International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Security of Data with RGB Color and AES Encryption Techniques

Prajakta Dusane[1], Jagruti Patil[2], Urvashi Jain[3], Ruchita Pandya[4]

[1]*Student, Dept. of Computer Engineering, SSBT COET, Bambhori, Jalgaon, Maharashtra, India.*
[2]*Student, Dept. of Computer Engineering, SSBT COET, Bambhori, Jalgaon, Maharashtra, India.*
[3]*Student, Dept. of Computer Engineering, SSBT COET, Bambhori, Jalgaon, Maharashtra, India.*
[4] *Student, Dept. of Computer Engineering, SSBT COET, Bambhori, Jalgaon, Maharashtra, India.*

Abstract - *In RSA algorithm, the encryption is done utilizing the receivers public key. Since a users public key is available to everyone in the network. RSA provides confidentiality but the dominant disadvantage of RSA is that there is no authentication i.e anyone can send messages to anyone. In existing work RSA algorithm is utilized with RGB model for providing confidentiality and authentication but with less accuracy. Due to less accuracy existing system isn't totally secured. In proposed work AES encryption technique with RGB color is use to extend the accuracy of the system. It'll provides confidentiality, authentication and greater privacy to the data which is sent across the network.*

Key Words: **RSA, AES, ECC, DES, RGB color model, encryption, decryption, public key, private key**

1.INTRODUCTION

There are many encryption algorithms available and used in information security. These algorithms can be categorized into Symmetric and Asymmetric key encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt data while in Asymmetric keys, two keys are used; private and public keys. The public key is used for encryption and private key is used for decryption for example, RSA. There are examples of symmetric cryptographic algorithms like AES and DES. AES uses various 128,192,256 bit keys while DES uses one 64-bits key[4]. All these algorithms can provide authentication, integrity, confidentiality and authorization to data travel from one point another point.

Authentication services provides the 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[1].

Confidential 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[1].

2. LITERATURE SURVEY

G. SankaraRao et al.[1] illustrated a technique that integrates the RGB Color model public key cryptographic algorithm RSA. The RSA algorithm is used to perform encryption and decryption. To provide authentication between sender and receiver along with security, COLORS are used. With the help of colors, both sender and receiver will get validated.

Prof. ManojDhande et al.[3] explained a new encryption technique that uses the AES algorithm using color code and palindrome numbers for encrypting any type of file which provides more security than any other approach. This approach gives a technique to send data over the network in a set of three keys (palindrome number, alphanumeric, random key and ASCII value of color code).

Dr. PrernaMahajan et al.[8] implemented three encryption techniques like AES, DES and RSA algorithms and compared their performance of encryption techniques based on the analysis of its stimulated time at the time of encryption and decryption. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using the decryption technique the receiver can view the original data.

VanyaDiwan et al. [4] explained Cloud security implementation using various cryptographic algorithms, DES AES, RSA and ECC. It describes the comparison among these algorithm. To secure the Cloud means secure the "databases hosted by the Cloud provider". Security goals of data include three points, namely: Confidentiality, Integrity, and Availability (CIA).

Nentawe Y. Goshwe et al [2] presented a design of data encryption and decryption in a network environment using the RSA algorithm with a specific message block size. The algorithm allows sender to generate a public key to encrypt the message and the receiver is sent a generated private key using a secured database. An incorrect private key will still decrypt the encrypted message, but in different format than original message.

3. EXISTING SYSTEM

The RSA algorithm was invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT. The RSA algorithm is the most widely known asymmetric key cryptographic algorithms[1]. The entire RSA algorithm can be performed using three steps:

i. Key generation

ii. Encryption

iii. Decryption

RSA uses two exponents, e and d, in which e is public and d is private. The plaintext is P and C is cipher text, then at encryption side:

$$C = P^e \bmod n$$

And at decryption side:

$$P = C^d \bmod n$$

Where, n is a very large number, created during key generation process[8].

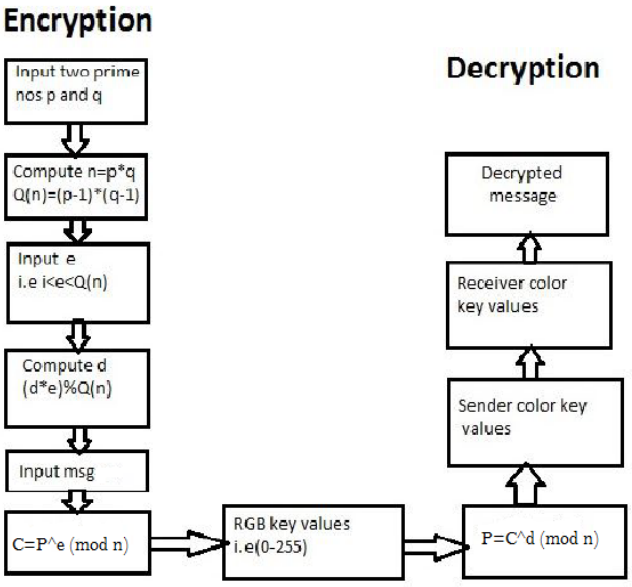

Fig-1: RSA Encryption and Decryption

When RSA is used with RGB color, provides security with less accuracy and it requires more execution time as shown in Fig-1. Therefore, in proposed system, AES encryption algorithm is used to provide security with greater accuracy.

4. PROPOSED SYSTEM:

Proposed system deals with providing security to data with colors and AES encryption technique. This security is in the form of confidentiality and authentication. When providing security to the data simultaneously comparison of the AES algorithm with other encryption algorithm also take place.

Encryption is a technology which protects sensitive data. Combination of Public and Private Key encryption is used to hide the confidential data of users, and cipher text retrieval[4].

4.4 Advanced Encryption Standard(AES):

Advanced Encryption Standard is a symmetric- key encryption algorithm published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). It is carefully tested for many security applications. AES algorithm encrypts data with block size of 128-bits. It uses 10, 12 or 14 rounds. The key size may be 128, 192, or 256 bits, depending on the number of rounds[8] as shown in Fig-2.

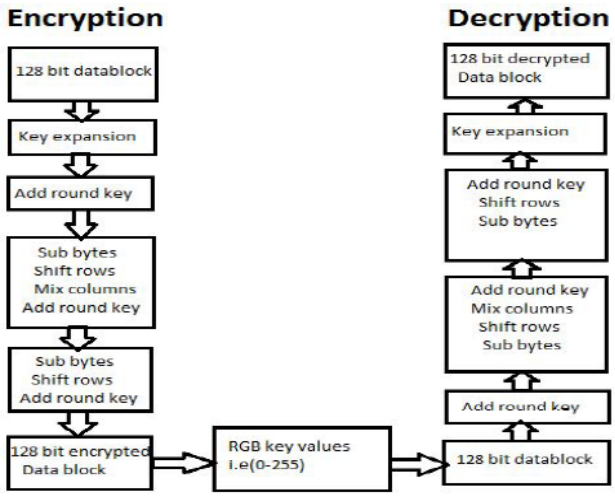

Fig-2: AES Encryption and Decryption

4.2 Data Encryption Standard (DES):

The Data Encryption Standard (DES) is a symmetric- key encryption algorithm published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). DES takes a 64-bit plaintext and generates a 64-bit cipher text, at the encryption site while at the decryption site, it takes a 64-bit cipher text and generates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption operation is made of two permutations (P-boxes), which are called final and initial permutation, and sixteen Feistel rounds. Each round uses a 48-bit round key differently, generated from the cipher key according to a predefined algorithm[8].

4.3 ECC Algorithm:

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in many integer factorization algorithms having applications in cryptography. Smaller key size, reducing storage and transmission requirements are the primary advantage given by ECC, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key. For current cryptographic purposes, an elliptic curve is a plane curve over a finite field which consists of the points satisfying the equation,

$$y2=x3+ax+b,$$

along with a distinguished point at infinity, denoted ∞.This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety[8].

4.4 RGB Color Model:

The RGB color model is based on the work of Thomas Young and Hermann von Helmholtz in the 19th century is a theory of trichromatic color vision, and on James Clerk Maxwell's color triangle that elaborated that theory.

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

Three colored light beams, each of red, green and blue must be superimposed, for forming a color with RGB. 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[1] as shown in Fig-3.

The full intensity of each component gives a white color while zero intensity for each gives the darkest color that is, no light, considered as black color. The quality of white color 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. If the intensities for all the color components are same, then the result is a shade of gray, darker or lighter depending on the intensity. When the intensities are different, color shades are also different 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 of 0 to 255, the range that a single 8-bit byte can offer. These are represented as either decimal or hexadecimal numbers[1].

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-3: RGB color model

4.5 Comparison of various Algorithm:

A common aim for cryptographic algorithms is to provide confidentiality and authentication. A cryptographic algorithm is considered to be computationally secured if it cannot be broken with standard resources. An efficient cryptosystem can produce possible results if the key size is comparable to the size of the packet to be transmitted over the network[8]. The algorithm is compared on the basis of parameters like key-length, block-size, security rate and execution time as shown in Table-1:

Table -1: Comparison of Algorithms

Factors	DES	AES	RSA	ECC
Contributor	IBM 75	Rijman, Joan	Rivest, Shamir 78	Neal Koblitz, Victor S. Miller
Key Length	56-bits	128, 192 and 256	Based on No. of bits in N=p*q	135-bits
Block Size	64-bits	128 bits	Variants	Variant
Security Rate	Not enough	Excellent	Good	Less
Execution Time	Slow	More fast	Slowest	Fastest

5. RESULT:

The system shows result on the basis of inserting messages. It will generate a different graph for different input message. The graph shows a comparison between all four algorithm with respect to time (execution time). For example, consider input1 as "Welcome to SSBT COET, Bambhori", it will generate the graph shown in Chart-1. The graph shows the time required by each algorithm to execute given input message.

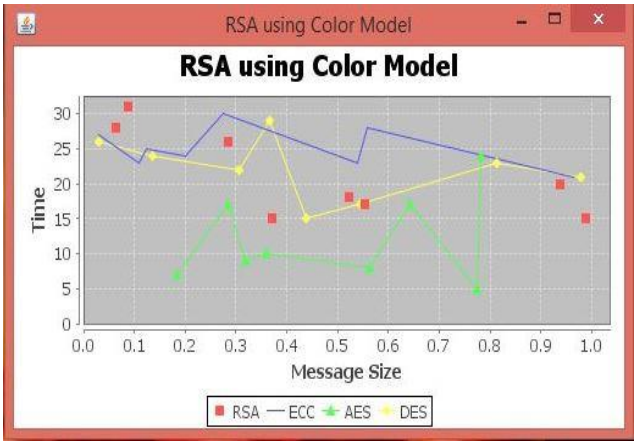

Chart-1: Graph for input1

Considering another example input2 as "Hello, I am Student", it will generate the graph shown in Chart-2. The graph shows some variations from the graph generated by input1.

Hence on the basis of size of message different graph will be generated for different message input. By considering a number of different input graph states that AES works better with the RGB model as it takes less execution time.

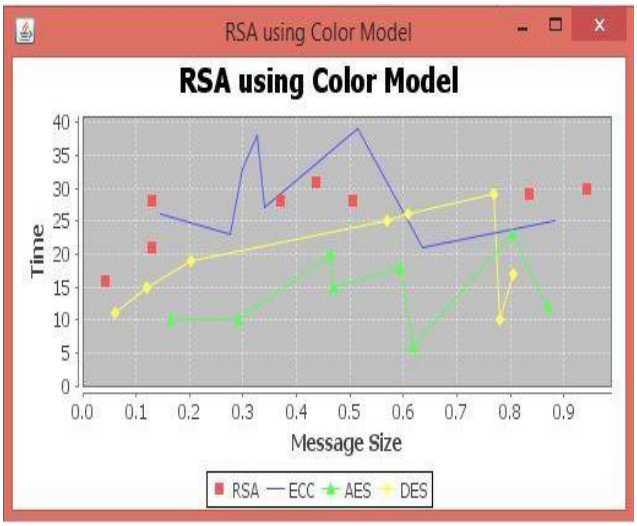

Chart-2: Graph for input2

Hence on the basis of size of message different graph will be generated for different message input. By considering a number of different input graph states that AES works better with the RGB model as it takes less execution time.

6. CONCLUSIONS

Encryption algorithm plays very crucial role in communication security. Research work surveyed the performance of AES encryption technique used with RGB

Color models to provide security by comparing with different encryption techniques like ECC, DES and RSA algorithms. The color model and AES encryption technique are the two main factors in proposed system which gives assurance for secured data message transmission which is made available to authorized persons. Based on the texts used and the experimental result, it was concluded that the AES algorithm consumes least encryption and ECC consumes longest encryption time. It also observed that Decryption of AES algorithm is better than other algorithms. From the simulation result, evaluated that AES algorithm is much better than DES, ECC and RSA algorithm. Hence, both authentication and confidentiality are provided with more accuracy.

Future work will focus on compared and analysed existing cryptographic algorithm like AES, DES, ECC and RSA. It will include experiments on image and audio data and focus will be to improve encryption time and decryption time.

REFERENCES

[1] G. SankaraRao et al. "Data Security With Colors Using RSA", Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 9(Version 3), pp.95-99, September 2014.

[2] Nentawe Y. Goshwe "Data Encryption and Decryption Using RSA Algorithm in a Network Environment" IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013.

[3] Prof. ManojDhande, AkshayaSawant, NidhiPandey, PoojaSahu, "Secure Data Communication using AES Algorithm, Palindrome Number and Color Code", International Journal on Recent and Innovation Trends in Computing and Communication ISSN : 2321-8169 Volume: 4 IJRITCC April 2016.

[4] Dr. PrernaMahajan and AbhishekSachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web and Security Volume 13 Issue 15 Version 1.0 Year 2013.

[5] Dr.R.Shanmugalakshmi and M.Prabu, "Research Issues on Elliptic Curve Cryptography and Its applications", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.

[6] Sharad Kumar Verma and Dr. D.B. Ojha, "A Discussion on Elliptic Curve Cryptography and Its Applications", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, ISSN (Online): 1694-0814, January 2012.

[7] Shaza D. Rihan, Ahmed Khalid and SaifeEldin F. Osman, "A Performance Comparison of Encryption Algorithms AES and DES", International Journal of Engineering Research and Technology (IJERT) ISSN : 2278-0181 Vol. 4 Issue 12, December-2015.

[8] Diwan et al.,"Cloud Security Solutions: Comparison among Various Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering 4(4), pp. 1146-1148, April - 2014.

[9] Roger Pressman, "Software Engineering: A Practioner's Approach", McGraw-Hill, Seventh Edition, pp.449-490. ISBN-10: 0073375977 ISBN-13:978-007337597, retrieved 2 September, 2016.

[10] Grady Booch, James Rumbaugh, Ivar Jacobson, "The Unified Modeling Language User Guide", Pearson, Second Edition, 2005, pp. 225-284. ISBN: 978-03-2126-79-79, retrieved 5 September, 2016.

[11] AsmaChaouch, BelgacemBouallegue and OuniBouraoui, "Software Application for Simulation-Based AES, RSA and Elliptic-Curve Algorithms", 2nd International Conference on Advanced Technologies for Signal and Image Processing - ATSIP, Monastir, Tunisia, IEEE, March 21-24 2016.

[12] Fei Shao, Zinan Chang, Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", Second International Conference on Communication Software and Networks, IEEE 2010.

[13] Mr. NiteenSurv et.al, "Framework for Client Side AES Encryption Technique in Cloud Computing",IEEE International Advance Computing Conference (IACC), 2015.

BIOGRAPHIES

Miss. Prajakta Dusane currently pursuing her graduate Engineering degree in Computer Engineering from SSBT COET, Bambhori, Jalgaon under North Maharashtra University, Jalgaon, India.

Miss. Jagruti Patil currently pursuing her graduate Engineering degree in Computer Engineering from SSBT COET, Bambhori, Jalgaon under North Maharashtra University, Jalgaon, India.

Miss. Urvashi Jain currently pursuing her graduate Engineering degree in Computer Engineering from SSBT COET, Bambhori, Jalgaon under North Maharashtra University, Jalgaon, India.

Miss. Ruchita Pandya currently pursuing her graduate Engineering degree in Computer Engineering from SSBT COET, Bambhori, Jalgaon under North Maharashtra University, Jalgaon, India.