International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Comparative Study of AES, DES, and RSA for File Encryption Performance

Abhi Shah, Shyamal Jani, Vedant Sharma, Riya Jain, Kartik Hajela, Prof. Vijaysinh Jadeja

Department of Computer Engineering, Sal College of Engineering, Ahmedabad – 380060

ABSTRACT—

Encryption is a fundamental aspect of information se- curity, ensuring that sensitive data remains confidential and protected from unauthorized access. Among the various encryption algorithms available, AES (Advanced Encryption Standard), DES (Data En- cryption Standard), and RSA (Rivest–Shamir–Adleman) are widely used due to their distinct features and performance characteristics. This paper presents a comparative study of these three algorithms by analyzing their encryption and decryption performance on text files of varying sizes. Files ranging from small (1 KB) to large (10 MB) were generated with random content, and execution times were measured to evaluate efficiency. The results demonstrate significant differences in processing speed and scalability, with AES consistently outperforming DES in both encryption and decryption tasks, while RSA was limited to small file sizes due to its high computational overhead. The findings provide practical insights into selecting the most appropriate algorithm for different applications, highlighting AES as the preferred choice for large-scale file encryption and DES and RSA for specific legacy or key-exchange scenarios. This study contributes to a deeper understanding of the trade-offs between security and performance in file encryption, offering guidance for both academic research and real-world implementations.

***Keywords*—**File Encryption, AES, DES, RSA, Encryption Perfor- mance, Information Security, Comparative Study

1. Introduction

In today’s digital era, the volume of data being gener- ated, stored, and transmitted has grown exponentially across various domains such as finance, healthcare, communication, and cloud computing. With this rapid growth, ensuring the confidentiality, integrity, and security of sensitive informa- tion has become a critical concern. Encryption serves as a fundamental mechanism to protect data from unauthorized access by converting readable information into an unread- able format, which can only be restored using the correct decryption key. Among the widely used encryption algorithms, AES (Advanced Encryption Standard) has gained prominence for its high security, efficiency, and suitability for encrypt- ing large datasets. DES (Data Encryption Standard), though historically significant, has become less secure due to its shorter key length and susceptibility to brute-force attacks. RSA (Rivest–Shamir–Adleman), an asymmetric encryption algorithm, is commonly employed for secure key exchange and digital signatures rather than bulk data encryption due to its computational overhead. Evaluating the performance of these algorithms is essential because the encryption and decryption times can significantly impact system performance, especially when processing files of varying sizes. This study aims to provide a detailed comparative analysis of AES, DES, and RSA by measuring their execution times on text files ranging from small to moderately large sizes. By analyzing the performance differences, this research provides practical insights into the selection of suitable encryption algorithms based on data size and computational constraints, thereby contributing to more efficient and secure information handling in both academic research and real-world applications.

2. Data Description

For this study, three text files of varying sizes were gen- erated to evaluate the performance of AES, DES, and RSA encryption algorithms. The files were created with random ASCII characters to simulate generic textual data while ensur- ing reproducibility of results. The file sizes chosen represent different scales of data handling:

- **file_1KB.txt:** A small file of approximately 1 kilobyte, used to observe the performance on minimal data and to test the feasibility of RSA encryption.
- **file_1MB.txt:** A medium-sized file of around 1 megabyte, representative of typical document or report sizes.
- **file_10MB.txt:** A larger file of approximately 10 megabytes, designed to assess the scalability and effi- ciency of the algorithms on more substantial data.

These files were generated using Python scripts to ensure randomness and uniformity in data content. The variety in file sizes allows for a comprehensive evaluation of each algo- rithm's performance across small, medium, and large datasets, providing meaningful insights into their suitability for different real-world applications.

3. Methodology

The methodology followed in this study involves measuring the encryption and decryption performance of three widely used algorithms: AES, DES, and RSA. The steps are described below:

A. File Preparation

Three text files of different sizes (1 KB, 1 MB, and 10 MB) were generated with random ASCII characters to simulate generic textual data. The files were designed to cover small, medium, and large-scale scenarios for evaluating algorithm performance.

B. Encryption and Decryption

Python scripts were used to implement each encryption algorithm. For AES and DES, both encryption and decryption were applied to all three files. Due to RSA's computational complexity, encryption and decryption were performed only on the 1 KB file. The algorithms were tested using standard library implementations to ensure accurate and reliable perfor- mance measurements.

C. Performance Measurement

Execution times for encryption and decryption were recorded in seconds using Python's time module. Each operation was performed multiple times, and the average time was considered to reduce the effect of transient system fluctua- tions. The recorded times were then tabulated for comparative analysis.

D. Evaluation Metrics

The primary metric used in this study is the execution time (in seconds) for both encryption and decryption processes. This metric allows for a direct comparison of algorithm efficiency and scalability across different file sizes. The re- sults provide insights into the trade-offs between speed and computational overhead for each encryption method.

4. Results

A. Observations

- AES consistently exhibits the fastest encryption and decryption times across all file sizes, demonstrating its efficiency and suitability for large datasets.
- DES performs slower than AES, with noticeable increases in execution time for larger files, highlighting its limita- tions for modern applications.
- RSA encryption and decryption were only feasible for the 1 KB file due to its high computational overhead, making it unsuitable for large files and emphasizing its primary use in secure key exchange rather than bulk data encryption.
- Encryption and decryption times generally increase with file size, showing an approximately linear relationship for AES and DES.

B. Performance Table

The measured encryption and decryption times are summa- rized in Table I.

TABLE I

Encryption and decryption times for AES, DES, and RSA (in seconds).

File	Size (KB)	AES Enc	AES Dec	DES Enc	DES Dec	RSA Enc	RSA Dec
file_1KB.txt	1.0	0.000000	0.000000	0.000000	0.000000	0.004443	0.008428
file_1MB.txt	1024.0	0.009220	0.005231	0.027137	0.037768	-	-
file_10MB.txt	10240.0	0.048126	0.072379	0.324352	0.314376	-	-

C. Graphical Representation

The encryption and decryption times for AES and DES are visualized in Figure 1, highlighting the performance differ- ences between the two algorithms across different file sizes.

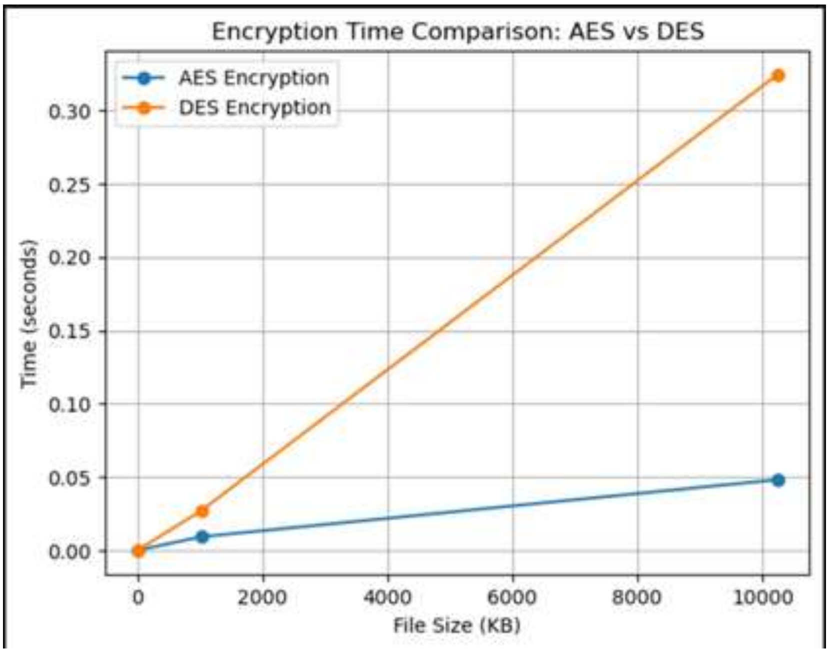

Fig. 1. Encryption and decryption times for AES and DES algorithms across different file sizes.

5. Discussion

The results indicate clear performance differences among AES, DES, and RSA encryption algorithms. AES consistently outperformed DES in both encryption and decryption tasks across all file sizes, confirming its reputation as an efficient and secure algorithm suitable for modern applications. The nearly linear increase in execution time with file size suggests that AES scales well, making it reliable for encrypting large datasets.

DES, while historically important, shows considerably slower performance, especially for larger files. This demon- strates its limitations for contemporary use, where high-speed processing and strong security are required. Although DES can still be used for legacy systems, it is no longer recommended for applications involving sensitive or high-volume data.

RSA was only applied to the smallest file due to its significant computational overhead. Its performance highlights why RSA is not practical for encrypting large files; instead, it is primarily used for secure key exchange, digital signatures, or encrypting small amounts of critical information.

Overall, the comparative analysis emphasizes that algo- rithm selection should consider both security requirements and performance constraints. AES is the most suitable choice for general-purpose file encryption, DES may be limited to legacy or educational use, and RSA remains specialized for asymmetric encryption tasks. The study provides practical guidance for developers and researchers to balance efficiency and security when implementing encryption solutions.

6. Conclusion

This study presented a comparative analysis of three widely used encryption algorithms: AES, DES, and RSA, focusing on their performance in encrypting and decrypting text files of different sizes. The results clearly demonstrate that AES

outperforms DES and RSA in terms of speed and scalability, making it the most efficient and practical choice for general- purpose file encryption. DES, although historically significant, is slower and less suitable for modern applications involving large datasets. RSA, being an asymmetric algorithm, is compu- tationally intensive and therefore only practical for small files or tasks such as secure key exchange and digital signatures.

The findings provide valuable guidance for selecting encryp- tion algorithms based on both performance and application requirements. AES is recommended for high-speed, large- scale encryption tasks, while DES may be restricted to legacy or educational purposes, and RSA remains suitable for spe- cialized asymmetric encryption operations. This comparative study highlights the trade-offs between security, efficiency, and scalability, offering practical insights for researchers and developers in the field of information security.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Prac- tice*, 8th ed. Pearson, 2020.

[2] M. Singh and R. Kumar, “Comparative analysis of AES, DES and RSA cryptographic algorithms,” *International Journal of Computer Applications*, vol. 67, no. 19, pp. 1–7, 2013.

[3] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer, 2002.

[4] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[5] A. Kaur and S. Singh, “Performance evaluation of symmetric and asymmetric encryption algorithms,” *International Journal of Computer Science and Information Security*, vol. 14, no. 5, pp. 1–6, 2016.

[6] S. Gupta, P. Verma, and M. Kumar, “A study on encryption techniques and their performance metrics,” *Procedia Computer Science*, vol. 132, pp. 1039–1046, 2018.

[7] H. N. Bhatti and M. A. Shah, “Comparative study of AES and DES encryption algorithms,” *International Journal of Engineering Research & Technology*, vol. 5, no. 8, pp. 622–625, 2016.

[8] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, 2nd ed. Springer, 2010.

[9] S. Bhasin, A. Choudhary, and A. Singh, “Evaluation of symmetric key cryptographic algorithms,” *Journal of Information Security*, vol. 7, pp. 123–132, 2016.

[10] M. Subramanian, “A performance comparison of AES, DES, and RSA encryption algorithms,” *International Journal of Advanced Research in Computer Science*, vol. 9, no. 3, pp. 45–50, 2018.