International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 711-715 Jan 2019-June 2019 www.csjournals.com

A Review of RSA and XOR Base Encryption Mechanism to Secure the Cloud

[1]Sandeep Singh, [2]Dr Vishal Verma
[1]Research Scholar, [2]Asst. Professor
Deptt. Of computer science and application, chaudhary ranbir singh university, Jind, Haryana, India

Abstract: In this paper, a review of RSA and XOR based encryption and decryption has been proposed. RSA has been considered an algorithm applied by modern computers in order to encrypt along with decrypt the information. The RSA algorithm includes the four phase. These are key generation, key distribution, encryption and decryption. Here the brief discussion has been made of traditional security technique along with their working and limitations. The existing research has discussed almost field related to the encryption and decryption mechanism using RSA and XOR. The research work would be beneficial to secure data from RSA attack as the probability of Brute force attack is more in case of tradition RSA. It would also be beneficial to save data from Timing attack as the probability of timing attack is more in case of previous RSA. As packet increases, the probability of timing attack also increases. Threat of attack on data using timing attack in proposed technique would be negligible as compare to traditional when then number of packet increases.
Keywords: RSA, XOR encryption, decryption.

[1] INTRODUCTION

RSA has been considered an algorithm applied by modern computers in order to encrypt along with decrypt the information. This algorithm is an asymmetric cryptographic algorithm. By the word Asymmetric, means to say that there exists two separate keys. It has been also described as public key cryptography. Its cause is that any person may be get one of the keys. The RSA algorithm includes the four phase. These are key generation, key distribution, encryption and decryption. RSA is considered as an algorithm that has been used in modern computers in order to perform encryption. It also performs decryption of the information. Such mechanism has been count as asymmetric cryptographic algorithm. Asymmetric means that there are two keys. It has been also described as public key cryptography. Its cause is that intruder could get one of the keys. The RSA algorithm includes the four phase. The first is key generation. The second is key distribution. The third is encryption data and the forth is the decryption of data. The user of RSA creates a public key. Then he publishes the public key, with an auxiliary value. The public key is dependent on two huge prime numbers. Here it is vital to provide the security to these prime numbers. Anybody can apply the public key to do the encryption of data. On the other hand with today's methods the public key is sufficient. Only the person knows the prime numbers is capable to do the decoding of data feasibly. To broke down the RSA encryption has been referred as the RSA issue. .

FLOW CHART FOR RSA ENCRYPTION

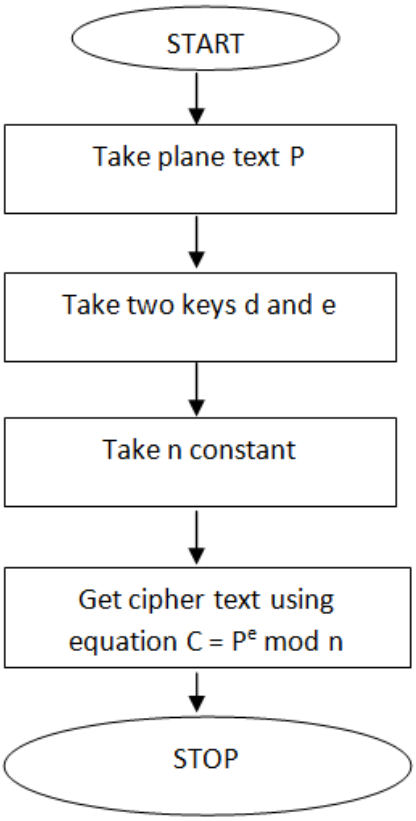

Fig 1 RSA Encryption Flow Chart

[2]XOR TECHNIQUE

The proposed technique is more secure and more efficient as compare to traditional security technique. Design of Integrating to enhance the security of Steganography technique has resolved the issues with traditional researches. Design secure encoding and decoding mechanism to enhance the protection of system would allow user to transfer data over network without delay and loss of data. Cryptography is consisting creation of codes. Such type of programs is providing security to information. It is transforming data where information is in cipher form. Cryptography makes data transfer lacking of entities that are not authorized. It decrypts information back into plain text. Data security is applicable on cryptography at various levels. Information cannot be understood without decryption. Information is retaining its integrity at time of transmission. It performs same at the time of its storage. Cryptography is not performing denial. It is confirming sender and make the delivery of data. Use of XOR operator has been proven capable to boost network protection. XOR key has been found capable to encrypt information efficiently than traditional algorithm. Encryption and decryption process are dependent to XOR key.

Working

[3] LITERATUERE REVIEW

Here the brief discussion has been made of traditional security technique along with their working and limitations.

In 2003, **Erin Michaud et. al. [1]** proposed a system that was to study and did analysis of many freeware appliances. These appliances use some usual technique to hide the data in the form of digital files. They have found the pattern by which anyone can normally embed the sensitive data. This data is related to normally exchange graphic, audio as well as text file formats. There are many overviews of several techniques of Steganography for every kind of file. This synopsis had been followed by evaluation of appliance.

In 2004, **A. Perrig, J. Stankovic et. al[2]** describe on security in wireless sensor networks. They have considered threat to security of wireless sensor network. They also discussed the limitation of existing mechanism with proposed security mechanism.

In 2004 **H. Anderson. et. al [3]** found her views on Introduction to Computer Security. They have considered general security need in case of computer. They explained the threats to computer security and present security mechanism.

In 2004, **Kristin Lauter, et. al " [4]** proposed explained elliptic curve cryptography advantages. These are used for wireless security. This system is more secure as compare to proposed work. The use of elliptic curve has made the system more secure which was less efficient in case of traditional mechanism.

In 2005, **Z.Z Kermani et. al [5]** explained a robust steganography algorithm. This algorithm is based on texture correspondence. This algorithm is found more robust and secure as compare to previous techniques. Here the concept of texture similarity has been as research methodology.

In 2005, **A.I. Hashad, et. al. [6]** proposed a robust steganography technique. For this purpose the discrete cosine transform insertion. The use of discrete cosine transformation has introduced the twist in security. This approach has made steganography robust as compare to traditional techniques.

In 2006, **X. Zhang et. al, [7]** focus on efficient steganographic embedding by exploiting. They have considered threat to security in network. They explained the limitation of existing mechanism with proposed security mechanism.

In 2007, **A. Savoldi, et. al, [8]** describe the Data secrete in SIM/USIM cards. They explained a steganographic review. This research is an attempt to provide security of SIM/USIM cards.

In 2008, **Vivek Kapoor,et al. [9]** focus on Elliptic curve cryptography. This system has been found more secure than proposed work. The utilization of elliptic curve has made the system more secure which was less efficient in case of previous cryptography mechanism.

In 2008, **F. Amin, A. H. jahangir et. al [10]** proposed analysis the public key cryptography . These key has been used in wireless sensor networks security. They have considered threat to security of wireless sensor network. They also discussed use of public key cryptography along with limitation of previous security mechanism.

In 2009, **Dipti Kapoor Sarmahet. al. [11]** describes represented System for data hiding using Cryptography & Steganography. They had proposed a new system. This system is applicable to combine the cryptography and Steganography. It has been for these purpose four keys are used. It would be extremely protected technique used in data transmission in future. Their system had required quality of graphic. These systems are with little alteration in graphic.

In 2009, **Dragoş Dumitrescu et.al. [12]** System described that purpose of work was to perform an analysis over most widely-used image Steganography mechanism were focusing on different categories that comprise this discipline. Findings represented that one may observe that all Steganography mechanism described throughout that research were shown to be broken under some type of statistic or artificial intelligence-based tests.

In 2010, **George Abboud et. al. [13]** proposed system and stated that Steganography & Visual Cryptography in Computer Forensics in which description of Steganography. Visual cryptography had been described with several review executed on several algorithms of each kind. Separate algorithms for Steganography as well as visual cryptography include several merit and energy, along with demerit and limitation.

In 2011,**Masoud Nosrati et.al. [14]** Introduced that Steganography methods were going to express several kind of Steganography having cover data. As first phase, they would talk about text Steganography and examine the decription of it. At last, audio Steganography has LSB Coding, Phase Coding. It also has Spread Spectrum and Echo Hiding mechanism that were described.

In 2012,**Pranab Garg et.al. [15]** Proposed system on Cryptography & Significance of Key Length stated that Cryptography has been emerged is an as vital method to transfer the data. Several algorithms of cryptography have been reviewed here. In the case if the benefits related to these algorithms are attached to one algorithm, then there would be increment in efficiency within key length.

In 2012, **Pria Bharti, et.al[16]** Proposed a concept of Data Hiding in Images. They have used the Cryptography & Steganography. They have showed that Cryptography is the method to use mathematics. It has been done to do the encryption and decryption data. Along with this the Steganography has been determined as an art and science which is used to hide the transmission the Results has defined that a novel scheme for embedding data in graphics was Cryp Steg. By the way the attached use of cryptography and Steganography procedure is used in one algorithm. First of all they did the encryption of data and then embedded within graphic. It has been done within new algorithm of Steganography.

In 2015, **Pradnya S. Nagdive et. al.** Proposed work of Visual Cryptography & steganography states that privacy & consideration of graphic are a spirited space of evaluation. For these two totally separate concepts, the graphics are encrypted by applying encoding algorithms with the use of keys. Overall the result has indicated that the second concept includes the secret data. This concept is useful with data hiding algorithms. It has been done to maintain the secrecy of graphic.

In 2015, **S.M. Poonkuzhali1, et. al.** describe research on data hiding . For this purpose they have visual cryptography to secure the dealing. The data hiding methods have applied by them. They have used several frames are there which are used to secure the data transmission of data over network. In conclusion the hacker that wants to hack was efficient to watch the secret graphic.

In 2015, **Archana.O.Vyas , et al.** described Overview of Image Steganographic mechanism. They also did evaluation of some of most established algorithms. These algorithms are used in graphic Steganography in different embedding domains. These domains have dependency on security degree, capacity as well as factors. They also have been pointed out the future usefulness related to the research. The area of the research is graphic Steganography.

In 2015,**Priyanka B. Kutade, et al.** Proposed Survey on Various Approaches of Image Steganography interpreted that Steganography has been determined as an art of concealing the fact. It has been done to fulfill the purpose of dealing. The Steganography is capable to hide the sensitive data from other data. The evaluation results have indicated that every technique carries the benefits along with limitation.

In 2016, **Priyanka Mor, et al.** Describe the paper method of Online Payment System. For this purpose they have used Steganography and Visual Cryptography. They has applied text dependent Steganography with visual cryptography were discussed. The finding represented innovative view that gave restricted data for fund sending. That technique secured user data and enhancing user's self-confidence and remove recognized robbery.

In 2016, **K.S. Seethalakshmi, et al.** proposed algorithm which Use of Visual Cryptography & Neural Networks to Enhance Security in Image Steganography provides high protection and graphic quality. Visual Cryptography ensured secure transmission of image over internet. Future scope was added private or public key for encryption increase number of shares in visual cryptography to compare improvement in quality.

In 2016, **A. Joseph Amalraj1 et al.** proposed survey paper that was a complete review of Cryptography techniques. Using these algorithms and perception the protection of data has been considered very vital. The reason is that the process of selling and purchasing of goods by the open network is made regularly. By this review the researchers have reviewed the traditional works on encryption technique. At last they evaluated the efficiency of selected symmetric algorithms.

In 2017, **Priyanka Bubna,et al.** Proposed paper a Review on Implementation Visual Cryptography & Steganography for Secure Authentication was presented. The present chapters describe existing research in field of Steganography Tools and Methods. After taking the review of these existing researches, it has been come to know that beside of the advantages, these reviews have their loop holes also. But it provides a base for an innovative research.

[4]PROBLEM STATEMENT

The tradition algorithms have certain limitations. Use of traditional encryption and decryption security technique has slow down the performance of network. Research by Erin Current on Steganography Tools & Methods has discussed steganography [2] tools that are hiding information but these tools make the poor performance during data transmission. Researches of Dipti Kapoor also have same limitation. Research by Dragoş, George, and Masoud has provided the security to network using steganography technique but they ignored the IP level security. However this mechanism would hide the data. These mechanisms are not going to prevent attacker from destroying data. Some of the researches are using Image[7] Steganographic technique that takes long time to encrypt data.

[5] PROBLEM FORMULATION

However the protection to data has been provided using traditional technique but they have certain limitation. If attacker is not able to understand the information he

could destroy the information. If security technique is integrated the performance of system slows down. Tradition systems are either securing network connection only or network data only. In proposed technique the objective is to provide security to data as well as security to network connection. Moreover, there is also focus on performance of system along with security.

[6] CONCLUSION

The proposed technique is more secure in all sense as it is immune to brute force attack as well as timing attack. The XOR based security has been improved the performance of encryption and decryption. Additional security technique such as IP verification restricts the attacks from hacker end. In this research real image is loaded for encryption. The key image is then loaded to perform XOR operation From above results in case of timing attack comparison of traditional and proposed work, it is clear that the strength of proposed work as compare to traditional RSA work. From the above analysis it has been clear that the probability of Timing attack is more in case of tradition RSA. As the number of packet increase, the probability of timing attack enlarges. Chances of unauthentic data access from Timing attack in proposed technique is less in proportion to traditional when then packet got increased.

[7] FUTURE SCOPE

The project scope is that it would limit the unauthorized execution. It would offer the better protection at the time of data transmission. The research work would be beneficial to secure data from RSA attack as the probability of Brute force attack is more in case of tradition RSA. It would also be beneficial to save data from Timing attack as the probability of timing attack is more in case of previous RSA. As packet increases, the probability of timing attack also increases. Threat of attack on data using timing attack in proposed technique would be negligible as compare to traditional when then number of packet increases.

REFERENCE

[1]. Erin Michaud(2003) "Current Steganography Tools and Methods", SANS Institute 2003, As part of GIAC practical repository, GSEC Practical, Version 1.4b April, 2003

[2] A. Perrig, J. Stankovic, and D. Wagner,"Security In Wireless Sensor Networks,"ACM,Vol. 47, No.653.2004.

[3] H. Anderson. Introduction to Computer Security, Prentice Hall, 2004,pp: 85-86

[4] Kristin Lauter,"The Advantages of Elliptic Curve Cryptography for Wireless security", IEEE Wireless Communication, Feb 2004.

[5] Z.Z Kermani and M. Jamzad. "A robust steganography algorithm based on texture similarity using Gabor filter." in Proc. of IEEE 5th International Symposium on Signal Processing and Information Technology ISSPIT, 2005. pp. 578-582.

[6] A.I. Hashad, A.S. Madani and A.E.M.A. W ahdan. "A robust steganography technique using Discrete Cosine Transform insertion." In Proc. of IEEE/ITI 3rd International Conference on Information and Communications Technology, 2005. pp. 255-264.

[7] X. Zhang, and S. Wang,"Efficient steganographic embedding by exploiting modification direction, "Communications (Volume:10 , Issue: 11) November 2006,page(s):781-783.

[8] A. Savoldi, and P. Gubian,"Data hiding in SIM/USIM cards: A steganographic approach,"Systematic approaches to digital forensic engineering, 2007. SADFE 2007. second international workshop on 10-12 April 2007,page(s):86-100.

[9]Vivek Kapoor et al., "Elliptic Curve Cryptography," ACM Ubiquity, Volume 9,Issue 20,(20-26)-may-2008.

[10].F. Amin, A. H. Jahangir and H. Rasifard,"Analysis Of Publickey Cryptography For Wireless Sensor Networks Security,"In Proceedings of World Academy of Science, Engineering and Technology, ISSN 1 307-6884,2008

[11] Dipti Kapoor Sarmah1, Neha Bajpai (2009) "Proposed System for data hiding using Cryptography and Steganography",

[12] Dragoş Dumitrescu1, Ioan-Mihail Stan1, Emil Simion (2009) "Steganography mechanism",

[13] George Abboud (2010) "Steganography & Visual Cryptography in Computer Forensics " 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering

[14] Masoud Nosrati, Ronak Karimi (2011) "An introduction to Steganography methods", World Applied Programming, Vol (1), No (3), August 2011. 191-195

[15] Pranab Garg, Jaswinder Singh Dilawari (2012) "A Review Paper on Cryptography and Significance of Key Length", International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012

[16] Pria Bharti, Roopali Soni (2012) "New Approach of information Hiding in graph with the use of Cryptography and Steganography ", IJCA. Volume 58– No.18, November 2012

[17] Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay (2013) "Review and Analysis of Cryptography mechanism", International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013

[18] C.P.Sumathi, T.Santanam and G.Umamaheswari (2013) "A Study of Various Steganographic mechanism using for data Hiding", IJCSE Vol.4, No.6, Dec. 2013

[19] Rakhi1, Suresh Gawande (2013) "A Review on Steganography Methods", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 10, October 2013

[20]Anjula Gupta Navpreet Kaur Walia (2014) " Cryptography Algorithms: A Review", 2014 IJEDR | Volume 2, Issue 2 |

[21] Vikas Yadav Vaishali Ingale Ashwini Sapkal and Geeta Patil (2014) "Cryptographic Steganography ", Computer Science & Information Technology
[22] Mr. Falesh M. Shelke1, Miss. Ashwini A. Dongre (2014) "Comparison of different mechanism for Steganography in images", International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 2, February 2014
[23] Anjali Tiwari, Seema Rani Yadav, N.K. Mittal(2014) "A Review on Different Image Steganography mechanism", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 7, January 2014
[24] Souvik Roy and P. Venkateswaran (2014) "Online Payment System with the use Steganography and Visual Cryptography", 2014 IEEE.
[25] Sana Shiva, A.Hari Teja (2015) Secure E-marketing Using Steganography & Emergence of Cryptography Journal of Computer Science & Information Technology IJCSMC, Vol. 4, Issue. 1, January 2015, pg.532 – 538
[26] S. R. Navale1 , S. S. Khandagale, R. A. Malpekar3, Prof. N. K. Chouhan4 (2015) Approach for Secure Online transaction using Visual Cryptography & Text Steganography International Journal of Engineering Research & Technology (IJERT) Vol. 4 Issue 03, March-2015
[27] Pradnya S. Nagdive (2015) Visual Cryptography & Steganography : A Review International Journal of Advance Research in Computer Science & Management Studies Volume 3, Issue 1, January 2015
[28] S.M.Poonkuzhali1 , M.Therasa (2015) "Data Hiding Using Visual Cryptography for Secure Transmission", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 4, April 2015
[29] Archana.O.Vyas, Sanjay.V. Dudul (2015) "An Overview of Image Steganographic mechanism", International Journal of Advanced Research in Computer Science, Volume 6, No. 5, May - June 2015
[30] Priyanka More, Pooja Tiwari, Leena Waingankar, Vivek Kumar,A. M. Bagul (2016) Online Payment System using Steganography & Visual Cryptography, International Journal of Computer Engineering In Research Trends, Volume 3, Issue 4, April-2016, pp. 157-161
[31] K.S.Seethalakshmi (2016) "Use of Visual Cryptography and Neural Networks to Enhance Security in Image Steganography ", IOSR Journal of Computer Engineering Special Issue - AETM'16
[32] A. Joseph Amalraj1, Dr. J. John Raybin Jose (2016) "A Survey Paper on Cryptography mechanism", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, August- 2016, pg. 55-59
[33] Priyanka Bubna, Anshula Panchabudhe, Pallavi Choudhari (2017) "Review on Implementation Visual Cryptography & Steganography for Secure Authentication", International Research Journal of Engineering and Technology Volume: 04 Issue: 02 | Feb -2017
[34] Priyanka B. Kutade, Parul S. Arora Bhalotra (2015) "A Survey on Various Approaches of Image Steganography ", International Journal of Computer Applications Volume 109 – No. 3, January 2015
[35] Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceeding of IEEE Students' Conference on Electrical, Electronics and Computer Science , Jadavpur University, Kolkata-700032, India, 2014.
[36] Thiyagarajan, P. Venkatesan, V.P. Aghila, G. "Anti-Phishing Technique using Automated Challenge Response Method", in Proceedings of IEEE, 2010.
[37] N. Chou, R. Ledesma, Y. Teraguchi, and D. Boneh, ‚Client-side defense against web-based identity theft,' in Proc. 11th Annu. Netw. Distribut. Syst. Secure. Symp, San Diego, CA, Feb. 2005.
[38] Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3,n 4, October/December 2006.
[39] Odai M. Al-Shatanawi and Nameer N. El. Emam (2015) "A new image Steganography algorithm dependent On mlsb method with random pixels Selection", IJNSA, Vol.7, No.2, March 2015.