SHODH SANGAM -- A RKDF University Journal of Science and Engineering

An Enhanced Methodology for Data Security Using RSA Algorithm

[1]Sangeeta Niranjan, [2]Dr. Akant Kumar Raghuwanshi, [3]Dr. Balajeee Sharma
[1]M. Tech Scholar, [2]Associat Professor, [3]Associat Professor
[1]Department of Electronics and Communication Engineering, Vedica Institute of Technology Bhopal, (M.P.)
[2]Department of Electronics and Communication Engineering, Vedica Institute of Technology Bhopal,, (M.P.)
[3]Department of Electronics and Communication Engineering, Vedica Institute of Technology Bhopal,, (M.P.)
Email-: [1]sangeetaniranjan1@gmail.com, [2]akantthakur7@gmail.com, [3]sharmabalajee@gmail.com

Abstract:- In the present scenario, big data is facing many challenges regarding the data storage, data theft and unauthorized access. Many researchers are concentrated on developing the security mechanism for big data storage. To overcome the above issue, this work concentrated on developing the encryption algorithm for storing big data using RSA Algorithm based on Vedic multiplier. This work is dedicated to study different encryption technique for designing security algorithm for Big data. The work is dedicated to design a faster, secure and effective RSA algorithm with application of Vedic multiplier.

Keywords:- Data Security, Encryption, Vedic Multiplier

I. INTRODUCTION

The Vedic Multiplier, rooted in ancient Indian mathematics, offers a highly efficient multiplication technique by reducing the number of steps involved in arithmetic operations. By integrating the Vedic Multiplier into the RSA algorithm, the overall encryption and decryption processes can be accelerated, leading to faster key generation and data handling. This improvement is especially relevant in environments where rapid data processing is critical, such as in real-time communication systems, financial transactions, and cloud computing.

The combination of RSA's strong encryption with the computational efficiency of the Vedic Multiplier creates a balanced approach to data security. This hybrid system not only enhances the performance of cryptographic operations but also ensures that the security standards of RSA remain intact. The approach offers a promising solution to modern data security challenges, particularly in scenarios requiring both high security and efficient processing speeds.

The RSA algorithm, named after its creators Rivest, Shamir, and Adleman, is one of the most widely used public-key cryptosystems. Its security is based on the mathematical challenge of factoring large prime numbers. RSA involves three main processes: key generation, encryption, and decryption.

Vedic Mathematics is an ancient system of mathematics that traces its roots to the Vedas, the oldest scriptures of Indian knowledge, dating back over 3,000 years. Rediscovered in the early 20th century by Indian mathematician Bharati Krishna Tirthaji, this system presents a collection of mathematical techniques or sutras that simplify complex arithmetic operations. Unlike traditional methods, Vedic Mathematics offers faster and more efficient approaches to calculations, making it particularly useful in mental math, competitive exams, and computational tasks.

The core philosophy of Vedic Mathematics lies in its simplicity and flexibility. It consists of 16 main sutras (aphorisms) and 13 sub-sutras, each of which can be applied to various mathematical problems, including multiplication, division, factorization, and algebraic equations. One of its most notable applications is the "Urdhva Tiryagbhyam" (vertical and crosswise) sutra, which simplifies multiplication by reducing the number of steps required, making it an attractive tool for high-speed computing.

II. LITERATURE REVIEW

Singh et al. [5] explored the creation of an Advanced Encryption System that is suitable for areas that require maximal size minimization, such as mobile phones. The Verilog hardware description language is used to develop the layout, which enables for quick hardware execution. The hardware implementation of the system is faster than traditional designs. They employed Vedic maths approaches to do this. Comparisons with conventional layouts are used to highlight the advantages of the recommended layout.

Saju et al [6] presented Elliptic Curve Cryptography (ECC) in this study due to its short key size, small memory footprint, and fast response time. Scalar multiplication of elliptic curves is an essential aspect of elliptic curve systems. Because the space usage of the Karatsuba multiplier is minimal, scalar multiplication is achieved with the assistance of a hybrid Karatsuba multiplier. This article also discusses an alternate digital signature technique, the Elliptic Curve Digital Signature Algorithm (ECDSA), as well as the fundamental functions of elliptic curves.

Kumar et al [7] in this work has utilized ancient mathematics techniques and algorithms in various projective coordinates systems (Jacobian, Chudnovsky-Jacobian, Modified Jacobian coordinates system) to reduce the number of stages in the addition and doubling algorithms, as well as improve the speed of computation time in ECC operational processes (points addition, points doubling).

Matta et al [8] In this article, have looked at some of the most important methods and approaches for data encryption and decryption. Furthermore, they conducted a comparative study of the various encryption and decryption algorithms in order to forecast their adoption depending on the application. The primary goal of this project is to put a stronger emphasis on data encryption techniques and to highlight the significant

difficulties and implementation domains where these encryption methods perform well.

Zaminkar et al [9] in this study have employed a reliable hybrid technique with encryption as an effective way for addressing the Low-Power and Lossy Networks (RPL) protocol problems and for connecting the devices in a secure manner.

Sahasrabuddhe et al [10] presents a cryptographic approach for protecting multiple digital photographs transmitted over the internet. Chaos theory and elliptic curves are used in the algorithm. The Elgamal cryptosystem is used to generate the cypher image and share the key.

Arora et al [11] in this research developed a hybrid approach of digital picture protection based on image concealment and encryption. A hidden picture will be given two levels of protection in this suggested approach. The stego picture was obtained after the secret image was initially hidden under a cover picture by utilizing LSB concealing technique. The stego picture was then encrypted utilizing the AES encryption technique, when it has been obtained.

Shukla et al [12] have suggested a novel encryption-based technique for cloud computing in this research work. The suggested method was compared against a number of other commonly utilized encryption techniques, such as DES, AES, and Blowfish, and also the presented algorithm. The functioning of the presented approach has been evaluated using a variety of factors such as encryption time for different block sizes, as well as the avalanche impact on plain text.

Munir et al [13] have highlighted security issues in a newly proposed Internet of Health Things (IoHT) encryption approach based on a chaotic map, in this research. The approach used a new chaotic map, a customized Mandelbrot set, and a conditional shift algorithm to prove that the encryption algorithm was safe. To recover the key from the understudy cryptosystem, they used cryptographic assaults. Utilizing a chosen-plaintext threat and one known plaintext ciphertext combination, the key was obtained in a short amount of time.

Pushpalatha et al [14] has provided a quick overview of different standard encryption algorithms, cryptographic requirements for chaotic-based cryptosystem layout, and chaos-based speech encryption techniques. This research also offers a number of statistical measures to examine when determining whether binary sequences created by hardware or software are acceptable for use as important sequences in cryptographic applications.

Fukami et al [15] in this study, have discussed the influence of enhanced encryption and safety mechanisms of smartphones on conventional forensic information recovery methodologies for law enforcement reasons. They suggested that new mobile forensic approaches depend on circumventing security characteristics and using system flaws to solve encryption problems. A novel forensic acquisition model is offered. The methodology is backed up by a legal framework that emphasises the usefulness of digital evidence gained by exploiting vulnerabilities.

Jegadish et al [18] developed an effective 8 X 8 Vedic multiplier and implement it in the Field Programmable Gate Array using Xilinx - ISE Design Suite 14.7. The RSA algorithm is used to secure sensitive data over unsecured networks like the Internet. However, traditional multipliers have high propagation delay due to the number of adders and digital circuits. The Vedic Multiplier can overcome this issue and operate efficiently.

Sengottaiyan et al [19] discusses four methods to improve ECC performance, including DMM-Optimized Carry Look Ahead Adder, DMM-Optimized Carry Bypass Adder, DMM-Look up Table Carry Select Adder, and Dual Field Vedic Multiplier – LCSLA.

III. PROPOSED METHODOLOGY

With the rise of electronic communication, privacy and security have taken on a more significant role. A method for making the message safe is cryptography. Various cryptographic algorithms exist, including RSA (Rivest-Shamir-Adleman), AES (Advance Encryption System), and ECC (Elliptic Curve Cryptography). A well-liked technique in public key cryptography is the RSA public key cryptosystem. to provide security in a big data network. The most secure high-quality standard algorithm is RSA. In order to reduce the need for hardware resources and processing time, researchers advise using vedic shortcuts in algorithms. In addition to speeding up other cryptographic algorithms, these shortcuts might also enable cryptographers to use larger key sizes for higher security. Consequently, the purpose of this study is to use a vedic multiplier when creating a secure encryption technique.

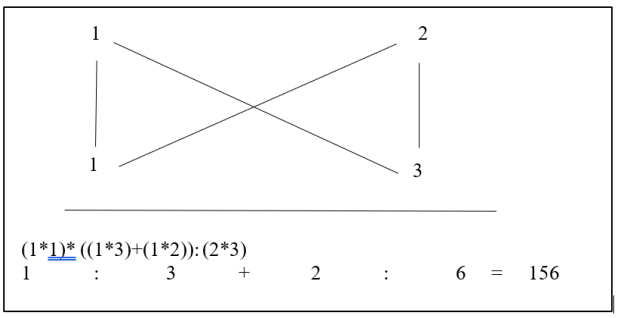

Figure 1: Multiplication using UTS

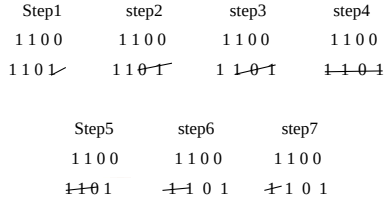

Figure 2: Example of UTS Multiplication

At MIT, Ron Rivest, Adi Shamir, and Len Adleman created RSA in 1977. The most used public-key cryptosystem is RSA. It offers digital signature, key exchange, and data secrecy. A block cypher is used. Large prime numbers serve

as the foundation for private and public keys. For the standard RSA algorithm to encrypt and decrypt data, the following steps are necessary:

- Let p and q be two large prime numbers
- Then let n = p * q
- Select public key 'e' such that, gcd(((p-1)*(q-1)), e) =1; 1<e < (p-1) *(q-1)
- Select private key 'd' such that, $d= e^{-1} \bmod (p-1)(q-1)$
- For encryption, $CT= PT^e \bmod n$
- For decryption, $PT = CT^d \bmod n$

The RSA encryption/decryption system is implemented using the Vedic mathematical algorithm to increase the processing speed. The advantage of Vedic Multiplier is that it calculates the partial products in one step and there are no switching operations, which saves time and memory utilization. As the number of bits in the message increases, the gate delay and area slowly increase. Therefore, it can be used effectively in all cryptographic applications.

Key points of proposed methodology:

- In RSA algorithm there is slow encryption due to large prime generation. So, in this work fast prime generation is performed using Vedic mathematics so that there is no possibility to access the Big Data from the cloud without the permission of data owner.
- It has been believed that if integer factorization of n is unknown, finding d from e is difficult. So, vedic factorization algorithm reduces the complexity for finding d and e.

Algorithm for Proposed Vedic-RSA Encryption algorithm for Big data Security:

- Generate prime numbers, p and q using Vedic mathematics
- Then generate n = p * q using Nikhilam sutra/ Urdhva Tiryakbhyam Sutra
- Select public key 'e' using Gauss reduction algorithm
- Evaluate private key 'd' such that, $d= e^{-1} \bmod (p-1)(q-1)$ using Vedic multiplier
- Apply Vedic multiplier for encryption and decryption

Performance Parameters

Encryption time: This measures the duration to convert plaintext into ciphertext using a cryptographic algorithm and key.

$$Encryption\ time = (Enc\_Stop\_time - Enc\_Start\_time) \quad (1)$$

Decryption time: Similar to encryption time, this refers to the time taken to revert ciphertext back to its original plaintext. It is evaluated as:

$$Decryption\ time = (Dec\_Stop\_time - Dec\_Start\_time) \quad (2)$$

IV. CONCLUSION AND FUTURE SCOPE

In conventional RSA algorithms, exponents are obtained using Euclid algorithm that is modified using vedic multiplier. The public exponents obtained from Euclid algorithm is roughly selected. In this work, RSA algorithm is modified using vedic multiplier algorithm to make it more secure and fast while dealing with Big Data. The result analysis was compared between two vedic multiplier performance i.e., Urdhva Tiryakbhyam Sutra (UTS) and Nikhilam Sutra (NS).

REFERENCES

[1] Kapoor, Jitaksh, and Divyansh Thakur. "Analysis of Symmetric and Asymmetric Key Algorithms." *ICT Analysis and Applications*. Springer, Singapore, 2022. 133-143.

[2] Kynigopoulos, Charalampos. "ENCRYPTION TECHNOLOGIES AND CIPHERS."

[3] Dinca, Alexandru, Nicoleta Angelescu, and Dan Popescu. "Web Data Management Platform Integrating Encryption Algorithms." 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). IEEE, 2021.

[4] Wahid, M. Nazeh Abdul, et al. "A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish for guessing attacks prevention." Journal Computer Science Applications and Information Technology 3.2 (2018): 1-7.

[5] Singh, Saurabh, and Sunita Soni. "Report on Cryptographic Hardware Design using Vedic Mathematics." *2021 International Conference on Technological Advancements and Innovations (ICTAI)*. IEEE, 2021.

[6] Saju, Nikita Susan, and K. N. Sreehari. "Design and Execution of Highly Adaptable Elliptic Curve Cryptographic Processor and Algorithm on FPGA using Verilog HDL." *2021 International Conference on Communication, Control and Information Sciences (ICCISc)*. Vol. 1. IEEE, 2021.

[7] Kumar, Ankur, Pratik Gupta, and Manoj Kumar. "The Techniques of Vedic Mathematics for ECC Over Weierstrass Elliptic Curve Y 2= X 3+ Ax+ B." *Advances in Communication and Computational Technology*. Springer, Singapore, 2021. 501-515.

[8] Matta, Priya, Minit Arora, and Deepika Sharma. "A comparative survey on data encryption Techniques: Big data perspective." *Materials Today: Proceedings* (2021).

[9] Zaminkar, Mina, Fateme Sarkohaki, and Reza Fotohi. "A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem." *International Journal of Communication Systems* 34.3 (2021): e4693.

[10] Sahasrabuddhe, Aasawari, and Dolendro Singh Laiphrakpam. "Multiple images encryption based on 3D scrambling and hyper-chaotic system." *Information Sciences* 550 (2021): 252-267.

[11] Arora, Himanshu, et al. "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption." *2021 6th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 2021.

[12] Shukla, Dhirendra KR, Vijay KR Dwivedi, and Munesh C. Trivedi. "Encryption algorithm in cloud

computing." *Materials Today: Proceedings* 37 (2021): 1869-1875.

[13] Munir, Noor, et al. "Cryptanalysis of internet of health things encryption scheme based on chaotic maps." *IEEE Access* 9 (2021): 105678-105685.

[14] Pushpalatha, G. S., and S. Ramesh. "Chaotic based encryption algorithms for speech signal and cryptographic requirements: A brief survey." *Materials Today: Proceedings* (2021).

[15] Fukami, Aya, Radina Stoykova, and Zeno Geradts. "A new model for forensic data extraction from encrypted mobile devices." Forensic Science International: Digital Investigation 38 (2021): 301169.

[16] A. Jain and A. Jain, "Design, implementation & comparison of vedic multipliers with conventional multiplier," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 1039-1045, doi: 10.1109/ICECDS.2017.8389596.

[17] Prabhu, E., H. Mangalam, and P. R. Gokul. "A delay efficient vedic multiplier." Proceedings of the National Academy of Sciences, India Section A: Physical Sciences 89.2 (2019): 257-268.

[18] J. K. K J, K. P, G. V, and S. K, "Efficient FPGA Implementation of RSA Algorithm Using Vedic Multiplier," in 2023 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), 2023, pp. 1–5. doi: 10.1109/WiSPNET57748.2023.10134210.

[19] S. Sengottaiyan, V. Subramaniam, Y. Thangavel, and K. Sekar, "Power Efficient Implementation of ECC Using LCSLA Based Dual Field Vedic Multiplier," Proc. Bulg. Acad. Sci., vol. 76, no. 12, pp. 1868–1876, 2023, doi: 10.7546/CRABS.2023.12.09.