# ENHANCEMENT OF SECURITY IN RSA ASYMMETRIC ALGORITHM TO SECURE THE COMMUNICATION

Sweta Ranjan[1], Dr. Sunil Gupta[2]
[1]M. Tech Scholar (CSE) , [2]Professor (CSE)
Global Institute of Technology, Rajasthan

***Abstract: Inthiseraofdigitalage a lot ofsecretandnon-secret data is transmitted over the internet. Cryptography is one of the many techniques to secure data on network. It is one of the techniques that can be used to ensure information security and data privacy. It is used to secure data in rest as well as data in transit. RSA in the most commonly used cryptographic algorithm and it is also used for the creation on Digital Certificates. RSA algorithm is now not considered to be as secure due to advancement in technology and newer attack vectors. This paper proposed an algorithm for security enhancement of RSA algorithm by increasing prime numbers count. Proposed algorithm has been implemented to encrypt and decrypt the data and execution results for encryption and decryption time have beencomparedforincreasedprimenumbers count.Thisproposed algorithm of RSA can be used to replace the existing RSA algorithm in digital signature certificates as well as in all other places where the base RSA algorithm is currently being used. In the proposed technique, as the number of prime number count increases, prime factor calculation becomes difficult. If the attackerhasencryptionkey(e)andProductofprimenumbers(N) then it is not easy to find out the prime number combinations and hence decryption key (d) will be more secure by using proposed algorithm.Thiswillbemoredifficultbecausegivenanumbern,it is easy to find two numbers whose product is equal to n using Shor's algorithm and Grover's Search Algorithm but it is notvery difficult and time taking to exactly determine m numbers whose product is equal ton.***

***Keywords: Cipher Text, Decryption, Decryption Time, Encryption, Encryption Time, Plain Text, RSA Algorithm.***

## I. INTRODUCTION

Cryptography is a technique to make a readable data into unreadabledata.Moderncryptographyispartofmathematics and technology of computerscience.[1],[2],[3]

Goals of Security (Purpose ofCryptography)

There are some specific security requirements within the context of any application-to-application communication, including these goals.[3],[4],[5]

Confidentiality: It specifies that only sender and intended recipient should able to access the contentsof message.The attack on the availability is calledinterception. There are two main threats to confidentiality, snooping and trafficanalysis.[3],[4],[5]

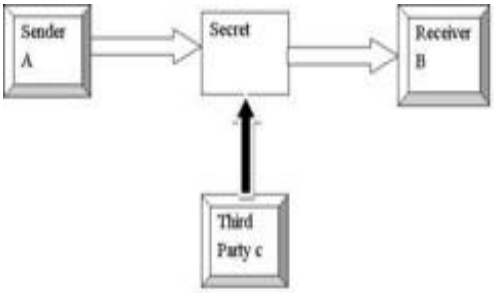


Fig. 1.Loss of Confidentiality [4]

Integrity: When sender sends a message andensuring that the receiver receives the message as it was, wholly and error free without any changes. Attack on the integrity is called modification.[3],[4],[5]

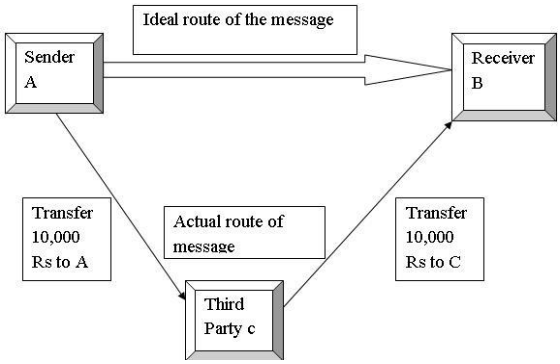


Fig. 2.Loss of Integrity [4]

Availability: Availability is ensuring that those who havetherightstoinformationormaterialhavealwaysgotthe access to it or resources should be available to authorized parties at all time. The attack on the availability is called interruption[3],[4],[5].

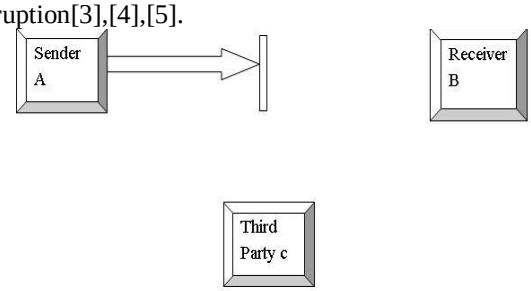


Fig. 3.Attack on Availability [4]

Authentication:Ithelpsestablishproofofidentities.It ensuresthattheoriginofadocumentsormessageiscorrectly identified. Suppose that third party C sends an electronic message over the internet to receiver B. However, the third-party C had posed as Sender A when C sent this document to user B. How would Receiver B know that the messagehascomefromC.WhoisposingasSenderA.?This type

  

of attack is called as fabrication[3],[4],[5].

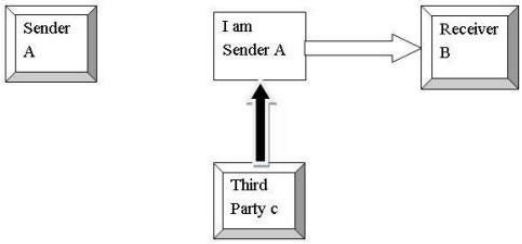


Fig. 4.Absence of Authentication [4]

Non-repudiation: It is a mechanism to prove that sender really sent this message[3],[4],[5].

Types ofCryptosystem

There are two types of cryptosystem:

Symmetric Key Cryptography: If sender and receiver sharethesamekeyforencryptionanddecryptionofmessage than it is called symmetric keycryptography.[7],[9]

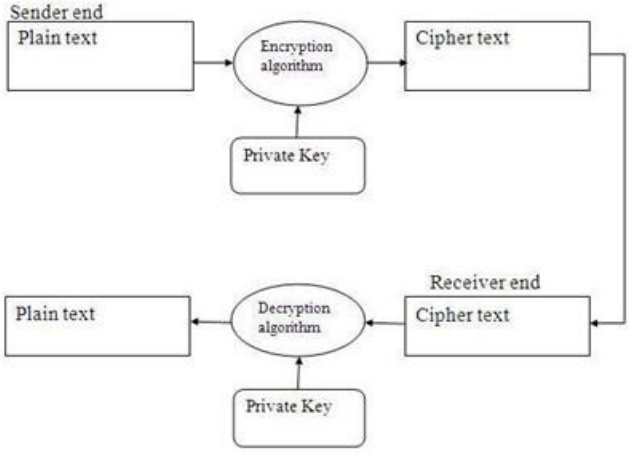


Fig. 5.Private Key Cryptography

AsymmetricKeyCryptography:Ifsenderandreceiver share the one key for encryption and another key decryption of message than it is called asymmetric key cryptography.[6],[7],[9]

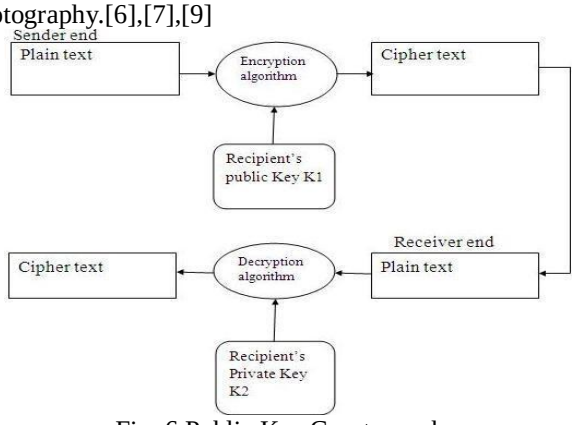


Fig. 6.Public Key Cryptography

RSA Cryptography is the most commonlyimplemented Asymmetric Key Cryptography.[7],[8],[9],[10]

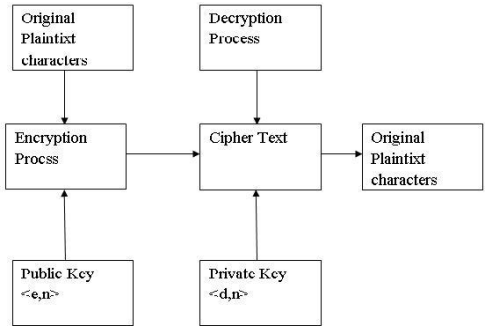


Fig. 7.RSA Model [4]

## II. PROPOSED ALGORITHM

Step1–Takethenprimenumbers($P_1$,$P_2$,$P_3$, ,$P_n$) InsteadoftwoprimenumbersthatisusedinRSAAlgorithm.

Step 2 – Calculate the product of these primenumbers (N = $P_1$x $P_2$x$P_3$x $P_n$)

Step3–Now,selecttheencryptionkeye,suchthatitisnota factor of numbers (($P_1$-1),($P_2$-1),($P_3$-1) ($P_n$-1))

Step 4 – Calculate the decryption key d, such that (d x e) mod (($P_1$-1), ($P_2$-1), ($P_3$-1) ……. ($P_n$-1)) = 1

Step 5 – Calculate cipher text (CP) from plain text (PT) as $CT = PT^e mod n$

Step 6 – At the receiver's end, calculate plain text (PT) as $PT = CT^d mod n$

FLOWCHART

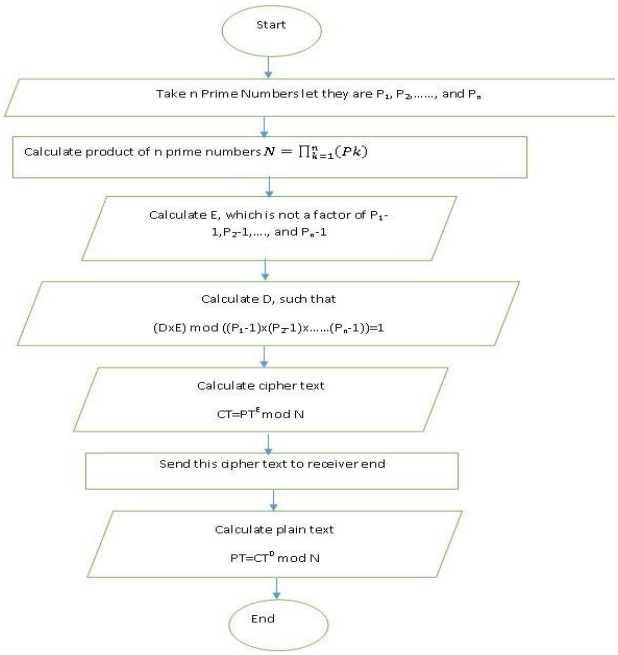


Fig. 8.Flowchart of Proposed Algorithm

PROPOSED ALGORITHMIMPLEMENTATION RESULT

The proposed algorithm is implemented in C and python. We take here 4 types of examples. In these example there is plain text is same for all example that is "India is a Nation." Andthereare2,3,4and5 different prime numbers are used and we calculate the value of N, encryption key value, decryption key value, Encryptiontime, Decryptiontime, ciphertext and again plain text from cipher text for differentcombinations.

  

We check variations in encryption and decryption time accordingtotheprimenumberscountandcheckthebehavior oftimegraphs.Heretheprimenumbersaresmallformaking calculationseasy,butwecantakelargeprimenumbersinour practicallife.

Table- I: List of Prime Numbers Used in this Experiment

| | **P1** | **P2** | **P3** | **P4** | **P5** |
|---|---|---|---|---|---|
| **1** | 23 | 53 | 11 | 37 | 17 |
| **2** | 29 | 59 | 13 | 41 | 19 |
| **3** | 31 | 61 | 17 | 43 | 23 |
| **4** | 37 | 67 | 19 | 47 | 29 |
| **5** | 41 | 71 | 23 | 53 | 31 |
| **6** | 43 | 73 | 29 | 59 | 37 |
| **7** | 47 | 79 | 31 | 61 | 41 |
| **8** | 53 | 83 | 37 | 67 | 43 |
| **9** | 59 | 89 | 41 | 71 | 47 |
| **10** | 61 | 97 | 43 | 73 | 53 |

If we are using 2 prime numbers, then P1 and P2 are used. If weareusing3primenumbersthenP1,P2andP3areused.If we are using 4 prime numbers then P1, P2, P3and P4 are used.
If we are using 5 prime numbers then P1, P2, P3, P4 and P5 are used.

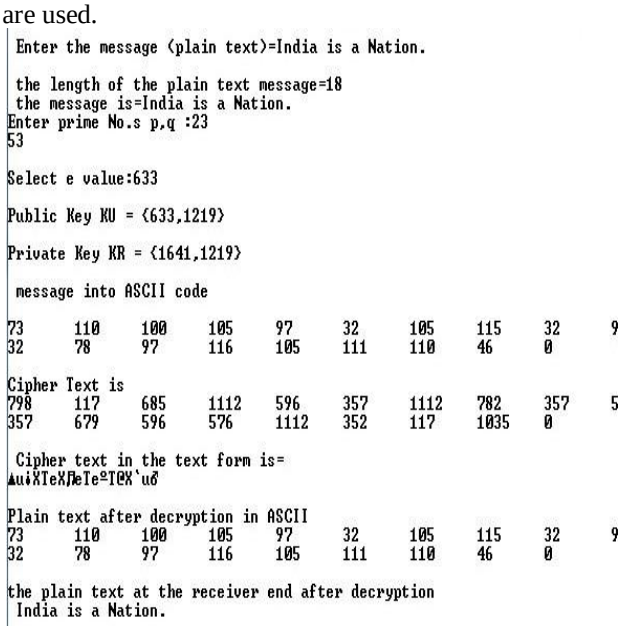


Fig. 9.Example for Two Prime Numbers

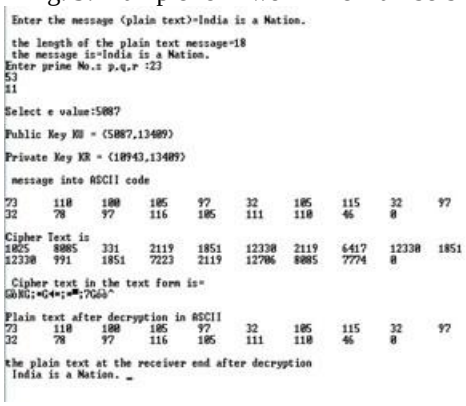


Fig. 10. Example for Three Prime Numbers

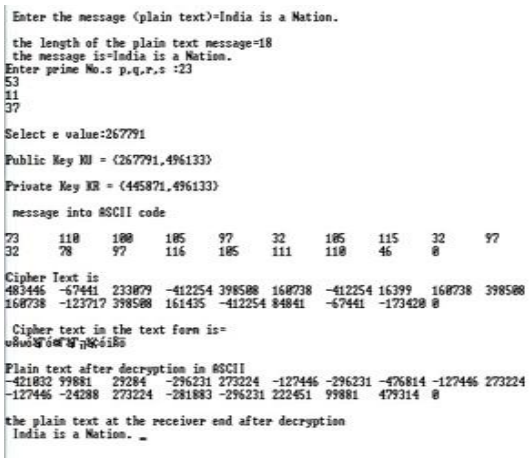


Fig. 11. Example for Four PrimeNumbers

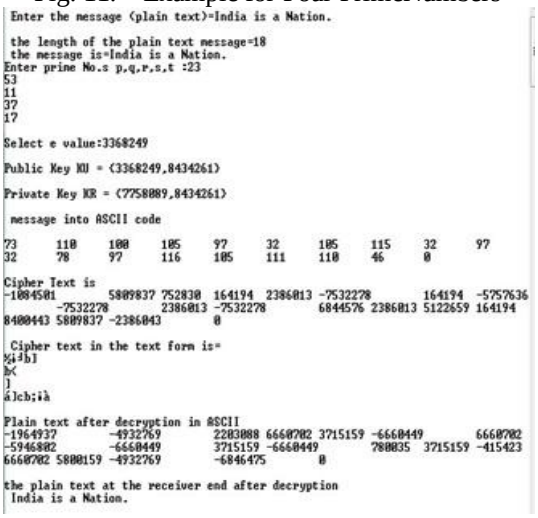


Fig. 12. Example for Five PrimeNumbers

## III. PERFORMANCE ANALYSIS OFPROPOSED ALGORITHM

10setsfor2,3,4and5primenumbershavebeentaken. Tables II,III,IV and V shows the values obtained during the use of two, three, four and five primenumbers.

Table- II: List of Values obtained using Two Prime Numbers

| $P_1$ | $P_2$ | n | e | d | encryption time (in sec) | decryption time (in sec) |
|---|---|---|---|---|---|---|
| 23 | 53 | 1219 | 633 | 1641 | 0.000062900000003197 | 0.000061999999997844 |
| 29 | 59 | 1711 | 429 | 1677 | 0.000057400000002872 | 0.000063700000054400 |
| 31 | 61 | 1891 | 799 | 1399 | 0.000069099999997491 | 0.000073200000027710 |
| 37 | 67 | 2479 | 779 | 2315 | 0.000058899999999085 | 0.000065299999957160 |
| 41 | 71 | 2911 | 277 | 4013 | 0.000055599999996048 | 0.000074499999966467 |
| 43 | 73 | 3139 | 319 | 2095 | 0.000058299999999178 | 0.000066600000038025 |
| 47 | 79 | 3713 | 511 | 2935 | 0.000060699999998803 | 0.000119300000014880 |
| 53 | 83 | 4399 | 1263 | 2711 | 0.000069000000003427 | 0.000068200000011840 |
| 59 | 89 | 5251 | 1095 | 3687 | 0.000074800000000153 | 0.000078700000030957 |
| 61 | 97 | 5917 | 5563 | 3187 | 0.000091199999999958 | 0.000078500000007585 |

Table- III: List of Values obtained using Three Prime Numbers

| $P_1$ | $P_2$ | $P_3$ | N | e | d | encryption time (in sec) | decryption time (in sec) |
|---|---|---|---|---|---|---|---|
| 23 | 53 | 11 | 13409 | 5087 | 10943 | 0.000092100000033700 | 0.000094500000029950 |
| 29 | 59 | 13 | 22243 | 11957 | 13469 | 0.000084999999985585 | 0.000077599999973465 |
| 31 | 61 | 17 | 32147 | 27403 | 21667 | 0.000090099999942087 | 0.000086400000007081 |
| 37 | 67 | 19 | 47101 | 8689 | 25585 | 0.000084700000021580 | 0.000089500000014079 |
| 41 | 71 | 23 | 66953 | 45811 | 72091 | 0.000106799999975200 | 0.000108400000020070 |
| 43 | 73 | 29 | 91031 | 18749 | 123989 | 0.000097400000013575 | 0.000103600000027570 |
| 47 | 79 | 31 | 115103 | 52093 | 61237 | 0.000109699999958820 | 0.000101899999899960 |
| 53 | 83 | 37 | 162763 | 104861 | 126005 | 0.000114199999987320 | 0.000105800000000450 |
| 59 | 89 | 41 | 215291 | 133999 | 205839 | 0.000119699999990570 | 0.000109199999971450 |
| 61 | 97 | 43 | 254431 | 4283 | 186227 | 0.000084899999902844 | 0.000145799999985300 |

Table- IV: List of Values obtained using Four Prime Numbers

  

| $P_1$ | $P_2$ | $P_3$ | $P_4$ | N | e | d | encryption time (in sec) | decryption time (in sec) |
|---|---|---|---|---|---|---|---|---|
| 23 | 53 | 11 | 37 | 496133 | 257791 | 432511 | 0.000124400000042430 | 0.000119999999954570 |
| 29 | 59 | 13 | 41 | 911963 | 617993 | 1126457 | 0.000129700000022310 | 0.000126599999873200 |
| 31 | 61 | 17 | 43 | 1382321 | 675587 | 1271723 | 0.000128400000083550 | 0.000137199999975060 |
| 37 | 67 | 19 | 47 | 2213747 | 1403035 | 1429843 | 0.000137499999939060 | 0.000130200000009680 |
| 41 | 71 | 23 | 53 | 3548509 | 1670597 | 3166733 | 0.000143100000025050 | 0.000133800000004060 |
| 43 | 73 | 29 | 59 | 5370829 | 4226941 | 5490901 | 0.000209600000051390 | 0.000146399999913310 |
| 47 | 79 | 31 | 61 | 7021283 | 2868137 | 7946873 | 0.000144699999927810 | 0.000147099999924060 |
| 53 | 83 | 37 | 67 | 10905121 | 1542943 | 11135071 | 0.000138500000198030 | 0.000154300000197030 |
| 59 | 89 | 41 | 71 | 15285661 | 12370703 | 9366767 | 0.000184700000054780 | 0.000154799999900190 |
| 61 | 97 | 43 | 73 | 18573463 | 6919681 | 23585281 | 0.000140500000431760 | 0.000147799999792700 |

Table- V: List of Values obtained using Five Prime Numbers

| $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | N | e | d | encryption time (in sec) | decryption time (in sec) |
|---|---|---|---|---|---|---|---|---|---|
| 23 | 53 | 11 | 37 | 17 | 8434261 | 3368249 | 7758089 | 0.000145800000056360 | 0.000140500000005430 |
| 29 | 59 | 13 | 41 | 19 | 17327297 | 5298563 | 12062507 | 0.000150000000049800 | 0.000153400000020800 |
| 31 | 61 | 17 | 43 | 23 | 31793383 | 21087041 | 18400961 | 0.000155399999828190 | 0.000147999999958180 |
| 37 | 67 | 19 | 47 | 29 | 64198663 | 36667549 | 28792117 | 0.000172599999848680 | 0.000163799999957170 |
| 41 | 71 | 23 | 53 | 31 | 1.1E+08 | 51873697 | 87112033 | 0.000175999999867030 | 0.000173000000179640 |
| 43 | 73 | 29 | 59 | 37 | 1.99E+08 | 1.49E+08 | 227267713 | 0.000188600000013150 | 0.000174600000366620 |
| 47 | 79 | 31 | 61 | 41 | 2.88E+08 | 64729411 | 184227691 | 0.000173800000841570 | 0.000187799999814360 |
| 53 | 83 | 37 | 67 | 43 | 4.69E+08 | 3.05E+08 | 394023173 | 0.000196599999911170 | 0.000186199999164250 |
| 59 | 89 | 41 | 71 | 47 | 7.18E+08 | 2.64E+08 | 513683237 | 0.000269699999898250 | 0.000226499999317129 90 |
| 61 | 97 | 43 | 73 | 53 | 9.84E+08 | 1.03E+08 | 465483839 | 0.000301099998978316 0 | 0.000197299999854295 0 |

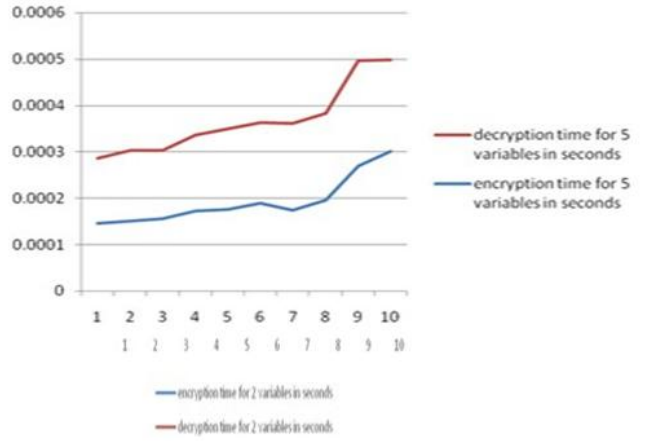


Fig. 13. Encryption-Decryption Time Graph for Two Prime Numbers (based on TableII)

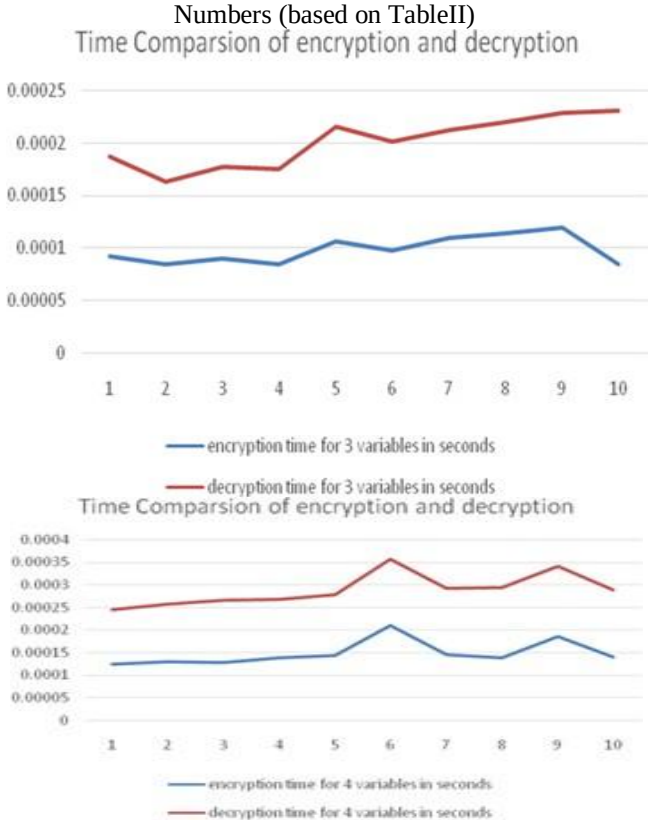


Fig.14. Encryption-Decryption Time Graph forFour Prime Numbers (based on TableIV)

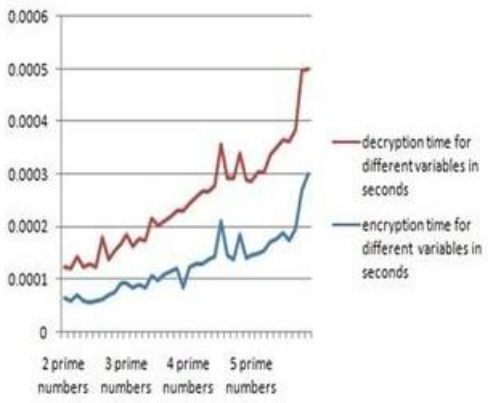


Fig. 15. Behavior of Encryption-Decryption Time Graph for all combinations from 2, 3, 4 and 5 Prime Numbers

By analysis of these graphs we can say that if we increase the prime number then encryption and decryption time will be increased in terms of $e^x$.

## ADVANTAGES OF PROPOSEDALGORITHM

It is very hard to find out the factors of N. In this case (($P_1$-1), ($P_2$-1), ($P_3$-1) ……. ($P_n$-1)) because when we increase number of prime numbers then its product is also a bignumber.

The security aspects are not compromised here like confidentiality, availability, integrity,Authentication.

## IV. CONCLUSION

Attheendbycomparingandcheckingalltheparametersof proposed algorithm with existing algorithm, we can say that when we increase the number of prime numbers in RSA algorithm then its security also improves because it's hard to find the factor of N, while there are more than two prime numbers.

EncryptionandDecryptiontimeisdependsonthevalueof e(encryptionkey)andd(decryptionkey)andherevalueofe is smaller because we are using more than 2 prime numbers so due to this the value of d is also not so big and by this process the encryption and decryption time isless.

## REFERENCES

[1] RSAalgorithmusingmodifiedsubsetsumcryptosyste m,SonalSharma, Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011

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

[3] An advanced secure (t, n) threshold proxy signature scheme based on RSAcryptosystemforknownsigners,Kumar, R,Dept.of Computer Sci. and Eng, pp 293-298, IEEE2010.

[4] An efficient decryption method for RSA cryptosystem, Ren-Junn Hwang, Dept. of Compute. Sci. and Inf. Eng, pp-585-590, IEEE2005.

[5] A new RSA cryptosystem hardware design based on Montgomery's algorithm, Ching Chao Yang, Dept. of Electron. Eng, pp- 908-913, IEEE 1998.

[6] A systolic RSA public key cryptosystem, Po – Song

  

Chen, Dept. of Electron. Eng, pp 408-411, IEEE1996.

[7] "Secure Key Exchange using RSA in Extended Playfair Cipher Technique" Surendra Singh Chauhan, International Journal of Computer Applications (0975 – 8887) Volume 104 – No 15, October 2014.

[8] Blocking method for RSA cryptosystem without expanding cipher length, NEC Corp, Kanagawa, Japan, pp 773-774, IEEE1989.

[9] A method orobtaining digital signatures and publickeycryptosystems, R.Rivest, A.Shamir and L.Adleman "communication of the association for computing machinery " 1978, pp120-126.

[10] A modified RSA cryptosystem based on 'n' prime numbers", B.PersisUrbanaIvy, Purshotam Mandiwa. MukeshKumar,InternationalJournal Of Engineering And Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012 Page No.63-66

  