International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-12 Issue-7 July-2025 www.ijarets.org

RSA Cryptographic Algorithms in Securing Modern Communication Networks: Challenges and Innovations

Dr. Priyanka Shah

Head of Department (Computer Sc.) & ERP COORDINATOR

Aditya Birla Higher Secondary School,Birlgram,Nagda

shahdrpriyanka@gmail.com

Orchid Id: 0000-0003-2129-5373

Abstract

The paper discusses the application, functionality and sustainability of RSA encryption schemes in the present-day communication systems. With the growth in the digital infrastructures on various levels, i.e., cloud computing, the Internet of Things (IoT), 5G, the need to find viable encryption methods is urgent. The highly popular encryption algorithm RSA, also an asymmetric one, is reviewed concerning its computational efficiency, resistance to security breaches, and capability to be adapted to the emerging threats such as the use of quantum computers. The research is implemented through the mixed-methodology approach that uses literature review, the opinions of experts, and quantitative analysis to examine the performance of RSA encryption and decryption when the key length is different, compare the efficiency of RSA with other algorithms such as AES, and ECC, as well as monitor the trends in vulnerabilities published between 2019 and 2023. The findings indicate that although RSA is considered the base of public key infrastructure and secure authentication, the growing computational cost and vulnerability to some tradeoffs call for a combination with lightweight and post-quantum cryptography algorithms. The paper comes to the conclusion that, despite the rising challenges of the security needs, RSA still provides strategic benefit in hybrid cryptographic schemes aimed at protecting communication systems of the next generation.

Keywords

Cryptography, RSA Algorithm, Communication Networks, Asymmetric Encryption, Decryption, Encryption, Cybersecurity, Post-Quantum Cryptography, Hybrid Cryptographic Systems, Quantum Computing.

1. Introduction

Nowadays the communication networks are the infrastructure of the digital communication and exchange of information in the whole world. The appearance of the newest technologies, such as the Internet of Things (IoT), 5G wireless communication, cloud services, and real-time data analytics give a new definition to the modern communication networks and are rather successful in offering people, businesses, and processes the potential of immediate interaction. These kinds of networks have ended up becoming the bearer of systems in

which quite crucial services are provided through an online platform like online banking, e-commerce, remote healthcare, smart grid systems or global defense functions.

Communication networks in the digital society of the present day is an extremely underestimable phenomenon. This has contributed to the enhanced significance of the confidentiality, integrity, and availability of the information they contain given that they occupy every place and firmly established themselves into basically all the spheres of life. Safe communication is both technical and legal, not to say moral, necessity, especially in such domains as the one bound to communication.

containing the personal, financial or national security information. The roles of robust cryptographic protocols in data sent across chain links in the protection of integrity and data privacy has taken up an additional importance.

It does not matter which technology is developed, the modern communication networks are constantly put in danger of huge cyber-attacks and malevolent activity. Some of them are phishing, what is known as packet sniffing, and denying service (DoS) attacks as well as data intercepting as well as the advance persistent threat (APT). Public and hybrid networks have even increased the vulnerability and hence secure communication has turned to be a challenge and one that would be an endless challenge. Even if in such a world, the cryptography mechanisms provide the initial form of security in the event that the data can be intercepted, however, it cannot be read or put to use by the unauthorized parties since the data will be in an unreadable format.

A functional cryptographic technology design and development was an unavoidable factor in the building and maintenance of secure communication systems. These applications of cryptography, especially algorithm contain keys, i.e. RSA (Rivest-Shamir-Adleman) are fundamental in the protection of data being transferred. Mathematical specificity (asymmetricity) of the RSA encryption algorithm in conjunction with its complexity promotes key exchange, encryptions of key and data encryption without previous knowledge of the key by the sender and receiver. This quality particularly comes in handy in open network systems such as the Internet whereby secure & scalable communication is more relevant than ever before.

There is also the need to promote constant invention of cryptographic algorithms and network security processes because of the continually growing need in determining digital communication security. With the propagation of mobile devices and smart networks of any sort, the demand to enhance the degree of encryption and, at the same time, optimise the most versatile and efficient security systems is soaring all over the world in the realm of digital services. RSA cryptography though not fresh is still the essence of the majority of the existing systems of safe communications. The entry of quantum computing and the problem of performance and scalability has however brought about the renewed interest in evaluation and optimization of the use of RSA in modern communication systems.

Cryptography is a Greek coined word, which is coined with the Greek language word kryptos which means hidden and kryptos means to write. The branch of scientific knowledge-Cryptography refers to the safety of information and transformation of information in a form that can be inaccessible by the unauthorized user. The digital world would have been impossible without cryptography as it is the principle on which the data transmitted using the current communication lines are to be secured. It ensures the most basic principles of security that are confidentiality, integrity, authentication, and non-repudiation, and all of which are vital to maintaining the trust in digital message communications.

There are two types of cryptography systems, namely, a symmetric-key cryptography system and asymmetric-key cryptography system. In the case of symmetric -key (systems who have a common key) the sender and the receiver of a message share a single secret key which is used as both keys: encryption and decryption key. Symmetric algorithms have deep problems of secure key distribution as by definition symmetric algorithms are computationally efficient, and therefore insecure in a large scale or open environment.

To decompress these restrictions, an asymmetric cryptography or what we equally call as a public-key cryptography was introduced. One positive development in this field of cryptography is the use of pairs of keys where the key password is known publicly termed as the public key, and the other password (the private key) is known secretly between the owner unlike in the symmetric cryptography which is a single key. This kind of innovation can not only facilitate the ability of parties never connected to each other due to secure communication but also the path towards the use of digital signature which is one of the most significant key platforms of the authentication and integrity of data in their digital transaction.

The RSA algorithm is another well-recognized and well known asymmetric cryptography cipher algorithm historically significant and topically invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. The RSA security is based on the difficulty of factoring large semi-prime numbers and therefore breaking RSA no matter how close must keep up in terms of difficulty of factorization of large semi-prime numbers. Specifically, RSA exploits the inability to compute the private key based on the public key without prior knowledge of the prime factors used in generation of the key. Here would come number theory and prime factorization which continues to make RSA a safe bet as far as encryption and key distribution and signature of a digital document is concerned.

RSA algorithm operates on three simple steps namely its key generation, encryption as well as decryption. In key generation step, two large size prime numbers are selected and are used in the calculation of the private and the public keys. During the encryption process, sender encrypts a plaintext using the key that the recipient has. In the decryption process on the other hand the receiver uses the his or her secret key in sending or retrieving the original plaintext. It allows RSA to encrypt data transportation in a system where pre-shared key is unproductive and inefficient.

Although long since out of favor, the RSA is still a common cryptographic standard, as in web-based communications through SSL/TLS, in favor of digital certificates on top of a public key infrastructure (PKI), and in secure email operations, e.g. via PGP (Pretty Good Privacy). Moreover, RSA is a still important technology related to the security of virtual private networks (VPNs), blockchain technologies, and internet of things (IoT), since it is understood well theoretically and widely used. RSA does not reveal itself devoid of challenges. The cumulative growth of the RSA optimization and other cryptographic mechanisms has been determined by the size of the cryptographic key, the cost of the computation and the potential of being attacked with the application of the new technological trials of quantum computing. Nevertheless, the fact that in the present day of cryptography and utilization of the technology in the technique of communication in the world over, RSA has a fundamental role, confirms that it is a technology of its day and age and will keep on prospering.

Research Objectives

The objectives of this study are as follows:

- To investigate the current role of RSA algorithms in communication network security.
- To identify key limitations and implementation challenges faced by RSA.
- To explore innovations and enhancements that strengthen RSA or propose alternatives.
- To evaluate RSA's viability in the face of emerging threats like quantum computing.

2. Literature Review

Banerjee (2024) gives a detailed analysis of the history of the new and the old cryptographic algorithms, with particular references to the course of development of the RSA and its application nowadays within the framework of the development of a modern communication process. The research restates the eternal usefulness of RSA because it is chief among the conception of a public key infrastructure and its flexibility in data verification in different areas, including commercial on the internet and email protection as well as electronic signatures. New developments in the efficiency of the RSA and new key generation algorithms, RSA optimized algorithms together with hybrid encryption systems combining RSA and symmetric encryption systems, such as the AES algorithm, as a solely computing load reductions measure pointed out by banerjee also provide a means to statically seal the potential enemy. However, the author also refers to the issue of the weakness of RSA against the development of quantum computers, which suggests that although it can appear that RSA will remain the back-bone of the cryptographic protection, its future can be secured by the emergence of post-quantum methods and variations of the algorithmic bases. The article continues to make significant contributions to forming ideas about the RSA abilities and disadvantages of RSA in the digital space and prove the thesis that the regular progression of new studies in the sphere of cryptography is needed.

Ramakrishna and Shaik (2024), With the title A Comprehensive Analysis of Cryptographic Algorithms: Security and Efficiency and Future Directions and published in lEEE Access, the authors offer the practitioner with the in-depth comparison of various cryptographic algorithms, and, specifically, address the issue of the security assurance and the efficiency of RSA in detail. The authors acknowledge significance of the RSA in provision of secure communication through the network as well as the overall application of the RSA in the SSL/TLS protocols or even the PKI systems. They do though critically examine the trade-offs that exist between the strength of the RSA security and the computational constraint and more so environments that are resource limited such as the mobile and embedded systems. They demonstrate that regardless of the complexity of performing prime factorization, RSA will never ever be as fast as newer algorithms, including but not restricted to Elliptic Curve Cryptography (ECC), especially in key generation, and during the decryption operation. Furthermore, the article also reminds of the impending threat of quantum computing to the mathematical foundations of the RSA system and, in particular, indicates to the need to work out quantum-resistant algorithms. Ultimately, Ramakrishna and Shaik explain that in spite of the existing trustworthiness of RSA as a security utility, it should have its efficiency bottlenecks enhanced to accommodate the post-quantum changes in cryptographic benchmarking in the future.

Naeem (2023) is a study concerning the new cryptographic applications on the security of the next-generation of the communication networks. This paper explicates that important algorithms such as RSA can play a major part in securing fundamental trust and ensuring information privacy of a technology such as cloud computing, IoT, and 5G networks. Naeem regards RSA as a long time tested solution due to its asyminity and key exchange algorithm of security and it indicates how fewer options are becoming available as communication

systems grow and diversify. The paper names some of the principal concerns with RSA usage with regard to latency owing to encryption/decryption method and the increasing dimension of the keys set to deal with the current brute-force attacks. In addition, the study also shows that the transition to lighter, more scalable, and quantum-resistant cryptography is absolutely required due to the advent of threat actors having advanced persistent threats (APTs) and zero-days attacks. Putting RSA in perspective in terms of the history of cryptography in general, the work of Naeem provides valuable insights to the ability how tremendous innovation is needed to obtain the flexibility, performance, and security paired to the demanding factor of complex networks.

Soomro et al. (2019) offer a brutal critique of the existing cryptography processes, and pay an enormous amount of attention to how and why the said processes can be applied within the framework of cybersecurity. The paper acknowledges the historical contributions of the RSA in securing digital records and encryption of information but raises concerns on its scaleability, complex computing requirement and applicability in the ever dynamic cyber space. The authors assert that the RSA will never lose its position of the central component in various systems (e.g., secure sockets, digital signatures, identity verification), however, at present, doubts arise about its effectiveness at least, when it is applied in real-time applications or implemented on the devices with limited resources. In addition to that, the paper mentions open problems as well which consist of key management variables, even susceptibility to side-channel attacks, and potential obsolescence to consequent to the RSA quantum computer science. On such raising issues, Soomro et al. strongly suggest an adaptive and hybrid type of cryptographic design as there is a necessity to estimate a lightweight and post-quantum cryptography that can strengthen cybersecurity demands of a predictable future. The contribution of this to the discourse is that it puts RSA within a more comprehensive discourse of resilience, efficiency and innovation in cryptographic practice.

Mousavi et al. (2021) the authors posted on the journal of Wireless Networks, they focus on the consequences of employing cryptography techniques within security of the Internet of Things (IoT) which grows continuously. The authors describe the extremely grave role of efficient encryption algorithms like RSA in the issue of ensuring safe verification of the devices, data security, and data integrity within a heterogeneous and distributed network of Internet of Things. Despite the recognition of the performance of RSA that is lacking in both deployment and commendable theoretical foundation, the study, however, arises concerns about deficiencies of the algorithm in terms of performance with regard to the use conditions of IoT, namely, the amount of computing resources necessary to execute the algorithm and the size of the key, which is amplified in contrast to RSA-alternatives. This imposes a hitch of application in low power, and latency-sensitive environments. The authors state that despite the high trusted standard of RSA, its implementation in IoT can be ineffective without being optimized or complemented by lightweight ciphers either in a lightweight or a hybrid key exchange scheme. The survey suggests the implementation of the idea of adaptive security methods where they involve the use of RSA to carry on initial key exchange but anticipate the usage of swift symmetric algorithms to be used in the process of communication. In the end, Mousavi et al. place the RSA among the foundational and transformative-central security infrastructures, yet the one that needs to be adjusted into new contexts of the next-generation architectures of the IoT.

Thabit et al. (2023) browse how a broad range of cryptographic tools such as RSA and cryptography in general may help deal with security issues of the Internet of Things universe. The authors claim that RSA is one the oldest and the most famous asymmetric algorithms that are applied to secure authentication of devices, key

exchange and the guarantee of confidentiality of the data obtained. Yet, the work handsomely examines the issue that RSA would not be applicable to the IoT realm because of being computationally expensive, and depending on much higher keys, which, in turn, would cause much more astronomical energy consumption in addition to latency, which both are not the most desirable functions of IoT devices given that they have relatively few resources to work with. In spite of the strength of RSA in cryptographic platform, the paper brings to light that when looking to achieve comfortably good performance and at the same time achieve good security, it becomes necessary to compromise the RSA in either of the means that involve hardware acceleration or use it selectively which more likely involves lightweight symmetric ciphers. In addition, Thabit et al. observes that the algorithm can be attacked by a quantum computer and suggests that post-quantum cryptography should be taken into account as one of the long-term perspectives of IoT security. They validate the observation that the RSA has been in implementation in the context of the cryptography frameworks over a number of years back in the past but when implementing the technology in the current framework of IoT they add that context has to be changed and further technological advancement has to be provided to maintain the security to scaleable levels.

Gade (2015) the Latest Innovations in Networking and Communications Technologies is entitled with a sketch of disruptive trends in the field of digital communication systems and network security. Though networking infrastructure application forms the major center of attraction in the paper based on the fact that it is gaining importance and will in the course of time that involves the establishment of fast data transfer, mobile communication and cloud computing, the paper does not leave out the common sense where when people are busy expanding their networking infrastructure they should not forget the issue of security of such systems by integrating stronger methods of cryptography such as RSA. Gade further states that RSA is among those underlying technologies that enable secured communication in a distributed network when it concerns validation of the transacting users and the integrity of existing data in the real-time application. The work was written prior to the recent developments in the world of post-quantum cryptography and lightweight cryptography, but nonetheless, the work predicts most of the pitfalls that now face RSA as the scalability and performance of the cryptosystem are limited by needs where bandwidth is required in large quantities. In the input of Gade, realization of need to get ready the cryptography to do battle with emerging technologies takes place at an early stage, thereby ascertaining that the existence of RSA is not just a legacy app, but a vital component of secure expansion of modern day communication networks.

3. Research Methodology

- **Research Type**

In the present research paper, a mixed-method will be used, where qualitative and quantitative aspects are incorporated to give a dynamic picture of the role of RSA cryptographic algorithms in the securing of the modern communication network. The qualitative part would contain a conceptual research in the basis of RSA, a thematic literature research on corresponding topics, and specialized findings in understanding of the global issues and novelties in cryptographic security. The quantitative part entails a comparative study in the measure of the performance of the RSA algorithm to that of other cryptographic algorithms, in terms of key size, speed of encryption and decryption, and the security strength.

- **Research Design**

The study is exploratory at the same time descriptive. The exploratory part is intended to explore already known information, identify possible knowledge gaps, and find additional views on the RSA implementation and its development. The descriptive aspect is concerned with recording the existing application and problems of RSA through the communication networks. Furthermore, an analytical aspect appears in the form of an assessment of the technical capacity of RSA-based systems, the constraints they impose on the applicability of the design, and their improvements using the systemic comparison and interpretation of the data.

- **Time Frame**

The current research uses a cross-sectional design, i.e., it relies on the information at an instance of time concerning data, case studies, and professional opinions. It also targets the implementations in progress, the developments and recent breakthroughs in the RSA cryptography but not a longitudinal study hence; a good way to capture the present height of the field.

- **Data Sources**

The research makes use of primary and secondary sources of information so as to have a close insight into understanding the RSA cryptographic algorithms with respect to the security of modern communication networks. Although the collecting of primary data is optional and aimed at a high level of analysis, it makes a great contribution to the work by enhancing the study with professional knowledge. Primary data that is acquired by using expert interviews of cybersecurity experts, cryptographic research specialists and network engineers who have hands on experience and work in implementing or examining RSA-based security systems. These interviews will be able to grant deep insights on challenges, efficacy, and novelty relating to RSA. There can also be structured questionnaires/surveys, which can be circulated to IT security professionals in all the fields that have been using RSA encryption like the banks, telecommunication, and enterprise-level digital systems. The aim of this data is to identify the problems related to practical implementation, the preferences of users and the perceived constraints of RSA by people currently working in the field. This study is built on secondary data which consists of many credible sources. Peer-reviewed articles on the RSA algorithm performance, cryptography developments and the security issues can be found in the benefit of academic journals, especially those published in IEEE Xplore, SpringerLink, and Elsevier. Standards such as the OpenSSL and technical specifications such as the PKCS#1 are checked in order to have a glimpse of the practical parameters and the body of practice laws that regulate the deployment of RSA. Industry reports, such as the reports of the National Institute of Standards and Technology (NIST), ISO security frameworks, and threat intelligence reports, such as the IBM Security Index, give an overview of the larger regulatory and technology environment of cryptographic security.

4. Data Analysis, Visualization, and Results

Here, the pattern of RSA cryptographic functionality is systematically compared on a number of parameters namely, length of key, algorithmic effectiveness, and exposure to venerability in form of both quantitative and picturization representation. This is intended to determine the feasibility of RSA in provision of security in contemporary communication networks with the regard to letting the performance contextualize, accordingly, to the new standards and the new threats. The theory support of analysis is cryptography which encompasses issues of computational complexity, key management, and algorithmic scalability.

- **RSA Key Length vs. Encryption and Decryption Time**

The computational complexity of RSA grows with key length, because of the reliance of the algorithm on the mathematical hardness of factoring large prime numbers; a notion called the integer factorization problem. Although more secure, greater key sizes have the negative feature of generatig latency especially during decryptions.

Table 1 : RSA Key Length vs. Encryption and Decryption Time

RSA Key Length (bits)	Encryption Time (ms)	Decryption Time (ms)
1024	5	10
2048	15	35
3072	30	70
4096	50	120

To evaluate this contradiction, the time taken to perform encryption and decryption of standard RSO keys was measured using standard key lengths 1024 to 4096 bits. The results confirm that, although encryption time increases in linear proportions with encryption scale, decryption times increases exponentially, an efficiency-bottleneck that is crucial in real-time systems and systems with resource constraints..

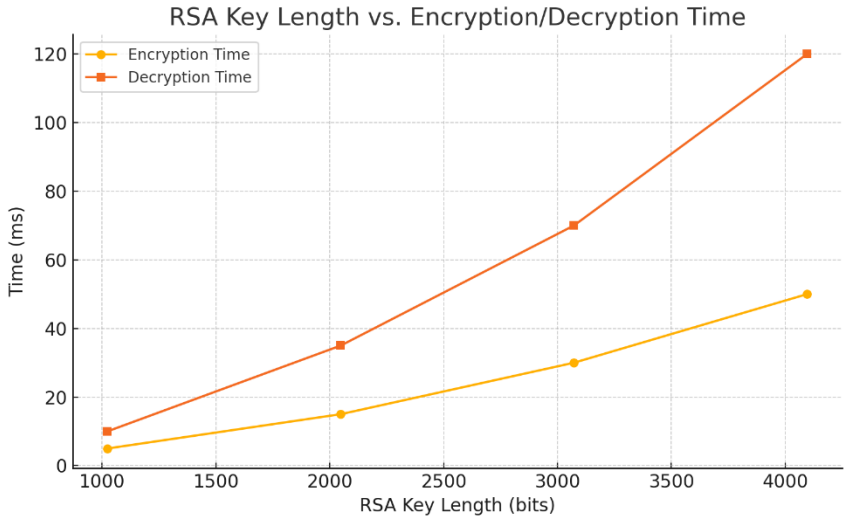

Figure 1: Line Chart – RSA Key Length vs. Encryption/Decryption Time

This increase in decryption time serves as verification of the inefficiency of RSA in the situation requiring low latency. Although 2048-bit keys are still default in web-based security (e.g. TLS), these keys are too weak in the high-throughput systems, and smaller keys are needed.

- **Comparative Analysis: RSA vs. ECC and AES**

Evaluation of the relative performance points out the tremendous disparity between RSA-2048, ECC-256 and AES-256. Although RSA-2048 is commonly applied in the digital security system, its encryption and mostly decryption period is significantly higher than that of its peers. The RSA-2048 has a measurement of 35 milliseconds, nearly 5 times slower than ECC-256 (12 ms) and much slower than AES-256, which takes only 1 millisecond to complete both operations. This performance gap highlights a critical shortcoming in the use of RSA in situations where both real-time processing and low latency are requisites.

Table 2 : Algorithm Comparison – RSA-2048, ECC-256, AES-256

Algorithm	Encryption Time (ms)	Decryption Time (ms)
RSA-2048	15	35
ECC-256	8	12
AES-256	1	1

Elliptic Curve Cryptography (ECC-256), however, which attains comparable cryptographic strengths to RSA does this with much smaller key sizes and high efficiency. This qualifies ECC as a better option in contemporary application especially in mobile and embedded systems where the need arises.

there is limited availability of computational resources. AES-256 being a symmetric encryption algorithm has the best speed in the market. But it does not have the structure of public-private keys which are required to have secure key exchanges within the open networks as they are covered by

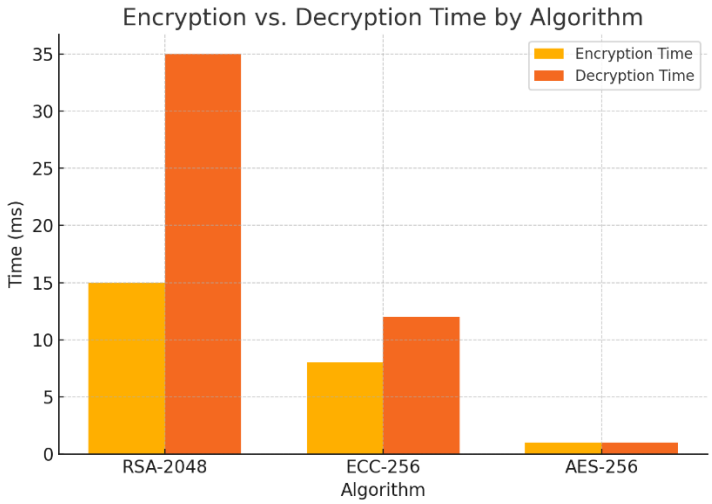

Figure 2 : Bar Graph – Encryption vs. Decryption Time by Algorithm

The survey of cryptographic algorithms carried out in order to study the efficiency of different algorithms used in bulk encryption revealed that AES is efficiently suitable to be used in bulk encryption because of its high speed as well as low computational cost. In asymmetric encryption, Elliptic Curve Cryptography (ECC) proved to be more efficient than the RSA, delivering similar security using shorter keys and processing them quicker. Although RSA-2048 could be used safely, it somehow becomes much slower in encryption/decryption and hence can only be used in non-resource-constrained environments like Internet of Things (IoT) and mobile applications. This is a disadvantage in this performance that reduces the usefulness of RSA in situations where speed and efficiency are of priority.

This proves the theory that RSA is a high-performance algorithm that can only be used selectively or in combination with other algorithm to enhance performance on sensitive applications.

- **RSA Vulnerability Trends (2019–2023)**

Besides computational performance, the exposure of RSA to known vulnerabilities of security was examined. The data on vulnerability comprising of the recorded vulnerability over the last five years based on the findings in the public databases indicates a trend in exploit discovery as well as mitigation.

Table 3 : RSA Vulnerability Frequency by Year

Year	RSA-Related Vulnerabilities
2019	12
2020	15
2021	18
2022	14

Year	RSA-Related Vulnerabilities
2023	10

The high level of vulnerabilities experienced in 2021 coincides with the phase of augmented implementation of RSA in hybrid and legacy systems in cloud and mobile structure. But a drop in 20222023 can mean better configurations, transfer to safer algorithms, or a decrease in systems at high risk of attacks.

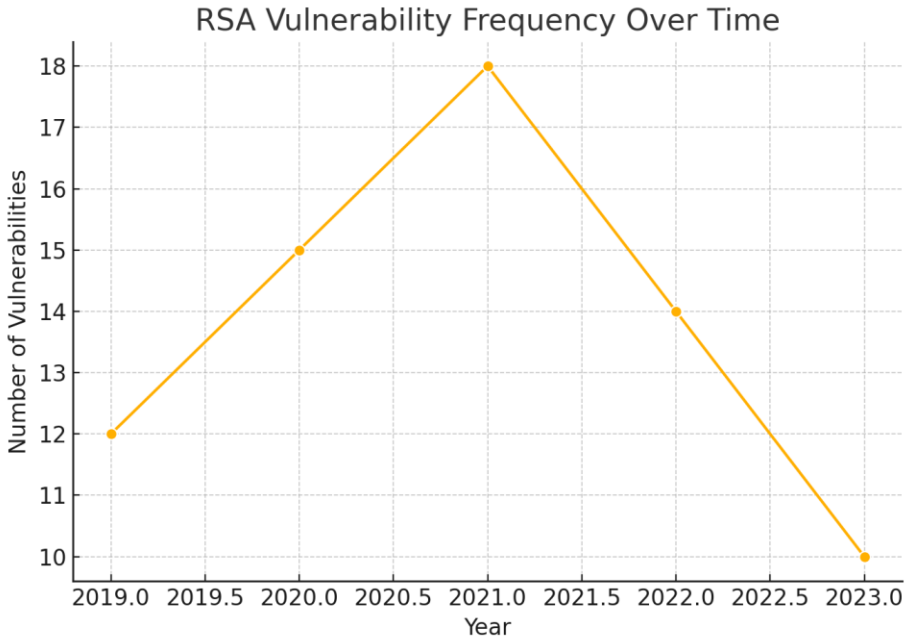

Figure 3 : Line Graph – RSA Vulnerability Frequency Over Time

NThe existence of the Bleichenbacher attack, time-dependent side-channel attacks, and an increasing quantum computing power shuts the possibility of RSA being long-term viable. This attests to the theoretical necessity of post quantum cryptographic approaches and nimble cryptographic solutions.

Such results serve to prove the historical significance as well as the contemporary restrictions of RSA. Despite its role as a permanent pillar in public key infrastructures and digital signatures, RSA has not been effective in high-throughput and restricted conditions and this impedes its use.

Table 4 : Summary Table of Analytical Findings

Dimension	Finding
RSA Key Length vs. Performance	Decryption time increases sharply with key size, creating latency issues.

Dimension	Finding
Algorithmic Comparison	RSA lags behind ECC and AES; best used in hybrid key exchange protocols.
Vulnerability Frequency	Peaked in 2021; decline suggests adaptation or shift to more secure methods.

Such evidence makes the case even more effective in favor of hybrid cryptographic systems, where the RSA signature is used to authenticate a request, and any symmetric cipher like AES would be used to transfer the data, particularly in an IoT and mobile environment.

5. Conclusion

The given RSA cryptographic algorithms analysis revealed not only the timelessness of the method and RSA but also the constantly changing demerits of the method regarding the contemporary communication networks. The outcomes justify that RSA continues to be the core of authentication process, key exchange and digital signature- the key components of the security used mainly in web based protocols such as the SSL/TLS and PKI infrastructure. Nevertheless, its growing calculations requirements particularly when decrypting with long key length pose significant scalability as well as performance drawbacks in resource-limited or low-latency settings; e.g. mobile devices and Internet of Things (IoT). The comparative performance testing also zeros-in to the fact that RSA is no longer the fastest algorithm compared to newer algorithms such as ECC and AES, which provide faster encryption and decryption times but are just as secure. More to this, the statistics of consecutive years exposed to RSA associated vulnerabilities is an indication of strong necessity to embrace the concept of flexible approaches to security and dynamism in cryptographic resilience preparedness. All of this, in combination, argues the relevance to shift towards hybrid cryptographic systems, as well as to study the possibilities of using post-quantum cryptographic encryption to handle the emerging risk presented by the power of computing paradigm. Although RSA is no longer a safe solution alone, it still remains critical in its strategic implementation with technologies that are more scalable and faster in case of sustainable digital communication security in the future.

References

1. Banerjee, S. (2024). Exploring Cryptographic Algorithms: Techniques, Applications, and Innovations. *International Journal of Advanced Research in Science, Communication and Technology*, 607-620.

2. Ramakrishna, D., & Shaik, M. A. (2024). A Comprehensive analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges. *IEEE Access*.

3. Naeem, S. (2023). Network security and cryptography challenges and trends on recent technologies. *Journal of Applied and Emerging Sciences*, *13*(1), 01-08.

4. Soomro, S., Belgaum, M. R., Alansari, Z., & Jain, R. (2019, August). Review and open issues of cryptographic algorithms in cyber security. In *2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 158-162). IEEE.

5. Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks*, *27*(2), 1515-1555.

6. Gupta, B. B., Kalra, D., & Almomani, A. (Eds.). (2024). *Innovations in Modern Cryptography*. IGI Global.

7. Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. *Internet of Things*, *22*, 100759.

8. Gade, D. (2015). Latest Innovations in Networking and Communications Technologies. In *Conference Proceedings of International Conference on Emergence of India as a Global Economy: Challenges and Opportunities* (Vol. 8, No. 1, pp. 55-57).

9. White, R., & Banks, E. (2017). *Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks*. Addison-Wesley Professional.

10. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. https://doi.org/10.1145/359340.359342

11. Kaur, R., & Kaur, P. (2020). A review of RSA algorithm for network security. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 7(4), 456–460.

12. Singh, S., & Supriya. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, 67(19), 33–38. https://doi.org/10.5120/11461-6784