ACAFP: Asymmetric Key based Cryptographic Algorithm using Four Prime Numbers to Secure Message Communication.

A Review on RSA Algorithm

Punit Chaudhury
Student, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
punitchaudhary7@gmail.com

Susmita Dhang
Student, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
susmitadhang@gmail.com

Monpreet Roy
Student, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
roy.monpreet.001@gmail.com

Saurav Deb
Student, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
sauravdeb98@gmail.com

Jyotirmoy Saha
Student, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
jyotirmoysahajyotirmoy@gmail.com

Aditya Mallik
Student, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
adikungfu@gmail.com

Sauvik Bal
Assistant Professor, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
sauvik.bal@uem.edu.in

Saraswata Roy
Student, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
saraswataroy21@gmail.com

Mrinal Kanti Sarkar
Assistant Professor, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
mrinalk.sarkar@uem.edu.in

Dr. Sanjay Kumar
Associate Professor, Dept. of CSE,
JNU Jaipur, Rajasthan, India
sanjaysatyam786@gmail.com

Rupayan Das
Assistant Professor, Dept. of CSE, UEM, Jaipur
Jaipur, Rajasthan, India
rupayan.das@uem.edu.in

***Abstract*— RSA algorithm is used to hide and retrieve the data in an insecure network environment. The advantage of RSA algorithm is to increase security and accessibility. The private keys never required to be transferred or exposed to everybody. In a shared-key cryptographic system, the secret keys must be shared since exactly the same key is used for encryption and decryption. So there may be a chance that an intruder can find the secret key during the data transmission. There are so many limitations present in RSA algorithm. Various types of attack may be happen in RSA algorithm, like forward search attack, common modulus attack etc. Another disadvantage of using RSA cryptography for encryption is factorization problem and computation speed. In this paper we use a modified RSA cryptosystem algorithm called "Asymmetric key based Cryptographic Algorithm using Four Prime numbers to secure message communication (ACAFP)" to handle four prime numbers and provide security. Four prime numbers are not easily disintegrated and increased the effectiveness throughout the networks.**

Keywords—*Cryptography, Encryption, Decryption, Cipher, Security.*

I. INTRODUCTION

Cryptography [1] is an important area to encrypt messages using various encryption algorithms and also retrieving the actual message using same or different decryption algorithms. The original messages generally known as plain text in sender side is encoded based on some algorithmic steps to produce an encrypted message also known as Cipher text [2]. Encryption

978-1-5386-2215-5/17/$31.00 ©2017 IEEE

algorithm helps to encrypt plain text by using encryption key sometimes referred as public key or private key. Again at the receiver end, the cipher text is transformed in to plain text by using private key or public key and the entire process is known as decryption. The process model of asymmetric key cryptography is given below.

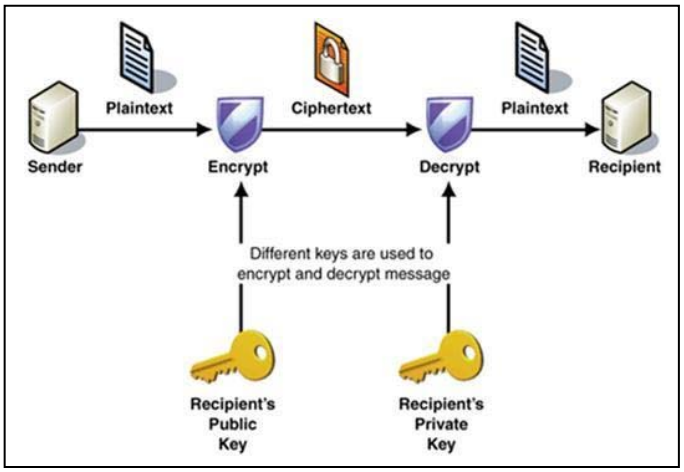

Fig-1: Process model of Asymmetric Key Cryptography

Now with the emergence of computer and collective trust on it for message communication also increased the attention on message security. Various security logics were proposed to secure information from being tempered or eavesdropped. Cryptographic algorithms are the state of the art in order to provide security at node level, network level and internet level. Security algorithms mainly cryptographic algorithms are generally classified in to two types one is symmetric key based cryptographic algorithm and another one is asymmetric key based cryptographic algorithm. Symmetric key based cryptographic algorithm deals with only one key (also known as secret or shared key) both for encryption and decryption. In asymmetric key based cryptographic algorithm two separate keys (also known as public and private key) is used. RSA [3] algorithm is one of the most important asymmetric cryptography based algorithm. The algorithm developed by Ron Rivest , Adi Shamir and Leonard Adleman [4,6], consists of two large prime numbers in order to produce two different keys called public and private key. In this algorithm plain text (original message) is encrypted by modulus operation using public key and decryption process is performed using private key at receiver side. Some advantages of RSA algorithm includes

1. It deals with two large prime number [5] and that is why encrypted message is not easily breakable.
2. It is quite difficult to get access of private key through the factorization from public key.
3. To make the RSA safety, sender must choose large prime numbers (choose 100 decimal digits)

Along with the advantages there are some limitations [8] present in RSA algorithm. Various types of attack may disrupt the functions of RSA algorithm, like forward search attack, common modulus attack etc. Speed is the shortcoming of RSA [7] cryptography for encryption. In this paper we use Asymmetric key based Cryptographic Algorithm using four Prime numbers called ACAFP to handle four prime numbers and provide security.

The entire paper includes Introduction, details about our proposed algorithm, Mathematical explanation, result & analysis and finally conclusion in section-I, II, III, IV and V respectively.

II. PROPOSED ALGORITHM

In this paper we propose an asymmetric key based cryptographic algorithm using four prime numbers. The method is divided in to three parts

1. Key generation algorithm
2. Encryption algorithm
3. Decryption algorithm

The Key generation algorithm, Encryption algorithm and Decryption algorithm is given in Algorithm-1, Algorithm-2 and Algorithm-3 respectively.

Algorithm 1: Key Generation Algorithm

Procedure;

Begin;

1. **Initialization/notation:**
   long integer w, x ,y, z; # w, x, y, z are the four prime numbers can be divisible by 1 and that number only.#
   Long integer n=0; # n is any large number initialized to zero#
   long integer f(n): # productive function#
   integer p; # any integer between 1 and f(n)#
   integer d; # any integer between 1 and f(n)#
2. Choose four large prime numbers w,x,yand z randomly and independently of each other. All prime numbers should be equivalent in length.
3. $n = wxyz;$
4. $f(n) = (w-1)(x-1)(y-1)(z-1);$
5. Choose an integer e, where $1 < p < f(n)$ such that gcd($p, f(n)$) = 1 and p and f(n) are co-prime
6. Compute the secret exponent d, where $1 < d < f(n)$ such that $(p \times d) \bmod f(n) = 1$
7. 'd' should be kept private
8. so public key: (p,n);
9. private key: (d,n);

End Procedure;

Algorithm-2: Encryption Algorithm;

Procedure;

Begin:

1. **Initialization/notation:**

long integer m; # input message #

integer p; # any integer between 1 and f(n), f(n) and p is calculated from step-4 and step-5 respectively from algorithm-1#

long integer n=0; # n is any large number initialized to zero and the value of n is calculated from step-3 of algorithm-1#

long integer CT; # cipher text c#

2. $CT = (m^p) \bmod n$; # Encryption process #

End procedure;

Algorithm-3: Decryption Algorithm;

Procedure;

Begin:

1. **Initialization/notation:**

long integer CT; # output message , cipher text calculated from step-2 of algorithm-2 #

integer d; # any integer between 1 and f(n), f(n) and d is calculated from step-4 and step-6 respectively from algorithm-1##

long integer n=0; # n is any large number initialized to zero and the value of n is calculated from step-3 of algorithm-1#

long integer m; # original message #

2. $m = (CT^d) \bmod n$; # Decryption process #

End procedure;

Architecture:

Our scheme ACAFP is a modification of RSA algorithm. Like RSA algorithm, our scheme is also support asymmetric key cryptographic process. As mentioned earlier asymmetric key based cryptographic algorithm consists of two types of keys: public key and private key. Here in our scheme we have two keys. We have used 'p' as a public key and whereas 'd' as a private key. RSA algorithm is also used same number of keys and the process of encryption and decryption is also same as ACAFP. But the process of key generation is different from RSA. RSA is used two large prime numbers whereas ACAFP used four small prime numbers. The detailed architecture of our scheme is given in figure-2

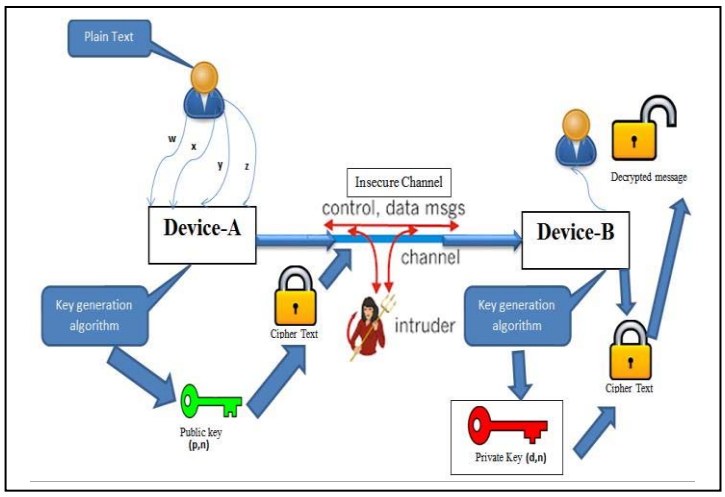

Fig-2: Architecture of proposed scheme

III. MATHEMATICAL EXPLANATION

A. Why ACAFP deals with four prime numbers:

ACAFP deals with four small prime numbers because, if we consider the following equations for smallest prime numbers with respect to constant 'p' then we get,

(d*p)mod f(n)=1 ------(1)

f(n)=wx-----(2) where w,x be the smallest prime numbers.

Now, by solving eqn-1 & eqn-2, we get d=smallest number=d_2, which is very easy to be used in case of decryption.

Now consider f(n)=wxy---(3), where w,x,y be the smallest prime numbers.

Now, by solving eqn-1 & 3 we get d=small number greater than d_2 =d_3 which is easy to be used in case of decryption process

Now consider f(n)=wxyz----(4) , where w,x,y,z be the smallest prime numbers.

Now, by solving eqn-1 & 4 we get d=greater than d_3 =d_4 which is comparatively big number to be used in case of decryption process but easily computable.

Now consider f(n)=wxyzt----(5) , where w,x,y,z,t be the smallest prime numbers.

Now, by solving eqn-1 & 5 we get d=greater than d_4 =d_5 which is a big number to be used in case of decryption process but not easily computable and so on. If you increased number of prime numbers then the value of'd' will be increased with respect to constant 'p'.

The 'd' value with respect to p=3 for two prime numbers (T_2) , three prime numbers (T_3) , four prime numbers (T_4) and five prime numbers (T_5) are compared in the following graph.

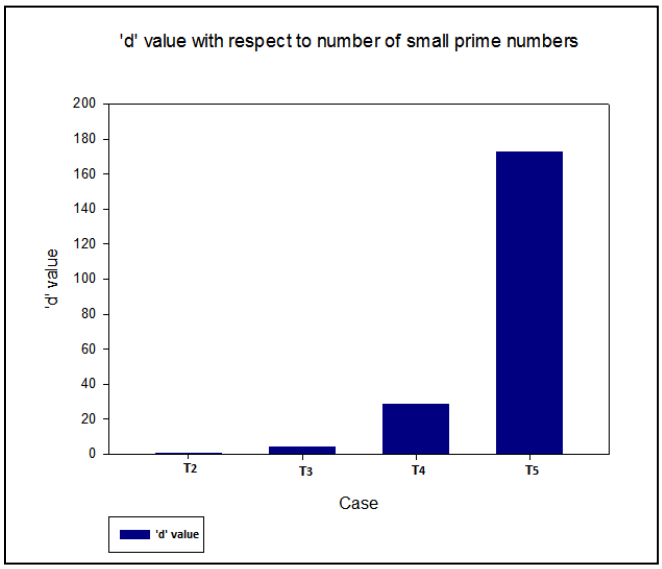

Fig-3: 'd' value with respect to number of prime numbers

B. *Example of the proposed algorithm:*

Below is given an example of our proposed algorithm in which we used four prime numbers and get public key and private key. Select four prime numbers.

i. *Selection of four prime numbers:*

w=7, x=5, y=3, z=2

ii. *Calculation of n:*

n=w*x*y*z = 7*5*3*2= 210.

iii. *Calculation of f(n):* f(n)=(w-1)(x-1)(y-1)(z-1) f(210) = (7-1) (5-1) (3-1)(2-1)

f(210) = (7-1) (5-1) (3-1) (2-1)=48

f(n)=48

iv. *Calculation of 'p':*

Select any number 1<p<48

f(n) must not be divisible by 'p' , Let p=5

v. *Calculation of 'd':*

Select 'd', multiplicative of p(mod f(n))

So d= 29,

vi. *Selection of public key:*

Public Key is (n = 210,e = 5)

vii. *Selection of private key:*

Private Key is (n = 210, d = 29)

viii. *Encryption process using public key:*

Given message m = 5.

Encryption: Cipher Text=CT= 5^5 mod 210 = 185

So CT = 185

ix. *Decryption process using private key:*

Decryption: m = 185^{29} mod 210 = 5

Original message= 5

C. *Explanation:*

The basic principle of arithmetic says that almost every integer number has a factorization into powers of prime numbers that is exclusive to the integer number, save for the order of the factors.

Suppose we select two prime numbers in order to find the value of 'n'. Now if we choose large prime numbers then the factorization of the numbers will be difficult compare to small size integer number.

Let's consider n is 21. If we try to find the possible factors then we have to try until we find 3 and 7. This is quite easy because of the small size prime numbers. But for big prime numbers the entire factorization procedure will be quite harder. There is no effective method to do that. This complicacy may arise in case of RSA algorithm. Basically it takes researchers a long time to find the factor of a 232-digit number. Even if somebody use hundreds of parallel computers then the problem will be remain unsolved. And for that reason RSA algorithm is more effective in terms of security but there may be computational complexity still remain. This computational complexity can be solved by increasing the number of prime number and that makes the algorithm more effective. Some attacks called Chosen cipher attack, Mathematical attack can also be mitigated. In our scheme, we used four small prime numbers and that is why its computational complexity is less and more over we can get effective service then RSA. It is quite easy to multiply prime numbers together. But there is no easy steps to find the product and return it back to its original primes. "trapdoor" is a function in crypto jargon that helps us to go one way easily, but not the other. These types of one-way functions are at the end of all public-key encryption. They make asymmetric ciphers possible. In RSA, Alice first secretly selects two large prime numbers of hundred digits long. This is easier than it may sound: there is an infinite supply of prime numbers.

D. *Complexity Analysis:*

In ACAFP scheme, we able to keep the same complexity like RSA. Proof as follows:

Encryption: CT= $(m)^p$ mod n

Decryption: m= $(CT)^d$ mod n

Assuming, a=log n, b=log e, c=log d

Time complexity respectively, O (a^2.b) and O (a^2.c)

IV. RESULT AND ANALYSIS

Our proposed algorithm ACAFP deals with four small size prime numbers and that is why it is very easy compute the factor. Hence our method needs less memory and less power is compare to RSA.

We run the scheme using JAVA compiler and the snapshot of the result is shown in Figure-4. The detailed simulation results are given in Table-1. We have taken some sample original text and we have experiment the samples on RSA and ACAFP. The memory required for RSA is much higher than ACAFP. Comparison graph between RSA and our scheme in terms of memory consumption is given in Figure-5. Figure-6 shows the comparison graph between RSA and our scheme in terms of ACAFP.

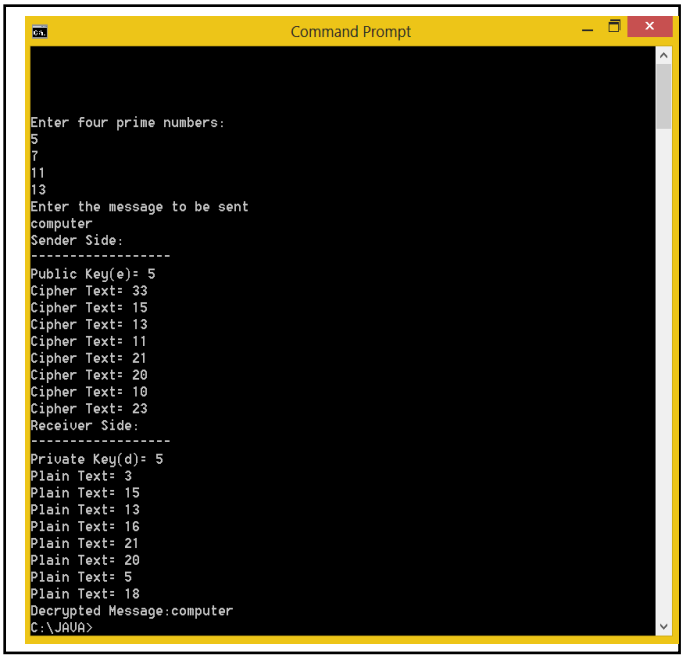

Fig-4: Snapshot of the result

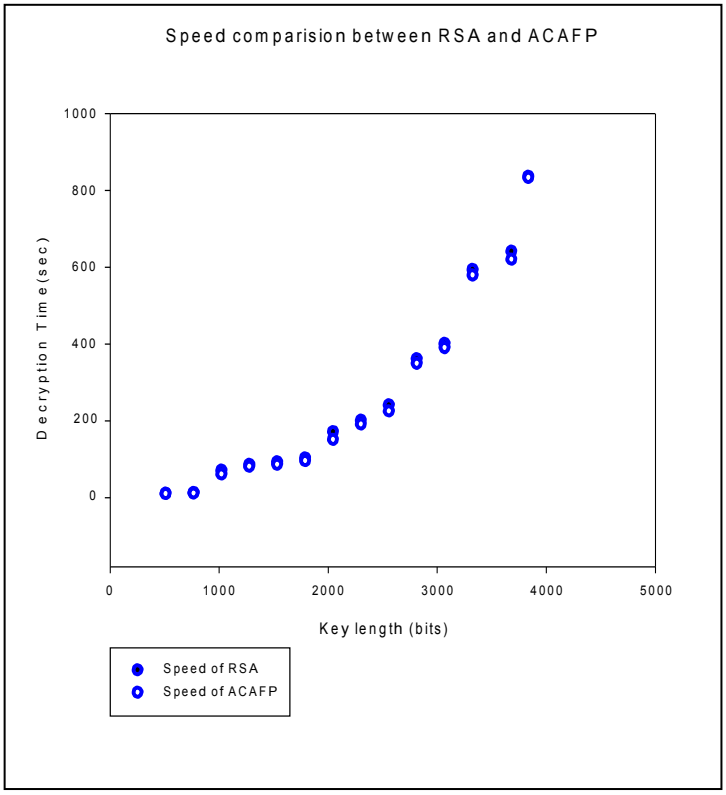

Fig-6: Speed comparison between RSA and ACAFP

\

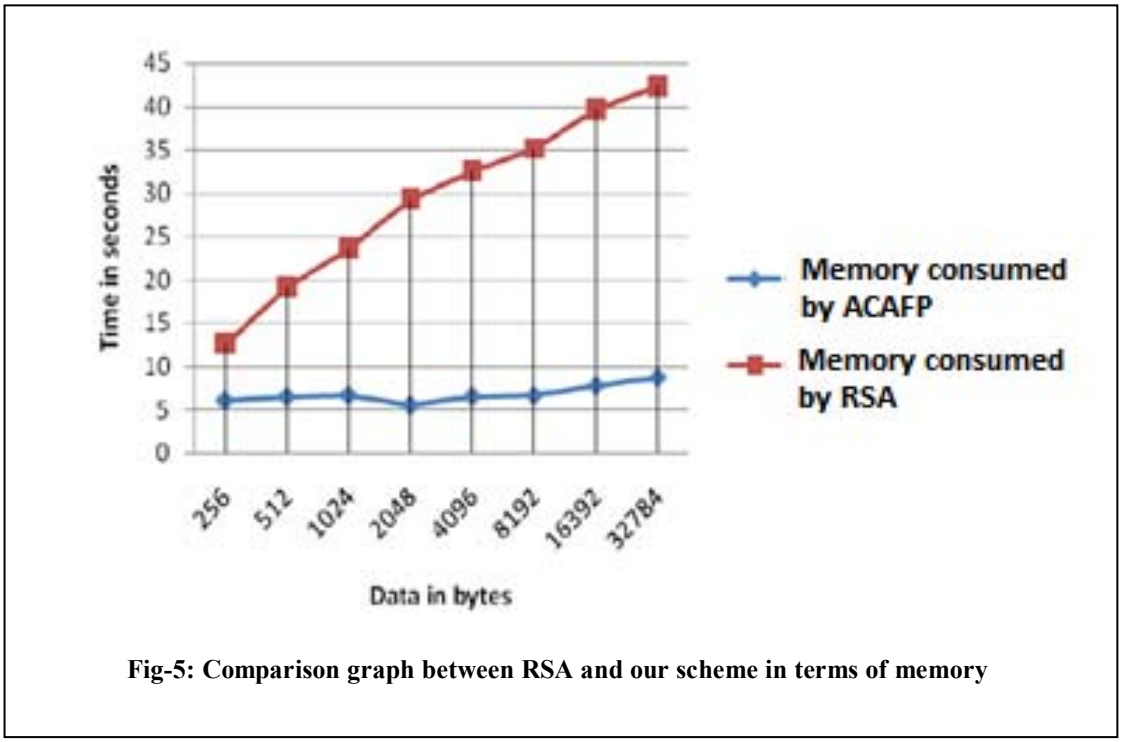

Fig-5: Comparison graph between RSA and our scheme in terms of memory

TABLE-1

w	x	y	z	n	f(n)	p	d	Given message, m	Encrypted (CT)	decrypted
7	5	3	2	210	48	5	29	5	185	5
2	3	5	17	510	128	3	43	11	311	11
3	7	11	13	3003	1440	7	823	2	59	2
5	7	11	13	5005	2880	7	3703	11	1091	11
7	11	13	17	17017	11520	7	6583	6	7664	6
11	13	17	19	46189	34560	17	2033	2	37494	2
13	17	19	23	96577	76032	19	64027	2	41403	2
17	19	23	29	215441	177408	23	38567	2	50432	2
19	23	29	31	392863	332640	29	298229	2	224890	2
23	29	31	37	765049	665280	13	255877	4	549601	4
29	31	37	41	1363783	1209600	19	381979	5	779999	5

V. CONCLUSION

ACAFP is a modification RSA algorithm. ACAFP can solve the factorization problem of RSA by including smallest prime numbers and hence the scheme is much advanced in terms of memory consumption and computational speed. More over the scheme ACAFP is capable enough to secure the data like RSA. In future, we will perform resilience analysis on this scheme under various network attacks.

REFERENCES

[1] William Stallings: ―Cryptography and Network Security: Principles and Practices 4th Edition, Prentice Hall‖

[2] Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. P. 21. ISBN 978-1-118-03138-4

[3] Sonal Sharma, " RSA algorithm using modified subset sum Cryptosystem" Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011

[4] NaQi, Wei, Jing Zhang, Wei Wang, Jinwei Zhao, Junhuai Li, Peiyi Shen,Xiaoyan Yin, Xiangrong Xiao and Jie Hu, " Analysis and Research of the RSA Algorithm", information technology Journal, 12:1818-1824. DOI:10.3923/itj.2013.1818.1824

[5] Hang Qing, " The large prime numbers based on genetic algorithm", (ICISIE) pp-434-437, IEEE 2011.

[6] Kumar, "An avdanced secure(t,n) threshold proxy signature scheme based on RSA cryptosystem for known signers", R, Dept. of compute. Sci. and Eng, pp 293-298, IEEE 2010

[7] R. Rivest, A.Shamir and L.Adleman, " A method for obtaining digital Signatures and public key cryptosystems", "communication of the Association for computing machinery "1978,pp 120-126.

[8] M.Preetha, M.Nithya, "A study and Performance Analysis of RSA Algorithm", IJCSME, Vol.2 Issue.6, June, pg.126-139, ISSN 2320.