GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

DATA ENCYPTION AND DATA DECRYPTION BY AN IMPROVED RSA ALGORITHM

Jarajapu Chaitanya[1], Dr. Arpit Solanki[2]
[1]Student, Dr. A.P.J. Abdul Kalam University, Indore, M.P., India
[2]Assistant Professor & HOD, Dr. A.P.J. Abdul Kalam University, Indore, M.P., India

ABSTRACT

Now days the global organization faces many changes. In current time, Whole Word shifted to internet and strong data security techniques is required for secure transmission of important and confidential data. Cryptography techniques are playing important role for providing security to such important data. There are lots of research done in the field of cryptography, but still, it is one of the most important and promising area of research. On the basis of study and review we found that RSA algorithm is one most popularly used algorithm. But this cryptography techniques involve a number of issues is to achieve higher security. Among the various issue time complexity is one of most crucial issue. In this paper, a new improved and faster RSA algorithm has been Proposed and implement for protect important data.

Keyword - Security, Cryptography, RSA, Encryption, Decryption.

INTRODUCTION

The network security plays an important role in area of network development. With rapid growth in uses of internet, network security became a major concern for every organization. In this information age, the network security issue is increasing day by day. Security issue becomes crucial when communication is done by any information via an unsecure channel. In addition to this number of hackers and viruses are rapidly increase. This data may be containing payment transaction information, financial data, and confidential information of organization or nation. Security is crucial whenever a common man pay any bill online, a normal user select ATM for withdraw money or any company or nation policy.

Many academics and experts worked together to develop basic policy and standard principles and procedure for security like antivirus software, password protection and firewall etc. Various corporate organization, governments departments, social media platforms, school and academics institute and other organization have too much amount of data of their client, students, employees, supplier etc. Security of this data is very important for organization even a minor mistake or leakage can damage reputation of organization. In this situation, cryptography techniques are playing important role for providing security to such important data. [1]

The concepts of cryptography were born out from the requirement of transfer of sensitive information or data through unsecure network, in cryptography, sender is used a secret key to encrypt data and other hands receiver used same or a different key to decrypts data. In this case, only receiver can understand the information. There are number of cryptography algorithms are available now, but still RSA Algorithms is one of the most popular and widely used algorithm for securing of information. In 1977, three scientist Ron Rivest, Adi Shamir and Leonard Adleman develop this algorithm. For creating name of algorithm, they use first letter of all three scientist. Encryption speed of RSA algorithms high but decryption speed is very low. Overall, it takes higher time for completion of algorithms. In this paper, to address these issues and offer the solution an improved RSA algorithm has also discussed.

RELATED STUDY

In order to give the concealed information dual protection and make it compressible and invisible to others, Yang Ren-er, ZhengZhiwei, Tao Shun, and Ding Shilei [12] introduced the DES algorithm for encryption in addition to the LBS technique. The DES algorithm was the research's issue. These days, it breaks easily.

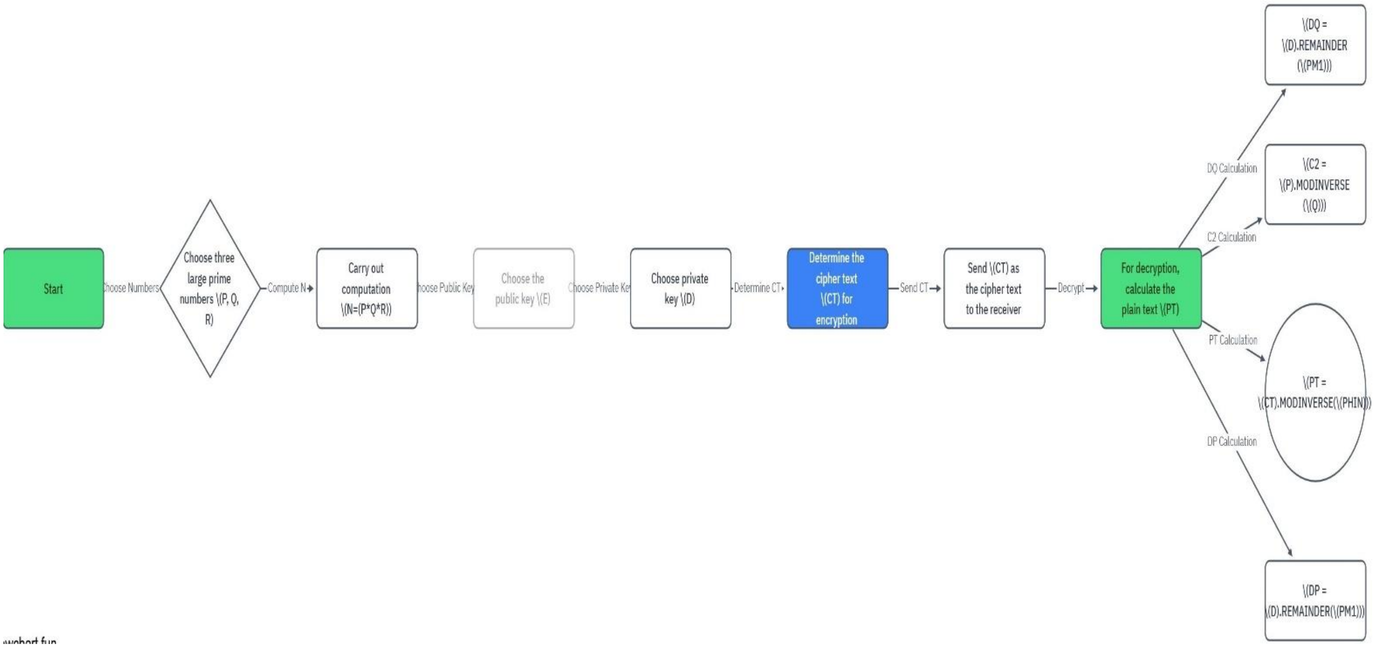
The writers, Mr. Madhusudhan Mishra, Mr. Gangadhar, Tiwari, and Mr. Arun Kumar Yadav, [13], have employed a novel method. In addition to the F5 algorithm, the author has employed the RSA algorithm for encryption. The author has also employed two tiers of security, first utilizing a cryptography key and then a stego key, to conceal the encrypted message in the lower image.

Nidhi Sharma, Manu Devi, [14] the suggested system LBS steganography was employed by the author to embed images. The PSNR has been estimated by the author to improve image quality, and the calculation process has also been explained. The quality of the stego image increases with the PSNR value. The primary goal of the study was to create a new and improved method of data concealment. The primary goal was to completely impenetrable from the inside of the encrypted message.

The proposed paradigm by Phad Vitthal S., Bhosale Rajkumar S., and Panhalkar Archana R. [9] provides two levels of security for confidential information. Additionally, our suggested approach provides high embedding capacity and high-quality stegoimages by encrypting the secret message using the advanced encryption standard (AES) algorithm and then hiding the encrypted message in a true color RGB image using pixel value differencing (PVD) with least-significant-bit (LSB) substitution.

PROPOSED SOLUTION

The Proposed Improved RSA algorithm has following steps:


Start
Choose Numbers
Choose three large prime numbers \(P, Q, R)
Compute N
Carry out computation \(N=(P*Q*R))
hoose Public Key
Choose the public key \(E)
Choose Private Ke
Choose private key \(D)
Determine CT
Determine the cipher text \(CT) for encryption
Send CT
Send \(CT) as the cipher text to the receiver
Decrypt
For decryption, calculate the plain text \(PT)
DQ Calculation
\(DQ = \(D).REMAINDER (\(PM1)))
C2 Calculation
\(C2 = \(P).MODINVERSE (\(Q)))
PT Calculation
\(PT = \(CT).MODINVERSE(\(PHIN)))
DP Calculation
\(DP = \(D).REMAINDER(\(PM1)))
owchart fun

RESULTS ANALYSIS

In this section, performance of proposed improved RSA algorithm is evaluated. Additionally, a performance comparison with traditional RSA algorithm has also been presented. To evaluated performance overall or total time taken parameter has been considered.

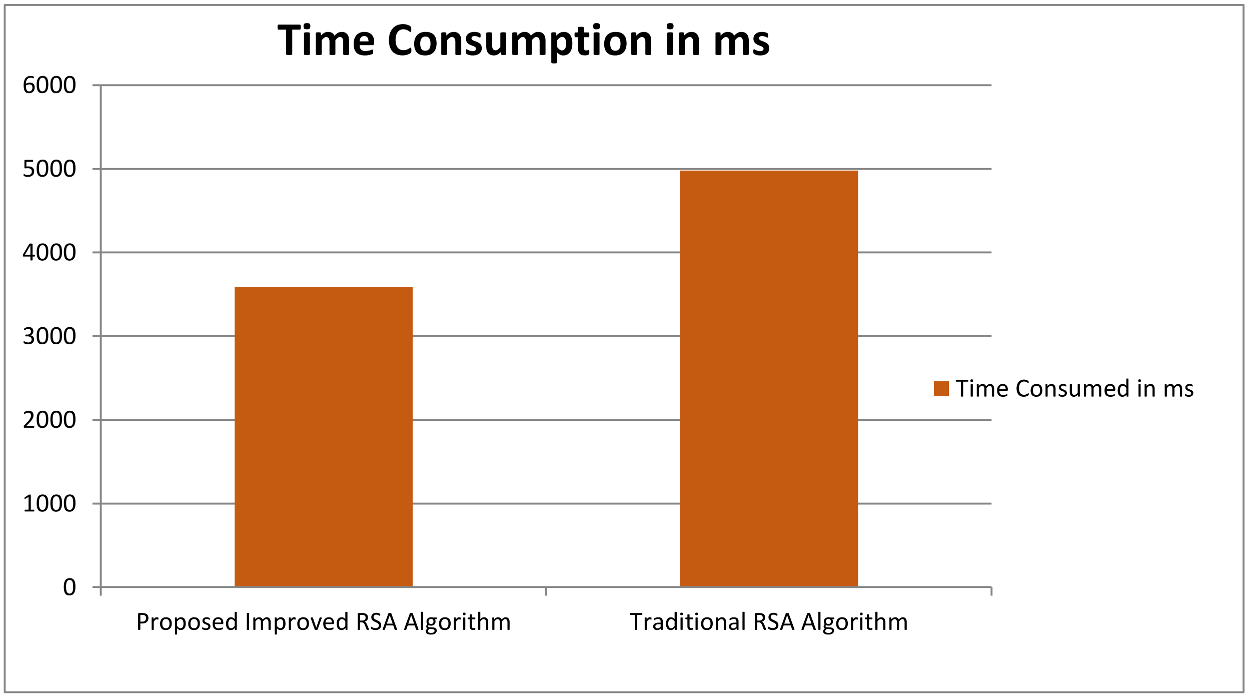


Figure1: Time Consumption Comparison

Figure 4.1 shows the time consumption by Traditional RSA algorithm and proposed improved RSA algorithm. According obtain result, time consumption by proposed improved RSA algorithm is lesser than Traditional RSA algorithm. This compare shows that performance of proposed improved RSA algorithm is better than Traditional RSA Algorithm.

CONCLUSION

The aim of proposed work is to propose a new faster version of RSA in such a manner that the time consumption would be less as compared to the traditional RSA algorithm. we have done this by focusing the basic concept of cryptography and the key management schemes. Additionally, review and study of various cryptography algorithm is also done in brief. In this study we understand and analysis the advantages and disadvantages of some most widely used algorithms. On basis of this study a research gap is identified and the problem was formulated. In this research we found that time taken by traditional RSA algorithm is higher due to slow decryption speed. To Overcome this limitation of RSA algorithm, propose a improve and faster version of RSA algorithm including encryption and decryption algorithm. To evaluated the time consumption of proposed algorithm, proposed algorithm implemented in Java. Additionally, a performance comparison with traditional RSA algorithm has also been presented. According obtain result, time consumption by proposed improved RSA algorithm is lesser than Traditional RSA algorithm. This compare shows that performance of proposed improved RSA algorithm is better than Traditional RSA Algorithm.

REFERENCES

[1] William Stallings “Network Security Essentials (Applications and Standards)”, Pearson Education, 2004

[2] National Bureau of Standards, “Data Encryption Standard,” FIPS Publication 46, 1977.

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

[4] Prof. Dr. Alaa Hussein Al-Hamami, Ibrahem Abdallah Aldariseh, “Enhanced Method for RSA Cryptosystem Algorithm” 2012International Conference on Advanced Computer Science. Applications and Technologies, IEEE 2012.

[5] V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[6] Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis of Encryption Algorithms for Data Communication", IJCST Vol. 2, Issue 2, June 2011 pp.192-192.

[7] Dr. S.A.M Rizvi1, Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa" A Comparative Study of Two Symmetric Encryption Algorithms across Different Platforms",

[8] G. jai Arul Jose, research scholar, Sathyabama University, Chennai-possible Attack on RSA Signature.

[9] Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R A Novel Security Scheme for Secret Data using Cryptography and Steganography. DOI: 10.5815/ijcnis.2012.02.06

[10] Manjunath N, S.G.Hiremath Image and Text Steganography Based on RSA and Chaos Cryptography Algorithm with Hash-LSB Technique ISSN : 2347-2820, Volume -3,Issue-5 2015.

[11] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena Security Improvisation in Image Steganography using DES 978-1-4673-4529-3/12/_c 2012 IEEE.

[12] Yang Ren-er, Zheng Zhiwei, Tao Shun, Ding Shilei image Steganography Combined with DES Encryption Pre-processing 978-1-4799-3434-8/14 © 2014 IEEE DOI10.1109/ICMTMA.2014.80

[13] Mr. Madhusudhan Mishra, Mr. Gangadhar Tiwari, Mr. Arun Kumar Yadav Secret Communication using public key Steganography [978-1-4799-4040-0/14/$31.00 ©2014 IEEE

[14] Manu Devi Nidhi Sharma Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images 978-1-4799-2291-8/14/$31.00 ©2014 IEEE

[15] C. J. N. Cheltha, ``An innovative encryption method for images using RSA, honey encryption and inaccuracy tolerant system using Hamming codes," International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), 2017, pp. 796-799.

[16] https://flowchart.fun/