Enhanced Rsa Cryptosystem Based On Three Prime Numbers

Vivek Choudhary[1] and Mr. N. praveen[2]

[1] Post Graduate Scholar, Department of Computer Science & Engineering, SRM University,
Chennai, Tamilnadu, India

[2] Assistant Professor, Department of Computer Science & Engineering, SRM University,
Chennai, Tamilnadu, India

Abstract

Public key cryptography consists of set of methods which are used to encrypt secret messages so that they can be read only by the intended receiver. The most common public key algorithm is RSA cryptosystem used for encryption and decryption. Security of RSA Algorithm can be compromised using mathematical attack, by guessing the factors of a large number. It may also be compromised if one can guess the private key. In accordance with the mathematical attack, we propose a secure algorithm in this paper. This includes the architectural design and enhanced form of RSA algorithm through the use of third prime number in order to make a modulus n which is not easily decomposable by intruders. Further, this approach eliminates the need to transfer *n,* the product of two random but essentially big prime numbers, in the public key due to which it becomes difficult for the intruder to guess the factors of *n* and hence the encrypted message remains safe from the hackers.

Keywords: *RSA, cryptography, indexes, public key, private key.*

1. 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.

At present, the best known and most widely used public key system is RSA, which was first proposed by RL Rivest, Shamir, Adleman [4]. 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 [6]. 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.

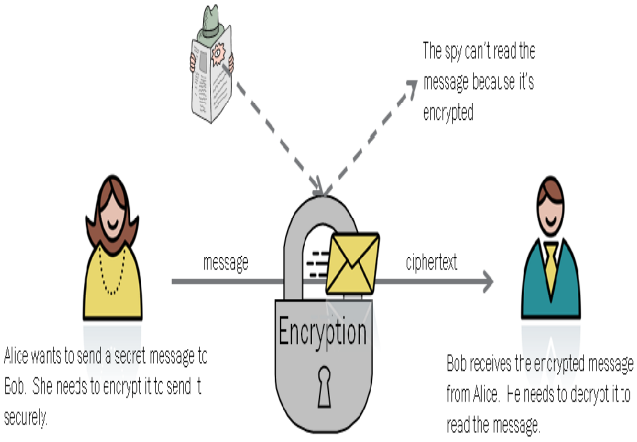
The spy can't read the message because it's encrypted
message
ciphertext
Encryption
Alice wants to send a secret message to Bob. She needs to encrypt it to send it securely.
Bob receives the encrypted message from Alice. He needs to decrypt it to read the message.

Fig 1: Encryption process

1.1. The RSA Cryptosystem

The key feature of public-key cryptosystem is that the encryption and decryption procedure are done with two different keys - public key and private key, and the private key cannot be derived from the public key, that enables the publication of the encryption key without the risk of leaking the secrets. The most significant approach of public key cryptography algorithm is RSA, which can resist almost all the known passwords attacks so far. RSA algorithm, which is named after the inventors, is the first algorithm that can be used both for data encryption and digital signatures [4]. RSA algorithm's security depends on the difficulty of decomposition of large numbers. In the algorithm, two large prime numbers are used for constructing the public key and the private-key. It is estimated that the difficulty of guessing the plaintext from signal key and the cipher text equals to that decomposition of the product of two large prime numbers.

1.2. Implementation of RSA Cryptosystem

To implement RSA cryptosystem is a rather complex process, which involves the generation of prime numbers, large integer modular arithmetic and other mathematical calculations. In RSA cryptosystem, p and q are large prime numbers. To achieve it, the most important factor is the efficiency in generate large prime numbers. This should be: p, q are large prime numbers, when seeking primes p and q with the method of factorization , then the difficulty is actually the same as to attack to RSA (the decomposition of large composite number) , it's feasible as to the computer .

1.3. Existing System

RSA cryptosystem, named after R. Rivest, A. Shamir, and L. Adleman, who invented RSA in 1978, is the public-key cryptosystem which is used the most widely. It can be used to provide both secrecy and digital signatures [4].

RSA Algorithm consists of three phases:

- Key Generation:Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted. RSA algorithm uses a public key and a private key [4]. The public key is made available to anyone (often by means of a digital certificate). A sender encrypts data with the public key; only the holder of the private key can decrypt this data [3].
- Encryption:Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted [5]. An encryption scheme usually uses a pseudo-random encryption keygenerated by an algorithm. An authorized recipient can easily decrypt the message with the key, provided by the originator to recipients but not to unauthorized interceptors.
- Decryption: Decryption is the process of decoding the cipher text to get the plain message in readable form. An authorized recipient can easily decrypt the message with the key. A key is required to decrypt a message.

1.4. RSA Algorithm

Key Generation:

- Select p and q both prime number, p is not equal to q.
- Calculate n = p x q.
- Calculate ø (n) = (p -1) x (q-1).
- Select integer e whose gcd (Ø (n), e) = 1; 1 < e <Ø (n).
- Calculate private key d = e-1 (mod Ø (n)).
- Public key PU = {e, n}.
- Private Key PR = {d, n}.

Encryption:

$C = M^e \bmod n.$

Decryption:

$M = C^d \bmod n.$

Where,	C	- Cipher text
	M	- Message,
	p and q	- Prime Numbers,
	N	- Common Modulus,
	e and d	- Public and Private Keys

1.5. Disadvantages of RSA algorithm

- Loss Of Private Key May Break The Security.
- Attacks on RSA can break security fore.g-factorization problem, low decryption exponent, common modulus, short message, cyclic attack etc.
- High Computational Cost.
- As n is transmitted in public key, thus its factors can be found out by hit and trial, due to which the security quotient of RSA algorithm gets reduced.

2. Related Work

R. Rivest, A. Shamir, and L. Adleman has proposed a method for implementing a public –key cryptosystem whose security rest in a part on the difficulty of factoring the large numbers.it permits secure communication to be established without the use of couriers to carry key and it also permits one to 'sign' digitized documents [3].

An Encryption method is presented with the novel property that publically revealing an Encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

- Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key [4].
- A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signature cannot be forged, a signer cannot deny the validity of his signature [4].

This has obvious applications in "Electronic mail" and "electronic fund transfer" system.

XinZhou and Xiaofei Tang proposed an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm [5]. In addition, the encrypt procedure and code implementation is provided in details. Encryption and decryption algorithm's security depends on the algorithm [5], it also depends on the key confidentiality. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless. Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption algorithm.

Ishwarya M and Dr.Ramesh Kumar proposed implementation of the RSA algorithm during data transmission between different communication networks and Internet, which is calculated to generate the keys by a program and then save these values of the keys in the databases. Its advancing the existing database systems and increasing the security and efficiency of the systems. This is achieved with a new concept to implement a real world anonymous database [2] which improves the secure efficient system for protection of data, restricting the access to data even by the administrator thus maintaining the secrecy of individual patients [2].

AayushChhabra, SruthiMathurproposed that the security of RSA can be further increased with the use of third prime number along with a new approach for encryption and decryption [1]. This approach eliminates the need to transfer *n*, the product of two random but essentially big prime numbers, in the public key due to which it becomes difficult for the intruder to guess the factors of *n* and hence the encrypted message remains safe from the hackers. Thus this approach provides a more secure path for transmission and reception of messages through public key cryptography [1].

3. Problem Definition

RSA algorithm security can be compromised over the network. To increase security of computation of RSA algorithm we need to modify the RSA algorithm which can be done by third prime number and using a new variable for Encryption and Decryption.

4. Proposed Method:

In the proposed method, we are using three prime numbers to generate the common modulus n and the three prime numbers [3] along with n is used to generate a new variable, which is used for Encryption and Decryption of data.

Three phases are as follows:

- Key Generation
- Encryption
- Decryption

Key Generation:

- Select the random values p, q, and r.
- Calculate $n=p*q*r$.
- Calculate $Ø (n) = (p-1) (q-1) (r-1)$.
- Compute kp:

  $\lg n < kp < n$

  (kp must be co-prime to n)
- Compute d:

  If $p > q$ THEN $n-p < d < n$

  If $p < q$ THEN $n-q < d < n$

  (d must be co-prime to n)
- A general formula to find d : $kp * ks \bmod (d) = 1$
- ks is found by the formula: $ks * kp = 1 * \bmod (d)$

Encryption:

- $c = m^{kp} \bmod (d)$

Decryption:

- $m = [\, c^{ks} \bmod (d) \,]^{½}$

Where,

p, q, r : prime numbers

kp	: Public key exponent
ks	: Private key exponent
m	: Plain Message
c	: Cipher Text

The flow chart for the proposed RSA algorithm is shown below in fig 2.

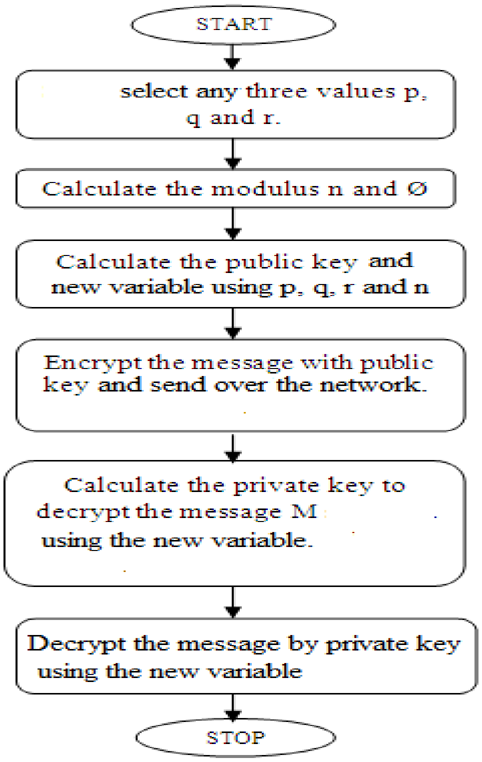
START
select any three values p, q and r.
Calculate the modulus n and Ø
Calculate the public key and new variable using p, q, r and n
Encrypt the message with public key and send over the network.
Calculate the private key to decrypt the message M using the new variable.
Decrypt the message by private key using the new variable
STOP

Fig 2: Flow chart

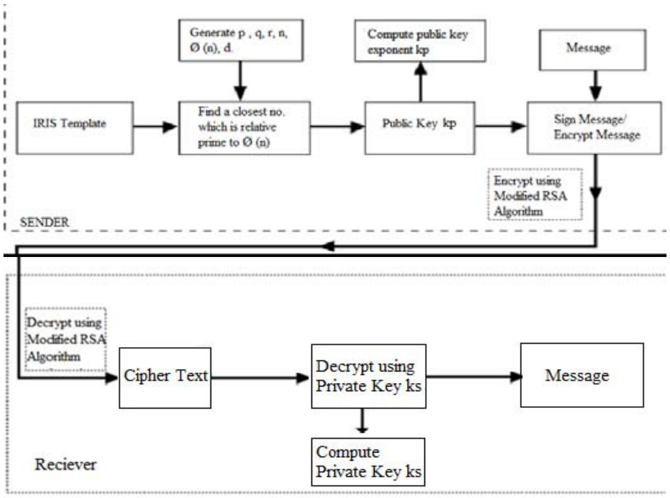
Generate p , q, r, n, Ø (n), d
Compute public key exponent kp
Message
IRIS Template
Find a closest no. which is relative prime to Ø (n)
Public Key kp
Sign Message/ Encrypt Message
Encrypt using Modified RSA Algorithm
SENDER
Decrypt using Modified RSA Algorithm
Cipher Text
Decrypt using Private Key ks
Message
Compute Private Key ks
Reciever

Fig 3: Architecture diagram

4.1. Advantages of Proposed Method

- The strength of large prime number depend on three variables p, q and r. It is difficult to break the large prime number into three.
- Eliminate the use of common modulus n by generating a new variable from value of n and the prime numbers.
- Using new variable for encryption and decryption gives more security for data transfer.

Table 1. Comparison of existing and proposed method

Existing rsa system	Proposed rsa system
• Two prime numbers are selected to generate common modulus n.	• Three prime are selected to generate the common modulus n.
• Strength of large number depends on two variables.	• Strength of large prime number depends on three prime numbers.
• Common modulus n is used for Encryption and Decryption.	• A new variable d is generated used for encryption and decryption.

5. CONCLUSION

The proposed method is more secure than RSA algorithm as the public key exponent *d* can be found out only by knowing the two prime numbers *p* and *q* and which can be known only through *n*, but as n is not transmitted in public key, thus it is very difficult to know the value of *d*, hence the encrypted message cannot be read easily.

References

[1] AayushChhabra, SruthiMathur, “Modified RSA Algorithm”, International Conference on Computational Intelligence and Communication Systems, ISSN: 978-0-7695-4587-5/11,pp. 545-548, 2011.Qian Zhao, Chang-Zheng Shi, Liang-Ping Luo , “Role of the texture features of images in the diagnosis of solitary pulmonary nodules in different sizes” , Chinese Journal Of Cancer Research,ISSN:1000-9604, pp. 451-458, August 2014

[2] Ishwarya M and Dr.Ramesh Kumar, “Privacy Preserving Updates for Anonymous and Confidential Databases Using RSA Algorithm”,International Journal of Modern Engineering Research (IJMER), ISSN: 2249-6645, Vol.-2, Issue 5, pp-3717-3722, September-October 2012

[3] Ms.RituPatidar, Mrs.RupaliBhartiya, “Modified RSA Cryptosystem Based on Offline Storage and Prime Number”, IJCAT International Journal of Computing and Technology,ISSN : 2348 - 6090 , Vol. 1, Issue 2, March 2014.

[4] R. Rivest, A. Shamir, and L. Adleman,“A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of ACM, Vol.-21, Issue-2, February 1978.

[5] XinZhou and Xiaofei Tang, “Research and Implementation of RSA Algorithm for Encryption and Decryption”,The 6th International Forum on Strategic Technology ISSN: 978-1-4577-0399-7/11, pp. 1118-1121, August 2011.