IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Development of "RSA" Encryption Algorithm for Secure Communication

Abhishek Guru[1*], Asha Ambhaikar[2]

[1]PhD Research Scholar (Computer Science) Kalinga University Naya Raipur, India
[2]Professor and Dean Student Welfare Kalinga University Naya Raipur, India

Corresponding Author: abhishekguru0703@gmail.com, Tel.: +91-70247-70703

DOI: https://doi.org/10.26438/ijcse/v7i6.581585 | Available online at: www.ijcseonline.org

Accepted: 12/Jun/2019, Published: 30/Jun/2019

***Abstract*—** In this paper there are modifications in the RSA algorithm by using more than four prime numbers in the combination of public and private key by using this factoring complexity of variables is increased. This is a new technique to provide max security for data over the internet. In this technique we are using more than four prime numbers which is not easily decomposed this technique provides more efficiency and reliability over the network. In this paper we try to increase the level of security by modifying the RSA Encryption Algorithm.

***Keywords*—**RSA Algorithm, Prime Numbers, Complexisity, Public Key, Private Key.

I. INTRODUCTION

In traditional telecommunication systems, securing the channel meant securing the messages. With the advent of internet and advancement in packet switching Techniques, securing the channel are neither possible nor effective. This increases the importance of cryptography. Cryptography involves creating written or generated codes that allow data to be kept secure. Cryptography converts data into a format that unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format these compromising the data [9]. RSA (Rivest Shamir Adleman) Algorithm is a public-key cryptography [1] and is considered as one of the great advances in the field of public key cryptography. It is suitable for both signing decryption and encryption. The RSA is more secure from multiple attacks, but the demerits of the RSA are low speed, demand for key deposit, and inappropriate for global system [7]. Rivest, Adi Shamir and Leonard Adleman are the developer of the RSA Encryption Algorithm. It was described in 1978. In this technique we used RSA encryption algorithm, in which the private key and public key included. This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers) [16]. The public key is made available to everyone. With this key a user can encrypt the data but can't decrypt it, the person who can decrypt it is the one who possesses the private key.

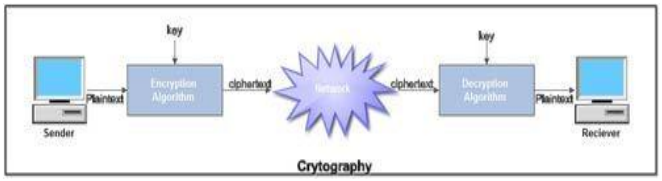

Figure 1: Cryptography

Purpose of Cryptography

Cryptography provides a number of security goals to secure the privacy of data, non alteration of data and soon. Due to the various security features of cryptography it is widely used today. Following are the various goals of cryptography [5].

1. Authentication: The process of proving one's identity. This includes verifying the message's source. Authentication is of two types: (i) Peer entity authentication, and (ii) Data origin authentication.

2. Privacy/confidentiality: Confidentiality means protection against unauthorized disclosure of information. It may be applied to whole messages, parts of messages, and even existence of messages. Confidentiality provides the protection of transmitted data from passive attacks.

3. Integrity: It assures the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.

4. Non-repudiation: Sender or receiver cannot deny for a transmitted message. When a message is sent, the receiver can prove that the sender in fact sent the message.

5. Service Reliability and Availability: Secure systems usually get assailing by intruders, which may affect their type of service to their users. Such systems provide a way to grant their users the quality of service they expect.

Basic Terminology of Cryptography

1.

[14] The terminology used in cryptography is given below:

1. **Plaintext.** The original message or data which is fed into the algorithm as input is called plaintext
2. **Encryption algorithm**. The encryption algorithm is the algorithm that performs various substitutions and transformations on the plaintext. Encryption is the process in which we change plaintext into cipher text.
3. **Cipher text.** Cipher text is the encrypted form the message. It is the scrambled message produced as output. It depends upon the plaintext and the key.
4. **Decryption algorithm.** The process in which we change Cipher text into plain text is known as decryption. Decryption algorithm is reverse of encryption. It takes the Cipher text and the key produces the original plaintext.
5. **Key**. It also plays as input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm based on the key. The key is a number or a set of number that the algorithm uses to perform encryption and decryption.

CLASSIFICATION OF ENCRYPTION ALGORITHMS:

Encryption algorithms can be classified into two categories- Symmetric and Asymmetric key encryption.

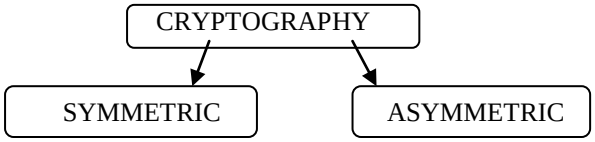

Figure 2: Classification of Cryptography

SYMMETRIC CRYPTOGRAPHY

In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems. It is used to provide confidentiality of the messages. The following symmetric algorithms such as DES, 3DES, Blow Fish, IDEA, TEA, CAST 5, AES, RC6, Serpent, Two Fish and MARS are described in details according to their overview of architecture and security [15].

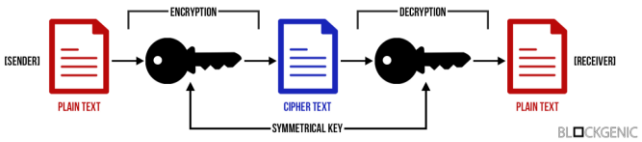

Figure 3: Symmetric Cryptography

ASYMMETRIC CRYPTOGRAPHY

The asymmetric cryptography where a secret key can be divided into two parts a public key and a private key. The public key can be given to anyone, while the private key must be kept secret (just like the key in symmetric cryptography). Asymmetric cryptography has two major use cases: authentication and confidentiality. Using asymmetric cryptography, messages can be signed with a private key, and then anyone with the public key is able to verify that the Message was created by someone possessing the corresponding private key[8]. This can be combined with a proof of identity system to know what entity (person or group) actually owns that private key, providing authentication. Encryption with asymmetric cryptography works in different way from symmetric encryption. Someone with the public key is able to encrypt a message, providing confidentiality, and then only the person in possession of the private key is able to decrypt it.

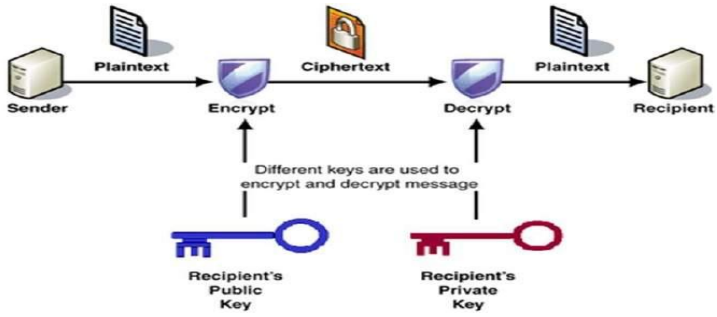

Figure 4: Asymmetric Cryptography

Now following figure shows some different Symmetric and Asymmetric Cryptographic Algorithms

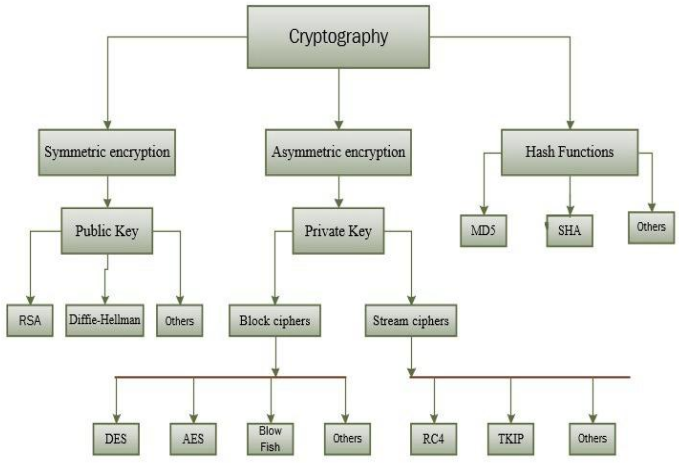

Figure 5: Different Symmetric & Asymmetric Cryptographic Algorithms

RSA

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The RSA algorithm works on a public and private key system. The public key is made available to everyone to encrypt data

but cannot decrypt, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key; this makes the RSA algorithm a very popular choice in data encryption [6].

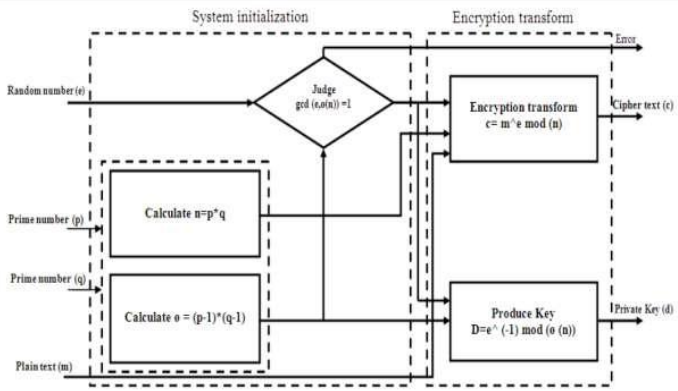

Figure 6: RSA Algorithm workflow diagram

II. RELATED WORK

Omar G. Abood and Shawkat K. Guirguis, A Survey On Cryptography Algorithm, 2018, In this paper author survey various encryption algorithm for data encryption and decryption and also compare them to each other to find that which algorithm is very secure [16].

Sarthak R Patel et al, Study on Improvements in RSA Algorithm, 2017, In this paper author studied the various research paper based on Implementation on RSA encryption algorithm and compare the result of all research papers and also proposed some modification on RSA algorithm for batter performance [11].

Arpit Agrawal Gunjan Patankar, Design of Hybrid Cryptography Algorithm for Secure Communication, 2016, In this paper author uses the AES and DES algorithm and provide a hybrid cryptography algorithm to make our information very secure and transmit it tone user to another [10].

B. Persis Urbana Ivy et al., A modified RSA cryptosystem based on 'n' prime numbers,2012, In this paper the author implement a method on RSA algorithm which is using the forth prime number for calculate the public and private key to increase the performance of the RSA algorithm [2].

III. METHODOLOGY

In this paper we developed an algorithm that is based on modified RSA algorithm based on prime numbers. This algorithm is useful to get the high security over the network. We endeavoured to evolve prime numbers for security throws the networks. Because prime numbers are not easily decomposed and increased the efficiency throw the networks. In this paper we will use JAVA language to get the private key and public Key.

RSA algorithm:

• Select five different prime numbers p and q

For security aim, the integer's p and q must be prime numbers.

• Calculate n=p*q

n will be used as the module for public key and private key.

• Calculate f (n) = (q-1) (p-1)

Where f is a function of Euler's

• Select an integer e such that 1<e<f(n) and GCD (e, f(n))=1; e and f(n) are co prime.

• Determine d:

d is multiplicative inverse of e mod (f(n)) (e * d) mod f (n) = 1 d is the private key

Encryption:

A transfer the data m with the public key (e, n) to B receives the data m with the private key (d, n)

Such that 0<m<n

$C=m^e \bmod n$

Decryption:

B will be gotten the data or message m throws the cipher text to plain text. B is used private key d. $m= c^d \bmod n$ A will be used the public key and transfer the data plain text to cipher text. Mod n B can recover the original data or message.

The above is a normal RSA algorithm which is used widely for encrypt and decrypt the data or information. In which we use two prime numbers. Now below is an example where we use more than four prime numbers to encrypt the data or information. In this example first we select five variable for five different prime numbers, than calculate the value of 'n' by multiplying those variables (p*q*r*s*t), after that we calculate f(n) by subtracting those variable by 1(one) and multiply (p-1)*(q-1)*(r-1)*(s-1)*(t-1).

Than we have to select 'e' which we will use to get the ciphertext but the 'e' must be a number which 1<e<f(n),

After that we get public key=(n,e),than we calculate the 'd' which is use for private key so the 'd' multiplicative of e(mod f(n)), now we have private key =(n,d). After getting public key and private key we have to put a massage or data in a formula to get the ciphertext which is:

$$\mathbf{c=m^e \bmod n}$$

Here c= ciphertext, m=message or data. After calculating we get our ciphertext which is sent to network. To decrypt the ciphertext into original message we have:

$$\mathbf{m=c^d \bmod n}$$

Here m= message or data, c=ciphertext. After calculating this we get the original message which is sent by the first user. This process can be understood by an example which is given below:

Example:
Below is an example of RSA algorithm in which we use five prime numbers and get public key and private key.
Select five prime numbers.
• Calculate n=p*q*r*s*t
n=2*3*5*7*11
n=2310
• Calculate f(n)=(p-1)(q-1)(r-1)(s-1)(t-1)
f(2310) = (2-1) (3-1) (5-1)(7-1)(11-1) =480 f (n)=480
• Select any number 1<e<480
F (n) must not be divisible by e Let e=7
• Select d, multiplicative of e(mod f(n))
d= 343
The public key is (n = 2310,e = 7)
Private key is (n = 2310,d = 343)
Given message m = 5
Encryption:
$C= 5^7 \bmod 2310 = C = 1895.$
Decryption:
$M = 1895^{343} \bmod 2310 = 5$
B got the original message (5) which is sent by A.

IV. RESULTS AND DISCUSSION

There are many cryptographic algorithms are available which are used to encrypt and decrypt the data over the network. The methods which we are going to apply provide improvement to secure our data and also help to transmit the data over the network if we apply these methods in RSA algorithm its make the algorithm very effective and more secure the proposed outcome of this research is to provide a better way to secure the data on internet from unauthorized users. The asymmetric key encryption algorithm RSA provides a batter result and makes our data very secure.

V. CONCLUSION AND FUTURE SCOPE

In this paper we use five prime numbers which provides more security over the network. In which we strive to get the quality that make the cryptography to have a best use of prime numbers. The prime numbers act very important role in RSA Algorithm. The large number is easily factorized or decomposes and the limited prime numbers are easily decomposed which will not be provided security over the networks. That's why we used more than four prime numbers to provide more security and it is also not easily factorized or decomposes. To develop the RSA algorithm for prime numbers it can also used for more than five prime numbers.

REFERENCES

[1]. Pratik A. Vanjara, "Analysis and Design of Cryptography Algorithms", "International Journal of Computer Application & Information Technology", Vol: 1, Issue: 2, **2012**.
[2]. B.Persis Urbana Ivy,Purshotam Mandiwa, Mukesh Kumar, "A Modified RSA Cryptosystem Based on 'n' Prime Number", "International Journal of Engineering and Computer Science",Vol:1,Issue:2,**2012**.
[3]. B, Padmavathi, S. Ranjita Kumari, "A Survey on Performance Analysis of DES,AES and RSA Algorithm along with LSB Substitution Technique ", "International Journal of Science and Research",Vol:2,Issue:4,**2013**.
[4]. Nitin jirwan, Ajay Singh,Sandip Vijay,"Review and Analysis of Cryptography Techique", "International Journal of Scientific & Engineering Research",Vol:4,Issue:3,**2013 .**
[5]. Manisha Vishwakarma,"Comparative study of Cryptography Algorithms", "International Journal of Advanced Research in Computer Science",Vol:4,Issue:3,**2013**.
[6]. Gurpreet Singh,Supriya,"A Study of Encryption Algorithms (RSA,DES,3DES and AES)for Information Security","International Journal of Computer Application", Vol: 67,Issue: 19,**2013**.
[7]. Rejani. R,Deepu. V. Krishnan, "Study of Symmetric Key Cryptography Algorithms", "International Journal of ComputerTechniques", Vol:2, Issue:2, **2015**,
[8]. S.Suguna,V. Dhanakoti,R. Manjupriya "A Study on Symmetric And Asymmetric Key Encryption Algorithms ", "International Research Journal of Engineering and Technology",Vol:3,Issue:4,**2016.**
[9]. A. Joseph Amalraj,Dr. J. John Raybin Jose, "A Survey Paper on Cryptography Techniques", "International Journal of Computer Science and Mobile Computing",Vol:5,Issue:8,pp55-59,**2016**.
[10]. Arpit Agrawal,Gunjan Patanker, "Design Hybrid Cryptography Algorithm for Secure Communication", "International Research Journal of Engineering and Technology", Vol:3,Issue:1,**2016**
[11]. Sarthak R Patel,Khushbu Shah,Gaurav R Patel, "Study on Improvements in RSA Algorithm", "International Journal of Engineering Development and Research",**2017.**
[12]. Sarita Kumari, "A research paper on Cryptography Encryption and Compression Techniques","International Journal of Engineering And Computer Science",Vol:6,Issue:4,pp: 20915-20919,**2017**.
[13]. Venkat Prasad .K, S. Magesh, "A Survey on Encryption Using Modern Technique","International Journal of Pure and Applied Mathematics",Vol:117,Issue:16,**2017**.
[14]. Shivani Sharma,Yash Gupta,"Study on Cryptography and Techniques","International Journal of Scientific Research in Computer Science",Vol:2,Issue:1,**2017**.
[15]. Faiqa Maqsood,Muhammad Ahmed, Muhammad Mumtaz Ali,Munam Ali Shah, "Cryptography: A Comparative Analysis for Modern Techniques","International Journal of Advanced Computer Science and Application", Vol: 8, Issue: 6, **2017**.
[16]. Omar G. Abood,Shawkat K.Guirguis, " A Survey on Cryptography Algorithms ", " International Journal of Science and Research Publications ", Vol:8,Issue:7,**2018**.
[17]. Swapnil Chaudhari,Mangesh Pahade ,Sahil Bhat,Chetan Jadhav,Tejaswini Sawant, "A Research Paper on New Hybrid Cryptography Algorithm ", "International Journal for Research & Development in Technology ",Vol:9,Issue:5,**2018**.

Authors Profile

Mr. Abhishek Guru received B.C.A. degree from Makhanlal Chaturvedi National University of Journalism and Communication Bhopal in 2009 MSc. Computer Science degree from Makhanlal Chaturvedi National University of Journalism and Communication Bhopal, having Diploma In Software Testing from Seed Infotech Indore M.P. and pursuing Phd

from Kalinga University Naya Raipur and Assistant Professor and HOD of Computer Science Department in Gurukul College Pathalgaon Jashpur C.G., having 5 years of Teaching experience and also participate the national Conference on Recent Innovations in Smart IT & Communication for Rural Development conducted by Development of Computer Science & Information Technology Kalinga University Naya Raipur and Chhattisgarh Council of Science and Technology(CGCOST) Govt. of Chhattisgarh, Raipur.

Dr. Prof. Asha Ambhaikar , Professor and Dean Students Welfare, Kalinga University, Naya Raipur. She has also worked as a Principal in G. H. Raisoni college of Engineering and Management, Amravati (Maharashtra). She has 25 years of Academic experience. She has Guided 3 Ph.D Scholars and 8 undergoing. She has published more than 75 research papers in reputed National and International Journals. She was a chairman Board of studies and Member of Academic Council of Information Technology in Chhattisgarh Swami Vivekananda Technical University, Bhilai(C.G.). She is a member of Editorial Board and Reviewer of various Reputed international journal's and conferences. She is also the member of various professional societies like Life member of IAENG (International Association of Engineers, Hong Kong, IEEE, Indian Society of Technical Education (ISTE), Computer Society of India (CSI), IET, ASDF Computer Science Teachers Association (CSTA), Association for Computing Machinery (ACM), New York, USA, IACSIT (International Association of Computer Science and Information Technology, Singapore. Member of SDIWC (The Society of Digital Information and Wireless Communication, USA. She has also chaired various National and International Conferences around various countries as a keynote speaker. She has also published two books by Lambert Publication, Germany. She has also received a various Awards like: 1. Best Personality of India 2015 at New Delhi, India. 2. Bharat Excellence Award 2015 at New Delhi, India. 3. Outstanding Teacher's Award 2014, 2015 on 5th September, at RCET Bhilai, India. 4. ASDF Global Award for Best Dean (Academics) of the Year 2014 at Bangkok- Thailand on 30th December 2014. 5. ASDF Global Award for Best Professor of the Year 2013 at Pondicherry, India. 6. Best Research paper Award in the year 2009. 7. SPARC Europe Award 2009 for the research paper "Exploring the Behavior of Mobile adhoc Network Routing Protocols with reference to Speed and Terrain Range". She is also guiding Ph.D. Scholars in various universities, her area of research includes Computer Networking, Mobile Adhoc Networking, Sensor Networks, Data Mining, Distributed system, information systems and security and Cloud Computing etc.

