International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 224 – 228

Simulation and Analysis of Modified RSA Cryptographic Algorithm using Five Prime Numbers

Dharitri Talukdar[1]
PhD Research Scholar, CSE Deptt.
Assam down town University, Guwahati, India
dharitritalukdar03@gmail.com

Lakshmi Prasad Saikia[2]
Professor & Head, Dept. of Computer Sc. & Engineering
Assam down town University, Guwahati, India
lp_saikia@yahoo.co.in

Abstract—Today, internet is being widely used by everyone with different ages of people. Every day we share our valuable information such as credit card, bank account details over network. So security is an important parameter to protect our secret information from unauthorized access. Security in network is based on cryptography. Cryptography is a phenomenon to hide original information to unreadable form so that they can be read only by the intended receiver. The most common public key cryptographic algorithm is RSA used for encryption and decryption. Strong encryption algorithms and optimized key management techniques always help in achieving confidentiality, authentication and integrity of data and reduce the overheads of the system. Keeping in view the importance of dynamic keys for secure data transmission, the paper is focused on the use of dynamic keys for data security.This includes the architectural design and enhanced form of RSA algorithm through the use of five prime numbers in order to make a modulus n which is not easily decomposable by intruders. Simulations of results have been achieved by using MATLAB12a.

Keywords-*RSA, encryption, decryption, security, cryptography, dynamic keys.*

*****

I. INTRODUCTION

Encryption is one of the principal means to ensure the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security and etc. Therefore, the purpose of adopting encryption techniques is to ensure the information's confidentiality, integrity and certainty, prevent information from tampering, forgery and counterfeiting [1].

There are basically two types of cryptography:

- ***Symmetric cryptography:*** Symmetric key encryption uses the same key for encryption and decryption of message.
- ***Asymmetric cryptography:*** Asymmetric key uses different keys are used for encryption and decryption it is also known as the public-key encryption.

At present, most popular and widely used public key cryptosystem is RSA. RSA was first proposed by Ron Rivest, Shamir, and Adleman in 1977. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. Its security is based on the difficulty of the large number prime factorization, which is a well known mathematical problem that has no effective solution. RSA public key cryptosystem is one of the most typical ways that most widely used for public key cryptography in encryption and digital signature standards [1]. RSA has two keys- private key and public key. Both keys are used for encryption and decryption purpose. RSA algorithm is broadly classified into three steps [2]:

[1]. Key generation
[2]. Encryption
[3]. Decryption

Key generation

- Select two different prime numbers p and q
- Calculate n=p*q
- Calculate phi=(q-1)(p-1)
- Select an integer e such that 1<e<phi and GCD (e, phi) =1; e and phi are co prime.
- Choose a number relatively prime to phi and call it d.
- Find d such that e*d=1mod phi
- Public key is (n, e)
- Private key is (n, d)

Encryption- Cipher text, $C= M^e \bmod n$
Decryption- Plain text, $M= C^d \bmod n$

II. OBJECTIVES

1) The first objective is to design an optimized algorithm based upon dynamic keys for data encryption.
2) The second objective is to compare and analyze the performance of RSA cryptographic algorithm and enhanced RSA cryptographic algorithm.

III. METHODOLOGY

The methodology of the research has been shown with the help of following diagram.

ISSN: 2321-8169
224 – 228

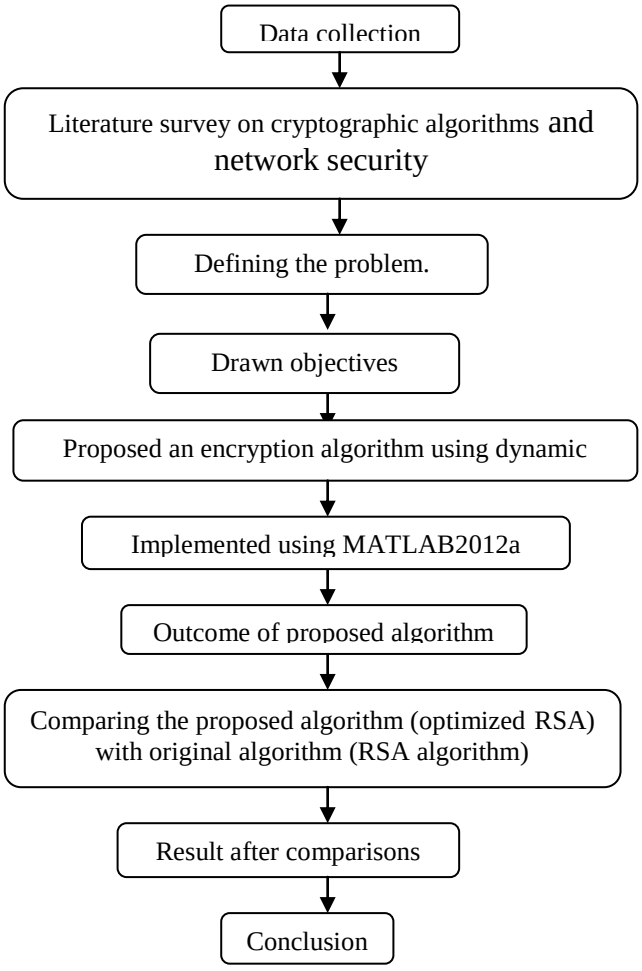

Fig1: Methodology flowchart of proposed research work

IV. REVIEW OF EXISTING LITERATURE

In 2000, James H. Yu and Tom K. Le, concluded that most people do not know they are at risk until an attack occurs. The general rule is that as network security increases, cost increases, and the overall system network performance decreases [5].

Othman O. Khalifa et.al. in 2004 discussed basic concepts, characteristics, and goals of various cryptography. In today's information age, communication plays an important role which is contributed to growth of technologies therefore privacy is needed to assure the security that is sent over communication media [3].

Aljawarneh et.al. in 2010, proposed a secure Wireless Fidelity (sWIFI) system which provides more efficiency, security and authentication for transmitted data over the network[4].

M. Lakshmi et.al in 2013 concluded that Keyless User Defined Optimal Security Encryption (KUDOS) is based on the concept of user customization. The algorithm doesn't use the traditional approach of using an encryption key; but defines a series of sequence-counters for encoding. The cryptosystem gives extra power to the user i.e. to choose the sequence-counters [6].

Lalit Singh et al. in 2013conclude that IB_mRSA is the first best algorithm and Blowfish is the second best has better performance than other algorithms. Secondly, IB_mRSA has advantage over the other algorithms in terms of throughput & processing time except Blowfish. Third point is that RSA has the least performance among all the algorithms mentioned here [7].

Thakur et al showed that AES can be implemented more comfortably in high and low level language as compared to DES. Blowfish has better performance when packet size is changing as compared to AES, DES, 3DES, RC2, and RC6 [8].

Pramendra et al. concluded that where the cryptography only change the format of the information that cannot be understood by any unauthorized user, the steganography hide the complete information in the cover media, so no one can easily identify that any message is hidden in the presented content. However both of these techniques provide the security to information but the standalone approach based of either of these techniques is not so good for practice. Therefore to provide more security to the information at the time of communication over unsecured channel a novel advance technique for data security is needed [9].

Yousif Elfatih Yousif et.al in 2015, concluded that - encryption/decryption speed for DES algorithms is faster than RSA; AES is more secure compared to DES; the throughput rates for BLOWFISH are greater than all symmetric algorithms, while the power consumption of BLOWFISH is the least among all algorithms; and RC6 algorithm uses a variable number of bits ranging from 8 to 1024 bits and encrypts the data 16 times, therefore making it difficult for a hacker to decrypt it[10].

Ako Muhammad Abdullah et.al in 2016 said that a cryptography and steganography methods have proposed for providing better security of data in a network environment. With system that they have proposed data can be transferred between sender and receiver via unsecured network environment. Obviously, in a network environment this system is one of the best ways of hiding the secret of message from intruders. Cryptography method i.e Affine cipher algorithm has been implemented to encrypt the secret message and converted into ASCII code before embedding it in the image so that it is not easy to intruder to break the encryption without

the keys and password. In addition, Hash based Least Significant Bit (H- LSB) technique has been implemented for embedding encrypt message into cover images. To evaluate this system they tested a number of images with various sizes of data to be hidden with the proposed algorithms. According to the tested we found that the system has the ability to provide a better security and easy way to encrypt, embedding and decrypt secret message without the quality of image is decreased as seen by the naked eyes [11].

Musaria K. Mahmood et.al in 2017, concluded that SAFER+ presents an encryption decryption algorithm with good hardware software implementation. An encryption decryption platform is implemented by SAFER+ using MATLAB. This platform can be used for data encryption from personal use or for small institution with insignificant cost. Results of the implementation show a good performance in encryption of pictures and in general. The speed of SAFER+ routine presents an opportunity to use it for the encryption of all type data of data [12].

V. PROPOSED APPROACH OF RSA CRYPTOGRAPHIC ALGORITHM

The proposed approach is instead of using two prime numbers to generate public and private key, we will going to generate five prime numbers with reduced size which will generate variable N with large size. Hence factorization in this case will be more difficult than original algorithm.

The three phases are as follows-

- Key generation
- Encryption
- Decryption

Key generation:

- Select five prime numbers- p, q, r, s and t.
- Calculate n=p*q*r*s*t.
- Calculate phi = (p-1)*(q-1)*(r-1)*(s-1)*(t-1).
- Select an integer e such that 1<e<phi and GCD (e, phi) =1; e and phi are co prime.
- Choose a number relatively prime to phi and call it d.
- Find d such that e*d=1mod phi

Encryption-

Cipher text, $C= M^e \bmod n$

Decryption-

Plain text, $M= C^d \bmod n$

VI. FLOW CHART OF PROPOSED RESEARCH WORK

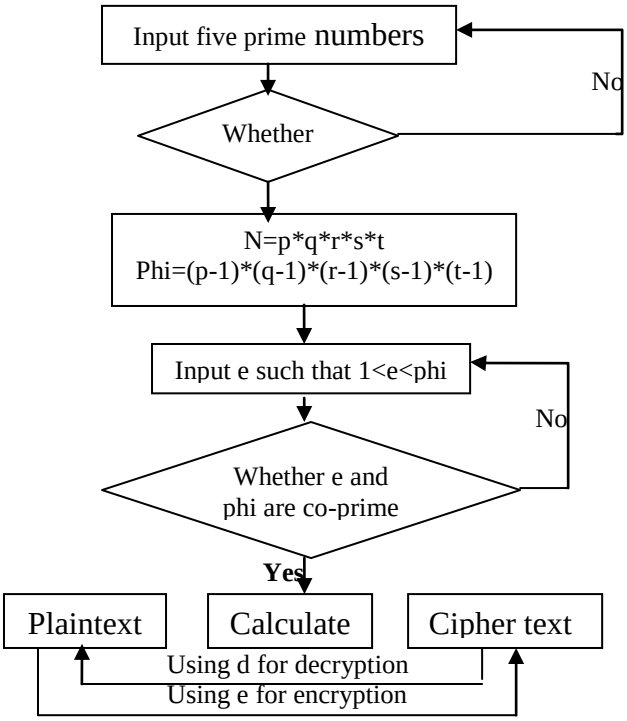

Fig2: Flow chart for proposed algorithm

VII.RESULT AND ANALYSIS

Simulation results have also been drawn using MATLAB 12a. To implement proposed algorithm we have to focus on three parts which are a) key generation, b) encryption process, and c) decryption process.

Key Generation:

Generate five large prime numbers p, q, r, s and t. Here first we have to input five large prime numbers and then we calculate the value of d and e which were used to generate private and public key respectively.
Choose
p=51 **q**=43 **r**=13 **s**=19 **t**=7
Compute **N**= 3791697
Compute **phi**= 2721600
Let **e**=41
Find **d** such that **e*d=1 mod phi**
d= 132761
Public key (e, n) = (41, 3791697)
Private Key (d, n) = (132761, 3791697)

Encryption Process:

With the help of public key we are able to encrypt the value of plain text. Enter the value of plain text and we get the cipher text.
Suppose the message to be encrypted is: **HELLO**

TABLE1: ENCRYPTION PROCESS

Plain text letter	m (*ASCII code*)	m^e	Cipher text (m^e *mod n*)
H	72	14145957653885679761892884164 43101721917564361657473675602 4242800599259676672	446730
E	69	24706584990989220424756174091 92285433067939556380902322915 037637678266264869	2381259
L	76	12982468679182254319408563976 47511451022538383346318454734 5193926907802524057 6	1831486
L	76	12982468679182254319408563976 47511451022538383346318454734 5193926907802524057 6	1831486
O	79	63490791751778768787040188468 53379010136215327954435072395 57870430105727875279	1097968

Decryption Process:

With the help of the private key the cipher text can be converted to plain text. Compute $P=C^d$ mod n by using private key.

TABLE2: DECRYPTION PROCESS

Cipher text (m^e mod n)	c^d mod n	Plain text letter
446730	72	H
2381259	69	E
1831486	76	L
1831486	76	L
1097968	79	O

Decrypted value of the cipher text: **HELLO**

The following times were recorded while encrypting/decrypting data-

TABLE3: TIME ANALYSIS

File size (bytes)	RSA Cryptosystem		Modified RSA Algorithm	
	Encryption time(seconds)	*Decryption time (seconds)*	*Encryption time (seconds)*	*Decryption time (seconds)*
31	1.627547	0.542100	1.075914	0.035464
932	1.522997	0.051724	1.073711	0.031596
525	1.594673	0.546941	1.062067	0.035507

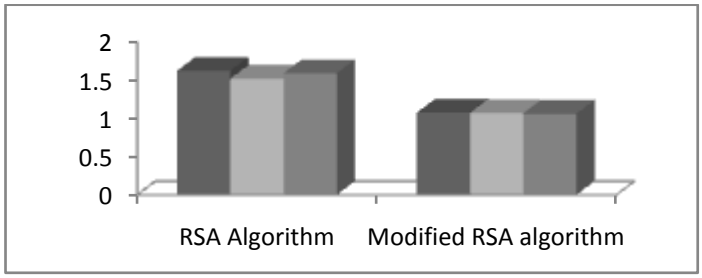

Figure3. Encryption time with different type of character

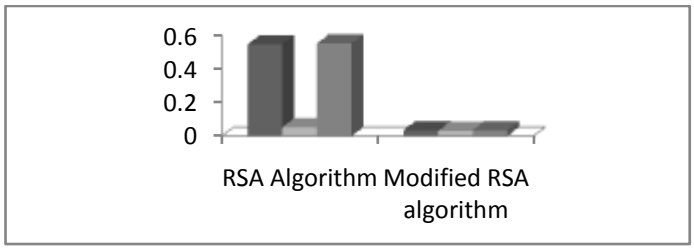

Figure4. Decryption time with different type of character

VIII. EXPERIMENTAL RESULTS AND DISCUSSIONS

When the cipher text is decrypted with the help of private key, same plain text has been observed. After analyzing RSA and modified RSA, it is found that the proposed algorithm increases the security of the system as it reduces the computation time. This shows that accuracy of optimized RSA cryptographic algorithm using dynamic keys is good.

IX. CONCLUSION

Study of various encryption algorithms has shown that the strength of the algorithm depends on the length of the key. Key length is directly proportional to security and inversely proportional to performance. Therefore hacking time is reduced which indicate that the time available for the hacker has been reduced.

X. REFERENCE

[1]. Vivek Choudhary and Mr. N. praveen, "Enhanced Rsa Cryptosystem Based On Three Prime Numbers", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10,December 2014, ISSN 2348 – 7968.

[2]. B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar, "A modified RSA cryptosystem based on 'n' prime numbers" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66.

[3]. Othman O. Khalifa, MD Rafiqul Islam, S. Khan and Mohammed S. Shebani, "Communication Cryptography",

2004 RF and Microwave Conference, Oct 5-6, Subang, Selangor, Malaysia.

[4]. Shadi R. Masadeh , Ahmad Azzazi, Bassam A. Y. Alqaralleh and Ali, Mousa.Al Sbou, "A Novel Paradigm In Authentication System Using Swifi Encryption /Decryption Approach", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[5]. Dr. James H. Yu & Mr. Tom K. Le, "Internet and Network Security", "Journal of industrial technology", Volume 17, Number 1 - November 2000 to January 2001.

[6]. M. Lakshmi, S. Kavitha, "Keyless User Defined Optimal Security Encryption ", International Journal Of Engineering And Computer Science, ISSN:2319-7242 Volume 2 Issue 6 June, 2013

[7]. Lalit Singh and Dr. R.K. Bharti , "Comparative Performance Analysis of Cryptographic Algorithms" ,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013 ISSN: 2277 128X.

[8]. Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011, ISSN 2250-2459.

[9]. Pramendra Kumar and Vijay Kumar Sharma, "Information Security Based on Steganography & Cryptography Techniques: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014 ISSN: 2277 128X

[10]. Yousif Elfatih Yousif, Dr.Amin Babiker A/Nabi Mustafa, Dr.Gasm Elseed Ibrahim Mohammed, "Review on Comparative Study of Various Cryptography Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015 ISSN: 2277 128X.

[11]. Ako Muhammad Abdullah and Roza Hikmat Hama Aziz, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 143 – No.4, June 2016

[12]. Musaria K. Mahmood, Lujain S. Abdulla, Ahmed H. Mohsin, and Hamza A. Abdullah, "MATLAB Implementation of 128-key length SAFER+ Cipher System", Musaria K. Mahmood.et.al. Int. Journal of Engineering Research and Application www.ijera.com ISSN : 2248-9622, Vol. 7, Issue 2, (Part -5) February 2017, pp.49-55