RESEARCH ARTICLE OPEN ACCESS

Data Security With Colors Using Rsa

G. Sankara Rao, E. Jagadeeswararao, D. Mounica
Assistant Professor, Dept. of CSE, GVP College of Engg. for Women. Kommadi, Visakhapatnam, India
Lecturer, School of IT, JNTUH, Kukatpally, Hyderabad, India
Student- B.Tech, Dept. of CSE, GVP College of Engg. for Women. Kommadi, Visakhapatnam, India

Abstract –
Data Security with Colors using RSA technique that integrates the RGB Color model with the well-known public key cryptographic algorithm RSA (Rivest, Shamir and Adleman). This model provides both confidentiality and authentication to the data sent across the network. RSA algorithm uses public key and private key to encrypt and decrypt the data and thus provides confidentiality. But the public key is known to everyone and so anyone can encrypt the data and send the message. Hence authentication of users is needed. In this technique we use RGB color model to provide authentication. Every user will have a unique color assigned to him. A sender must know the receiver's color to send a message. The color value is encrypted using a key which is used as a password while decrypting the message. To decrypt the message, the receiver must provide his color values. If the decrypted color values and his color values are equal then the sender and receiver are send to be authentic. The data encryption and decryption follows RSA procedure. Thus both authentication and confidentiality are provided for the data.

Keywords*: DSCR, RSA, encryption, decryption, confidentiality, authentication, private key, public key.*

I. INTRODUCTION

In the present world scenario it is difficult to transmit data from one place to another with security. This is because hackers are becoming more powerful now a days. To ensure secure data transmission there are several techniques being followed. One among them is cryptography which involves encryption and decryption of data. In this paper we use RSA algorithm to perform encryption and decryption. To provide authentication between two intended along with security, COLORS are used. With the help of colors, both sender and receiver will get validated. RSA involves public key and private key where public key can know to everyone and is used for encrypting messages. Messages encrypted using public key can only be decrypted using corresponding private key.

We use RGB color model to provide authentication for both sender and receiver. The first step is to assign a unique color to each user. Each color is represented with a set of 3 values. To send a message, the sender must be aware of the receiver's color. This receiver's color is used as a password which is encrypted with asset of 3 key values. The receiver will decrypt the encrypted color values using the key. If the decrypted color values and his own color values are equal then the sender and receiver are said to be authentic.

In order to counter the common threats to communications, we can apply several of the fundamental security services, including authentication, integrity, confidentiality and authorization. A secure data transmission may use all or a combination of these services to achieve the desired security level.

Authentication services provide assurance of a participating host identity. Therefore, the availability and distribution of keys should be restricted to only authorize group members according to the policy of trust established for the session. Authentication mechanisms can identify the source of the key material and provide a means to counter various masquerades and replay attacks that may be launched against a secure data transmission.

Integrity requires the data and control packets originated at an authorized source not to be intercepted or altered while traversing through the network. The possibility of preventing a denial-of-service attack through the transmission of such packets can be minimized or eliminated.

Confidentiality services are essential in creating a private data transmission session. It should also be applied to key management transactions during the exchange of key material and can be applied to session announcements allowing them to advertise publicly through standard methods while keeping the details of the session private.

Authorization can be implied to only those entities with specific permission that may use the network to send messages after they have been suitably authenticated.

This paper is organized as follows: Section II presents implementation of RSA algorithm, RGB model. Section III describes how RSA and RGB are integrated. Finally, Section IV concludes the paper.

II. IMPLEMENTATION OF RSA ALGORITHM

A. *Cryptography*

Cryptography is the art and science of keeping information secure from unintended audiences, of encrypting it. Today, cryptography is used to provide secrecy and integrity to our data, and both authentication and anonymity to our communications. Modern cryptographers emphasize that security should not depend on the secrecy of the encryption method (or algorithm), only the secrecy of the keys. The secret keys must not be revealed when plaintext and cipher text are compared, and no person should have knowledge of the key (**fig.1**).

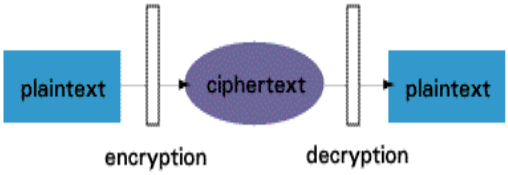

Fig. 1: Basic Encryption and Decryption

There are two types of key-based encryption:
1. Symmetric (or secret-key)
2. Asymmetric (or public-key) algorithms.

Symmetric algorithms (**Fig. 2**) use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key). Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers can encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.

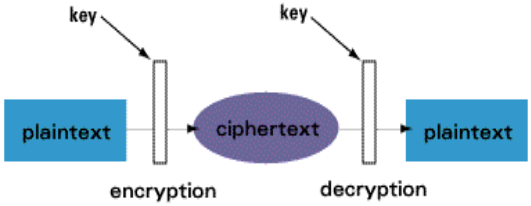

Fig. 2: Symmetric Algorithm

Asymmetric algorithms (**Fig. 3**) use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key. Asymmetric ciphers make a public key universally available, while only one individual possesses the private key. When data is encrypted with the public key, it can only be decrypted with the private key, and vice versa.

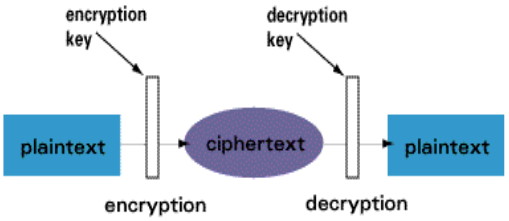

Fig 3: Asymmetric Algorithm

B. *RSA Procedure*

The RSA algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. It is the most widely known public key cryptographic algorithm.

The entire RSA algorithm can be performed using three steps:

i. Key generation:

- Generate two distinct prime numbers p and q.
- Find n such that n=pq, n will be used as modulus for both public and private keys.
- Find the Euler totient of n, $\Phi(n)$
  $\Phi(n) = (p-1)(q-1)$
- Choose e such that $1<e<\Phi(n)$, and such that e and $\Phi(n)$ share no divisors other than n(e and $\Phi(n)$ are relatively prime). e is kept as the public key exponent.
- Determine d (using modular arithmetic) which satisfies the congruence relation $de \equiv 1 \pmod{\Phi(n)}$.

In other words, pick d such that de-1 can be evenly divided by (p-1) (q-1), the totient or $\Phi(n)$.

This is often computed using the Extended Euclidean Algorithm, since e and $\Phi(n)$ are relatively prime and d is to be the modular multiplicative inverse of e. d is kept as the private key exponent.

The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n and the private (or decryption) exponent d, which is kept secret.

Fig. 4 explains the key generation process

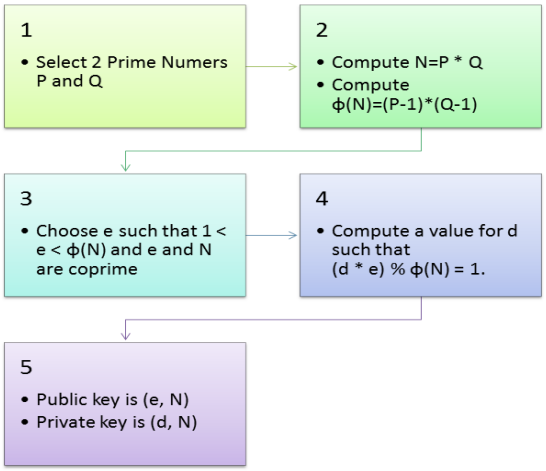

Fig. 4: Key generation in RSA

ii. **Encryption:**

The process of converting plain text to cipher text is known as encryption. It is also known as enciphering. Any algorithm which encrypts the data is known as encryption algorithm. The sender uses the encryption algorithm. Encryption process is done using the public key of the receiver. the cipher text is obtained by:

c □ mf (mod n), where m is the message and (e,n) is the public key.

iii. Decryption:

Restoring the plain text from the cipher text is known as deciphering or decryption. Any algorithm which decrypts the data is known as decryption algorithm. The receiver uses the decryption algorithm. The original message can be obtained using the cipher text as:

m □ c^{d} (mod n), where c is the cipher text and (d,n) is the private key.

Fig. 5 explains the entire RSA procedure.

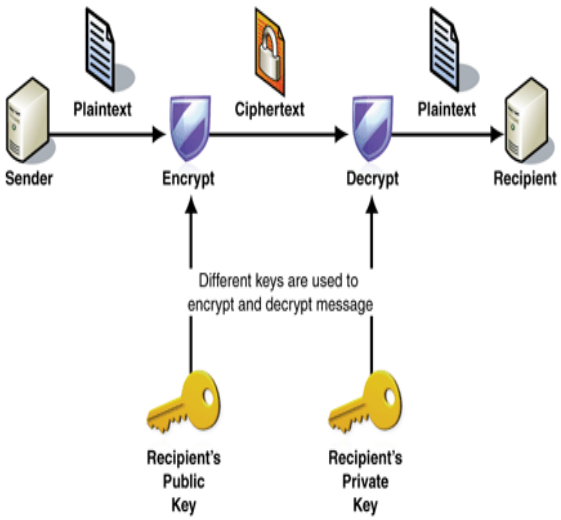

Fig. 5: RSA algorithm

C. *RGB Color Model*

The RGB color model is based on the Young–Helmholtz theory of trichromatic color vision, developed by Thomas Youngand Hermann Helmholtz in the early to mid nineteenth century, and on James Clerk Maxwell's color triangle that elaborated that theory.

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. The name of the model comes from the initials of the three additive primary colors, red, green, and blue.

To form a color with RGB, three colored light beams (one red, one green, and one blue) must be superimposed. Each of the three beams is called a *component* of that color, and each of them can have an arbitrary intensity, from fully off to fully on, in the mixture.

Zero intensity for each component gives the darkest color (no light, considered the *black*), and full intensity of each gives a white; the *quality* of this white depends on the nature of the primary light sources, but if they are properly balanced, the result is a neutral white matching the system's white point. When the intensities for all the components are the same, the result is a shade of gray, darker or lighter depending on the intensity. When the intensities are different, the result is a colorized hue, more or less saturated depending on the difference of the strongest and weakest of the intensities of the primary colors employed.

In computers, the component values are often stored as integer numbers in the range 0 to 255, the range that a single 8-bit byte can offer. These are often represented as either decimal or hexadecimal numbers. Figure 6 shows some of the colors and their RGB values in decimal format.

Color	Decimal Code (R,G,B)
	rgb(255,255,255)
	rgb(255,0,0)
	rgb(0,255,0)
	rgb(0,0,255)
	rgb(255,255,0)
	rgb(0,255,255)
	rgb(255,0,255)
	rgb(192,192,192)
	rgb(128,128,128)
	rgb(128,0,0)

Fig. 6: (R, G, B) values of some colors in decimal

D. *Hexa Decimal representation and conversion from hexadecimal to decimal*

Hexadecimal (also base 16 or hex) is a positional numerical system with a radix, or base, of 16. It uses sixteen distinct symbols, most often the symbols 0–9 to represent values zero to nine, and A, B, C, D, E, F (or alternatively a–f) to represent values ten to fifteen.

Each hexadecimal digit represents four binary digits (bits), and the primary use of hexadecimal notation is a human-friendly representation of binary-coded values in computing and digital electronics. One hexadecimal digit represents a nibble, which is half of an octet or byte (8 bits).

In the Hexadecimal number the color value is represented using 6 letters. The first two MSBs characters represent the R component, the next two G component and the two LSBs represent B component. Fig. 7 shows the conversion of hexa decimal to decimal.

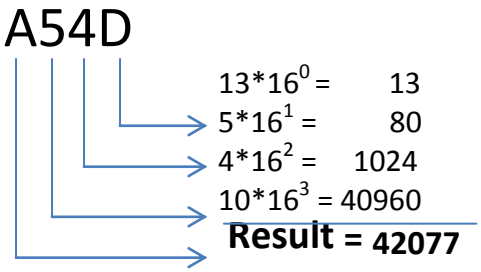

Fig. 7: conversion of hexadecimal to decimal

Fig. 8 shows some of the colors along with their hexadecimal and (R, G, B) Components.

Color	Color HEX	Color RGB
	#000000	rgb(0,0,0)
	#FF0000	rgb(255,0,0)
	#00FF00	rgb(0,255,0)
	#0000FF	rgb(0,0,255)
	#FFFF00	rgb(255,255,0)
	#00FFFF	rgb(0,255,255)
	#FF00FF	rgb(255,0,255)
	#C0C0C0	rgb(192,192,192)
	#FFFFFF	rgb(255,255,255)

Fig. 8: Hexadecimal and (R, G, B) values of some colors.

III. IMPLEMENTATION

First of all every user is assigned with a unique color. The (R, G, B) components of the assigned color are obtained. Next step is to assign unique public key and private key pair for the user. There are calculated using RSA key generations. The sender will know the color values of the receiver to which it wants to send the message. Now the message will be encrypted using public key of the receiver and the receiver's color values are encrypted using the key given by the user. This encrypted color value acts as a password. At the receiver's side, first the receiver has to prove his/her authenticity. For that we need to provide his color values. If the decrypted color values and original color values are equal then the receiver is said to be authentic and will proceed to decrypting the message. The message will be decrypted using receiver's private key(which is known only to the user) using RSA decryption. And thus both confidentiality and authenticity are provided.

RESULTS:

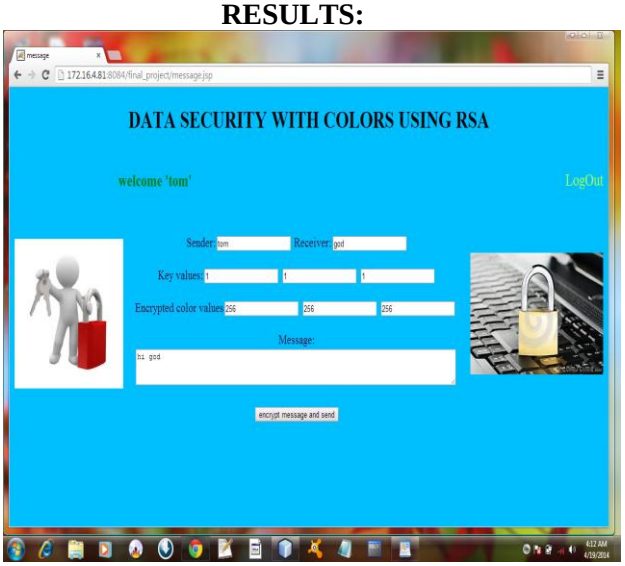

Fig. 9: Original message at sender side

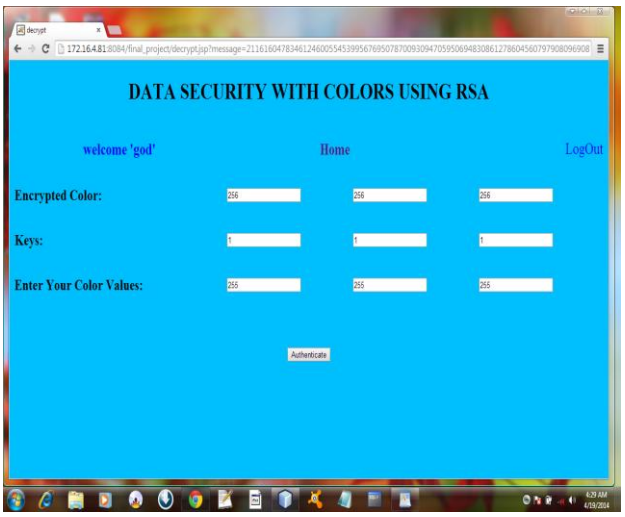

Fig. 10: Authentication at receiver side

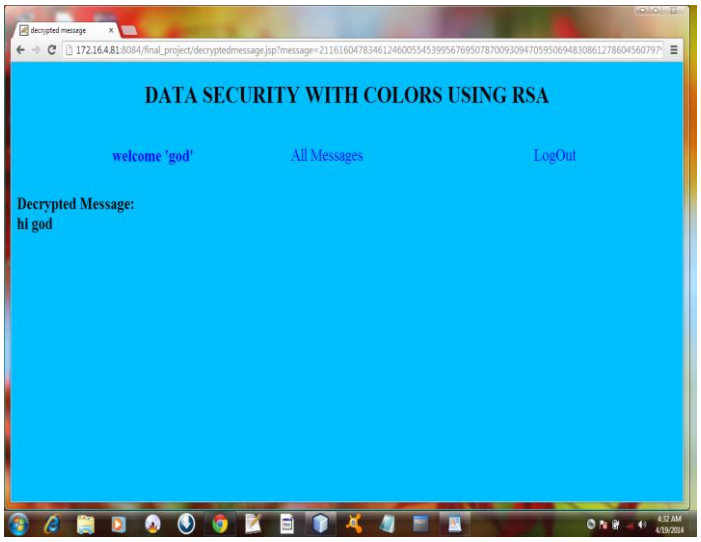

Fig. 11: Decrypted message at receiver side

IV. CONCLUSION

This paper provides a platform to send and receive messages in a secure manner by providing both authentication and confidentiality. We consider a basic cryptographic algorithm i.e RSA algorithm to encrypt and decrypt the messages sent from one person to another and this provides confidentiality. But the main disadvantage of RSA algorithm is that here the encryption is done using the receiver's public key. Since a user's public key is available to everyone in the network. There is no authentication i.e anyone can send messages to anyone. Therefore through this system we have overcome this disadvantage by providing authentication.

Authentication in the proposed system is provided using COLORS. Every user is assigned a unique color which is used in authenticating. The user should enter correct color values either to encrypt a message or to decrypt and view the message. Thus this is a complete system or a platform which can be used to send confidential messages within a group providing both confidentiality and authentication.

REFERENCES

[1] Advanced Encryption Standard",2001.Federal *Information Processing Standard Publications*.
[2] Hu, Zhihua,2011. "Progress on advanced encryption standard". *International conference on Intelligence Science and Information Engineering*.China.
[3] Cryptography and Network Security 4/e, by *William Stallings*
[4] http://www.ijitee.org/attachments/File/v1i1/A117051112.pdf
[5] http://interscience.ac.in/URJA/journals/urja_vol1no1/urja_paper18.pdf