Journal of Computer Science Engineering and Information Technology Research (JCSEITR)
ISSN(P): 2250-2416; ISSN(E): Applied
Vol. 6, Issue 2, Dec 2016, 15-22

TRANS STELLAR
•Journal Publications •Research Consultancy

AN EFFICIENT AND ROBUST MODIFIED RSA BASED SECURITY ALGORITHM IN MODERN CRYPTOGRAPHY

RAMKRISHNA GHOSH

Haldia Institute of Technology, India

ABSTRACT

In modern world, security plays a significant role to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a significant role in providing the data security against malevolent attacks.RSA algorithm is applied in the popular implementations of Public Key communications. Asymmetric key cryptography, also called Public Key cryptography uses two different keys. One key is used for encryption and other corresponding key must be used for decryption. No other key can decrypt the message not even the original key used for encryption. The importance of this method is that every communicating party requires a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he/she can communicate with anyone else. In our research paper, we have performed an efficient implementation of RSA algorithm and compared it with existing RSA algorithm.

KEYWORDS: Public Key, RSA Algorithm, Encryption & Decryption

Received: Nov 06, 2016; **Accepted:** Dec 13, 2016; **Published:** Dec 17, 2016; **Paper Id.:** JCSEITRDEC20162

Original Article

INTRODUCTION

Cryptography is an art of hiding the data and protects that data or information from various types of attacks. It is a procedure of accomplishing the security by converting the original information or message into coded or indecipherable form which is not understood by the third party [1].

The most ancient problem of cryptography is secure communication over an insecure channel. A concealed message which party M wants to send party N over a communication channel may be tapped by an attacker [2].The conventional solution to this problem is called private key encryption. In private key encryption A and B hold a meeting before the remote transmission occur and depend on a pair of encryption and decryption algorithms and an extra piece of information to be kept secret. We shall refer to S as the common secret key [4]. The intruder may know the encryption and decryption algorithms [10] E and D which are being used, but does not make out S. After the primary meeting when M wants to send N the clear text message m over the unsafe communication line, A encrypts m by computing the cipher text c = E(S; m) and sends c to B. After receiving it, B decrypts c by computing m =D(S; c). The line-rival who does not recognize S, would not be able to compute m from c. With the growth and improvement of research in cryptographic system, there exists some launched theory, techniques and algorithms. Researchers have developed different new models, techniques and algorithms to make information hiding system. Nevertheless, it is a very tough to find out the specific algorithm, because we have already understood that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. Also newer systems have set up for retrieving the concealed information.

Therefore there is a scope to develop a better cryptography system where the information cannot be taken back.

Literacy Survey

Cryptography can be used to ensure confidentiality, authentication and integrity of a message. Most encryption algorithms are widely useful for information security [8]. Some forms also provide for sender authenticity and proof of information delivery.

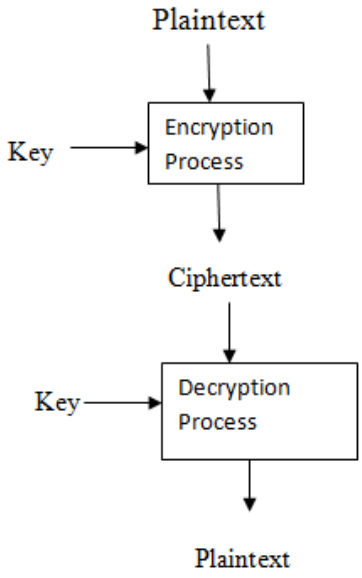

Figure 1: Cryptographic Process

Cryptography has the under mentioned goals

Confidentiality

It ensures that data remains private. The sender encrypts the message using a cryptographic key and the receiver decrypts it by using the same or different key used by the sender.

Data Integrity

Integrity ensures that the receiver gets the same message that was sent by the sender. It ensures that data is protected from accidental or malicious modification.

Authentication

Digital signatures are used to provide authentication. It assures that data originates from a particular party.

Non-Repudiation

It does not allow denial by the sender or receiver. The receiver proves the identification of the sender in case of disagreement by the sender. The sender finds the identification of the receiver in case of disagreement by the receiver.

Types of Cryptography

Cryptography is the art of achieving security by encoding messages to make them incomprehensible. Its main goal is to keep the data secure from unauthorized access.

Secret Key Cryptography

In traditional secret key (symmetric-key) cryptography [6], the sender and receiver of a message know and use the same secret key. The original message is termed as the plaintext. The coded message that is to be transmitted is referred to as the cipher text. The primary challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in different physical locations, they must expect a courier, a phone system, or any other transmission medium to resist the discovery of the concealed key.

Anyone who overhears or intercepts the key in transit can later read, modify messages encrypted using that key. The process of converting from the plaintext to the cipher text is known as enciphering or encryption. Restoring the plaintext from the cipher text is termed as deciphering or decryption.

Public Key Cryptography

In the public key(asymmetric key) cryptosystem[7] the cipher text is as : **C = f(Kpublic,P)**, and the plain text is as : **P = g(Kprivate,C)**.

The growth of the Internet and electronic commerce has brought the concern of privacy in electronic communication. Nowadays huge amount of personal and responsive information are electronically transmitted and stored. Examples of well-Known asymmetric key techniques for various purposes include: Diffie–Hellman key exchange protocol, El Gamal, DSS (Digital Signature Standard), which includes the Digital Signature Algorithm, various elliptic curve techniques, various password-authenticated key agreement techniques, RSA encryption algorithm, YAK authenticated key agreement protocol. Among all, RSA is the well known algorithm.

Hash Function

Another type of cryptography is hash function. It is a one way encryption. It uses no key for both encryption and decryption process. It is mainly useful for message integrity.

Existing Algorithm

RSA Algorithm

The most popular and secure public key cryptographic algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA) [6]. It was described in 1978. It uses two numbers, **e** and **d**, as the **public** and **private** keys.

It is dependent on the numerical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in RSA are based on very large (made up of 100 or more digits) prime numbers. The algorithm itself is quite straightforward unlike the symmetric key cryptographic algorithms. Howbeit, the real challenge in the case of RSA is the selection and generation of the public and private keys.

The whole process of **RSA algorithm** involves the following steps:

- Choose two large prime numbers **p** and **q**.
- Calculate **n = p * q.**
- Calculate **f(n) = (p – 1) * (q – 1).**
- Select the public key (i.e. encryption key) **e** such that

- **1<e<f(n)** and **GCD(e, f(n)) = 1**.
- Select the private key (i.e. decryption key) **d** such as **d** is multiplicative inverse of **e mod f(n) :**
- **(d * e) mod f(n) = 1**
- For **encryption**, calculate the cipher text **C** from the plain text **M** as follows:
- **$C = M^e \bmod n$**
- For **decryption**, calculate the plain text **M** from the cipher text **C** as follows:
- **$M = C^d \bmod n$**

Example

Below is an example of RSA algorithm in which two prime numbers are used to generate the public key and the private key.

- Choose two random prime numbers
- **p = 11** and **q = 3**
- Compute **n = p * q = 11 * 3 = 33**
- Compute **f(n) = (p-1) * (q-1) = 10 * 2 = 20**
- Choose **e** such that **1<e<f(n)** and **GCD(e, f(n)) = 1.**

  Hence, **e = 3**
- Choose **d** as the multiplicative inverse of **e mod f(n)** satisfying **(e * d) mod f(n) = 1.**

  Hence, **d = 7**
- The **public key** is **(n = 33, e = 3).** The encryption function is :

  $C = M^e \bmod n = M^3 \bmod 33$
- The **private key** is **(n = 33, d = 7).** The decryption function is :

  $M = C^d \bmod n = C^7 \bmod 33$

  For example, we want to encrypt M = 7, we calculate

  $C = 7^3 \bmod 33 = 13$

  And, to decrypt C = 13, we calculate

  $M = 13^7 \bmod 33 = 7$

  We have finally got the original message.

Our Modified Algorithm

This modified RSA is also a public key cryptographic algorithm in which we have used four prime numbers, two public keys for encryption and a private key for decryption. Both sender and receiver must know the values of n, b and a.

Only the receiver knows the value of d. Hence, in this modified algorithm, public keys are {b, n}, {a} and private key is {d,n}.

The whole process of modified RSA algorithm involves the following steps:

- Choose four large prime numbers **p, q, r** and **s**.
- Calculate **n1 = p * q * r * s.**
- Calculate the square root of **n1** and choose the next prime number of that result: **n2 = square root of n1 n1 = next prime number of n2**
- Calculate **n = n1 * p * r * s.**
- Calculate **f(n) = (p – 1) * (n1 – 1) * (r – 1) * (s – 1).**
- Select the public key (i.e. encryption key) **e** such that **1<e<f(n)** and **GCD(e, f(n)) = 1**.
- Select the private key (i.e. decryption key) **d** such as **d** is multiplicative inverse of **e mod f(n) : (d * e) mod f(n) = 1**
- Choose any prime number **a**.
- Calculate **b** such that **b = a * e**.
- For **encryption**, calculate the cipher text **C** from the plain text **M** as follows: $\mathbf{C = M^{(b/a)} \bmod n}$
- For **decryption**, calculate the plain text **M** from the cipher text **C** as follows: $\mathbf{M = C^{d} \bmod n}$

Example

Below is an example of RSA algorithm in which four prime numbers are used to generate the public keys and the private key.

- Choose four random prime numbers
- **p = 3**, **q = 7, r = 2 and s = 5**
- Compute **n1 = p * q * r * s = 3 * 7 * 2 * 5 = 210**
- Compute **n2 = sqrt(n1) = 14**
- Choose the next prime number of n2 and store it in **n1**, i.e., **n1 = 17**
- Compute **n = n1 * p * r * s = 17 * 3 * 2 * 5 = 510**
- Compute **f(n) = (p-1) * (n1-1) * (r-1) * (s-1) = 2 * 16 * 1 * 4 = 128**
- Choose **e** such that **1<e<f(n)** and **GCD(e, f(n)) = 1.**

  Hence, **e = 3**
- Choose **d** as the multiplicative inverse of **e mod f(n)** satisfying **(e * d) mod f(n) = 1.**

  Hence, **d = 43**

- Choose any random prime number **a**, i.e., **a = 2**
- Compute **b = a * e = 2 * 3 = 6**
- The **public key** is **(n = 510, a = 2, b = 6).** The encryption function is:
- **$C = M^{(b/a)} \bmod n = M^{(6/2)} \bmod 510$**
- The **private key** is **(n = 510, d = 43).** The decryption function is:

  $M = C^{d} \bmod n = C^{43} \bmod 510$

  For example, to encrypt M = 123, we calculate

  $C = 123^{(6/2)} \bmod 510 = 387$

  And, to decrypt **C = 387**, we calculate:

  $M = 387^{43} \bmod 510 = 123$

  Hence, we have got the original message.

The various methods of cryptography are not secured. Instead, the only analysis is to see if anyone can draw out how to decode a message without having through knowledge of the decryption key. The security of RSA method lies on the fact that it is really difficult to factor very large numbers.

The well known factoring algorithm would take too long for an attacker to ever break the code. Other methods for determining *d* without factoring *n* are equally as difficult.

Any cryptographic technique which can resist an attack is viewed as secure. At this point in time, the modified RSA algorithm is considered secure.

Table 1

RSA	MODIFIED RSA
Use only one public key.	Uses two public keys.
Less secure.	More secure.
More vulnerable to Brute-Force Attack.	Less vulnerable to Brute-Force Attack.
The Public key is sent once.	The Public key is sent separately twice.
Less communication overload.	High communication overload.

RESULTS AND INTERPRETATIONS

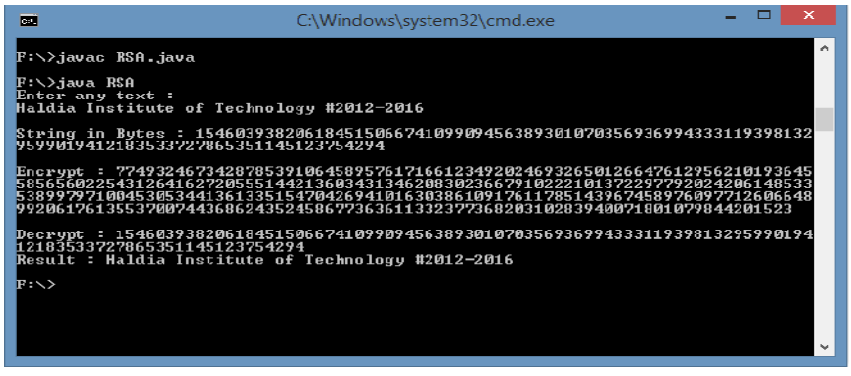

Figure 2: Result for Existing RSA algorithm

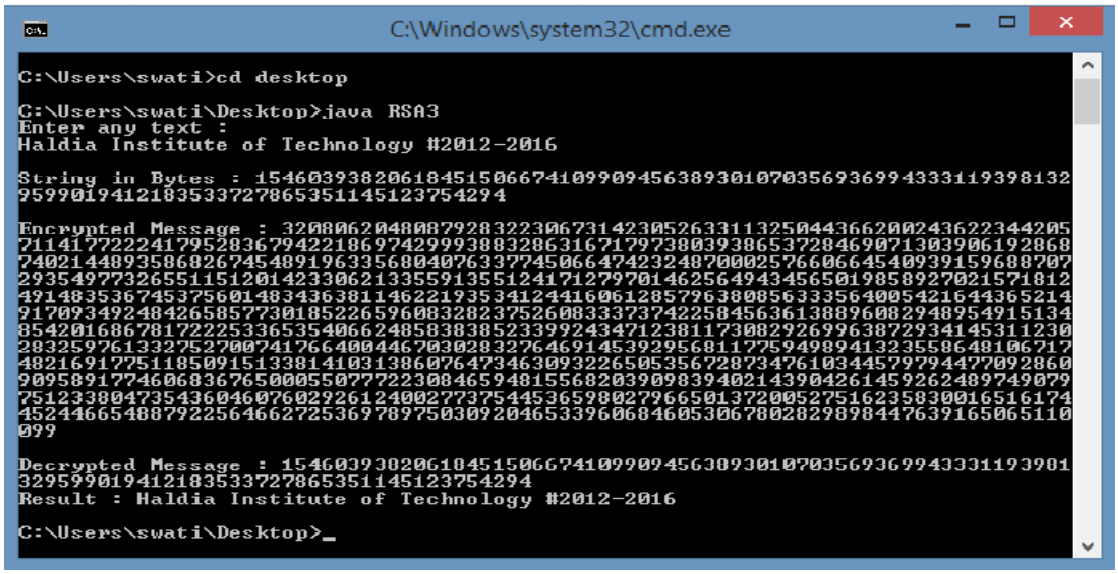

Figure 3: Result for Modified RSA Algorithm

Practical Applications of the Modified RSA Algorithm

Nowadays the RSA jointly with the AES algorithm is the widely used algorithm in commercial applications. It is used in order to protect web traffic in the Secure Socket Layer, to guarantee remote connection in SSH (Secure Shell). It plays a significant role in the modern payment systems through Secure Electronic Transaction.

RSA is applied vastly in most digital data, information and telephone security applications.

RSA is used widely in most digital data, information and security applications.

The RSA provides its advantages of being a reliable and safe system but it is very slow in data calculating. Because of this it is used in hybrid cryptographic systems that simultaneously use symmetric algorithms (AES) for the communication and data encryption phase and public key algorithms (RSA) for the safe delivery of the symmetric key (or session key) that is essential for encrypting and decrypting the message. There are different levels of encryption in telephone cryptography.

CONCLUSIONS

In order to achieve the most primary goals of cryptography like confidentiality, integrity, authentication, non repudiation etc. various cryptographic algorithms have developed. Among these algorithms, we have chosen the RSA Algorithm. The aim of this research was to design and implement a new algorithm based on the RSA Algorithm in which two public keys were used to enhance the security.

The thesis described above is some of the issues for information hiding through text. It also describes data encryption, some ciphers and various attacks on those ciphers due to which the research is still going on to provide security.

Going through these researches, we are planning to design our own algorithm to make an efficient step towards cryptography. We are planning to make an efficient algorithm to provide security against any attacks made by the adversaries.

REFERENCES

1. *Kahate A. Cryptography Techniques. Cryptography and Network Security. 3rd ed. New Delhi, India: McGraw; 2014; p. 32-36.*
2. *Ferguson, N., Schneier, B. and Kohno, T. Indianapolis, "Cryptography Engineering: Design Principles and Practical Applications." Wiley Publishing, Inc. 2010. pp.63, 64. ISBN 978-0-470-47424-2.*
3. *Simar Preet Singh, and Raman Maini,"Comparison of Data Encryption Algorithms" International Journal of Computer Science and Communication Vol.2, No. 1, January-June 2011, pp. 125-127.*
4. *Himanshu Gupta and Vinod Kumar Sharma," Multiphase Encryption: A New Concept in Modern Cryptography" International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.*
5. *Maheswari Losetti, Kanaka Raju Gariga, "An Enhanced RSA Algorithm for Low Computational Devices" International Journal of Advanced Research and Innovations Vol.1, Issue.2, pp 114-118.*
6. *W.Stallings, "Cryptography and network security, Principles and practices ", Fourth Edition. Pearson Prentice Hall, (2006),USA.*
7. *Forouzan., "Cryptography and Network Security " First Edition. McGraw-Hill, (2007),USA*
8. *D.Salomon" Data Privacy and Security " First Edition. Springer-Verlag New York, (2003):, Inc.USA.*
9. *J Hoffstein, et al An, "Introduction to Mathematical Cryptography ", First Edition. Springer Science& Business Media, (2008), Germany.*
10. *R. Bose, Information Theory, Coding and Cryptography, Second Reprint 2008, The Tata Mcgraw Hill Publication,pp. 313*
11. *NIST Special Publication 800-78-2, Cryptographic Algorithm and key sizes for Personal Identity verification, February 2010.*
12. *Y. Wang and M.Hu, " Timing Evaluation of the known Cryptographic Algorithms," in Proc. International conference on Computational intelligence and security, Beijing, China Dec 2009.*
13. *Shaid Bashir Dar, "Enhancing The Security of Caesar Cipher Using Double Substitution Method" International Journal of Computer Science &Engineering Technology (IJCSET) ISSN : 2229-3345 Vol.05 No.07 July 2014.*
14. *S G Srikantaswamy, Dr. H D Phaneendra, "Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption", International Journal on Cryptography and Information Security (IJCIS). Vol. 2, No.4. pp. 39-49, December 2012.*
15. *Gaurav Shrivastava, "Using Letters Frequency Analysis in Caesar Cipher with Double Columnar Transposition Technique" International Journal of Engineering Sciences & Research Technology. Vol. 2, Issue 6, Page No. 1475-1478, 01 June, 2013, ISSN: 2277-9655.*