ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

RSA ENCRYPTION ALGORITHM - A SURVEY ON ITS VARIOUS FORMS AND ITS SECURITY LEVEL

P.M. Durai Raj Vincent*
Associate Professor, School of Information Technology and Engineering, VIT University, Vellore, India,
Email:pmvincent@vit.ac.in

Received on 04-05-2016 *Accepted on 30-05-2016*

Abstract:

Security requirements will change time to time. It is always necessary to provide appropriate security services to any communication. Later 1970's many such mechanism has come. One among that is public key cryptography. The invention of RSA algorithm brings one of the significant improvements in the field of cryptography. Until that period, only symmetric key cryptography was in act which used only one key for both encryption and decryption. This makes that single key as the most sensitive one. Because of that key will be disclosed then entire communication will be compromised irrespective of the complexity of conversion applied over it. That is the reason why when this idea was proposed; it opened another window in the security providing arena. Hence the researchers have shown lot of interest in developing similar algorithms which gain some momentum over a period of time. At the same time this new approach has also started facing various hurdles in the name of various attacks. In that way this approach had a long history of over 40 years. During this period of time many modified approaches also were proposed by slightly modifying this one. On the other side some other approaches like elliptic curve cryptography also proposed based on the idea of public key cryptography. The purpose of this paper is to analyze the present scenario of RSA algorithm along with its past history in the modern cryptography era. Also this paper presents various related work done over a period of time related to this algorithm along with the summary of all the works.

Keywords: RSA, BMPRIME, EAMRSA, CRT

1. Introduction:

As in the abstract it has given that the invention of such public key approach as a significant moment for the entire field of cryptology. Since then the window was open for both symmetric key and asymmetric key cryptography. The main

reason for the idea to introduce two different keys to address the issue of growing sensitiveness over the component called key. Single key usage for both encryption and decryption has a very long history since Caesar's one. Modern block cipher played vital role in the late 1960's as it got wider acceptance by selecting IBM's lucifier cipher as a standard later. Simplified approach and faster execution with acceptable security levels made such ciphers more popular. But on the other side such cipher's security depends on the success of sharing the key also. A very effective key sharing approach was the requirement which determines the success of such algorithms. Because if the secret key is compromised then the whole security applied will be no use and one could be decrypting it.

This scenario turned few researchers includes Rivest, Shamir and Adleman to think beyond the current scenario which made to go beyond single key scenario. A two key structure is a phenomenal one that made possible because of mathematical brilliance. Bringing number theory concepts into cryptography achieved such a milestone in this field. A key used for encryption cannot used for decryption ensures even if one key is compromised, with that one cannot decrypt. By this way, this new idea has eliminated the sensitiveness over the component key. This is the reason why this approach has got immediate acceptance and wider exposure. Figure 1 shows the working procedure of the whole process.

As usual after every crypto algorithm, the cryptanalysts will start working on the vulnerabilities side. Their aim is to break the cipher to get back to the original plain text. Here even though the keys were inter related, it was very difficult to find the other key as the process involved in such a way at an initial point of time. Later these cryptanalysts found the way to break this process by the so called factoring attacks. Factoring attack will try to factorize the components 'p' and 'q' from the public key 'n'. Apparently from $\varphi(n)$ one can find the private key. That is the reason why this attack became possible up to some extent.

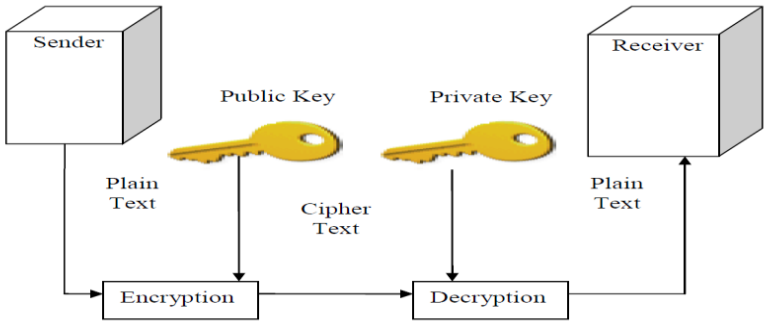

Fig 1: Asymmetric Cryptography

When the variety of factoring attacks was able to factorize the two components, the algorithm was responding to those attacks to some extent. Because of this the acceptable level of key sizes has risen to minimum of 1024 bits to counter the various factoring attacks existing.

Due to this increase in key sizes, the execution time of this algorithm becomes very high when compared to symmetric key algorithms. In order to utilize this idea some other similar cryptographic techniques were proposed like elliptic curve cryptography and elgamal crypto systems which were successful to some extent.

At the same time to make the given RSA cryptosystem a successful one, various modified versions of such system have come in the history to fight various issues it has faced in different period of time. One need to mention very particularly is the modified procedure for decryption using Chinese reminder theorem. This proposal was a successful one in reducing the execution time taken for decryption from the original version.

Similar like this various proposal were made to support the execution time issue or to counter the various attacks which was developed over a period of time. This paper is going to analyze both various versions of RSA algorithm as well it is going to discuss about the attacks which are tried to bring back the private key. This paper is organized as introduction, discussion about the survey followed by a summary and conclusion.

2. Literature Review:

This chapter is going to present some of the past work done in the field of public key cryptography with respect to RSA algorithm. This one includes the modifications done in the original methods along with about the attacks tried over it.

Hung-Min Sun et al. have proposed a modified approach based on the same same format of public key cryptography. The authors have used the same format followed in the original version. Process of providing authentication was achieved here through blind signatures. Security issue was addressed in this work by increasing complexity in the process but it reflects in the larger execution time.

Ravi Shankar Dhakar et al. made some modifications in the original steps. These corrections have begun from the very first step in the original process by having four different prime numbers in the place of only two. By this way both the public and private key had more components than the original. This approach straight away addressed the issue of factoring attacks but again failed to provide quicker execution time. Hung-Min Sun et al. have addressed the issue of execution time. These authors have tried a new approach like Chinese reminder theorem based decryption to have lesser

execution time. Even though these two types proposed are to address an important issue these two failed to do so the target.

Zulkarnain Md Ali et al. have taken both RSA algorithm and Elgamal crypto systems together to propose a new procedure as an alternative to RSA algorithm. This approach has increased the complexity over the process of providing security especially to counter factoring attacks. Instead of integer factorization discrete logarithm problem was chosen to counter the above said attacks. So this approach stands out as an alternate to the original algorithm to have a wider acceptance.

Aayush Chhabra et al. proposed another modified version of RSA algorithm which has gained some attention among the researchers. The procedure was modified in the key generation part. Thus this approach too tried to address the factoring attacks. Since some modifications brought the security enhancement from the original, this work also stands as the modified RSA algorithm but the novelty on addressing other issues was not considered in this approach.

Yunfei Li et al. proposed Encrypt Assistant Multi Prime RSA (EAMRSA) approach again based on the original algorithm. Unlike the previous approaches which were aimed to increase the security part, this one aimed at execution time. Since the execution time of original algorithm was a bottleneck in real time applications, reduction of execution time was very much required to use the algorithm for all the purposes. This reduction was applied to decryption procedure. The reduction was possible because of modules reduction and reduction of private exponents in modular exponentiation. Even this will be further reduced by parallel execution. Even multi core environment was considered and tested in this work and those results were also published in this work.

Krishnamurthy A. et al. proposed Multi-prime RSA, again this work too aimed at modifying the original algorithm to have wide spread usage. As the name suggested as multi prime RSA, the changes have brought to the key generation phase by bringing various prime numbers instead of only two prime numbers. This approach straight away addressed all kind of factoring attacks. Similar like traditional algorithm, multi-prime RSA required also used the squaring reduction and multiplication reduction of integers. Thangavel et.al proposed ESRKGS which stands for enhanced and secured key generation algorithm. The key generation part is enhanced in this proposed approach from the original algorithm. ‘n’,’m’,’g’ and ‘e’ are used as public keys and d, lamda and gamma are the private keys in this approach. Finally this approach also tried to prove that it will withstand to brute force attack better than other similar approaches.

Sattar Aboud et al. proposed the generalization of public key cryptography algorithm. In order to provide dynamic in nature and scalable to the demand, this proposed approach need to be generalized. In this proposed idea the authors had introduced a variable called 'g'. This new variable also will be involved in the existing procedure. The key used for decryption in the given range of phi(n) will be increased to g(n). The given new range is comparatively higher than the existing. h x h matrix was used for the calculation of the value g(n) in this approach. The only drawback in this approach is the longer execution time than the original one which is not an acceptable one.

Deepak Garg et al. proposed different type of RSA, This proposal came mainly because of the issue lies with the original RSA algorithm's execution time. This approach addressed such issue. This one combined both multi prime and rebalanced RSA approaches together. Chinese Reminder Theorem was also considered for this approach to have better results. In order to provide the better results this approach has adopted rebalanced approach's key generation procedure as well as the decryption part from multi RSA approach.

By combining these ideas together a better result was obtained. Sonal Sharma et al. proposed an idea for providing more security during the key generation process. $M > SUM_{i=1...n}(a_i)$, In this 'M' a new component was introduced along with earlier keys 'e' and 'd'. Another component 'W' was also introduced which is a multiplier and gcd of both the values was calculated. At last the values of 'B', 'n' and 'e' were considered as public key for the algorithm and the other components like 'A', 'M', 'W', 'n' and 'd' were all private keys. Along with the original steps here an additional step summation was introduced after which the other usual steps will be performed which is a difference in this approach. On the whole by introducing various other variables, this approach has considerably proved that a secured one than the other whereas the issue of longer execution time from the original approach was further extended here.

Subhamoy Maitra et al. proposed an approach to address the speed of execution. This proposed approach has adopted Chinese Reminder Theorem (CRT) in the decryption part. This approach has changed the larger modular arithmetic operations. RSA with CRT approach was different from the original RSA in key generation and decryption process. The value of private key 'd', the secret component cannot be left as a shorter one. If the private key value $d < N^{0.292}$, then it was vulnerable to factoring attack and the whole system could be totally broken. By doing these changes this algorithm's execution time will become three times faster than the original RSA algorithm. Hwang, R.J. et al. proposed an idea implement the algorithm in an efficient way to address the larger computational cost. So far due to larger

computational cost only smaller key sizes were considered during execution. Even though considering smaller public keys will result in higher values of decryption keys. Such scenario will make the decryption process to takes place in longer time duration. This work proposed an efficient decryption method not only based on Chinese Remainder Theorem (CRT) but also on the strong prime of RSA criterion. Final result shows that only 10% of the original time was taken in the newly proposed approach which brought the significant changes in the proposed idea.

Imad Khaled Saluh et al. demonstrated various attacks performed in RSA algorithm over a two decade of time period. These attacks are largely called as mathematical attacks. The various attacks includes integer factoring attacks, Hastad broadcasting attack, Franklin-Reiter related attack, Wiener's attack, Partial key exposure attack, Low public exponent attacks, chosen cipher attack, blinding attack, common modulus attack, Lenstra's attack, Davida's attack. These attacks were discussed in this paper with various limitations.

Sushma Pradhan et al. proposed BM-Prime method which was used to develop an efficient algorithm; the word BM came from Batch RSA and M-Prime RSA. In order to speed up the decryption process, this proposed approach tried to combine both of these approaches. This work also tried to show that the proposed one was less vulnerable to various attacks on RSA.

The results showed that the time taken for decryption process was lesser than the approach which used Chinese Reminder Theorem which one was traditional one. This proposed approach brought the significant advantage from the former approach.

3. Summary:

By summarizing the various works done relevant to RSA algorithm are given in the literature survey. The invention of public key cryptography was one of the very important innovation in the field of cryptography which faced two different issues in the later period. That is what all these related work says about. The two main issues addressed are the execution time and the factoring attacks. The success of RSA algorithm was mainly because of modular exponentiation and a very simple methodology to perform the steps. Later the same was attacked in the name of factoring attacks. Due to this the size of the keys were increased which created the longer execution time. These two are the main reasons for all the above proposals and ideas. Each idea was unique in terms of addressing the issues. But the two issues are equally important but opposite to each other. Because of this, each idea addressed one issue and complicated the other. Many of

such proposals were with the key generation part. In all these, by increasing the number of prime numbers used the factoring attacks were addressed but at the same time this caused the longer execution time by many times from the original.

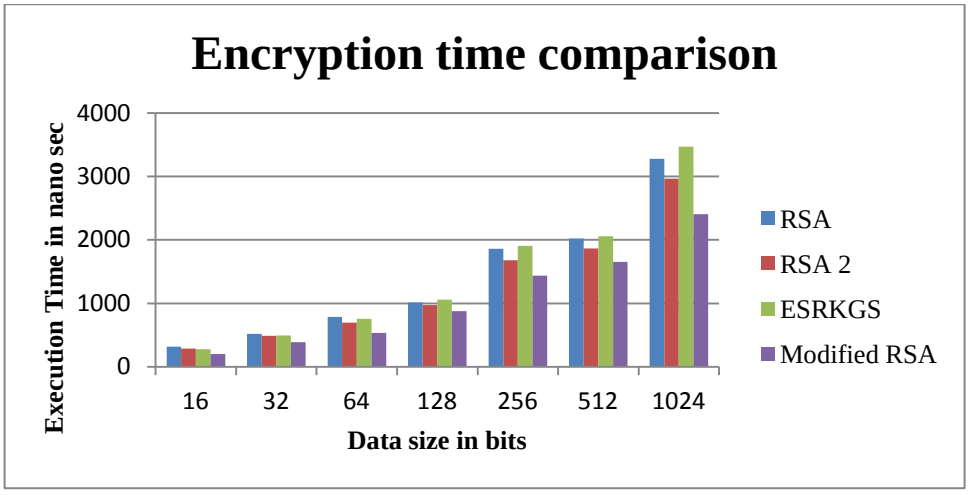

Fig 1: Execution time comparison between various algorithms

Figure 1 and 2 shows the encryption and decryption time for the various algorithms taken for the comparison. These two comparisons shows that the modified approach proposed [1] was taking lesser time when compared to other algorithms.

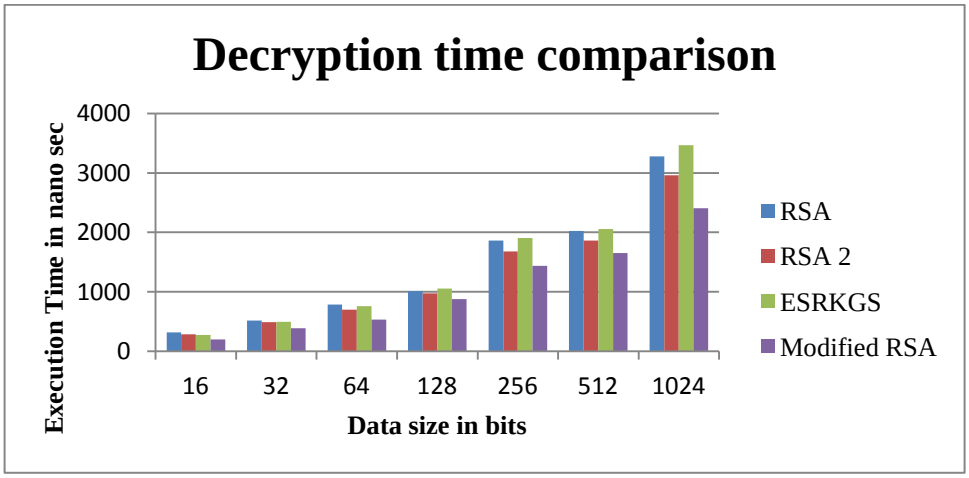

Fig 2: Decryption time comparison between various algorithms

Every attack has certain limitations, so reducing the key sizes will completely compromise the whole security providing scenario. That is the reason why several approaches have exclusively worked on reduction of execution time. The idea was started from introducing Chinese Remainder Theorem (CRT) based decryption which addressed the issue to a larger extent. Because in any scenario decryption time is the most time consuming when compared to encryption. Even it will take four to five time of encryption. That is the reason why that modified approach of decryption was accepted widely.

Following to that many similar approaches has come and tried to address the same issue. Among that most of the approaches have taken only the decryption part and also the Chinese reminder theorem approach also have considered. Other few approaches have concentrated on computational complexities and given solution for that to improve. When it comes to attacks, the most familiar attack is factoring attack. As it is an open challenge still only up to 786 bits are possible to attack and beyond that is not possible till date. Even though 1024 bits are safe from these attacks still it is suggested that to use 2048 bits for the assured security through this. Other important attack is wiener's attack which attacked the public key with continued fraction method.

This attack is successful if $d<1/3n^{1/4}$. Beyond that this attack will not work. So it is always safer to have higher 'd' value. Fermat factoring method is another approach which will attack the public key based on the representation of an odd integer as the difference of two squares. This attack will also successfully work for smaller values. Brute force is always a possible attack which will try all the possibilities. But in RSA it will not work at all as the key size is huge. Timing attacks and other possible attacks will work to the possible extent. So it is advisable to have 2048 bits as always a safer size to consider for any sensitive information to share.

Also brute force comparison was given[5] with the possibility of attacking the key with all the possibilities but the results shows that it is possible to crack the key up to key sizes lesser than 256 bits in a finite time which is not an issue unlike other algorithms. At present the usage of RSA algorithm in real time is very much minimal due to various issues discussed already. Even though the algorithm was designed for encrypting and decrypting plain text, now a days the algorithm is widely used for key sharing purpose.

The main reason for this is the keys are relatively small in size when compared to the size of the plain text. Also for almost all the real time applications only symmetric encryption algorithms are used for providing security. So it is very much necessary to share the secret key securely. For this purpose the RSA algorithm preferred over other algorithms available mainly because of its strong security providing nature.

On the whole the history of RSA had a very long travel at various levels when compared to any other encryption approaches used. This is mainly because of the wide acceptance initially due to its unique approach and later issues it faced one after another. Even though there were other few asymmetric algorithms came in the later period time had its own uniqueness in approaching the cipher were not able stand as like the RSA algorithm.

4. Conclusion:

In this paper one of the most important invention in the field of cryptography has taken and its historical existence was analyzed. The analysis was first considered the various works were proposed over the period of time. All such relevant and modified approaches were given in the literature survey part. Among that various attacks were also considered with its limitations. Later in the summary part the algorithm was analyzed in terms of its main issues as well its current acceptance level. In that mainly the issue with various possible attacks along with the issue of its longer execution time was discussed. If it closely viewed both are interrelated because the first issue caused the second one. By considering all these limitations, still the algorithm is in usage is the biggest achievement and credit must go to the people Rivest, Shamir and Adleman.

References

1. Vincent P.M.D.R, Sathiyamoorthy E, A Novel and efficient public key encryption system, *Int. J. Information and Communication Technology,* Vol. X, n. Y, Article in Press.
2. Deepak Garg, Seema Verma, "Improvement over public key cryptographic algorithm", *IEEE International Advance Computing Conference*, pp 734-739, 2009.
3. Verma S, Garg D "Improvement in rebalanced CRT RSA" International Arab Journal of Information Technology" Vol.12, No. 6, pp.524-532, 2015.
4. Zhang M, Wu C, Ye.G "A new RSA algorithm of data security by large numbers and binary stream processing methods", Journal of Information and Computational Science, Vol.12, No.14, pp.5411-5418, 2015.
5. Thangavel M, Varalakshmi P, Murali M, Nithya K, " An enhanced and secured RSA key generation scheme" Journal of Information security and Applications, Vol.20, pp.3-10, 2015.
6. Vincent P.M.D.R, Sathiyamoorthy E, "A Secured and Time Efficient Electronic Business Framework based on Public Key Cryptography", International Review on Computers and Software, Vol.9, No.10 pp.1791-1798, 2014.
7. Hwang, R.J., Su, F.F., Shiau, S.H, "An Efficient Decryption Method for RSA Cryptosystem, *International Conference on Advanced Information Networking and Applications,* pp. 585-590, 2009.
8. Imad Khaled Saluh, Abdullab Darwish, Saleh Oqeili, "Mathematical attacks on RSA cryptosystem", *Journal of computer science* Vol.2 No.8 pp.665-671, 2006.

9. Zulkarnain Md Ali1 And Jassim Mohammed Ahmed, "New Computation Technique for encryption and decryption based on RSA and elgamal cryptosystems", *Journal of Theoretical and Applied Information Technology,* Vol 47 No 1 pp.73-79, 2013.
10. Issad.M, Boudraa B, Anane.M, Anane.N, "Software/hardware co design of modular exponentiation for efficient RSA cryptosystem", *Journal of Circuits, systems and computers*, Vol 23 No 3, pp. 1450032, 2014.
11. Kaduskar R.G, "A new architecture for RSA algorithm using vedic mathematics", 4th *International Conference on Emerging Trends in Engineering and Technology,* pp.233-237, 2011.
12. Krishnamurthy, A., Tang, Y., Xu, C., "An efficient implementation of multi-prime RSA on DSP processor", *IEEE International Conference on Acoustics, Speech and signal processing*, pp. 413- 416, 2003.
13. Lein Harn, Chin-Chen Chang, and Hsiao-Ling Wu, "An Anonymous Multi-Receiver Encryption based on RSA", Vol 15 No 4 pp 311-316, 2013.
14. Nagar, S.A., Alshamma, S, "High speed implementation of RSA algorithm with modified keys exchange", Sciences of Electronics,Technologies of Information and Telecommunications, pp.639-642, 2012.
15. P.Kalyani, C.Chellappan, "Enhanced RSA-CRT for energy efficient authentication to wireless sensor Network security", *American Journal of Applied sciences*, Vol 9 No 10 pp 1660-1667, 2012.
16. R.Bhaskar, Ganapthi Hedge, P.R.Vaya, "An efficient hardware model for RSA encryption system using vedic mathematics", *Elsevier* pp 124-128, 2012.
17. Ravi Shankar Dhakar , Amit Kumar Gupta and Prashant Sharma, "Modified RSA Encryption Algorithm", *Second International Conference on Advanced Computing & Communication* pp.426-429, 2012.
18. Sachin Upadhyay, "Attack on RSA Cryptosystem" *International Journal of scientific & Engineering Research* Vol 2 No 9 pp.1-4, 2011.
19. Sattar Aboud, Mohammad A AL-Fayoumi, Mustafa Al-Fayoumi, Haridar S Jabbar, "An efficient RSA public key encryption scheme" *IEEE conference on information technology:New generations* pp 127-130, 2008.
20. Subhamoy Maitra, Santanu Sarkar, "Efficient CRT-RSA Decryption for Small Encryption Exponents", *springer* Lecture Notes in Computer Science Volume 5985, pp 26-40, 2010.

21. Sushma Pradhan, Birendra Kumar Sharma, "An efficient RSA cryptosystem with BM-PRIME method", *International journal of Information & Network security* Vol 2 No 1 pp.103-108, 2013.
22. Valstar, E. R., Vrooman, H. A., Toksvig-Larsen, S., Ryd, L., & Nelissen, R. G. H. H., "Digital automated RSA compared to manually operated RSA", *Journal of Biomechanics*, Vol *33 No* 12, 1593-1599, 2000.
23. X.D. Yu, M.Y. Zhang, M.Q. Zhu, K.H. Xu and Q.C. Xiang, "Improved RSA Algorithm in Hardware Encryption", Applied Mechanics and Materials, Volumes 543, pp.3610-3613, 2014.
24. Xin Zhou, Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption", *IEEE International forum on strategic technology*, pp.1118-1121, 2011.
25. Yunfei Li, Qing Liu, Tong Li, "Design and Implementation of an improved RSA Algorithm" *International Conference on E-health Networking, Digital Ecosystems and Technologies*, pp.390-393, 2010.
26. Aayush Chhabra and Srushti Mathur, "Modified RSA algorithm a secure approach", *International Conference on Computational Intelligence and Communication Systems*, pp. 58-63, 2011.
27. Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, Jason Hinek, "Dual RSA and Its Security Analysis", *IEEE Transactions on Information Theory* Vol 53 No 8 pp.2922-2933, 2007.
28. G.A.V.Rama Chanra Rao, P.V.Lakshmi, N.Ravi Shankar, "A Novel Modular Multiplication Algorithm and its Application to RSA Decryption", *International journal of Computer Science Issues* Vol.9 No.6 pp.303-309, 2012.
29. Hongbo Zhou, Matt W.Mutak, Lionel M.Ni, "Secure Autoconfiguration and Public-key Distribution for Mobile Ad-hoc Networks", *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, pp. 256-263, 2009.
30. Hung-Min Sun, Mu-En Wub, M. Jason Hinek , Cheng-Ta Yang, Vincent S. Tseng, " Trading decryption for speeding encryption in Rebalanced-RSA", *The Journal of Systems and Software* pp.1503–1512, 2009.

Corresponding Author:
P.M. Durai Raj Vincent,
Email: *pmvincent@vit.ac.in*