**ISSN: 2349-6495**

# RSA and Modified RSA algorithm using C Programming

M.Puneeth, Jasmine shafi Farha, N.Sandhya, M.Yamini
Department of ECE, Kluniversity, Vijayawada, India

***Abstract—****RSA algorithm is a process of encrypting plain text in blocks, every block has a binary value lesser than some n number. The size of block should be less than log (n) or equal to log (n), public-key cryptosystem was implemented by RSA algorithm In this Journal we are going to implement a RSA and modified RSA algorithm using c programing, modified RSA algorithm is somewhat slower than RSA but it is more secure*

***Keywords—decryption,digitalsignatures,encryption, key, RSA,***

## I. INTRODUCTION

Diffie and Hellman introduced the RSA algorithm at the time when electronic mail was expected to arise soon. Public key cryptography uses the algorithms that are mathematical relationships based. Though it is uncomplicated for the receiver for generating public key and private key, for decryption of the message with the help of private key, and simple for a sender for the encryption of the message with the help of public key, so it is too difficult for any person for the derivation of private key, when only public key is known. For signature verification purposes, generally, only a hash of the message is usually encrypted. Public-key cryptography is a basic, vital, and technology that which is used widely. It is used by many cryptosystems and cryptographic algorithms [3]. The encryption technique which is used to convert original (plain text) data to cipher text. The plain text is also called the clear text. The plain text is easily read by anyone. Second technique is decryption which is used to convert cipher text to plaintext (readable format).cipher text is also called the unreadable form [4]

RSA algorithm is having the important parameters of affecting its security level and speed. With the increase of modulus length it plays important role of increasing the difficulty level for the decomposition of that into its required factors. This increases private key length and hence it is very difficult to decrypt without having the decryption key [1]

The algorithm RSA, at present is the most successful use for ciphering keys and passwords or counts [2]

The two important ideas of RSA are:

1.1. Public-key encryption: In RSA algorithm the keys that are required to encrypt the data are public whereas the keys for decryption are not.so the person only who has the original decryption key only can decrypt the message. The decryption key should be done in such a manner that no other key should match public key of encryption to decrypt the message

1.1.1. Plain text: Plain text is the text that which can be readable by everyone

1.1.2: Encryption Algorithm: The encryption algorithm is an algorithm that which is used for performing several transformations on the plain text

1.1.3:Public and Private keys: Public and Private keys are pair of keys that which are selected for using one key for encryption and other for decryption

1.1.4. Cipher Text: Cipher text is a scrambled text that which is produced by using mathematical logics on plain text

1.1.5: Decryption Algorithm: Decryption algorithm is an algorithm that which is used for accepting matching key and cipher text that which is used for producing plain text

1.2: Digital signatures: The receiver wanted to verify that the message was sent by sender and not just came from authentication. This can be done using senders decryption key and the using public key of encryption anyone can verify it later. This RSA algorithm is used to secure electronic mail and also for electronic transmissions and transactions

## II. PUBLIC KEY CRYPTOSYSTEMS

Each and every user has his own procedure of encrypting and decrypting the message. These encryption and the decryption process were belonged to keys. In RSA algorithm there are two numbers as a set. The message is symbolized as “P” which is for encryption .There are four types of procedures which are essential to public key crypto systems:

2.1. Procedures of public key crypto systems:

2.1.1. Deciphering the enciphered message gives the original message

$$D(E(P)) = P$$

2.1.2. Reversing of procedure will return P

$$E(D(P)) = P$$

2.1.3. (E) and (D) are easy for computing

2.1.4. The publicity of encryption key does not affect the decryption that is it is not that much easy to find out decryption key (D) from (E)

If cipher text = C+E (P) then if somebody are trying to find out D by trying to match P in E (P) = C is complex. If he tries to match with number of messages then the number is large

E satisfies 2.1.1, 2.1.3 and 2.1.4 is called as “trapped door permutation” or it is also called as “trapped door function”

It is called as trap door because it’s inverse of decryption (D) is easy for computing if certain information of trap door is available ,on other hand it is hard .It is also a one way because it is easy for computing in one perspective but it is very hard in other perspective. It is also a permutation because it satisfies 2.1.2, it means that potential message is due to cipher text, every message may be a cipher text of some other message.2.1.2 is used for signatures

2.2. Privacy: The encryption process is done for providing privacy for the plain text. It should be make sure that intruder cannot bypass the cipher text. Without 2.4 property, the encryption process is not a public key still, which is similar to NBS standard.

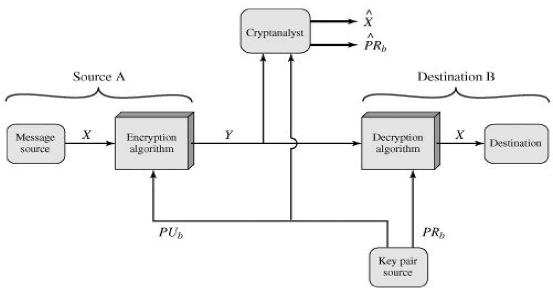


Fig. 1 Privacy

Suppose if Puneeth want’s send a private message to Jasmine .From the public file $E_A$ will be retrieved by him, P will be encoded and C= $E_A$(P) will be obtained, Jasmine decodes it by using her $D_A$, the cipher text will be decrypted by her only because of property (2.1.4)

2.3. Signatures: To ensure that message is sent by sender and it has not being sent by the third party. Who uses same type of encryption key. So that a digital signature is used to avoid this. Signature cannot be changed or modified so that there will be a good confidentiality between sender and receiver

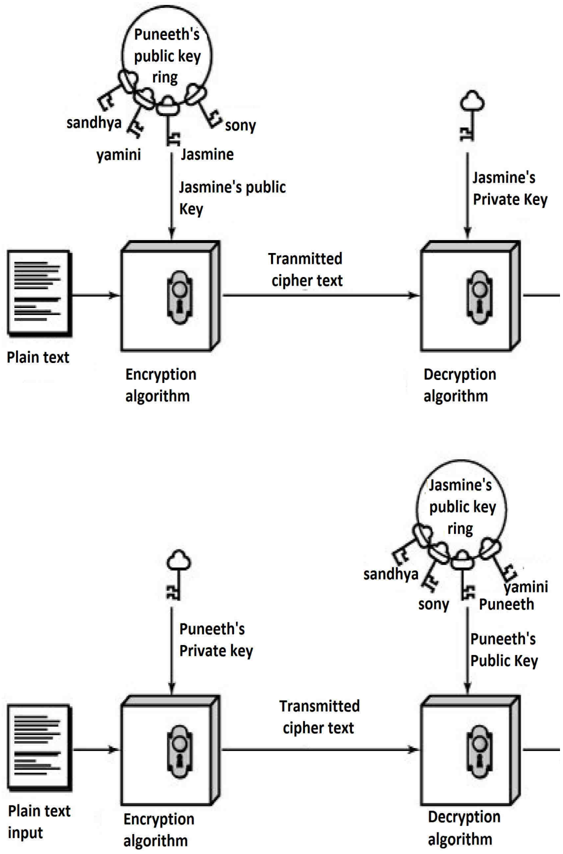


*Fig. 2 Encryption and authentication of public key cryptosystems*

Suppose if Puneeth wanted to send a private message for Jasmine, the document will be signed by assuming that RSA algorithm is a reliable and quick, it is obtained mostly by the property (2.1.3).The message will be decrypted by Puneeth’s key in which it allows the properties (2.1.1) and (2.1.2).It shows that every message will be a cipher text of other message

$$D_B (P) = J$$

Then J will be encrypted by encryption key of Jasmine

$$E_A (J) = E_A (D_B (P))$$

In this way we are confident that document will be decrypted by Jasmine only. When she encrypts the message, she will get the signature by $D_A (E_A (D_B (P)) = J$.

Now she will know that message is sent by Puneeth, Since the decryption key of Puneeth only computes the signature, separately the message will not be sent because By using Puneeth’s public key of encryption Jasmine can deduce the message with signature. Encryption key of Puneeth can be given as

**ISSN: 2349-6495**

$E_B(J) = E_B(D_B(P)) = P$.

J depends upon P and encrypted transmission sent by Puneeth depends upon J, the transmission that we had depends on signature and message, so from transmitted document both of them can be deduced

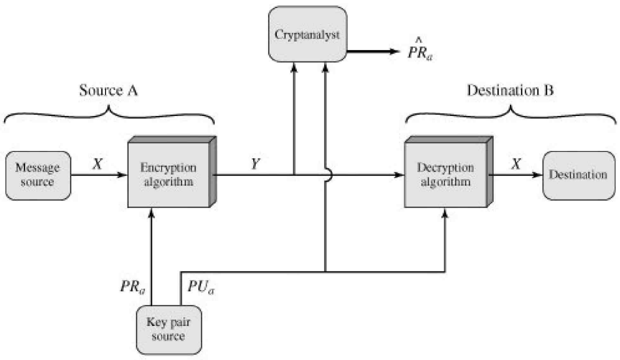


*Fig 3 Authentication*

## III. RSA MATH METHOD

Generally we will do the encryption and the decryption using simple arithmetic logics, now the message will be represented numerically.so that arithmetic algorithms will be performed on it, now message P will be represented in between (0 to n-1) with an integer. If there is a too long message then we have to sparse the message and it should be encrypted separately, some positive integers has to be taken. Let the positive integers be x, y, z with (x,z) as encryption key (y,z ) as decryption key=z=ab.Now the encryption can be done by increasing it to the xth power of modulo z for obtaining c,where c represents the cipher text,the cipher text c can be decrypted by raising that to xth power of modulo z for obtaining message P again

$$C = X(P) = P^x \ (\text{mod } Z)$$
$$P = Y(C) = C^y \ (\text{mod } n)$$

In between (0 to n-1), (P and C )are the integers and due to modular congruence equal size of information will be preserved by us this is due to the encrypted and decrypted keys were integer pairs (x,z) and (y,z).Now we have to take two large prime numbers ‘a’ and ‘b’ and we have to multiply them to obtain z=ab even though z is public ‘a’ and ‘b’ will not be revealed by that.Now appropriate x and y should be obtained by us we have to take y to be a larger random integer ,where it should be a coprime of (a-1).(b-1) so that it should justify the following equation

$$GCD(y(a-1).(b-1))=1$$

We know that is the Greatest Common Divisor

We have to compute x from y ,a and b,where x is the multiplicative inverse of the y.This means we have to satisfy

$$x.y=1(\text{mod}Ø(z)) \quad (1)$$

here euler totient function Ø(z) is introduced, the number of positive integers is the output which is less than z and they are coprime to z

$$Ø(z) = Ø(a).Ø(b)$$

$$Ø(z) = (a-1).(b-1)$$

$$z-(a+b)+1 \quad (2)$$

From this equation we have to substitute the above equation Ø (z) in equation (1) in order to obtain

$$x.y=1(\text{mod}Ø(z))$$

$$x.y=n.Ø(z)+1$$

## IV. SECURITY OF RSA

RSA algorithm is strongest algorithm Indeed but there is question that will RSA algorithm can with stand time of test or not. This is because no encryption technique is 100 percent secure by an attack from a cryptanalyst. Some of the techniques like brute force attack is simple but it is lengthy even though this attack is lengthy the message will be cracked easily. In order to show that how secure is RSA, firstly a cryptanalyst is to be considered how he will try for obtaining a decryption key from public-encryption key. They should design a device in such a manner that even though the encrypted and decrypted keys were obtained they should not be printed even for the owner they should take care of the key how you will take care of your gold or money

4.1. Avoiding reblocking for encryption of a signed message:Reblocking means breaking the signed message into number of smaller blocks.The designer of RSA should take care of reblocking.The blocking of message should depend upon signature of transmitter.

ISSN: 2349-6495

## V. APPLICATIONS OF RSA

RSA algorithm is used in electronic fund transmission why because the information of finance needs the high security This RSA algorithm can be used in electronic mail transformation, online shopping and electronic money transactions

## VI. ATTACKS ON RSA

There are four possible attacks on RSA algorithm the following are the attacks that possible on RSA

6.1.1: Brute-force attack: Brute-force attack is an attack that which involves in trying all the possible private keys

6.1.2: Mathematical attacks: The mathematical attack is the attack that which defines there are several type of approaches all the equivalent in effort for factorizing product of the two prime numbers

6.1.3: Timing attacks:timing attacks depend upon the time that which is taken to decrypt the algorithm.

6.1.4.chosen cipher text attacks:this type attack exploits RSA algorithm properties

## VII. CONCLUSION

We have obtained results of RSA and modified RSA using c programming we have encrypted and decrypted using the RSA algorithm

## VIII. RESULTS

8.1: RSA results

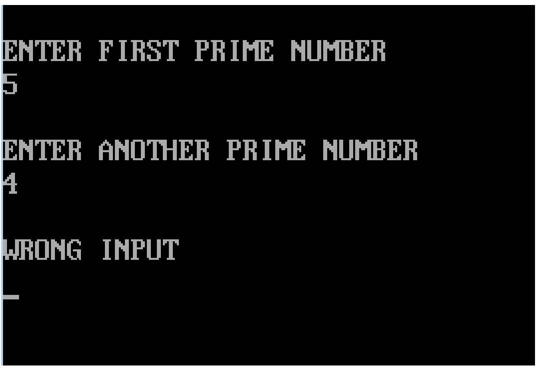


*Fig. 4 If a non-prime number is entered then It shows wrong input*

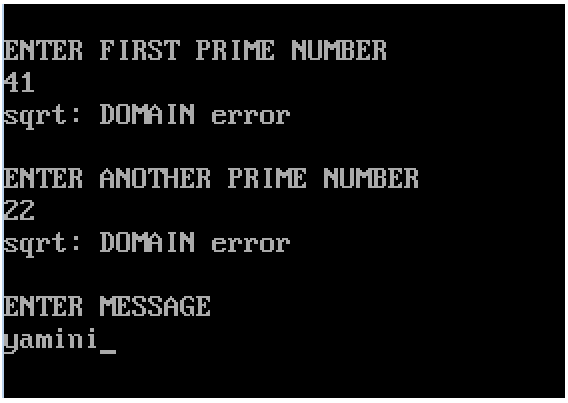


*Fig. 5 Two prime numbers and plain text*

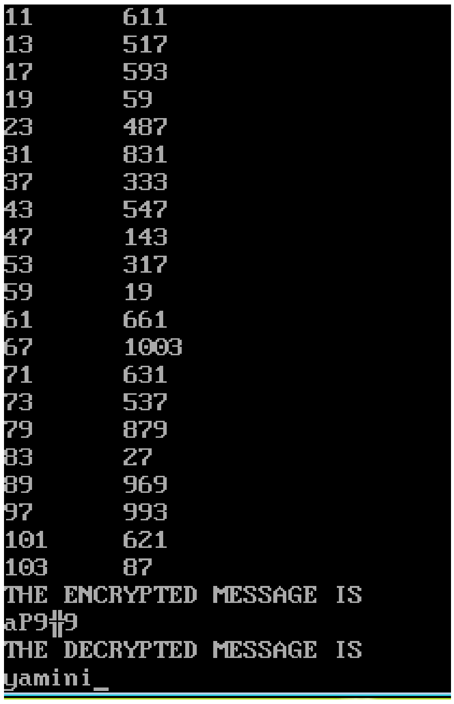


*Fig. 6 Encrypted and decrypted messages*


*Fig. 7Another plain text with different prime numbers*

ISSN: 2349-6495

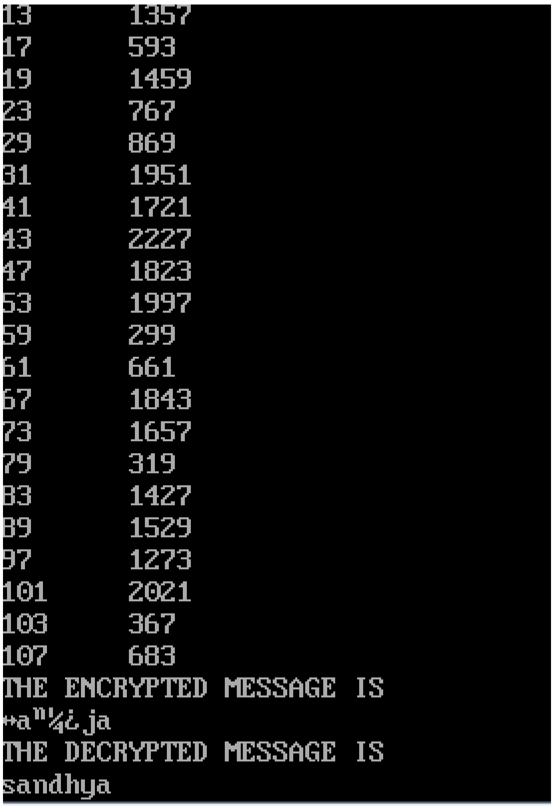


*Fig. 8 The encrypted and decrypted messages of Second Plain text*

8.2: Modified RSA results:

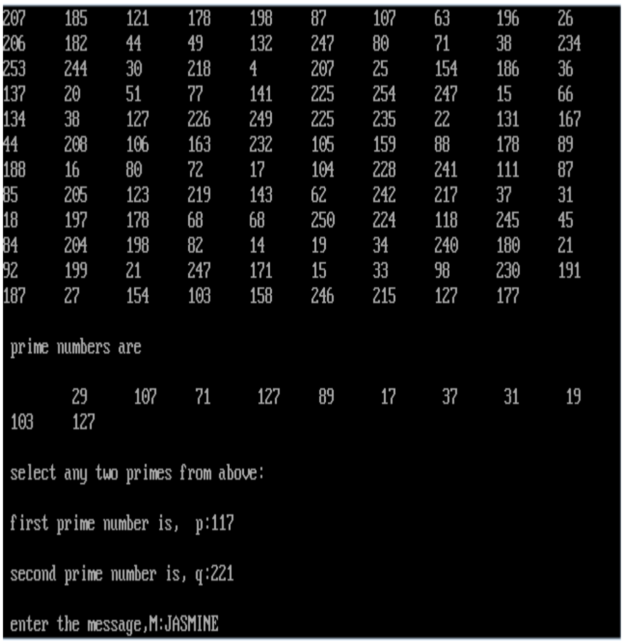


*Fig. 9 Plain text of modified RSA*


*Fig. 10 The encrypted and decrypted messages of Modified RSA*

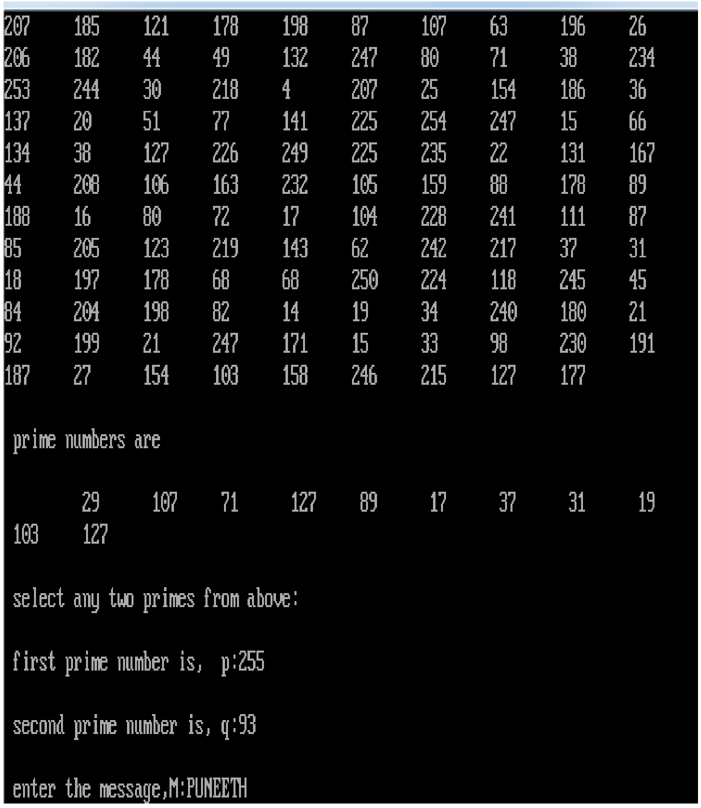


*Fig. 11 Second plain text of Modified RSA*


*Fig. 12 The encrypted and decrypted messages of second plain text in modified RSA*

## REFERENCES

[1] Sonal sharma,Jitendra Singh Yadav,Prasanth Sharma "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012

[2] Samoud Ali, Cherif Adnen. "RSA ALGORITHM IMPLEMENTATION FOR CIPHERING MEDICAL IMAGING "International Journal of Computer and Electronics Research, Volume 1, Issue 2, August 2012

[3] Amare Anagaw Ayele1 Dr. Vuda Sreenivasarao"A Modified RSA Encryption Technique Based on Multiple public keys" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2013

[4] B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar" A modified RSA cryptosystem based on 'n' prime numbers"Intenational journal of Engineering and science,volume1 ,issue2,Nov,2012