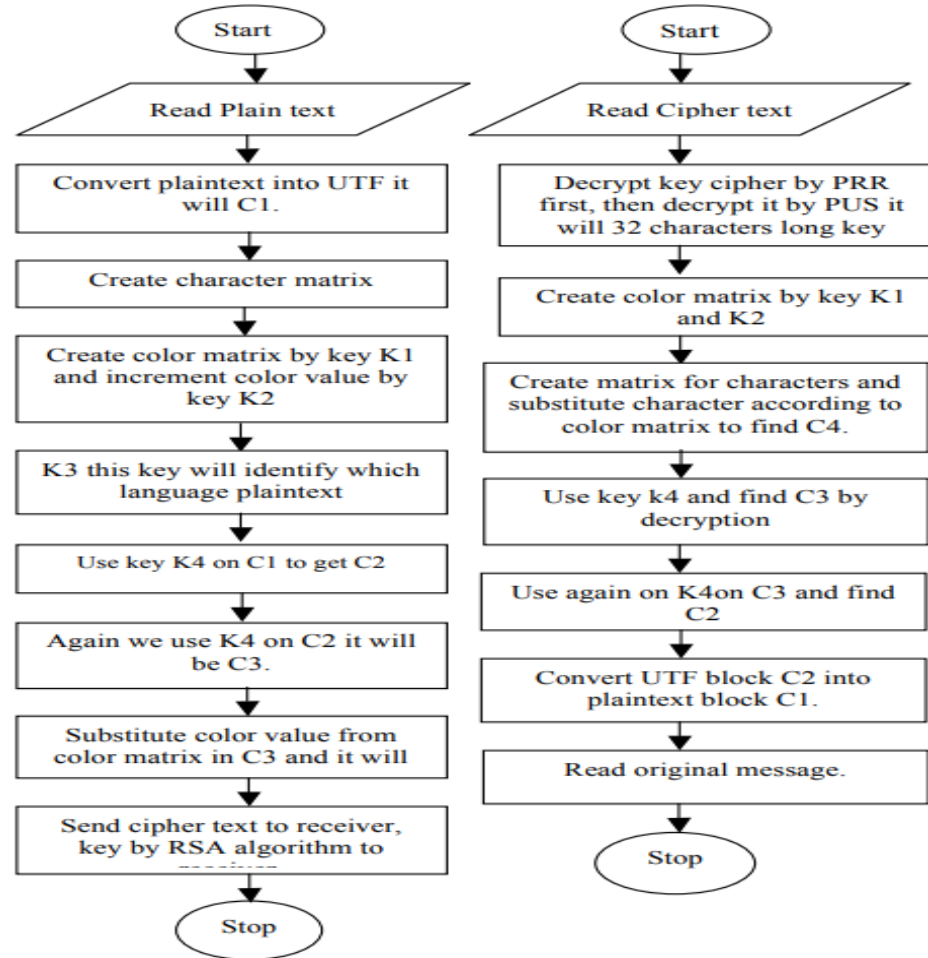
### **ENCRYPTION:**

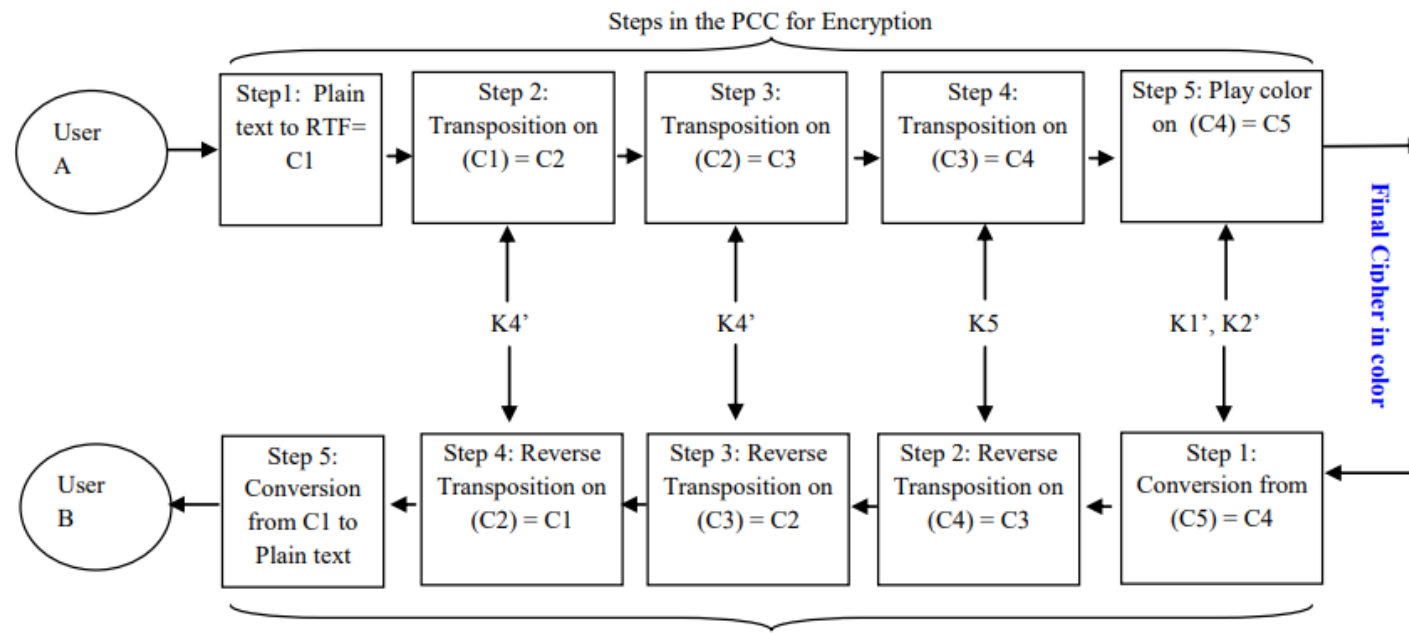
- RSA consists of 128-bit key which is divided into 4 parts K1, K2, K3, K4.
- Read the plain text and convert into UTF. Now create a block of plain text named C1.
- Apply initial permutation to C1 with key K4. The output will be cipher text C2.
- Now apply permutation for C2 with K4 and it will be C3.
- Substitute the characters in C3 with color matrix formed (process is discussed above).
- Now cipher text and key can be transmitted to receiver in the form of color blocks by using RSA algorithm.



## DECRYPTION:

- Receiver gets the encrypted key and decrypts it using receiver private key and sender's public key.
- Receiver gets the key after decryption as 32-bit long. Which then can be divided into 4 parts K1(1-15 bits), K2 (16-22 bits), K3(23<sup>rd</sup> bit), K4(24-32 bits) respectively.
- Now from character matrix color blocks can be substituted and C3 can be found.
- Use K4 in the same matrix and find out C2.
- Similar to reverse encryption, apply K4 to C2 which gives C1.
- C1 is in the form UTF and is converted to plain text.





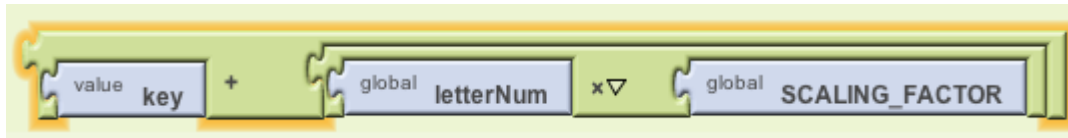
## EXAMPLE

Alice and Bob share one of the 16 million colors as secret key which they use to encrypt and decrypt messages which is used for both encryption and decryption. Now, we use a substitution cipher technique and replace colors with characters based on character matrix.

### To encrypt a letter into a color:

1. We first convert the letter to a number between 0 and 25, where 'a' is 0, 'b' is 1, and so on.
2. Then add all the colors. Now multiply sum with scaling factor. For example, our scaling factor is the color ORANGE.

In App Inventor blocks, here is how a letter is encrypted, where where letternum is the letter's number (0 to 25) and both key and scaling factor are colors:



**To decrypt a color into a letter, we perform the encrypt operations in reverse:**

1. We first subtract the key from the color.
2. We then divide the result by the scaling factor. This will give us a number between 0 and 25, which we then translate back into a letter between 'a' and 'z'.

In App Inventor blocks, here is how a letter is encrypted, where colorNum is color encryption of the letter and key1, and scaling factor are both colors:



# CRYPTANALYSIS

- In English, we have ten numbers and 26 characters so we will get key of  $26^{32}$  that have  $1.9 \times 10^{45}$  permutations when we perform one encryption per second it will take  $6 \times 10^{35}$  years to do an attack. Whereas, for ten numbers we will get key  $10^{32}$  when executed one encryption per microsecond  $3.1 \times 10^{29}$  years to do an attack.
- We transmit key of 23 bit using RSA algorithm it's key length is 92 bits and key space is  $2^{92} = 5.0 \times 10^{27}$  key. When one value is done for  $10^{-3}$  seconds then time required for key space is  $1585 \times 10^{14}$  years. If we perform one encryption per micro second it takes  $2.4 \times 10^{16}$  years and for  $10^6$  years it takes 1842.6 years.
- When we apply these two logics for 18 decillion number of colors it is impossible for anyone to perform Brute force attack or Man-in-Middle attack.




# ADVANTAGES & DISADVANTAGES

## **Advantages:**

- It is very easy to implement and is safe and secure for transmitting confidential data.
- Bulk data capacity and high correlation among pixels can be done easily.
- Transportation cost through this channel is very low and speed is very fast.

## **Disadvantages:**

- not much reliable
  - takes more time
- 

## CONCLUSION

We developed a play color cipher using substituting technique where we used RSA algorithm for key transmission to transfer information securely. We used RSA algorithm in order to provide more security for secret key transmission due to its maximum no. of permutations. We use a 32-bit long key for encryption and decryption process. In the beginning we convert plain text to UTF file as any kind of programming language can be used and UTF provides a better and faster algorithm than RTF.

This method also prevents Brute force attacks, Birthday attacks and many other which can be proved by performing cryptanalysis. A stronger cipher using 18 Decillion colors and their enormous permutations of color combinations is built. It also takes some decades to crack such kind of cipher.



## REFERENCES

- Andrey Bogdanov, D. K. (2011). Biclique Cryptanalysis of the Full AES. *Crypto 2011 cryptology conference*. Santa Barbara, California.
- Dinesh Sharma, R. P. (2017). Colour Based Cryptography. *International Research Journal of Engineering & Technology*.
- gaitonde, A. (2012). Color Coded Cryptography. *International Journal of Scientific & Engineering Research*, Volume-3, Issue-7.
- Pritha Johar, S. E. (2012). A Novel Approach to Substitution Play Color Cipher. *International Journal of Next Generation Computer Application*, Volume1.
- Prof. K. Ravindra, D. K. (2010). A block cipher generation using color substitution. *International Journal of Computer Applications*, (p. Volume1).
- Sastry V.U.K, S. U. (2006). A large block cipher using modular arithmetic inverse of a key matrix and mixing of the key matrix and the plain text. *Journal of Computer Science*.
- Stallings, W. (2008). *Cryptography and Network Security, principle and Practice, 5th edition*.

A decorative network pattern in the top-left corner, consisting of grey and blue nodes connected by lines, with some nodes highlighted in blue.

**THANK YOU**

A decorative network pattern in the bottom-right corner, consisting of grey and blue nodes connected by lines, with some nodes highlighted in blue.