# A Novel Approach for Security of Data Communication using Variant RSA Encryption Algorithm

Manish Sharma[1], Ankur Goyal[2]
M.Tech Scholar[1] , Assistant Professor[2],
Computer Science and Engineering[1,2]
Roorkey College of Engineering, Uttarakhand Technical University, Dehradun India.

**Abstract** *:* A system security or data security is one of the main issue in data communication. A data encryption is one of the solution for security issues in data communication. By using a unscrambling system / encryption method we create a new variant method for data hiding. There are not many end-clients today who utilize genuine security applications. These applications will in general be excessively confused, uncovering a lot of detail of the cryptographic procedure. Clients need basic inborn security that doesn't require a greater amount of them essentially tapping the safe checkbox. Cryptography is a first reflection to isolate explicit calculations from conventional cryptographic procedures so as to take out similarity and upgradeability issues. The center thought is upgrade the security of RSA calculation. In this exposition open key calculation RSA and improved RSA are analyzed investigation is set aside a few minutes dependent on execution time. A RSA algorithm is the widely utilized open key cryptosystem. It is the main open key cryptosystem. The quality of this cryptosystem depends on the bigger key size. There are numerous calculations & variations of RSA. Be that as it may, it is take a consuming point of research. Since the push to store information mystery is never going to end. In this thesis, we have recommended a writing survey of some cutting edge variations of the RSA calculation. No organization will be unaffected without the correct security conventions. Absence of security strategy, setup and the shortcoming in innovation were observed to be the purposes for framework weakness. Organizations that need to set a neighborhood with the advantages referenced in this proposal and actualize them in to their security approach will have a solid verified net-work. The experimental study shows that proposed algorithm gives accurate result for security in terms of cost, execution time, authentication and secure key generation.

***Index Terms*** **– Cryptosystem, Encryption, RSA, Security.**

## I. INTRODUCTION:-

A network or computer network architecture is a bunch of associated have PCs. There are on a very basic level two kinds of systems: open system and private system. An open system is where each host/hub/client can access and share an information and assets which are accessible in system while in a private system just an approved host/hub/client can get to an information and assets. Then again, Data communication is a significant part information sharing. So maintain an integrity of data we need a secure algorithm/system. To achieve this ,cryptography is a procedure to verify correspondence among sender and recipient. Cryptography comprises of the considerable number of standards and strategies for changing an understandable message called plaintext into one that is ambiguous called figure content and afterward retransforming that message back to its unique Form.

## II. Literature Survey:-

[1]Kun Ma et al in contains a novel Concurrent Error Detection plan to conquer the issue because of shortcoming based assault against RSA. This proposed technique depends on the idea of the multiplicative homomorphism property. The time overhead of this strategy is more.

[2] Paper [3] centers around the issue of how to forestall the quick RSA mark and unscrambling calculation with buildup number framework speedup from an equipment deficiency cryptanalysis in an exceedingly solid and effective methodology. The CRT-based speedup for RSA mark has been generally utilized.

[3]The creatorsproposed another extraordinary reason calculation to perform factorization. This calculation is contrasted and preliminary division calculation TDM. Proposed calculations runtime relies upon the distinction of variables and is autonomous of size of the modulus.

[4] Giraud proposed another countermeasure plan dependent on the idea of Montgomery Ladder Exponentiation. The proposed calculation performs two particular increases for each piece of example. While the square and increase calculation which performs all things considered 1.5 particular augmentations per bit of the type.

[5] The creators of proposed an improve calculation for the RSA cryptosystem. This new proposed cryptosystem utilizes a third prime number in figuring the estimation of n. This extra third prime number expands the factor multifaceted nature of n. It will give greater security to the RSA.

## III. PROBLEM STATEMENT

As we include early a system security or data security is one of the main issue in data communication. A data encryption is one of the solution for security issues in data communication. By using a unscrambling system / encryption method we create a new variant method for data hiding. We have a RSA encryption algorithm to solve security issue but it lead with some problems like: Not verify against different attacks , Slow speed, Easy to Crack if keys are not strong or small in size ,No provision for verify regular modulus attacks, low decoding type attack .

So we require greater security calculation to manage these issues. The focal point of this theory is coordinated towards on network security for remote framework correspondence . The objective of the work exhibited is to present another methodology for network security for remote framework. To substance/increment, this postulation watches the current calculations accessible for provisioning and rebuilding, and issues identified with execution parameters for those calculations, and after that endeavors to give reasonable proposed calculations to streamlined outcomes for network. cryptosystem depends on the bigger estimation of modulus. One of the subjects related to RSA crypto -system is factorization.

## IV. PROJECTED MODEL

- **Input :** The text dataset DS ;
- **Output :** generation of public key & private key for secure communication

**Start**

- Read text dataset;
- selection of four prime numbers namely b,c,q,p;
- calculating their product n = b*c*p*q;
- derived number (e)variable phi=(b-1)*(c-1)*(d-1)*(e-1);
- n.=d*e*c*b;
- a=zeros(1,1);
- v=1;
- print values of p,q,c,b,n;
- Now find A
- j=1;
- for i=2:phi-1
- if gcd(i,phi)==1
- Print A=i;
- break;
- end
- find B
- for i=2:phi-1
- if rem((A*i),phi)==1
- b=i;
- break;

```
 end
 ENCRYPTION part
T(1)=1;
for u=1:1:length(ASCI_TEXT)
for i=2:A+1
h =T(i-1).*ASCI_TEXT(u);
T(i)=mod(h,n);
end
Cipher(u)=T(end);
end
for z=1:1:length(Cipher)
Cipher_TEXT(z)=[Cipher(z),''];
end
Print cipher_text
Find  DECRYPTION
t(1)=1;
for x=1:1:length(Cipher)
for i=2:b+1
t(i)=rem(t(i-1)*Cipher(x),n);
end
Decrypted_array(x)=t(end);
for z=1:1:length(Decrypted_array)
   Decrypted_text(z)=[Decrypted_array(z),''];
print decrypt data/message
```

## V. RESULTS ANALYSIS

In this research work, we have evaluated public key, private key, execution time of algorithm and throughput of the proposed algorithm. To measure these performance parameters, we have used text data set. The main purpose of the proposed algorithm is to improve security issues and make a strong keys for communication. All the experiment execute on MATLAB R2016a.

### 5.1 Performance Parameters:-

The performance of proposed algorithm measure in different following parameters:

#### 5.1.1:Secure Key generation:-

The first performance parameter is despite generation of public key and private using two prime number and proposed algorithm concept using four numbers in MATLAB R2016a.

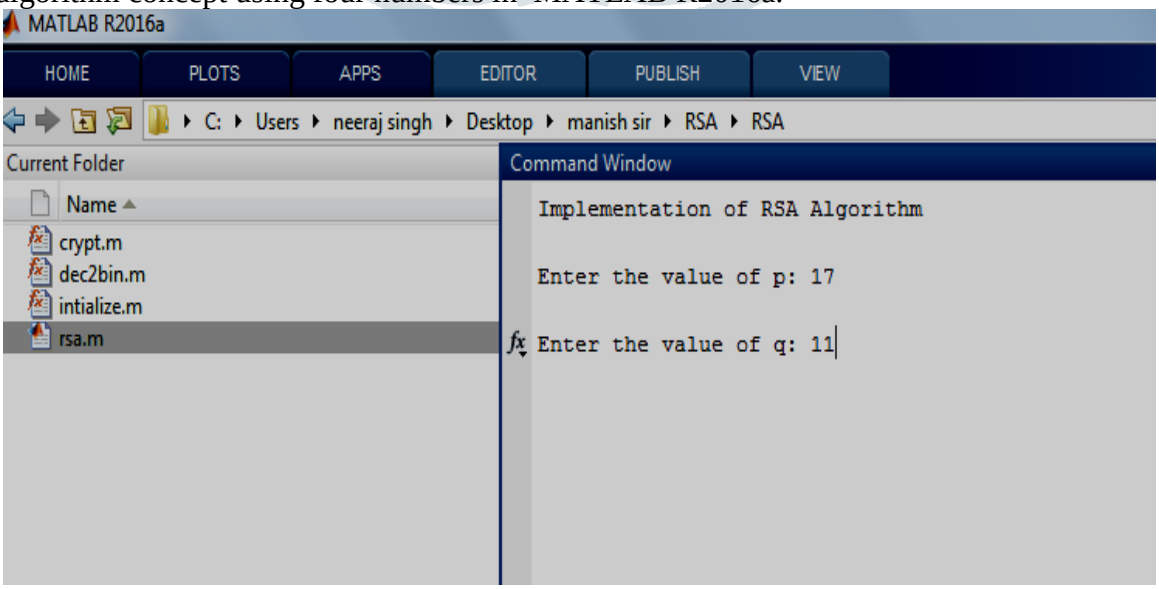


Fig:5.1.1 A traditional RSA algorithm scenario

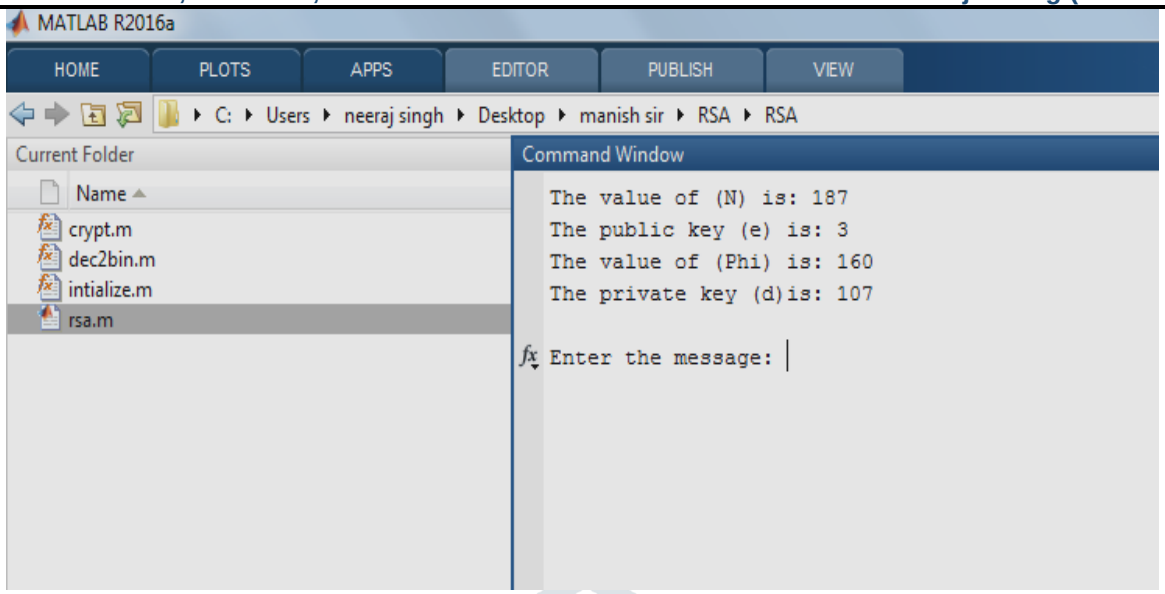


Fig5.1.2Key generation using two prime number

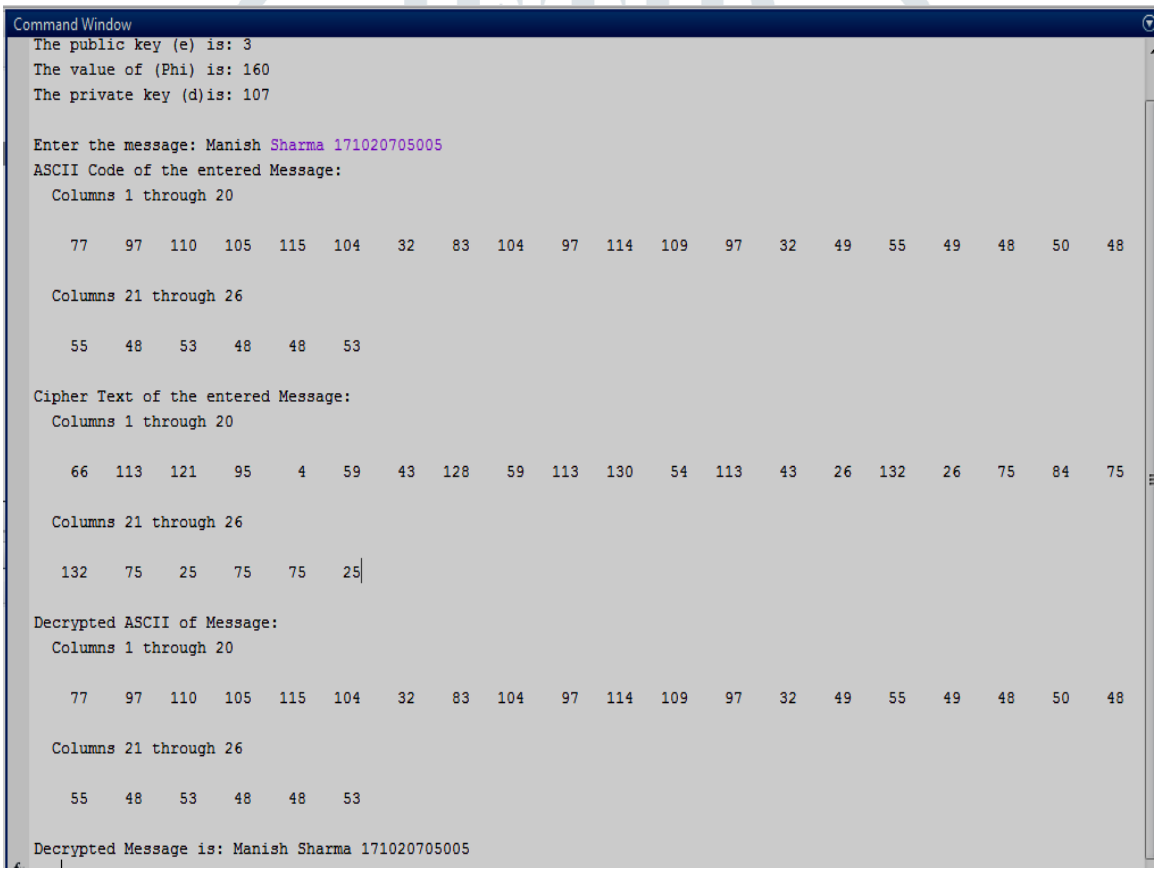


Fig:5.1.3 An encryption and decryption using RSA

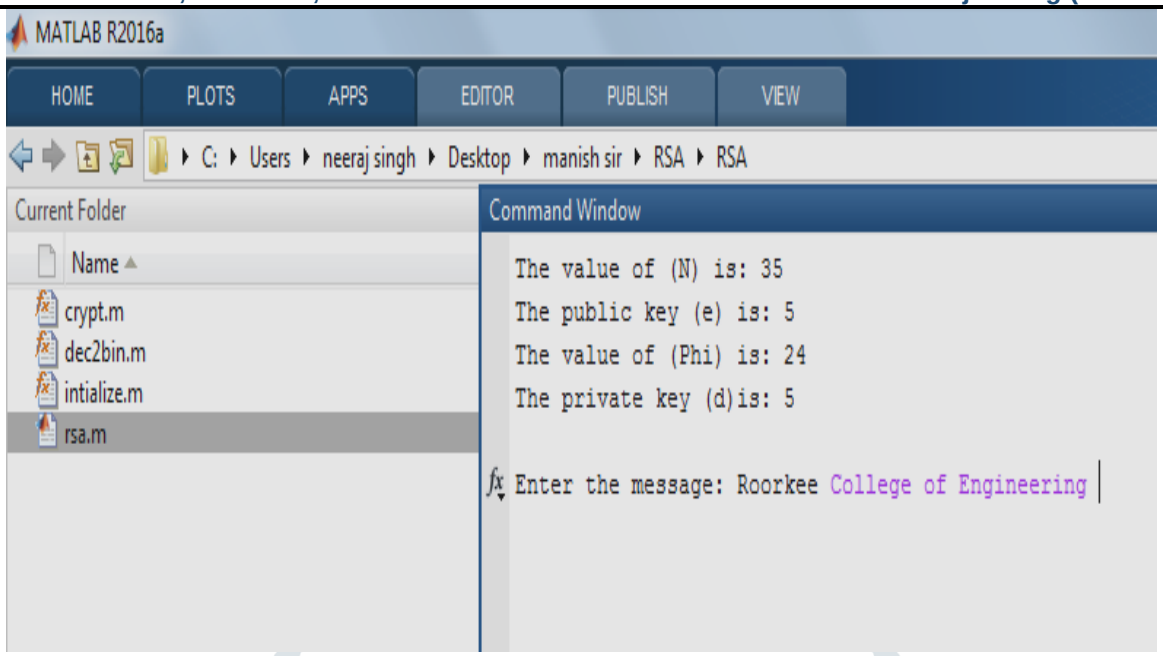


Fig:5.1.4 Generation of cipher text

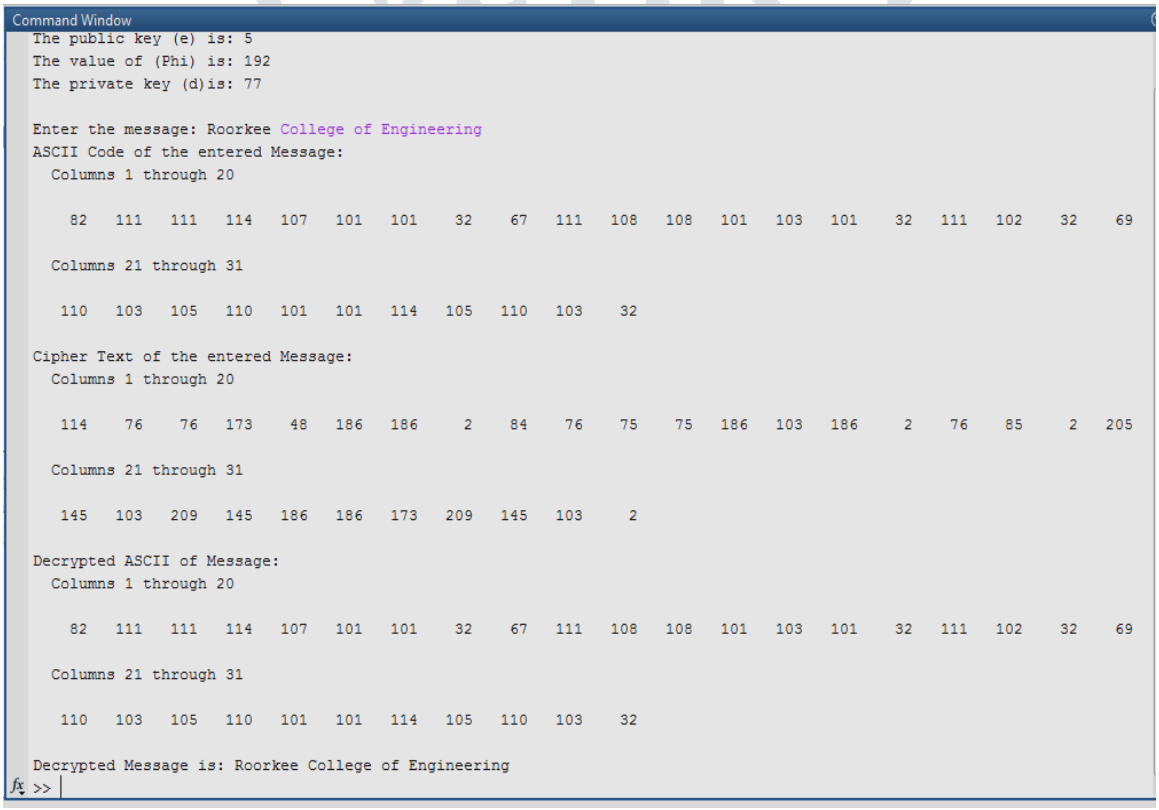


Fig:5.1.5 A decrypted message using RSA

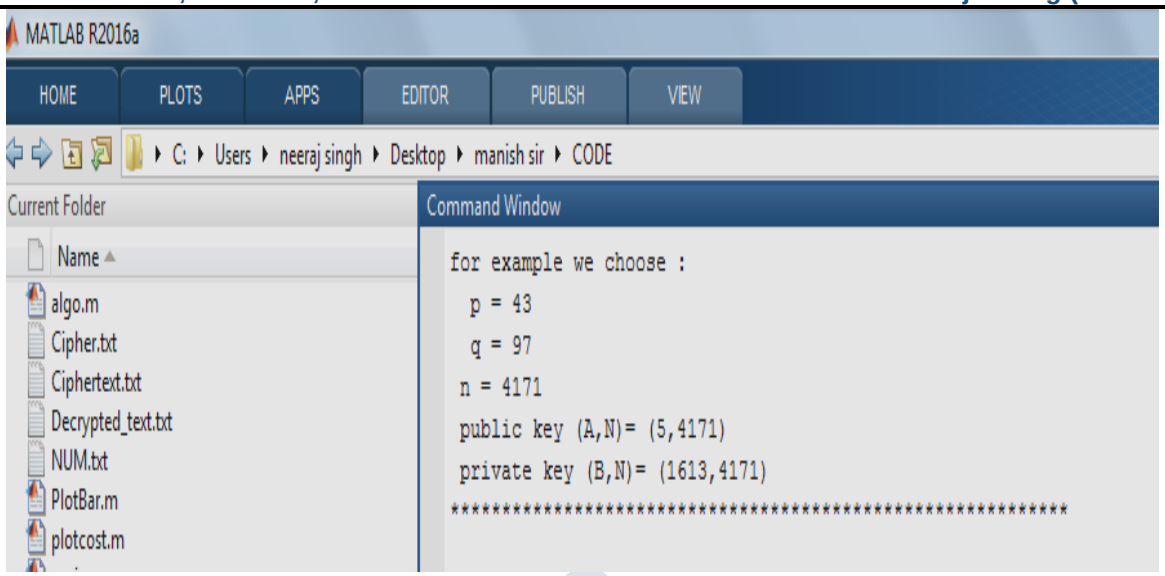


Fig 5.1.6 Generation of keys using Proposed algorithm

### 5.2.2 Computation Time :-

This parameters defines Net time difference between proposed algorithm Variant RSA and previous security algorithm.

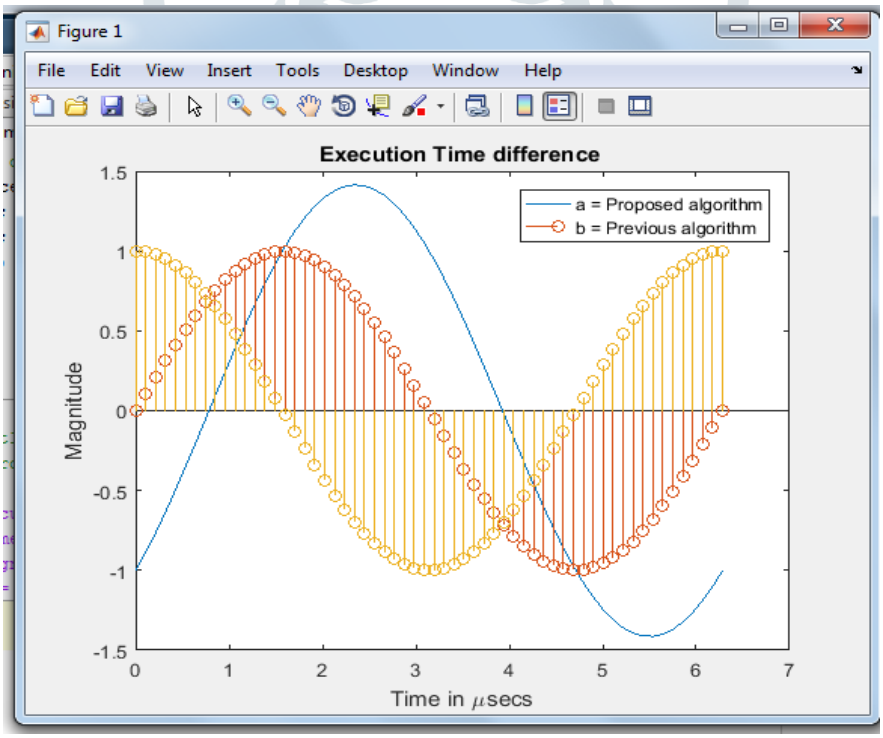


Fig5.2.2(a) Time/sequence graph for Variant RSA

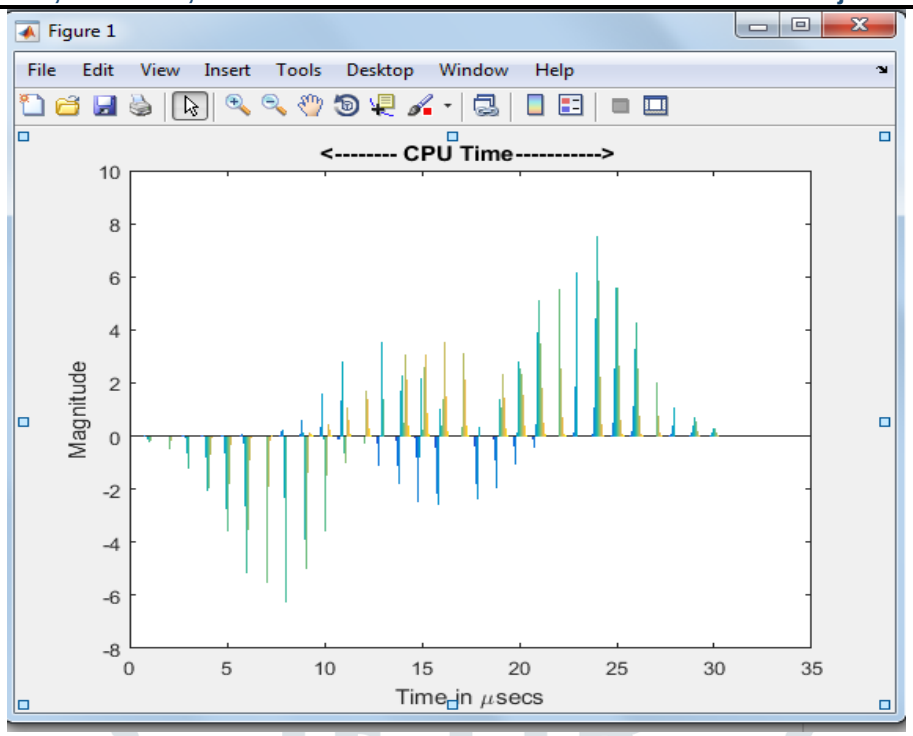


Fig.5.2.2(b) CPU time for traditional RSA algorithm & Variant RSA

**5.2.3 Cost** :- Creating VPN tunnels for communication over remote office is much cheaper than using leased lines.

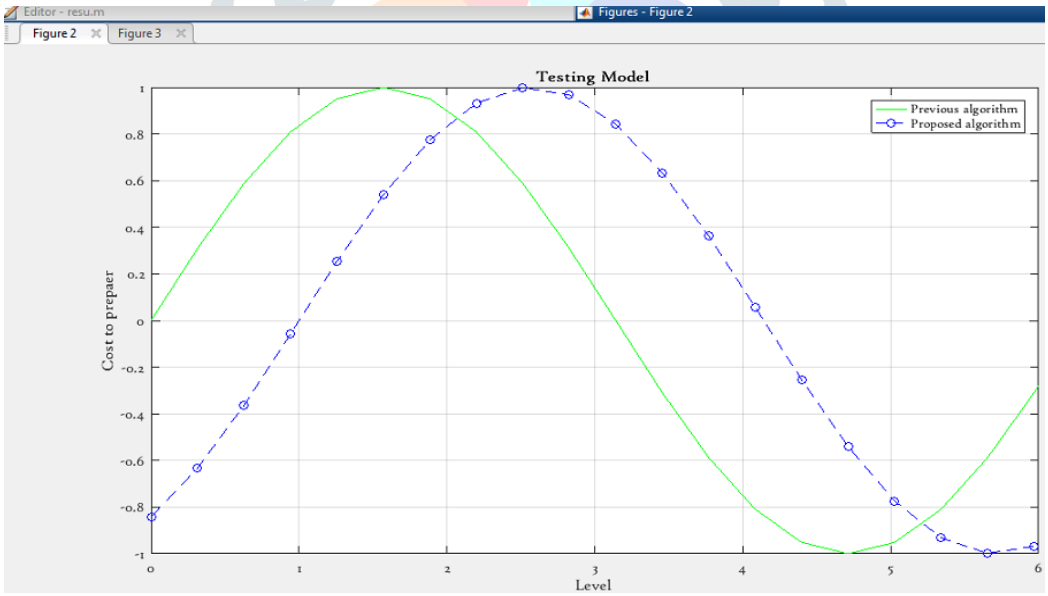


Fig:5.2.3(a) Cost comparison of proposed algorithm

### 5.2.4 Highly Secure /Confidentiality:-

Hacking Proposed algorithm is not possible because it is used with large numbers. The reasons which specify why it is difficult to hack proposed algorithm are as follows −

- Brute force attack would not work as there are too many possible keys to work through. Also, this consumes a lot of time.

- Dictionary attack will not work in this algorithm as the **keys** are numeric and does not include any characters in it.
- Frequency analysis of the characters is very difficult to follow as a single encrypted block represents various characters.
- There are no specific mathematical tricks to hack it.

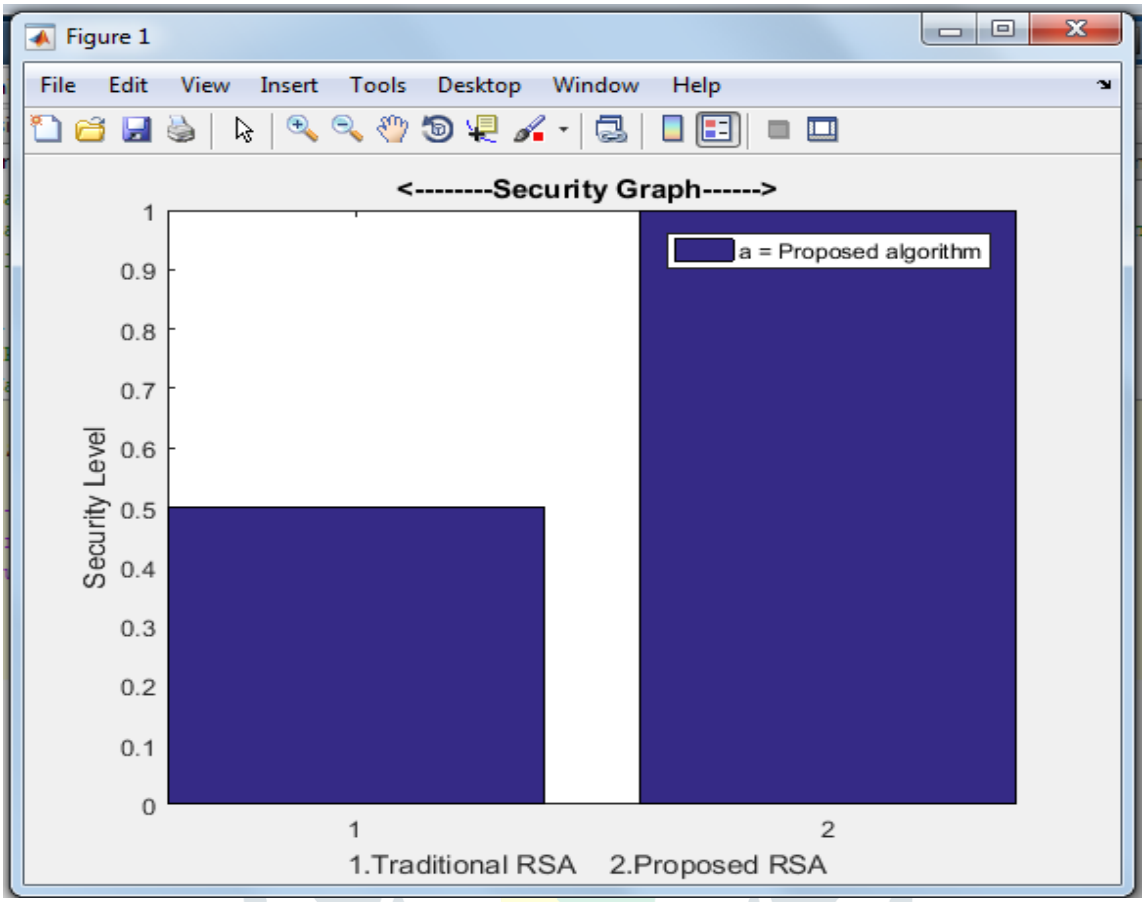


Fig5.2. Security level graph by proposed algorithm

### 5.2.5 Results comparison :-

| S.no | Parameter | Security Algorithm | Proposed algorithm(Variant RSA) |
|---|---|---|---|
| 1 | Secure Key generation | Moderate level | High level |
| 2 | Execution Time(ms) | High | Less |
| 3 | Cost | 0.5613 | 0.3590 |
| 4 | Highly Secure /Confidentiality | Less/ Moderate | High |
| 5. | CPU time | 0.5 | 1.0 |

Table 5.1 Result comparison

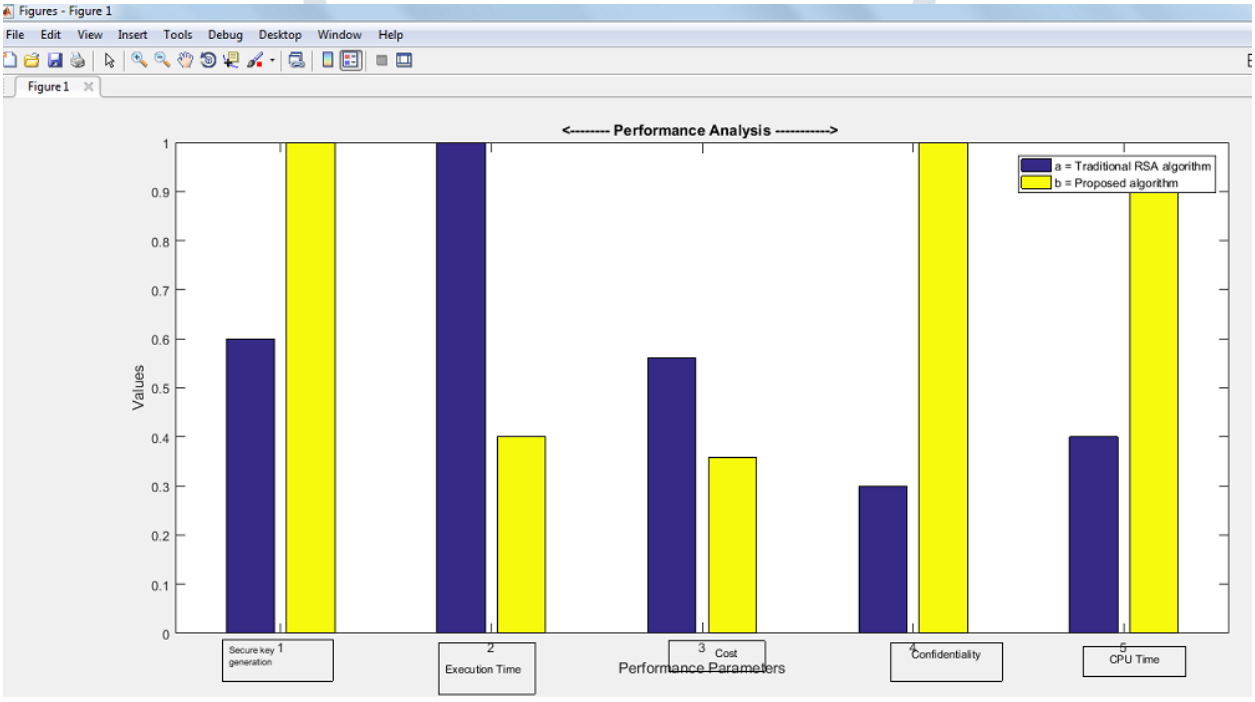


Fig:5.6 A performance analysis of proposed algorithm

## VI. CONCLUSION

Cryptography assumes indispensable job in unstable development of computerized information stockpiling and correspondence. In this paper, it has been studied that the current takes a shot at the RSA encryption strategies. Those encryption procedures are examined and dissected well to advance the presentation of the encryption strategies likewise to guarantee the security procedures. The different cryptanalysis assaults including inactive and dynamic assault can break the cryptosystem. The aggressor can utilized modulus administrator to break the RSA calculation.

The primary motivation behind this paper is to spread the fundamental information about the RSA based calculations and examination of accessible RSA put together encryption systems based with respect to certain parameters like weakness to assault, Uniqueness about the method, and so forth and here we have seen that RSA is progressively secure and it might be increasingly more grounded by applying a few procedures. Here

we have seen that all creators are discussing numerous strategy yet nobody is discussing picture pixel for security reason. So we can add picture pixel system to make all the more dominant RSA calculation.

An encryption is used to confirm customer traffic and information, essentially mentioning it objective fact confirmation to shield it from ISP checking, cybercriminals, and government observation. In this proposal we planned another calculation for improvement of security issues for better outcome and remote correspondence and producing a testing model on MATLAB R2016a. This dissertation defines the presentation and the use of cryptography.

For giving a security to remote framework we made another calculation Variant RSA algorithm which gives moderately better outcome as contrast with past calculations. In future work we improve this calculation with elliptic bend cryptosystem working guideline.

**REFERENCES**

1] Kun Ma, Han Liang, and Kaijie Wu, Member, IEEE, "Homomorphism Property-Based Concurrent Error Detection of RSA: A Countermeasure to Fault Attack", IEEE TRANSACTIONS ON COMPUTERS, VOL. 61, NO. 7, JULY 2012

[2] Alexandra Boldyreva, Hideki Imai, Life Fellow, IEEE, and Kazukuni Kobara, "How to Strengthen the Security of RSA-OAEP", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 56, NO. 11, NOVEMBER 2010

[3] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sang-Jae Moon," RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis"IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 4, APRIL 2003

[4] Prashant Sharma, "Modified Integer Factorization Algorithm using V-Factor Method", 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE 2012.

[5] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. Of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[6] Wireless LAN Medium Access Control(MAC)and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

[7] M. Wegmuller, j. P. Von der weid, p. Oberson, and n. Gisin, "high resolution fibber distributed measurements with coherent ofdr," in proc. Ecoc'00, 2000, paper 11.3.4, p. 109.

[8] R. E. Sorace, v. S. Reinhardt, and s. A. Vaughn, "high- speed digital-to-rf converter," u.s. patent 5 668 842, sept. 16, 1997. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[9]M. Shell. (2002) ieeetran homepage on CTAN. [Online]. Available:http://www.ctan.org/tex archive/macros/latex/contrib/supported/ieeetran/

[10] Karnik, "performance of tcp congestion control with rate feedback: tcp/abr and rate adaptive tcp/ip," m. Eng. Thesis, indian institute of science, bangalore, india, jan. 1999.

[11] J. Padhye, v. Firoiu, and d. Towsley, "a stochastic model of tcp reno congestion avoidance and control," univ. Of Massachusetts, Amherst, ma, cmpsci tech. Rep. 99-02, 1999. [15]Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

[12] Hamed Arshad, Vahid Teymoori,· Morteza Nikooghadam , Hassan Abbassi," On the Security of a Two-Factor Authentication and Key Agreement Scheme for Telecare Medicine Information Systems", Springer Science Business Media New York 2015, 31 January 2015 , 2 June 2015 / Published online: 18 June 2015

[13] Dheerendra Mishra," A Study On ID-based Authentication Schemes for Telecare Medical Information System", arXiv:1311.0151v3 [cs.CR] 4 Feb 2014.

[14]Ruhul Amin,1 SK Hafizul Islam,2 Muhammad Khurram Khan,3 Arijit Karati,4 Debasis Giri,5 and Saru Kumari," A Two-Factor RSA-Based Robust Authentication System for Multiserver Environments", Hindawi Security and Communication Networks Volume 2017, Article ID 5989151, 15 pages https://doi.org/10.1155/2017/5989151

[15] M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya, " Enhanced and Secured RSA Key Generation Scheme Information Technology, Anna University.

[16] Ms. Ritu Patidar, Mrs. Rupali Bhartiya, 2013, "Modified RSA Cryptosystem Based on Offline Storage and Prime Number", IEEE.

[17] Dr. D.I. George Amalarethinam, J.Sai Geetha, " level for Public Key Cryptosystem using MRGA Computing and Communication Technologies, 978 2014, IEEE.

[18] Dr. Abdulameer K. Hussain, "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K Neighbor Algorithm", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2, Issue 1, ISSN 2348 January 2015.

[19]Amare Anagaw Ayele, Dr. Vuda Sreenivasarao, "A Modified RSA Encryption Technique Based on Multiple public keys", Journal of Innovative Research in Computer and Communication Engineering,Vol. 1, Issue 4, ISSN 2320-9798, June 2013.

[20] Xianmeng Meng, Xuexin Zheng, "Cryptanalysis of RSA with a small parameter revisited", Information Processing Letters 115 Elsevier.

[21] Ritu Tripathi, Sanjay Agrawal, "Critical Analysis of RSA Public Key Cryptosystem", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, ISSN 2277 July 2014.

[22] Sangita A. Jaju, Santosh S. Chowhan, "A Modified RSA Algorithm to Enhance Security for Digital Signature", 978 IEEE.

[23] Aayush Chhabra, Srushti Mathur, "Modified RSA Algorithm Approach", International Conference on Computa Communication Systems, 978-0-7695-4587

[24] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj, "An Algorithm to Enhance Security in RSA", 4th ICCCNT, 2013, IEEE Technology" (IEEE-CICT 2017)

[25]W. Diffie, M.E. Hellman, "New directions in cryptography", *IEEE Transactions on InformationTheory*, vol. 22, pp. 644-654, 1976.

[26] Willam Stallings, "Cryptography and Network Security", 2012.

[27]R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", *Communications of the ACM*, vol. 21, pp. 120-126, 1978.

[28]RohitMinni, KaushalSultania, Saurabh Mishra, "An Algorithm to Enhance Security in RSA", *4th ICCCNT*, July 2013.

[29] Ovye Abari, P.B. John, "Shola Simon Philip Comparative Analysis Of Discrete Logarithm and Rsa Algorithm Data Cryptography", *(IJCSIS) International Journal of Computer Science and Information Security*, vol. 13, no. 2, 2015.

**[30]**P. Chitti Babu, K. Karpagavalli, V. Nirmala, *Dj Samatha Naidu Prevention Techniques for syllabic time-relay attacks during implementation using public key cryptographic algorithms IJESR*, vol. 05, february 2014.