


## Comparative Analysis of the RSA and AES Algorithms as Data Cryptosystems

[www.doi.org/10.62341/mhmc3027](http://www.doi.org/10.62341/mhmc3027)

Musab A. Aldali<sup>1</sup>, Hesham Saleh Almssmari<sup>2</sup>, Mustafa M. Salama<sup>3</sup>

<sup>1,2,3</sup> College of technical Sciences - Derna

<sup>1</sup>musabaldalii.1984@gmail.com 

<sup>2</sup>hso.std82@gmail.com

<sup>3</sup>mostafasalama2011@gmail.com

### Abstract

Data encryption IS defined as a method of transforming information into a coded format, ensuring that only authorized individuals can successfully decode and comprehend the content. In addition, cryptography is principally categorized into two distinct types: symmetric key cryptography and asymmetric key cryptography.

In this research, we conduct a comparative analysis of two cryptographic systems: RSA (asymmetric) and AES (symmetric key), specifically evaluating their performance in data encryption for point-to-point communications. The analysis focuses on the speed of file encryption and decryption as well as the length of the encrypted data. Experimental results reveal that both RSA and AES are robust encryption algorithms; however, AES outperforms RSA in terms of both encryption and decryption speeds while also producing a smaller remaining data size that could not be encrypted due. Finally, the paper has outlined strengths and weaknesses of reviewed algorithms which make it possible to effectively put these algorithms together in protecting information and satisfying the security needs of applications.

**Keywords:** Encryption – Decryption– Cryptosystems– Encryption Algorithm- RSA– AES.

## دراسة تحليلية مقارنة بين خوارزميتي RSA و AES كأنظمة تشفير للبيانات

مصعب عبدالله الدالي<sup>1</sup>، هشام صالح المسماري<sup>2</sup>، مصطفى محمود<sup>3</sup>  
<sup>1، 2، 3</sup> كلية العلوم التقنية - درنة

### الملخص

يُعرّف تشفير البيانات على أنه طريقة لتحويل المعلومات إلى صيغة مشفرة، مما يضمن أن الأفراد المصرح لهم فقط هم من يمكنهم فك تشفير المحتوى وفهمه بنجاح. بالإضافة إلى ذلك، يتم تصنيف التشفير بشكل أساسي إلى نوعين متميزين: التشفير بالمفتاح المتماثل والتشفير بالمفتاح غير المتماثل. في هذا البحث، نجري تحليلاً مقارناً لنظامي تشفير RSA للتشفير بالمفتاح غير المتماثل و AES للتشفير بالمفتاح المتماثل، وتحديدًا تقييم أدائهما في تشفير البيانات للاتصالات من نقطة إلى نقطة. يركز التحليل على سرعة تشفير الملفات وفك تشفيرها بالإضافة إلى طول البيانات المشفرة. وقد كشفت النتائج أن كلاً من RSA و AES تعدّ خوارزميات تشفير قوية، إلا أن AES تتفوق على RSA من حيث سرعة التشفير وفك التشفير مع فاقد أقل في حجم البيانات التي لا يمكن تشفيره. أخيراً، أثبتت الورقة البحثية أنه من الممكن دمج كلتا الخوارزميتين بفعالية لحماية المعلومات وتلبية الاحتياجات الأمنية للتطبيقات.

الكلمات المفتاحية: التشفير - فك التشفير - أنظمة التشفير - خوارزمية التشفير - RSA - AES -

### 1. Introduction

In recent years, network security has emerged as a critical area of concern. Encryption has been identified as a pivotal solution, playing an indispensable role in safeguarding information systems. Multitudes of techniques are essential to protect shared data effectively. Primarily, it is imperative that data transmitted between sender and receiver within the network is encrypted utilizing established encryption algorithms inherent to cryptography.

Cryptographic algorithms, such as DES and AES, exhibit a range of key strengths. The Data Encryption Standard (DES) employs a single 64-bit key. In contrast, the Advanced Encryption Standard (AES) utilizes keys of varying lengths: 128 bits, 192 bits, or 256 bits (Prerna Mahajan et al., 2013).

The Rivest, Shamir, and Adleman (RSA) public key cryptosystem is widely recognized as milestone advancement in data encryption. Central to its acclaim is the fact that RSA is both an exceptionally efficient algorithm for public key data encryption and an effective medium for key distribution. The introduction of the RSA algorithm has enabled the design and implementation of numerous applications that were previously impractical with symmetric private algorithms. For instance, the secure transmission of keys between users via a public channel is typically accomplished using RSA rather than symmetric algorithms. Data encrypted with an RSA public key can be decrypted only by the corresponding private key of the recipient, not with their own public key. Although RSA is algorithmically straightforward, our research indicates that it has several inherent limitations (Nedal Tahat et al., 2020).

## 2. Background of Data Encryption

Cryptography can be broadly categorized into symmetric key cryptography and asymmetric key cryptography. In symmetric key systems, a single secret key is used for both encryption and decryption processes within communications. Conversely, asymmetric key cryptography employs different keys for encrypting and decrypting data; secure communication is achieved through public-key infrastructure where only the corresponding private key can decipher messages initially encoded with its matching public counterpart.

The protection of critical information, including passwords, account details, messages, algorithms, and data, has consistently been a focal point for researchers. Data encryption represents the methodology of encoding such information to ensure that only individuals with authorized access can decode and comprehend it effectively (Nedal Tahat et al., 2020). Therefore, Cryptography presents itself as a comprehensive and reliable solution to the specific challenge of data

encryption. In this section, we will explore some of the fundamental principles behind asymmetric and symmetric key cryptography, with particular emphasis on RSA (a cryptosystem used for data encryption) and AES (a symmetric cryptographic algorithm used for data encryption).

### 3. Overview of AES

#### 3.1 Understanding Basics

AES stands for Advanced Encryption Standard. It is a Federal Information Processing Standard announced in 2001 by NIST after some competition it held for the standard of the encryption algorithm. AES is, thus, one of the most frequently used techniques of encryption due to its high efficiency and simplicity, hence a highly secure algorithm. AES is a symmetric block cipher that uses the same key for encryption and decryption. It has been found that AES differs from the DES. In AES, the block and key size may be chosen independently from 128, 160, 192, 224, 256 bits, whereas in the case of DES, it is 56 bits. AES differs from DES because it doesn't use the Feistel network. The Feistel structure normally uses half of the data block to modify the remaining half of the data block, after which these halves are swapped. While in AES, the whole data block is processed in parallel during each round through substitutions and permutations. It has been found that symmetric cipher is divided into two major categories: Stream cipher and Block cipher (Puneet Kumar, 2016).

#### 3.2 Encryption and Decryption Process

AES algorithm is among the most prevalent and widely-used symmetric block cipher algorithms globally. This algorithm has a distinctive structure designed for encrypting and decrypting sensitive data, applicable in both hardware and software across the world. The AES encryption method provides robust security, making it exceedingly challenging for hackers to access the encrypted data. To date, there is no documented evidence of this algorithm being compromised (Ako Abdullah, 2017). As shown in table (1),

### 3.4 key Block Size

AES supports three key sizes: 128-bit, 192-bit, and 256-bit; each variant operates with a 128-bit block size.

**Table 1. Comparison of block size, key length and number of rounds of AES keys**

Type	Block Size Nbwords	Block Size Nkwords	Number of Rounds Nr
AES-128 bits key	4	4	10
AES-192 bits key	4	6	12
AES-256 bits key	4	8	14

Key Expansion generates a Key Schedule used in Cipher and Inverse Cipher procedures. The Cipher and Inverse Cipher are composed of specific numbers of rounds. In the AES algorithm, the number of rounds to be performed during the implementation of the algorithm is a function of the key length. Since this is the only stage that uses the secret key, round 0 of the encryption and decryption process starts with this round. Round 0 only performs the Add Round-Key transformation on the state array and offers security (Nagarjun Bhat, 2012).

### 4. Overview of the RSA Algorithm

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman introduced a groundbreaking cryptographic algorithm designed to supplant the less secure National Bureau of Standards (NBS) algorithm. Notably, RSA incorporates both a public-key cryptosystem and digital signatures as shown in figure (1).

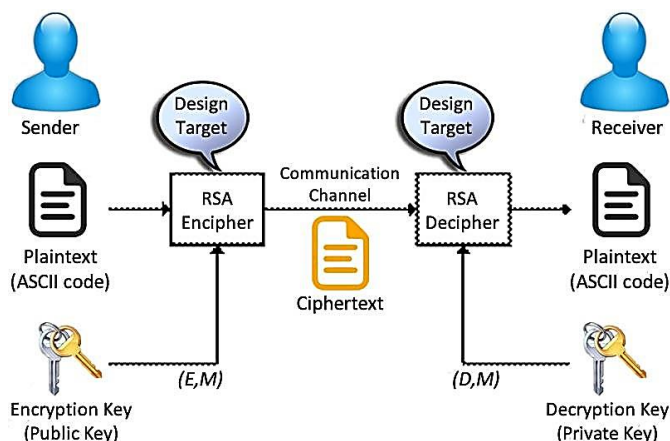


Figure (1) RSA algorithm structure (Hüseyin & Resul. (2015))

The inception of RSA was heavily inspired by the earlier theoretical frameworks laid out by Diffie and Hellman, who had conceptualized such an algorithm but did not bring it to fruition. Unveiled at a time when electronic email communication was poised for rapid growth, RSA integrated two pivotal innovations:

1. **Public-Key Encryption:** This paradigm eliminates the necessity of using couriers to deliver encryption keys via secure channels prior to message transmission. In the RSA system, encryption keys are made publicly available while decryption keys remain confidential – ensuring that only individuals possessing the correct decryption key can access an encrypted message. Each user possesses a unique pair of encryption and decryption keys crafted in such a manner that deducing the decryption key from its corresponding public encryption key is infeasible.

2. **Digital Signatures:** To ensure message authenticity and integrity, RSA employs digital signatures, which allow recipients to verify that messages indeed originate from their purported senders (signature verification). Utilizing the sender's private decryption key generates these signatures; subsequently, anyone can authenticate them with the sender's public encryption key. This mechanism precludes forgery and prevents signatories from repudiating their signed messages later on (Aradhana Sahoo et al., 2009).

## 5. Comparative Analysis and Key Differences

When conducting a comparative analysis between RSA and AES, the researchers have reviewed many articles that investigate the criteria of comparison considering performance, security, key management and flexibility of both algorithms.

### 5.1 Performance Comparison

In symmetric key cryptography, to which RSA belongs, the key length remains mainly unaltered, while the advent of the RSA algorithm increases the key length to increase its security-intense tasks. It is used to encrypt or decrypt the message having to use less complex codes, which are faster. With the AES algorithm, both the encryption process and the decryption process are fast, and AES is therefore more suitable in encrypting short and long messages. Due to the fast nature, it is utilized to encrypt huge streams of text at a supersonic speed (Priyadarshini Patil et al., 2016).

Each of the cited properties leads to RSA being computationally expensive; thus, extra time has to be utilized while encrypting and decrypting a document. Further, RSA is slow because it requires more computational memory and processing capability, compared with a symmetric key algorithm. Due to the slow nature of the RSA algorithm, RSA is utilized to encrypt short messages, typically the private or public keys used to initiate another system for exchanging the messages between the two ends (Prerna Mahajan et al., 2013).

To utilize RSA, the algorithm has to generate a pair of numbers that work exceptionally well in the performance of the encryption and decryption process for the particular message it desires to encrypt and send. Such numbers are created upon the two prime numbers by the algorithm, which generates the encryption and decryption keys. It might require to be modified, for practical use, and might have to perform prime factorization, which tends to be intense and might be time-consuming, especially in a scenario when the key lengths are large, which makes it time-consuming. The decryption process of RSA is significantly slow compared to the encryption (Abdullah Al Hasib et al., 2008).

The RSA algorithm tends to increase in terms of the complexities it undergoes in the whole encryption and decryption processes. It is

limited in terms of the lengths of message it can encrypt. To enlarge or increase the length of message it can encrypt, without having to impact on its performance, its public and private key lengths increase, corresponding to the message length, thus becoming increasingly difficult to implement. On the other hand, AES can utilize any key length to encrypt any length of message, and its performance speed is not negatively impacted by the message length, considered fast. (FHMS Al-Kadei et al., 2020)

The nature and roles of RSA and AES are utterly distinct. While RSA is a widely used public key cryptography algorithm, AES is a symmetric key block cipher algorithm. RSA utilizes two prime numbers for the generation of a public and private number pair, which is utilized in the encryption and decryption of a message, both found to be slow. The primary process in RSA is prime number factorization, which is the core of RSA. AES is a symmetric key system and utilizes identical keys in both sides of the process, either in the encryption or decryption process. Its encryption and decryption processes are incredibly fast. This is due to AES utilizing a table of elements which it utilizes in generating keys for either encryption or decryption, and then, after which it uses an algorithm, Advanced Encryption Standard Algorithm, in the encryption and decryption process, which has since been mathematically and crypt analytically, for most part optimized or streamlined. Its process is much simpler.

## 5.2. Security Comparison

Comparatively, RSA implementation is slower than AES implementation, and more intricacies have been involved in the encryption and decryption because of the nature of the RSA algorithm, which is computationally intensive than AES. The appropriate method of selecting data encryption methodologies is to always match the high entropy key size based on broad knowledge of the security considerations, which is the key size, the level of security assigned to the data being encrypted, the application in which the key is used, and the available hardware. That way, the benefits of larger key sizes can be attained. However, although the RSA algorithm has acceptance all the time, where two public keys



are exchanged to set up a 'symmetric session key' for a much faster algorithm, the RSA algorithm's effective key size also needs to be increased. After the researchers study the simulation results, one common conclusion they can draw is that RSA implementation is slower and more complex on-chip than AES implementation. (R Imam et al., 2022)

The intricacies of RSA and AES cryptographic algorithms primarily stem from their potential to render unauthorized decryption and data access virtually impossible. Techniques such as threshold analyses, sensitivity analysis, and evaluating the computational power available for attacks are commonly employed to identify scenarios that may simplify this task.

A substantial body of research highlights that RSA is inherently a slow algorithm due to its reliance on large keys for secure operations. This inherent complexity in encryption and decryption processes makes it inefficient for handling bulk data encryption. Additionally, there have been assumptions suggesting that increasing key length coupled with utilizing faster hardware could mitigate memory encryption duration when using RSA; however, empirical evidence across various application contexts refutes this notion. Conversely, AES exhibits significantly higher performance levels—approximately four times faster than Triple DES and roughly 64 times swifter compared to RSA (Abdullah Al Hasib et al., 2008).

## 6. Discussion

According to what has been recounted, it's pretty clear that RSA represents an asymmetric, public-key encryption algorithm. Asymmetric refers to the fact that it makes use of a pair of keys: a public key used in encryption and a private key used in decryption. It finds key applications in digital signatures, key exchange, and establishment of secure channels of communications. However, AES represents an algorithm for symmetric encryption, otherwise called a secret-key algorithm. It contains a single key for both encryption and decryption. Owing to its high speed, it is mainly applied in the bulk encryption of data. Table (2) shows key

differences between RSA and AES in term of speed, key size and the level of security.

**Table 2. Key differences between RSA and AES**

Feature	RSA	AES
Key Type	Asymmetric (Public/Private)	Symmetric (Single)
Speed	Slow (especially decryption)	Fast
Key Size	Typically 1024, 2048, or 4096 bits	128, 192, or 256 bits
Security	Based on the difficulty of factoring large numbers	Based on substitution and permutation

## 6.2 Key Distribution

**6.2.1 RSA (Asymmetric Encryption):** RSA involves a key pair: An RSA public

key and an RSA private key.

- Key Distribution: A public key may be freely distributed to any entity. It is used to encrypt data. The private key has to be kept secret and is used for decryption.
- Challenge: Distribution of the private key securely is crucial. In case of revealing the private key, this will compromise the whole system.

**6.2.2 AES (Symmetric Encryption):** AES uses just one single secret key, with the same keys in both encryption and decryption processes.

- Key Distribution: Most importantly, the key has to be securely shared between sender and receiver prior to the commencement of communication. This itself presents the major challenge associated with symmetric encryption.
- Methods:
  - Pre-Shared Key: The key may be pre-established through a secure channel.
  - Key Exchange Protocols: Algorithms like Diffie-Hellman or RSA can be used to establish a shared secret key across an

insecure channel. This is made secure using symmetric encryption in a hybrid approach.

### 6.3 Key Management Considerations

- Key Length: Longer keys provide stronger security but impact performance.
- Key Generation: Keys should be generated using cryptographically secure random number generators.
- Key Storage: Private keys must be stored securely.
- Key Rotation: Regularly changing keys helps mitigate risks if a key is compromised.
- Key Distribution: Secure methods for distributing keys are essential.

Consequently, RSA has a simpler form of key distribution. It's slow and less efficient for huge volumes of data. AES is faster, but this requires secure sharing of keys, which again is the problem. Hybrid encryption combines the strength of both by using RSA for exchanging the key and AES for data encryption.

### 6.4 Comparative Analysis and Critical Findings

AES and RSA are two pillars of modern cryptography. Table (3) shows the choice between the two depends on the specific requirements of the application. For bulk data encryption, AES is the preferred choice, owing to its speed and efficiency. On the other hand, RSA finds prominent usage in key exchange and digital signatures.

**Table 3. Summary Table**

Feature	RSA	AES
Type	Asymmetric (Public-key)	Symmetric (Secret-key)
Performance	Slower, especially for decryption. Suitable for small amounts of data or infrequent encryption.	Faster, suitable for large amounts of data and high-throughput applications.
Security	Considered secure for appropriate key lengths, but susceptible to quantum attacks in the future.	Provenly secure, no known practical attacks for standard key sizes.

Key Management	Complex due to the need to securely distribute public keys.	Simpler as only one key needs to be shared securely.
Flexibility	Versatile for various cryptographic operations (encryption, decryption, digital signatures).	Primarily used for bulk data encryption.

The main differences between the RSA and AES encryption algorithms were as follows: RSA is an asymmetric encryption algorithm that uses two keys for encryption (a public key and a private key), while AES is a symmetric encryption standard. RSA encryption is inherent, while AES encrypts in blocks. This means that for each encryption, we need a plaintext block of the same size as the key of the encryption algorithm.

RSA can be implemented on any computer with a processor that supports the Euclidean algorithm, while AES is typically found in specialized hardware.

RSA is based on modular arithmetic and its security relies on well-studied mathematical problems such as the factorization of prime numbers and the ECDLP (Discrete logarithm problem on elliptic curves). The security degree of these problems is widely accepted by the cryptographic community. However, factorizing a number takes much longer than discovering a prime number with a certain number of digits, even with sieve computers. This is because the required resources increase exponentially in both problems. RSA is much slower than AES because it does not make any computational assumptions about the key that an adversary is trying to break.

The small key sizes for RSA (1024 bits) that are used can be broken by ordinary computers. Even increasing the key size to 4 times, to 2048 bits, a quantum computer with many qubits can break RSA. The use of large key sizes could provide some security, but the decision on the best key size to be used is a trade-off between security and performance. The findings also revealed that a combination of RSA and AES could be effectively utilized within the realm of information protection. However, the choice between these algorithms should depend on the specific context of their application: RSA demonstrates superior performance with small-

sized data, such as in encrypting symmetric keys, while AES is optimally suited for encrypting large volumes of data. Finally, we hope that we have provided a concise and clear summary of the algorithms' performance metrics within comparison process.

## 9. Conclusion

This work aimed at analyzing the RSA and AES encryption algorithms in depth, discussing the problems that arise when implementing these standards. In this context, we have also introduced the reviewer to the most important characteristics of symmetric and asymmetric cryptosystems.

Finally, we would recommend the hybrid encryption to include both algorithms, and often it is used as follows:

- Key exchange: Any symmetric-encryption key is securely exchanged using RSA.
- Data encryption: Real data is encrypted with AES using the shared symmetric key.

This approach provides the security features of RSA key exchange along with the efficiency of AES for data encryption.

## 9. References

- A Sahoo, P Mohanty, PC Sethi - Intelligent Systems: Proceedings of ICMIB ..., 2022 - Springer. Image encryption using RSA algorithm. Researchgate.net - Cited by 16.
- Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. *Cryptography and Network Security*, 16 (1), 11 – Cited by 310.
- Al Hasib, A., & Haque, A. A. M. M. (2008, November). A comparative study of the performance and security issues of AES and RSA cryptography. In 2008 third international conference on convergence and hybrid information technology (Vol. 2, pp. 505-510). IEEE – Cited by 199.
- Bhat, Nagarjun & Sridhar, V. & Nn, Shylashree. (2012). FPGA IMPLEMENTATIONS OF ADVANCED ENCRYPTION STANDARD: A SURVEY.

- FHMS Al-Kadei, HA Mardan... - 2020 6th International ..., 2020 -  
ieeexplore.ieee.org. Speed up image encryption by using RSA  
algorithm. researchgate.net - Cited by 25.
- Hüseyin, Bodur & Resul, Kara. (2015). Secure SMS  
Encryption Using RSA Encryption Algorithm on Android  
Message Application.  
Sent from my iPhone. www.researchgate.net/figure/RSA-  
algorithm-structure\_fig2\_298298027 . Last seen: 16/07/2024  
12:02 pm.
- Kumar, P., & Rana, S. B. (2016). Development of modified AES  
algorithm for data security. Optik, 127(4), 2341-2345 – Cited by  
152.
- Mahajan, P., & Sachdeva, A. (2013). A study of encryption  
algorithms AES, DES and RSA for security. Global journal of  
computer science and technology, 13(15), 15-22 - Cited by 521.
- N Tahat, AA Tahat, M Abu-Dalu... - International Journal of ...,  
2020 - academia.edu. A new RSA public key encryption scheme  
with chaotic maps. academia.edu - Cited by 20.
- Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A  
comprehensive evaluation of cryptographic algorithms: DES,  
3DES, AES, RSA and Blowfish. Procedia Computer Science,  
78, 617-624 – Cited by 468.
- R Imam, F Anwer, M Nadeem - International Journal of Information  
..., 2022 - Springer. An effective and enhanced RSA based  
public key encryption scheme (XRSA). researchgate.net - Cited  
by 13.
- YK Kumar, RM Shafi - International Journal of Electrical and ...,  
2020 - academia.edu. An efficient and secure data storage in  
cloud computing using modified RSA public key cryptosystem.  
academia.edu - Cited by 33.