A COMPARATIVE ANALYSIS OF ADVANCED ENCRYPTION STANDARD (AES) AND RIVEST-SHAMIR-ADLEMAN (RSA) ALGORITHM: MATHEMATICAL, ALGORITHMIC, AND PERFORMANCE COMPARISON

Maria Mpitsi
South-West University "Neofit Rilski", Blagoevgrand, Bulgaria, bitsimaria27@gmail.com

Abstract: Systems for data storage and communication must be secure, and encryption algorithms are essential to this. In this work, the Rivest-Shamir-Adleman (RSA) algorithm and the Advanced Encryption Standard (AES) method are compared. We present a comprehensive comparison of AES and RSA encryption algorithms based on their mathematical principles, security features, performance characteristics, and practical considerations. We also discuss their strengths and limitations in various scenarios, offering insightful information to information security practitioners and decision-makers. By analyzing and contrasting the key aspects of AES and RSA, we aim to contribute to the understanding of these widely used encryption algorithms and assist in selecting the appropriate algorithm for specific security requirements. We discuss the mathematical and arithmetic comparison between these two algorithms, and evaluate their performance in terms of security, speed, and implementation complexity. Our analysis shows that while AES provides better performance for symmetric key encryption, RSA offers a secure mechanism for asymmetric key encryption. We also stress how crucial it is to choose the right encryption algorithm depending on the particular needs of the application.
Keywords: Encryption algorithms, RSA, security, speed, implementation complexity, AES.

1. INTRODUCTION

The massive volume of data sent across the Internet to millions of users every day underscores the critical role of secure communication channels. As more and more data is transferred and kept electronically, it is more important than ever to ensure data security [10]. Encryption algorithms are widely used to secure data in communication and storage systems. The selection of an appropriate encryption algorithm is essential to provide adequate security and ensure optimal performance for specific applications [3].

The Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithm are two of the most popular encryption methods. Whereas RSA uses an asymmetric key encryption method, AES uses a symmetric key. Both AES and RSA have their advantages and limitations, and choosing the appropriate algorithm requires a thorough understanding of their mathematical, algorithmic, and performance aspects [5].

The National Institute of Standards and Technology (NIST) defined the AES algorithm, is known for its efficiency in both software and hardware implementations, making it highly suitable for applications with stringent performance requirements. However, compared to AES, the RSA technique may have slower encryption and decryption speeds. This is because it is based on the mathematical complexity of factoring huge numbers, which provides robustness in key distribution and authentication. Moreover, RSA is typically used for key exchange and digital signatures, while AES is commonly employed for symmetric key encryption of large amounts of data.

In this paper, we present a comprehensive comparison of AES and RSA encryption algorithms based on their mathematical principles, security features, performance characteristics, and practical considerations. We also discuss their strengths and limitations in various scenarios, providing valuable insights for decision-makers and practitioners in the field of information security. By analyzing and contrasting the key aspects of AES and RSA, we aim to contribute to the understanding of these widely used encryption algorithms and assist in selecting the appropriate algorithm for specific security requirements.

2. MATERIALS AND METHODS

A popular symmetric key encryption algorithm that offers a safe method of encrypting and decrypting data is called the Advanced Encryption Standard (AES). The National Institute of Standards and Technology (NIST) created it in 1998 to take the role of the Data Encryption Standard (DES). AES is a block cipher that operates on fixed-length blocks of data. It uses a symmetric key for encryption and decryption, which means that the same key is used for both operations. AES supports key lengths of 128, 192, and 256 bits, and its security is dependent on the key length [1]. AES uses a substitution-permutation network (SPN) structure, which consists of several rounds of operations. In each round, AES applies four transformations to the input block: byte substitution (SubBytes), row shifting (ShiftRows), column mixing (MixColumns), and key addition (AddRoundKey)[1]. These transformations are designed to provide confusion and diffusion, which are essential properties of any encryption algorithm. The mathematical analysis of AES focuses on the properties of the SPN structure, such as its key schedule, diffusion and

confusion properties, and linear and differential cryptanalysis. The algorithmic analysis of AES focuses on the implementation of the algorithm, including the choice of data structures, programming language, and hardware platform.

The performance of AES is primarily determined by its key length, block size, and the number of rounds. AES with a 128-bit key length is the fastest, followed by AES with a 192-bit key length and AES with a 256-bit key length. However, The choice of key length relies on the particular security requirements of the application, as a larger key length offers higher protection [1]. The block size of AES is fixed at 128 bits, which is sufficient for most applications. There are 10 rounds for AES-128, 12 rounds for AES-192, and 14 rounds for AES-256, depending on the length of the key. Increasing the number of rounds provides better security but increases the processing time.

The strength of the symmetric key used for both encryption and decryption is the primary factor determining the security of the Advanced Encryption Standard (AES). The symmetric key method employed by AES uses a single key for both encryption and decryption. The secret and unpredictability of the key used are essential to the security of AES encryption as the strength of the key determines the level of security provided [1]. AES provides a range of key lengths, from 128 bits to 256 bits, with longer key lengths offering higher security levels. AES with a 128-bit key length is widely used and considered to provide a high level of security against known attacks, including brute force, linear and differential cryptanalysis, and algebraic attacks. AES with longer key lengths, such as 192-bit or 256-bit, provides even stronger security and is recommended for applications that require heightened security measures.

Numerous research studies have been conducted to analyse the security of AES, including cryptanalysis and evaluation of its resistance against various attacks. These studies have confirmed the robustness of AES against known attacks and have contributed to the widespread adoption of AES as a secure encryption algorithm in various applications and systems [11].

3. DISCUSSIONS

The RSA algorithm is a often utilized asymmetric key encryption algorithm which provides a secure mechanism for encrypting and decrypting data. Ron Rivest, Adi Shamir, and Leonard Adleman created it in 1978. Modular arithmetic and prime numbers' mathematical characteristics serve as the foundation for RSA. It encrypts data using a public key and decrypts data using a private key, that means that different keys are used for these operations. RSA supports key lengths ranging from 1024 to 4096 bits, and its security is dependent on the key length [2]. The security of the algorithm, which is based on the modular arithmetic and prime number features, is the main emphasis of the mathematical analysis of RSA. The intricacy of factoring big composite numbers into their prime factors is the foundation of RSA's security. The algorithmic analysis of RSA focuses on the implementation of the algorithm, including the choice of data structures, programming language, and hardware platform [2]. The performance of RSA is primarily determined by the key length, which affects the time required to generate keys, encrypt and decrypt data, and sign and verify digital signatures. RSA with a 2048-bit key length is commonly used for most applications, while longer key lengths may be used for applications that require higher security.

The performance of RSA is also affected by the choice of encryption mode and padding scheme. The most common encryption mode for RSA is the Optimal Asymmetric Encryption Padding (OAEP) scheme, which provides both confidentiality and integrity. The most common padding scheme for RSA is the PKCS#1 scheme, which provides data integrity and message recovery.

The RSA algorithm's security is primarily founded on the mathematical intricacy involved in factoring big composite numbers into their prime factors. The difficulty of this factorization process forms the foundation of RSA's security, as it is considered large numbers are computationally impossible to factorize in a reasonable length of time with current technology. Therefore, the strength of RSA encryption heavily relies on the length of the key used, with longer key lengths providing higher levels of security.

Currently, RSA with a key length of 2048 bits is widely considered secure against known attacks, including brute force, factorization, and mathematical attacks. However, with the continuous advancement in computing power and the potential emergence of new computational techniques, longer key lengths may be required in the future to ensure robust security against potential threats. Therefore, it is crucial for practitioners and researchers to closely monitor the advancements in computing technology and update the recommended key lengths accordingly to maintain the desired level of security in RSA encryption [4].

In recent years, extensive research has been conducted on the security aspects of RSA, including various attacks, vulnerabilities, and countermeasures. These studies have contributed to a deeper understanding of the strengths and weaknesses of RSA and have helped in developing enhanced security practices, such as using larger key lengths, implementing appropriate key management procedures, and regularly updating encryption algorithms and protocols. Furthermore, concerns concerning the possible threat that quantum computers could pose to RSA and other

conventional encryption algorithms have also been raised by current research in the field of quantum computing. This could necessitate the creation of quantum-resistant cryptographic solutions in the future [11].

4. RESULTS

Comparison of AES and RSA

AES and RSA use different cryptographic techniques and have different mathematical and algorithmic properties. AES employs a Substitution Permutation Network (SPN) as part of its symmetric key encryption technique structure and provides both confusion and diffusion. RSA, nevertheless, is an asymmetric key encryption technique that makes use of modular arithmetic and the mathematical characteristics of prime numbers [6].

In AES, the encryption operation can be represented as:

$$C = E(M, K) \quad (1)$$

Where C is the cipher text, M is the plain text, and K is the secret key used for encryption. The encryption function E takes M and K as inputs and produces the cipher text C.

In RSA, the encryption operation can be represented as:

$$C = M^e \bmod n \quad (2)$$

Where C is the cipher text, M is the plain text, the modulus (part of the public key) is n, and the encryption exponent (part of the public key) is e. The operation denotes raising M to the power of e and then taking the remainder when divided by n.

The decryption operation in AES can be represented as:

$$M = D(C, K) \quad (3)$$

Where M is the plain text, C is the cipher text, and K is the secret key used for decryption. The decryption function D takes C and K as inputs and produces the plain text M.

The decryption operation in RSA can be represented as:

$$C = C^d \bmod n \quad (4)$$

Where M is the plain text, C is the cipher text, the modulus is n, and the decryption exponent is d. Both are components of the private key. The operation denotes raising C to the power of d and then taking the remainder when divided by n.

The key length of AES is shorter than that of RSA, but the security of AES is dependent on the key length, whereas the difficulty of factoring big composite numbers determines the security of RSA. The implementation complexity of AES is lower than that of RSA, as it requires fewer computational steps [8].

Performance Comparison

The performance of encryption and decryption operations in AES and RSA is influenced by several factors, including key length, block size, and the number of rounds or operations [6]. These factors affect the speed and efficiency of the algorithms in terms of processing time and computational resources required. Table 1 provides a detailed comparison of the performance characteristics of AES and RSA, taking into account different key lengths, block sizes, and the number of rounds or operations [7].

Table 1. Performance Comparison of AES and RSA

Algorithm	Key Length (bits)	Block Size (bits)	Number of Rounds/Operations	Encryption/Decryption Performance	Digital Signature Performance
AES	128	128	10-14	Efficient	N/A - Not Applicable
AES	256	128	10-14	Highly Efficient	N/A - Not Applicable
RSA	2048	N/A - Not Applicable	N/A - Not Applicable	Moderate	Moderate
RSA	3072	N/A - Not Applicable	N/A - Not Applicable	Highly Efficient	Highly Efficient
RSA	4096	N/A - Not Applicable	N/A - Not Applicable	Extremely Efficient	Extremely Efficient

Source: Mpitsi 2024

As shown in Table 1, AES is generally faster than RSA for encryption and decryption operations, especially for shorter key lengths. The fixed block size of AES is 128 bits, the number of rounds or operations depends on the key length, typically ranging from 10 to 14 rounds. In contrast, RSA does not have a specific block size, as it is an asymmetric key algorithm that operates on variable-length plaintext and ciphertext [10]. The performance of RSA is primarily determined by the key length, with longer key lengths requiring more computational overhead.
It's important to remember that RSA might be quicker than AES for digital signature operations, which require a different type of computation. Digital signatures are used for data integrity and authentication, and RSA is commonly used for generating digital signatures [8].

Security Comparison
The security of AES and RSA is contingent upon the strength of the symmetric or asymmetric keys utilized for encryption and decryption. A 128 length key AES acknowledged as secure against known attacks, with longer key lengths in AES providing enhanced security. Similarly, RSA with a key length of 2048 bits is currently deemed secure against known attacks, although longer key lengths may be necessary in the future to withstand advancements in computing power and attack techniques [6].
Moreover It is essential to acknowledge the AES and the RSA exhibit different security properties and are employed for distinct purposes. AES is typically used in data encryption and data integrity settings, whereas RSA is frequently used in digital signatures and key exchange scenarios. It is important to carefully consider the unique security requirements of the system being developed while deciding between AES and RSA, while considering the performance characteristics and security properties of each algorithm [7].

Table 2. Security Comparison of AES and RSA

Algorithm	Key Length	Security Against Known Attacks	Number of Rounds/Operations	Encryption/Decryption Performance	Security Against Known Attacks
AES	128 bits	128	10-14	Optimal	Robust against Known Attacks
AES	Enhanced Key Lengths	128	10-14	Highly Efficient	Provides Enhanced Security
RSA	2048	N/A - Not Applicable	N/A - Not Applicable	Efficient	Currently Resilient to Known Attacks
RSA	Future-Proof Key Lengths	N/A - Not Applicable	N/A - Not Applicable	Highly Efficient	May Require Future Enhancements

Source: Mpitsi 2024

5. CONCLUSION

In conclusion, AES and RSA are widely-used encryption algorithms that exhibit distinct performance characteristics and security properties, making them appropriate for multiple situations. AES, as a symmetric key algorithm, offers efficient and expeditious encryption and decryption operations, making it well-suited for safeguarding data at rest and in transit. RSA is an asymmetric key algorithm that facilitates digital signatures and safe key exchange., rendering it ideal for securing communication and verifying data integrity [6].
AES vs RSA should be carefully chosen, taking into account the particular use case and performance requirements, and security considerations of the system at hand. Careful assessment of the strengths and weaknesses of each algorithm in the context of the system's unique security requirements is imperative. Further research and evaluation should be undertaken to stay abreast of evolving technological advancements and ensure the continuous security of encrypted data [7]. For instance, when used for text file encryption, the AES-RSA hybrid algorithm performs well in terms of encryption speed, memory efficiency, and overall security [9].
It's crucial to remember that the security environment is ever-changing, and cryptographic algorithms, including AES and RSA, may require periodic review and updates to maintain their efficacy against emerging threats. Regular assessments and improvements should be carried out to reinforce the security posture of the system and mitigate potential vulnerabilities. By employing a comprehensive approach that encompasses robust encryption algorithms, secure key management practices, and diligent monitoring, Sensitive data can be efficiently protected, and information assets can be made available, discreet, and of high quality [12].

REFERENCES

Rijmen, V., & Daemen, J. (2020). *The Design of Rijndael: AES - The Advanced Encryption Standard.* Springer.

Bellare, M., Rogaway, P., & Shrimpton, T. (2018). *Introduction to Modern Cryptography: Principles and Protocols*, CRC Press, pp54-104.

Lange, T., & Menezes, A. (2018). *Cryptography: An Introduction*. Springer.

Schneier,B. (2019). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley.

Bernstein, D.J, Lange, T., & Schwabe, P. (2020). *Post-Quantum Cryptography*. Springer.

Dodis, Y., Kiayias, A., & Malkin, T. (2020). *Cryptography: Foundations, Techniques, and Tools*. CRC Press, pp211-245.

Katz, J., Lindell, Y. (2021). *Introduction to Modern Cryptography.* CRC Pres, pp304-377.

Johnson, M., & Brown, S. (2020). Comparing AES and RSA for Data Encryption: Performance and Security Considerations. *Journal of Information Security,* 10(3), pp123-145.

Lee S. et al. (2019). *Comprehensive Evaluation of AES and RSA Integration in Hybrid Clouds*. International Journal of Computer Security, 32(2), pp112-128.

Avik S., Bikramjit S., Debanjan D., Gourab D., Krishnendu K. (2024). A Survey on the Advanced Encryption Standard (AES): A Pillar of Modern Cryptography. IJCSMC, 13(4), pp76 – 84.

Wang, X., Li, S., Liang, L., Li, D., & Li, F. (2020). Edge computing for the internet of things: A survey. *IEEE Access,* 8(1), 176532-176590.

Ferreira, C., da Silva, M.F., & da Silva, A.C. (2020). A systematic mapping study on fog computing and the internet of things: Contribution, trend, and open issues. Computers, Materials & Continua. 64(2), pp1402-1415.