IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306094|

A Review on Cryptography Using RSA Algorithm

Shravani Khanvilkar, Prof. Ajinkya Naphade

Department of M. C. A, Finolex Academy of Management and Technology, Ratnagiri, Mumbai University, India

Assistant Professor, Department of M. C. A, Finolex Academy of Management and Technology, Ratnagiri, Mumbai University, India

ABSTARCT: With the internet having reached the level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone accessible by the intend intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender.

KEYWORDSL: Cryptography, Security, Algorithm, Cipher, Decryption, Data Security

I. INTRODUCTION

In the dominion of current cryptography, the RSA algorithm stands as an stable keystone, revolutionizing the landscape of secure communication. Developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, the RSA algorithm marked a paradigm shift by introducing the concept cof public-key cryptography. Named after its inventors, RSA (Rivest-Shamir-Adleman) remains one of the most widely used cryptographic systems, underpinning the security infrastructure of countless digital transaction, communications and data protection mechanisms.

II. LITERATURE OVERVIEW

1] Nasrut Dinov and Tronin show that a expressive generality of RSA probable for a equitably wide class of associatory rings with identity. They labelled rings with commuting ideals; the class of rings permits generality of RSA Cryptosystem and comprehends mutually commutative and non-commutative rings. They showcased that to generalize the RSA Cryptosystem we should use only intersection of maximum ideals.

2] Kalpana Parsi deliberated data security in cloud computing using RSA algorithm in her research paper. She distinguished that cloud computing is an incipient paradigm which has become todays prime research area because of its capability to condense the cost assistant with computing due to this security has become the main hindrance which is hindering the deployment of cloud environment, so to ensure the security of data , she proposed a method by implementing RSA algorithm.

3] Sandeep Kumar established a multi-Phase encryption system using RSA algorithm, MRMAC (Modified Random Matrix Affine Cipher) and Chen's hyperchaotic map. He stated that in the present time the images are extensively used over the multimedia for distribution of the information. At the same time to ensure the security of images throughout transmission of data becomes a great contest for cryptographers. In this paper He anticipated a new multi-phases image encryption algorithm constructed on the RSA Cryptosystem and Arnold cat map are used to generate additional distraction from the relationship amongst the original image and ciphered image.

4] In the research paper of encryption and decryption of Signed Graph matrices through RSA algorithm where Deepa Sinha and Anshu Sethi deliberated that secret communication have been required by military officers and diplomats since ancient times, The prerequisite to preserve important information secure and confidential is also increasing day by day. They considered Signed Graphs and understood that the study of Signed Graphs as network is of countless importance where Signed Graphs can be used as matrices and this conversation can be implemented in various encryption and decryption techniques, where securities are represented as nodes of a Signed Graphs and edges represents the co-relation between the securities. They propose a new cryptography mechanism for secure data transmission and retrieval using a Signed Graph, its adjacency matrix and the RSA algorithm

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306094|

5] In the research paper[5] Dr M Gobi, R Sridevi and Priyadarshini referred the comparative study on the performance and the security of RSA and ECC algorithm. In the paper they designated a comprehensive performance comparison of RSA and ECC algorithms where equated based on their key size and the time taken to encrypt and decrypt the text, during this analysis they experiential and concluded that that ECC was the best when compared to RSA algorithm in term of authentication based on execution time, speed, scalability, flexibility, reliability, security and limitation that are essential for secure communication.

6] In the research paper [6] Zeinab, MD Yasin, Ali Saheli and Mohammad Saheli concluded that the number of IOT devices besides the amount of information that will be engendered is snowballing pointedly consequently key objectives are assuring the safety of IOT devices, data and users. In this paper from different facets mutually ECC and RSA algorithms are reviewed expansively, and in all parameters ECC could outrival RSA. The result displays that ECC is further efficacious in forms of some parameters like memory requirement energy consumption, etc.

III. THEORETICAL FOUNDATIONS

Mathematical Background Needed to Understand RSA:
The RSA algorithm is manufactured on numerous vital mathematical perceptions. Understanding these perceptions is decisive for avaricious how RSA works and why it is secure.

1. Prime Numbers:
- Definition: A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself.
- Importance in RSA: RSA relies on the difficulty of factoring large prime numbers. Key generation involves selecting two large prime numbers.

2. Modular Arithmetic:
- Definition: A system of arithmetic for integers, where numbers wrap around upon reaching a certain value, known as the modulus.
- Basic Operation: Assumed integers a, and n,a mod n gives the remainder when a is divided by n.

3. Euler's Totient Function ($\phi(n)$):
- Definition: For a given positive integer n, ϕ(n) is the number of integers up to n that are coprime with n.
- Formula: For n = p . q, where p and q are distinct prime numbers, ϕ(n) = (p -1) . (q -1).
- Use in RSA: The function is udes in the key generation process to ensure the public and private keys are inverses modulo ϕ(n).

4. Euler's Theorem:
- Statement: if a and n are coprime, then
- $a^{\phi(n)} \equiv 1 \bmod n$.
- Application: This theorem underpins the RSA encryption and decryption processes, ensuring that raising a number to the power of ϕ(n) modulo n yields 1.

5. Greatest Common Divisor (GCD):
- Definition: The largest positive integer that divides each of the integers without leaving a remainder.
- Use in RSA: The public exponent e is chosen such that $1 < e < \phi(n)$ and GCD $(e, \phi(n)) = 1$.

IV. RSA ALGORITHM

- **Key Generation Process**

The key generation process in RSA involves creating a pair of keys: a public key for encryption and a private key for decryption.

1. Choose Two Distinct Prime Numbers:
- Select two large prime numbers p and q. The primes should be of similar bit-length to ensure security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306094|

2. Compute n:
- Calculate the modulus n by multiplying the two prime numbers: $n=p\times q$.
- n is used as part of both the public and private keys.

3. Calculate Euler's Totient Function ϕ(n):
- Compute ϕ(n) as ϕ(n)=(p−1)×(q−1).

4. Choose Public Exponent e:
- Select an integer e such that 1<e<ϕ(n) and GCD (e,ϕ(n))=1.
- Common choices for e are 3, 17, or 65537, as they balance security and computational efficiency.

5. Compute Private Exponent d:
- Determine d as the modular multiplicative inverse of e modulo ϕ(n), which means d×e≡1modϕ(n).

6. Public and Private Keys:
- Public Key: The public key consists of the pair (e,n).
- Private Key: The private key consists of the pair (d,n).

- **EXAMPLE:**

- Choose primes p=61 and q=53.
- Compute n = 61×53 =3233.
- Compute ϕ(n)=(61−1)×(53−1)=3120.
- Choose e=17 (common choice and GCD(17,3120)=1).
- Compute d such that 17×d≡1mod3120. Using the Extended Euclidean Algorithm, d=2753.
- Public key is (17,3233) and private key is (2753,3233).

- **Encryption Process**

The encryption process in RSA uses the public key to transform plaintext data into ciphertext.
Obtain the Public Key:
- The sender needs the recipient's public key (e,n).

7. Convert the Plaintext to an Integer:
- Represent the plaintext message m as an integer in the range 0 to n−1.

8. Encrypt the Message:
- Compute the ciphertext c using the formula: $c\equiv m^e \bmod n$.

- **EXAMPLE:**

1. Message m=65.
2. Public key (e=17,n=3233).
3. Encrypt: $c\equiv 65^{17} \bmod 3233 = 2790$.

- **Decryption Process**

The decryption process in RSA uses the private key to transform ciphertext back into plaintext.
1. Obtain the Private Key:
- The recipient uses their private key (d,n).

2. Decrypt the Ciphertext:
- Compute the plaintext message m using the formula: $m \equiv c^d \bmod n$.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306094|

EXAMPLE:

1. Ciphertext c=2790.
2. Private key (d=2753,n=3233).
3. Decrypt: $m \equiv 2790^{2753} \bmod 3233 = 65$.

The decrypted message m=65 matches the original plaintext message, demonstrating the correctness of the RSA algorithm.

V. SECURITY ANALYSIS

- **Common Attacks on RSA :**

1. Brute-Force Attack:
- This involves trying all possible private keys to decrypt the ciphertext. However, with sufficiently large key sizes (e.g., 2048 bits), this becomes computationally impractical.

2. Mathematical Attacks:
- Factoring Attack: If an adversary can factor n into p and q, they can easily compute $\phi(n)$ and derive the private key
- d. Modern factorization algorithms like the General Number Field Sieve (GNFS) are powerful but require immense computational resources for large n.
- Timing Attack: This attack involves measuring the time taken to perform private key operations to gain information about the key. For example, differences in computation times for different keys might reveal private key information.
- Chosen Ciphertext Attack (CCA): The attacker sends a chosen ciphertext to be decrypted and uses the decrypted plaintext to gain information about the private key.

3. Implementation Attacks:
- Side-Channel Attacks: These include various methods like power analysis, electromagnetic analysis, and cache timing attacks that exploit physical implementations of the RSA algorithm to extract the private key.
- Fault Injection Attacks: Inducing faults in the computation process (e.g., by using laser beams or clock glitches) can reveal information about the private key.

- **Measures to Enhance the Security of RSA:**

1. Key Size:
- Use sufficiently large key sizes to make factorization impractical. Current recommendations suggest using at least 2048-bit keys for adequate security.

2. Padding Schemes:
- Optimal Asymmetric Encryption Padding (OAEP): OAEP adds randomness to the plaintext before encryption, ensuring that the same plaintext encrypted multiple times yields different ciphertexts. This prevents deterministic encryption and mitigates chosen plaintext and chosen ciphertext attacks.
- PKCS#1:Another padding standard that provides additional security by preventing certain types of attacks.

3. Blinding:
- RSA Blinding: Before performing a private key operation, the input is blinded by multiplying it with a random number. This randomization prevents timing and other side-channel attacks since the operations are performed on randomized data rather than the actual plaintext or ciphertext.

4. Constant-Time Implementations:
- Implement the RSA algorithm in a way that execution time does not depend on the input values, thus thwarting timing attacks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306094|

VI. APPLICATIONS OF RSA

1. Securing-Web Communications (SSL/TLS)
- Email Encryption: RSA is often used to encrypt emails, ensuring that only the intended recipient can read the content. This is commonly implemented in protocols like PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions).
- VPNs and Secure Tunnels: RSA is used in establishing secure connections, such as VPNs (Virtual Private Networks) and SSH (Secure Shell), which protect data in transit over public networks.

2. Digital Signatures:
- Authenticity and Integrity: RSA digital signatures ensure that messages or documents are authentic and have not been tampered with. The sender signs the message with their private key, and the recipient verifies the signature with the sender's public key.
- Software Distribution: RSA is used to sign software to verify its authenticity and integrity. This helps users confirm that the software they are installing comes from a trusted source and has not been altered.

3. Key Exchange:
- Secure Key Distribution: RSA facilitates the secure exchange of symmetric encryption keys over an insecure channel. Once the symmetric key is securely exchanged, it can be used for efficient bulk encryption using algorithms like AES (Advanced Encryption Standard).

VII. CHALLENGES AND LIMITATIONS

Despite its widespread use, cryptography faces several challenges and limitations:

- Computational Overhead: Encryption and decryption processes can be resource-intensive, affecting performance.
- Key Management: Securely generating, storing, and distributing cryptographic keys is complex and prone to human error.
- Algorithm Vulnerabilities: New cryptographic attacks and vulnerabilities are continually discovered, necessitating ongoing updates and improvements.
- Quantum Computing: The advent of quantum computers poses a threat to many current cryptographic algorithms, requiring the development of quantum-resistant solutions.

VIII. FUTURE SCOPE

The future of cryptography will likely focus on addressing current challenges and adapting to new technological advancements:

- Quantum-Resistant Algorithms: Developing and standardizing algorithms that can withstand quantum computing attacks.
- Enhanced Key Management: Improving methods for secure key generation, storage, and distribution.
- Integration with AI: Utilizing artificial intelligence to detect and respond to cryptographic attacks in real-time.
- IoT Security: Developing lightweight cryptographic solutions tailored for the resource-constrained environment of Internet of Things (IoT) devices

IX. CONCLUSION

Cryptography remains a cornerstone of modern data security, providing essential mechanisms to protect information in an increasingly digital world. While it faces ongoing challenges, continuous research and development are paving the way for more secure and efficient cryptographic techniques. As technology evolves, so too must cryptography, ensuring it remains robust against emerging threats and capable of safeguarding our digital future.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306094|

REFERENCES

[1] Ankit A. and Pushkar P., (2012)," Implementation of RSA Algorithm on FPGA", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 1 Issue 5.
[2] Na Qi, Jing P. and Qun D., (2011),"The implementation of FPGA –based RSA public key algorithm and its application in mobile –phone SMS encryption system" International Conference on Instrumentation, Mesurment, Computer, Communication and Control volume 21-No.5, pp. 700-703.
[3] Ridha G., El Amjed H., Talel K., Mbarek T. and Hichem T., (2006), "FPGA Implementation of RSA Cryptosystem", International Journal of Engineering and Applied Sciences, pp 2-3.
[4] Chiranth E, Chakravarthy H.V.A, Nagamohanareddy P, Umesh T.H, Chethan K. M., (2011), " Implementation of RSA Cryptosystem Using Verilog ", in International Journal of scientific & Engineering Research, Volume 2, Issue 5, 1ISSN 2229-5518.
[5] Gurpreet K. and Vishal A., (2013), "An Efficient Implementation of RSA Algorithm using FPGA and Big Prime Digit", International Journal of Computer & Communication Engineering Research (IJCCER), Volume 1 - Issue 4.
[6] Sushanta K. S. and Manoranjan P., (2011)," FPGA Implementation of RSA Encryption System", International Journal of Computer Applications (0975 – 8887), Volume 19– No.9,
[7] M. A. Smadi,Qasem A. and Abdullah A.,(2014), "Efficient FPGA Implementation of RSA Coprocessor Using Scalable Modules" , International Symposium on Emerging Inter-networks, Communication and Mobility, Procedia Computer Science 34, pp 647 – 654.
[8] Vibhor G. , Aruna c. (2011)."Architectural analysis of RSA crypto system on FPGA ", International Journal of Computer Applications , Volume 26-No8.
[9] Chiranth E, Chakravarthy H.V.A, Nagamohanareddy P, Umesh T.H, Chethan Kumar M., (2011),"Implementation of RSA Cryptosystem Using Verilog", International Journal of Scientific & Engineering Research, Volume 2, Issue 5, pp.1-7.
[10] Muhammad I. I., Mamun B.I. R., handaker A. and Sazzad H., (2007),"FPGA Implementation of RSA Encryption Engine with Flexible Key Size", International journal of communication, Issue 3, Volume 1, pp. 107-113.
[11] Rokon I.R., Rahman M.,(2009),"Efficient hardware implementation of RSA cryptography", 3rd International Conference on Anticounterfeiting, Security, and Ident
[12] Wulansari D, Muslim MA, Sugiharti E (2016) Implementation of RSA algorithm with Chinese remainder theorem for modulus n 1024 bit and 4096 bit, Indonesia. Int J Comput Sci Secur (IJCSS)
[13] Sarkar S, Maitra S (2013) Cryptanalytic results on 'dual crt' and 'common prime' RSA. Des Codes Crypt 66(1):157–174

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details