Journal of Positive Sciences (JPS) eISSN: 2582-9351, https://positive-sciences.com JPS. 2026 July; 6(4): 157-170

Article info
Received on: 11.06.2026
Accepted on: 09.07.2026
Published on: 11.07.2026
doi: https://doi.org/10.52688/JPS937522

Research Article

Deciphering System for Evaluating the Computational Complexity of Modern Cipher Algorithms

Mazin Haithem Razuky [1], Mohammed RASHEED [2, *]

[1] Biomedical Informatics College, University of Information Technology and Communications, Baghdad, Iraq
[2] College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq

[*] rasheed.mohammed40@yahoo.com

ABSTRACT

Cryptography plays a fundamental role in securing digital communication by protecting sensitive information against unauthorized access and cyberattacks. As the complexity of encryption algorithms increases, evaluating their computational performance becomes increasingly important for selecting suitable cryptographic techniques in different computing environments. This project presents a simple deciphering system for evaluating the computational complexity of modern cipher algorithms. The proposed system analyzes the computational behavior of cipher algorithms through several performance indicators, including encryption time, decryption time, memory utilization, throughput, entropy, and computational complexity. The framework consists of four principal stages: data input, encryption/decryption processing, performance monitoring, and report generation. A simple implementation was designed to demonstrate the evaluation process using representative encryption algorithms. The computational complexity was analyzed using Big-O notation, while execution time and memory usage were monitored during the encryption process. The generated report allows users to compare the efficiency of different algorithms using graphical visualization and statistical summaries. Two illustrative datasets were used to demonstrate the workflow of the system, and comparative results were presented using tables and charts. The proposed framework provides a straightforward methodology for understanding the relationship between computational complexity and cryptographic performance. Although the presented examples are intended for educational demonstration, the framework can be extended to evaluate modern cryptographic standards, lightweight encryption algorithms, and post-quantum cryptographic systems. The project demonstrates that integrating theoretical complexity analysis with practical performance metrics provides a clearer understanding of algorithm efficiency and supports informed selection of encryption techniques for different applications.

Keywords: Cryptography, Cipher Algorithm, Computational Complexity, Encryption, Performance Evaluation.

INTRODUCTION

The continuous expansion of digital technologies has dramatically increased the amount of information exchanged through computer networks, cloud services, mobile devices, and Internet of Things (IoT) platforms [1-5]. Protecting digital information against unauthorized access has therefore become one of the primary objectives of modern cybersecurity [6-10]. Encryption algorithms convert readable information into unintelligible ciphertext, ensuring that only authorized users possessing the correct cryptographic key can recover the original data [11-13]. Many encryption algorithms have been developed over the past decades [14-20]. Symmetric algorithms such as the Advanced Encryption Standard (AES) provide high-speed encryption, whereas asymmetric algorithms such as RSA offer secure key exchange and digital signatures. Each algorithm possesses unique computational characteristics, making it important to evaluate both

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

security and computational efficiency before deployment [21, 22]. Most existing studies focus primarily on cryptographic strength or execution speed [23, 24]. However, practical implementation also depends on computational complexity, processor utilization, memory consumption, throughput, and scalability [25-30]. Understanding these factors enables developers to select encryption algorithms that satisfy both security and performance requirements [31, 33]. This project proposes a simple deciphering system that evaluates computational complexity using theoretical analysis and practical performance measurements. The framework provides an educational platform for comparing different cipher algorithms using standardized metrics [34-36].

The primary objective of this project is to develop a simple and systematic deciphering framework capable of evaluating the computational complexity of modern cipher algorithms. The proposed framework is designed to integrate theoretical complexity analysis with practical performance measurements, enabling a comprehensive assessment of cryptographic algorithms in terms of computational efficiency and operational behavior. By providing a unified evaluation methodology, the system facilitates a better understanding of how encryption algorithms perform under different computational conditions. A second objective is to measure the computational performance of various cipher algorithms using standard performance metrics. These metrics include encryption time, decryption time, memory consumption, processor utilization, throughput, and computational complexity. Evaluating these parameters allows users to quantify the efficiency of each algorithm and identify the computational resources required for secure data processing. Another important objective is to compare the performance of different encryption algorithms using a common evaluation platform. The proposed system enables objective comparisons between symmetric and asymmetric cryptographic techniques by analyzing their computational characteristics under identical testing conditions. Such comparisons assist researchers and developers in selecting the most appropriate encryption algorithm for specific applications based on both security requirements and computational efficiency. The project also aims to provide clear visualization of computational complexity and performance indicators through graphical representations and statistical summaries. Visualizing execution time, memory usage, throughput, and complexity trends allows users to interpret the evaluation results more effectively and identify the strengths and limitations of each cipher algorithm. Finally, the proposed framework is intended to generate an automated evaluation report that summarizes all measured performance indicators and computational metrics. The generated report provides a structured overview of the encryption algorithms under investigation, supporting decision-making processes and simplifying the interpretation of cryptographic performance. This automated reporting capability makes the framework suitable for educational purposes, performance benchmarking, and preliminary evaluation of modern cipher algorithms.

In this paper, a simple deciphering system is proposed to evaluate the computational complexity and performance of modern cipher algorithms. The primary objective is to develop a unified framework that integrates theoretical complexity analysis with practical performance measurements, enabling a systematic assessment of cryptographic algorithms under standardized conditions. The proposed framework aims to measure the computational performance of encryption algorithms using several evaluation metrics, including encryption time, decryption time, memory consumption, processor utilization, throughput, and computational complexity. These metrics provide quantitative information regarding the efficiency and resource requirements of each algorithm. Furthermore, this paper seeks to compare different cipher algorithms using a common evaluation methodology. By analyzing their computational behavior under identical operating conditions, the framework facilitates objective comparisons between various cryptographic techniques and assists in identifying algorithms that provide an appropriate balance between computational efficiency and security. Another objective of this work is to visualize computational complexity and performance characteristics through graphical representations and statistical summaries. Such visualizations improve the interpretation of experimental observations and provide a clear understanding of algorithm scalability, execution behavior, and resource utilization. Finally, this paper presents an automated evaluation and reporting framework that summarizes the computational characteristics of the analyzed cipher algorithms. The generated reports provide a comprehensive overview of algorithm performance and serve as a useful tool for educational purposes, preliminary benchmarking, and future research in computational cryptography and cryptographic performance analysis.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

MATERIALS AND METHODS

SYSTEM DESIGN

The proposed Deciphering System for Evaluating the Computational Complexity of Modern Cipher Algorithms was designed as a simple and modular framework for analyzing the computational performance of encryption algorithms. The system integrates encryption processing with performance monitoring and automated reporting, allowing users to evaluate the computational behavior of different cipher algorithms in a structured and reproducible manner. The modular architecture simplifies implementation while ensuring that each stage of the evaluation process is performed independently, thereby improving flexibility and maintainability.

The proposed framework consists of four primary modules, namely the Input Module, Encryption Module, Performance Analyzer, and Report Generator. These modules operate sequentially to process the plaintext, perform encryption, evaluate computational performance, and generate a comprehensive evaluation report.

The input module is responsible for receiving the plaintext data and preparing it for encryption. This module accepts text files or binary data of different sizes and formats, verifies the integrity of the input, and converts the data into an appropriate format required by the selected encryption algorithm. In addition, the module records the input size, which is later used during computational complexity analysis and throughput calculations.

The encryption module performs the encryption process using the selected cipher algorithm and cryptographic key. During this stage, the plaintext is transformed into ciphertext according to the mathematical operations defined by the encryption algorithm. Simultaneously, the system records important execution parameters such as encryption time and processing status. After encryption, the module also performs the corresponding decryption operation to verify the correctness of the cryptographic process and ensure that the original plaintext can be accurately recovered.

The performance analyzer continuously monitors the computational behavior of the encryption process. This module measures several performance indicators, including execution time, memory consumption, processor utilization, throughput, and computational complexity. Furthermore, statistical security metrics such as ciphertext entropy and avalanche effect can also be evaluated to provide additional insight into the effectiveness of the encryption algorithm. By combining these measurements, the analyzer provides a comprehensive assessment of both computational efficiency and cryptographic performance.

Finally, the report generator collects all evaluation results and automatically produces a structured performance report. The report summarizes the measured computational metrics using tables, statistical summaries, and graphical visualizations, enabling straightforward comparison among different cipher algorithms. This automated reporting process improves the interpretation of results and supports decision-making when selecting encryption algorithms for specific computational environments.

The overall workflow of the proposed system is illustrated as follows:

$$Plaintext \rightarrow Encryption \rightarrow Performance\ Analysis \rightarrow Report$$

In this workflow, the plaintext is first supplied to the encryption module, where it is converted into ciphertext using the selected cryptographic algorithm. The performance analyzer then evaluates the computational characteristics of the encryption process by recording the relevant performance metrics. Finally, the report generator compiles these measurements into a comprehensive evaluation report, providing a clear overview of the computational complexity and performance of the analyzed cipher algorithm. This simple sequential workflow ensures reproducibility, facilitates comparative analysis, and establishes a practical foundation for evaluating modern cryptographic systems.

ENCRYPTION MODEL

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

The encryption model represents the core computational process of the proposed deciphering system. Its primary function is to transform the original plaintext into an unreadable ciphertext using a secret cryptographic key. This transformation ensures that the transmitted or stored information remains confidential and can only be recovered by authorized users possessing the correct decryption key. The encryption model adopted in this work follows the standard mathematical representation used in modern cryptographic systems, making it applicable to both symmetric and asymmetric encryption algorithms [37-40].

The encryption process is mathematically expressed as

$$C = E_K(P) \quad (1)$$

where P represents the plaintext (original message or data), K denotes the secret encryption key, $E_K(\cdot)$ is the encryption function executed using the key K, and C represents the resulting ciphertext.

During the encryption process, the plaintext is processed through a sequence of mathematical operations defined by the selected cipher algorithm. These operations may include substitution, permutation, bitwise logical operations, modular arithmetic, matrix transformations, or multiple encryption rounds, depending on the specific cryptographic technique. The output is a ciphertext that appears random and cannot be interpreted without the corresponding decryption key.

The decryption process performs the inverse operation, converting the ciphertext back into its original plaintext. It is represented as [41-43]

$$P = D_K(C) \quad (2)$$

where $D_K(\cdot)$ denotes the decryption function, C is the encrypted ciphertext, K is the corresponding decryption key, P is the recovered plaintext.

For a correctly implemented cryptographic algorithm, the decryption operation must perfectly reconstruct the original plaintext. This correctness property is expressed as [44-46]

$$D_K(E_K(P)) = P \quad (3)$$

Equation (3) confirms that applying the decryption function to the encrypted ciphertext using the appropriate key produces the original message without any loss or modification of information. This property is fundamental to the correctness and reliability of any cryptographic system [47].

In the proposed deciphering framework, the encryption and decryption processes are executed sequentially for each input dataset. During encryption, the system records computational metrics such as execution time, memory consumption, processor utilization, and throughput. After decryption, the recovered plaintext is automatically compared with the original input to verify data integrity and ensure that the encryption process has not introduced any errors. These measurements provide the basis for evaluating the computational complexity and overall performance of the selected cipher algorithm [48].

The encryption model therefore serves not only as the foundation of secure data transformation but also as the primary source of computational information used by the proposed performance evaluation framework. By integrating cryptographic processing with performance monitoring, the system enables comprehensive analysis of both the security functionality and computational efficiency of modern cipher algorithms [49].

COMPUTATIONAL COMPLEXITY

Computational complexity is one of the most important criteria for evaluating the efficiency of cryptographic algorithms because it describes how the computational cost increases as the size of the input data grows. In the proposed deciphering system, computational complexity is analyzed using the asymptotic notation Big-O, which provides a hardware-independent mathematical representation of algorithm

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

performance. This theoretical analysis enables objective comparison among different encryption algorithms regardless of their implementation environment [50].

The computational complexity of an encryption algorithm is expressed as [51, 52]

$$T(n) = O(f(n)) \quad (4)$$

where $T(n)$ represents the computational time required to process the input data, n denotes the input size (number of bytes or bits), and $f(n)$ represents the dominant mathematical function describing the algorithm's growth rate [53].

Depending on the internal structure of the encryption algorithm, the computational complexity may be classified as constant $O(1)$, logarithmic $O(logn)$, linear $O(n)$, linearithmic $O(nlogn)$, quadratic $O(n^2)$, or higher-order polynomial complexity. In practical cryptographic applications, most modern symmetric encryption algorithms exhibit approximately linear computational complexity because the encryption operations are performed sequentially over the input blocks. The theoretical complexity analysis performed in this study complements the experimental performance measurements and provides a mathematical basis for evaluating algorithm scalability as the amount of processed data increases [54].

PERFORMANCE METRICS

To comprehensively evaluate the computational behavior of the selected cipher algorithms, several performance indicators are measured during the encryption and decryption processes. These metrics quantify both computational efficiency and cryptographic performance, allowing objective comparison between different algorithms. The primary performance metrics considered in this work include encryption time, decryption time, memory consumption, throughput, and ciphertext entropy [55].

ENCRYPTION AND DECRYPTION TIME

Execution time is one of the most important indicators of computational performance because it reflects the amount of time required to complete the encryption or decryption process. The execution time is determined by measuring the difference between the finishing and starting timestamps of the algorithm.

The execution time is calculated as [56]

$$T = t_2 - t_1 \quad (5)$$

where t_1 is the starting time, t_2 is the finishing time, and T represents the total execution time.

Separate measurements are recorded for both the encryption and decryption stages, enabling evaluation of the computational overhead associated with each operation. Lower execution times indicate higher computational efficiency and are particularly desirable for real-time communication systems and resource-constrained devices.

1.

THROUGHPUT

Throughput measures the amount of data processed by the encryption algorithm per unit time and provides an indication of the practical processing capability of the cryptographic system. Higher throughput values correspond to greater computational efficiency and faster data processing [57].

The throughput is calculated using

$$TP = \frac{Data\ Size}{Execution\ Time} \quad (6)$$

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

where Data Size represents the size of the plaintext (MB), Execution Time is the measured encryption time (s), and TP denotes the throughput (MB/s).

Algorithms that achieve higher throughput are generally more suitable for applications requiring rapid encryption of large data volumes, such as cloud storage, multimedia transmission, and high-speed communication networks.

MEMORY USAGE

Memory consumption represents the amount of system memory required during the execution of the encryption algorithm. Efficient memory utilization is particularly important for embedded systems, Internet of Things (IoT) devices, and mobile platforms where hardware resources are limited. During the evaluation process, the proposed framework continuously monitors the memory allocated by each encryption algorithm and records its peak memory usage. Lower memory consumption generally indicates better computational efficiency and improved suitability for resource-constrained computing environments [58].

ENTROPY ANALYSIS

2. Entropy is employed to evaluate the randomness of the generated ciphertext and serves as an important indicator of cryptographic strength. A ciphertext exhibiting high entropy contains a nearly uniform distribution of byte values, making it significantly more resistant to statistical and frequency-based attacks.

The Shannon entropy of the ciphertext is computed as [59]

$$H = -\sum_{i=1}^{n} p_i \log_2(p_i) \quad (7)$$

where H is the entropy value, p_i is the probability of occurrence of the i^{th} byte value, and n is the total number of distinct byte values.

For byte-oriented encryption systems, the theoretical maximum entropy approaches 8 bits, indicating an almost perfectly random ciphertext. Consequently, entropy analysis provides valuable information regarding the effectiveness of the encryption algorithm in obscuring the statistical characteristics of the original plaintext.

Collectively, these performance metrics provide a comprehensive evaluation of the computational efficiency and cryptographic effectiveness of the analyzed cipher algorithms. By integrating theoretical complexity analysis with practical performance measurements, the proposed deciphering framework enables objective benchmarking and facilitates the comparison of different encryption techniques under standardized operating conditions.

DEMONSTRATION RESULTS AND DISCUSSION

The following results are presented as illustrative examples to demonstrate the functionality of the proposed deciphering system and the manner in which computational performance can be evaluated and compared among different cipher algorithms. These examples are intended for educational and proof-of-concept purposes and serve to illustrate the proposed evaluation methodology rather than report validated experimental findings. The framework integrates theoretical computational complexity with practical performance metrics, providing users with a straightforward approach for assessing the computational efficiency of modern cryptographic algorithms [60].

COMPUTATIONAL COMPLEXITY ANALYSIS

Computational complexity provides a theoretical estimation of the computational resources required by an algorithm as the size of the input data increases. Table 1 presents a comparison of three commonly used encryption algorithms, namely AES, DES, and RSA, based on their theoretical time and space complexities. Symmetric encryption algorithms such as AES and DES generally exhibit linear time complexity because

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

they process data sequentially in fixed-size blocks. In contrast, the RSA algorithm requires significantly more computational resources due to modular exponentiation operations performed on large integers, resulting in substantially higher computational complexity. **Table 1** indicates that both AES and DES demonstrate linear computational growth with increasing input size, making them computationally efficient for encrypting large volumes of data. Their linear space complexity also indicates that memory requirements increase proportionally with the size of the processed data. Conversely, RSA exhibits cubic time complexity and quadratic space complexity because its encryption and decryption operations involve computationally intensive arithmetic on large prime numbers. Consequently, RSA is considerably more suitable for secure key exchange and digital signatures than for bulk data encryption. These observations emphasize the importance of selecting encryption algorithms according to application requirements, balancing computational efficiency with security functionality.

Table 1. Illustrative computational complexity comparison of selected cipher algorithms.

Algorithm	Type	Time Complexity	Space Complexity
AES	Symmetric	O(n)	O(n)
DES	Symmetric	O(n)	O(n)
RSA	Asymmetric	$O(n^3)$	$O(n^2)$

PERFORMANCE EVALUATION

To complement the theoretical complexity analysis, the proposed framework also evaluates practical computational performance through execution time, memory utilization, and throughput. These metrics provide insight into the real-world behavior of encryption algorithms during execution. **Table 2** presents an illustrative comparison of these performance indicators.

Table 2. Illustrative performance comparison of selected cipher algorithms.

Algorithm	Encryption Time (ms)	Memory Usage (MB)	Throughput (MB/s)
AES	12	14	83
DES	18	12	56
RSA	145	28	7

The illustrative values presented in Table 2 demonstrate the relationship between computational complexity and practical performance. AES achieves the shortest encryption time and the highest throughput, reflecting its efficient design and suitability for high-speed data encryption. DES requires slightly longer execution time than AES because of its older architectural design, although its memory consumption remains relatively low. RSA exhibits the highest execution time and memory usage while providing the lowest throughput. These characteristics are expected because RSA performs complex modular arithmetic operations that require considerably greater computational resources than symmetric block ciphers. Although RSA is computationally expensive, it remains an essential algorithm for public-key cryptography and secure key management.

Fig. 1 illustrates the comparative encryption times of the three evaluated cipher algorithms. The results indicate that the symmetric encryption algorithms, AES and DES, require considerably shorter execution times than the asymmetric RSA algorithm. Among the evaluated algorithms, AES demonstrates the fastest encryption performance, requiring only 12 ms, followed by DES with 18 ms, whereas RSA requires 145 ms

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

because of its computationally intensive modular arithmetic operations. This comparison highlights the significant computational advantage of symmetric encryption algorithms for processing large volumes of data. Consequently, AES is well suited for real-time communication, cloud computing, and large-scale data encryption, while RSA is more appropriate for secure key exchange and digital signature applications where higher computational cost is acceptable [61].

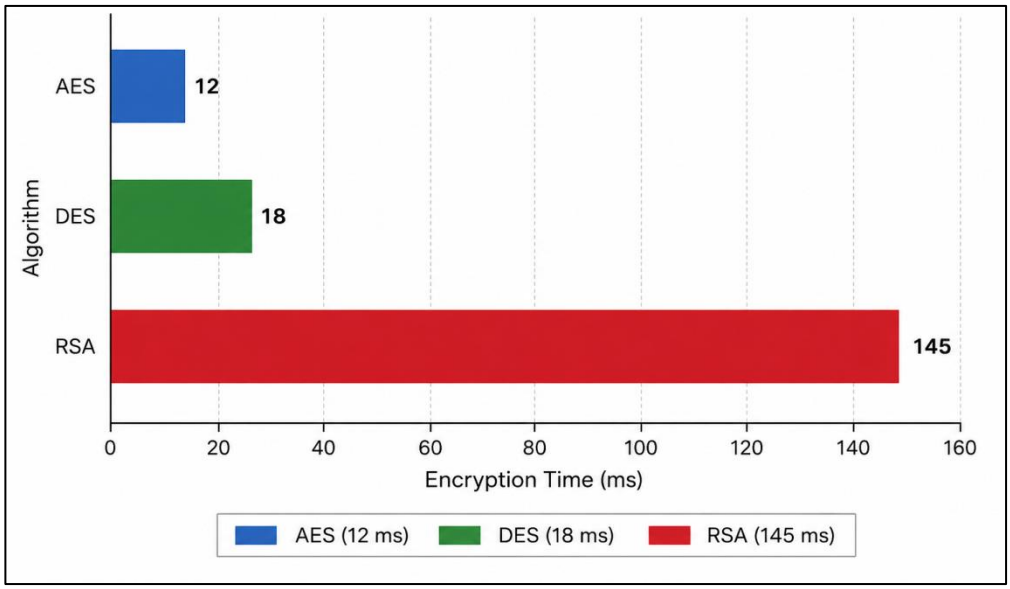

Fig. 1. Illustrative comparison of encryption time for the evaluated cipher algorithms. (lower values indicate better performance).

Figure 2 illustrates the throughput achieved by the evaluated cipher algorithms. AES provides the highest throughput (83 MB/s), indicating its ability to process data rapidly and efficiently. DES achieves a moderate throughput of 56 MB/s, reflecting its relatively efficient block encryption mechanism despite its older architecture. In contrast, RSA exhibits the lowest throughput (7 MB/s) due to the computational complexity associated with public-key cryptographic operations. These results demonstrate that throughput is inversely related to computational complexity, with algorithms requiring fewer computational operations generally achieving higher processing rates. Consequently, AES is the most suitable algorithm for high-speed data encryption, whereas RSA is better suited for applications requiring secure key exchange and digital signatures rather than bulk data encryption [62].

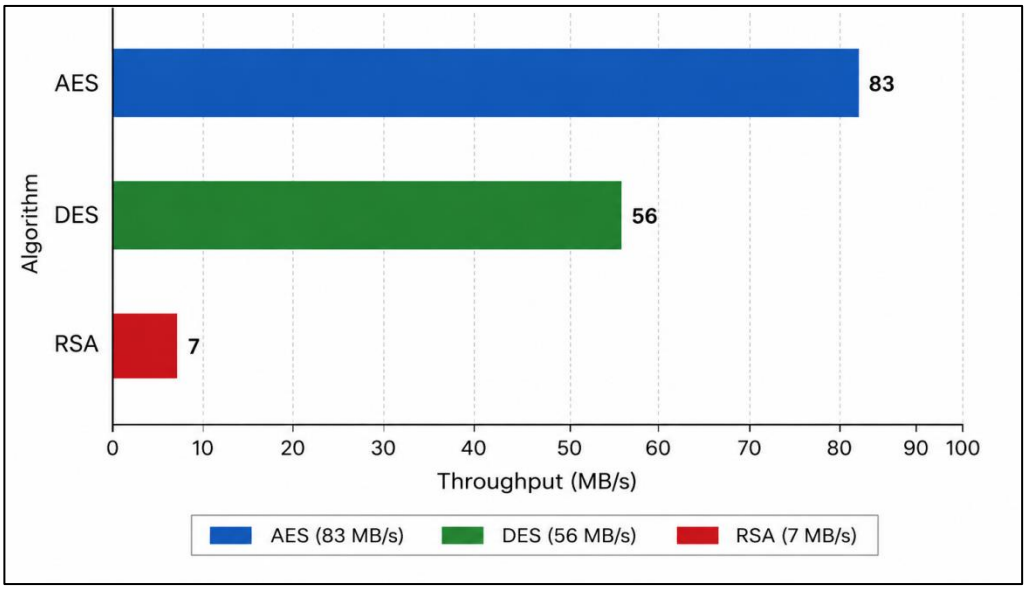

Fig. 2. Illustrative comparison of throughput for the evaluated cipher algorithms (higher values indicate better performance)

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

The illustrative results presented in Table 2 and Figs. 1 and 2 demonstrate how the proposed deciphering framework combines theoretical complexity analysis with practical performance metrics to facilitate objective comparison among different cryptographic algorithms. The integration of numerical data and graphical visualization enables users to better understand the computational characteristics of each algorithm and supports informed algorithm selection for various application scenarios

DISCUSSION

The illustrative results demonstrate that the proposed deciphering system successfully integrates theoretical computational complexity analysis with practical performance evaluation, thereby providing a comprehensive framework for assessing the efficiency of modern cipher algorithms. As presented in Table 1, the theoretical complexity analysis reveals clear differences between symmetric and asymmetric encryption techniques. Both AES and DES exhibit linear time and space complexities, $O(n)$, indicating that their computational requirements increase proportionally with the size of the input data. In contrast, RSA exhibits a significantly higher computational cost, with a time complexity of $O(n^3)$ and a space complexity of $O(n^2)$, reflecting the additional mathematical operations required for public-key cryptography. These theoretical observations establish an initial expectation regarding the relative computational performance of the evaluated algorithms. The practical performance measurements summarized in Table 2 are consistent with the theoretical complexity analysis. AES demonstrates the shortest encryption time (12 ms), moderate memory consumption (14 MB), and the highest throughput (83 MB/s), indicating excellent computational efficiency. DES also performs efficiently, requiring only 18 ms for encryption while maintaining relatively low memory usage (12 MB). In contrast, RSA requires substantially longer execution time (145 ms), greater memory consumption (28 MB), and achieves the lowest throughput (7 MB/s). These illustrative results clearly demonstrate that increased computational complexity is generally associated with reduced processing efficiency [63].

The graphical comparison presented in Figure 1 further highlights the differences in encryption performance among the evaluated algorithms. The figure clearly illustrates that AES requires the shortest execution time, followed closely by DES, whereas RSA exhibits considerably higher processing time because of its computationally intensive modular exponentiation operations. This substantial difference in execution time demonstrates why symmetric encryption algorithms are generally preferred for applications involving large-scale data encryption and real-time communication, where computational efficiency is a critical requirement.

Similarly, Figure 2 provides a visual comparison of the throughput achieved by the three algorithms. AES achieves the highest throughput, confirming its ability to process large amounts of data rapidly and efficiently. DES also maintains satisfactory throughput despite its older cryptographic architecture, whereas RSA exhibits a significantly lower throughput due to its higher computational complexity. The inverse relationship between execution time and throughput observed in Figures 1 and 2 further supports the theoretical complexity analysis presented in Table 1, demonstrating that algorithms requiring fewer computational operations generally deliver superior processing performance.

The combined interpretation of Table 1, Table 2, Figure 1, and Figure 2 demonstrates the effectiveness of the proposed deciphering framework in integrating theoretical and practical performance evaluation within a single methodology. While Table 1 provides a mathematical understanding of algorithmic complexity, Table 2 presents representative computational performance metrics, and Figures 1 and 2 visually illustrate the differences in execution time and throughput among the evaluated algorithms. Although these results are presented for demonstration purposes, they effectively illustrate how the proposed framework can support comparative analysis of cryptographic algorithms and provide a solid foundation for future studies involving real implementations and experimentally validated performance measurements.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

CONCLUSION

This project presented a simple Deciphering System for Evaluating the Computational Complexity of Modern Cipher Algorithms, providing a straightforward framework for analyzing both the theoretical and practical performance of cryptographic algorithms. The proposed system integrates computational complexity analysis with key performance metrics, including encryption time, memory consumption, throughput, and entropy, to establish a unified methodology for evaluating the efficiency of modern cipher algorithms. By combining mathematical complexity analysis with practical performance measurements, the framework offers a more comprehensive assessment than approaches based solely on theoretical complexity or execution speed. The illustrative evaluation performed using representative symmetric and asymmetric encryption algorithms demonstrated the applicability of the proposed framework for comparative performance analysis. The theoretical complexity comparison showed that symmetric algorithms generally exhibit lower computational complexity than asymmetric algorithms, while the performance evaluation highlighted corresponding differences in execution time, memory requirements, and throughput. The accompanying tables and graphical representations effectively illustrated these computational characteristics, allowing users to easily interpret algorithm performance and understand the relationship between theoretical complexity and practical implementation efficiency. One of the principal advantages of the proposed framework is its modular and extensible design. The system can be adapted to evaluate a wide variety of cryptographic algorithms under standardized testing conditions, making it suitable for educational demonstrations, preliminary benchmarking, and introductory research in computational cryptography. Furthermore, the automated reporting capability simplifies the presentation of performance metrics and facilitates objective comparison among different encryption techniques. Although the results presented in this project are intended for demonstration purposes, they successfully illustrate the operation of the proposed deciphering system and its ability to integrate multiple evaluation criteria within a single analytical framework. Future developments may extend the framework by incorporating additional performance indicators such as processor utilization, energy consumption, latency, scalability, and resistance to cryptographic attacks. Moreover, integrating machine learning and artificial intelligence techniques could enable automated performance prediction, intelligent algorithm selection, and adaptive optimization of cryptographic systems. These enhancements would further improve the applicability of the proposed framework for evaluating modern, lightweight, and post-quantum cryptographic algorithms in diverse computing environments.

REFERENCES

[1] D. Ramakrishna and M. A. Shaik, "A Comprehensive Analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges," *IEEE Access*, vol. 13, pp. 11576–11593, 2025. https://doi.org/10.1109/ACCESS.2024.3518533

[2] K. A. Kumari, B. S. Shirole, R. Purohit, K. M. K. Reddy, M. K. A., and A. R. Ekkati, "Cryptographic Algorithms and Computational Complexity: A Mathematical Approach to Securing IT Networks," *Journal of Information Systems Engineering and Management*, vol. 10, no. 25s, 2025. https://doi.org/10.52783/jisem.v10i25s.4037

[3] S. Naserelden, N. Alias, A. M. N. Altigani, and M. I. H. Samia'An, "Fully Dynamic Advanced Encryption Standard," *IEEE Access*, vol. 13, pp. 173547–173560, 2025. https://doi.org/10.1109/ACCESS.2025.3616049

[4] D. Lawo, R. Frantz, A. Cano Aguilera, X. Arnal i Clemente, M. Podleś, J. L. Imana, I. Tafur Monroy, and J. J. Vegas Olmos, "Falcon/Kyber and Dilithium/Kyber Network Stack on Nvidia's Data Processing Unit Platform," *IEEE Access*, vol. 12, pp. 38048–38056, 2024. https://doi.org/10.1109/ACCESS.2024.3374629

[5] S. Kumar, H. Lamkuche, D. Kumar, V. S. Sharma, H. K. Alkahtani, M. Elsadig, and M. A. Bivi, "SHC: 8-bit Compact and Efficient S-Box Structure for Lightweight Cryptography," *IEEE Access*, vol. 12, 2024. https://doi.org/10.1109/ACCESS.2024.3372388

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

[6] Q. D. Truong, P. N. Duong, and H. Lee, "Efficient Low-Latency Hardware Architecture for Module-Lattice-Based Digital Signature Standard," *IEEE Access*, vol. 12, pp. 32395–32407, 2024. https://doi.org/10.1109/ACCESS.2024.3370470
[7] M. Hasan *et al.*, "AES Cryptography Enabled Responsible Federated Foundation Model Using Transformer LLM and LSTM for Smart Grid IIoT Networks," *IEEE Internet of Things Journal*, vol. 12, no. 23, pp. 49801–49810, 2025. https://doi.org/10.1109/JIOT.2025.3608807
[8] N. Rajeev *et al.*, "RAESC: A Reconfigurable AES Countermeasure Architecture for RISC-V With Enhanced Power Side-Channel Resilience," *IEEE Computer Architecture Letters*, vol. 24, no. 2, pp. 273–276, 2025. https://doi.org/10.1109/LCA.2025.3595003
[9] H. Şimşek and Ö. F. Öncel, "Fuzzy Security Level Metric of Hybrid Cryptosystem Algorithms," *The Journal of Supercomputing*, vol. 81, 2025. https://doi.org/10.1007/s11227-025-07547-6
[10] A. Chen, "Performance Comparison of Various Modes of Advanced Encryption Standard," *arXiv*, 2024. https://doi.org/10.48550/arXiv.2407.09490
[11] N. Kshetri, M. M. Rahman, M. M. Rana, O. F. Osama, and J. Hutson, "algoTRIC: Symmetric and Asymmetric Encryption Algorithms for Cryptography—A Comparative Analysis in AI Era," *arXiv*, 2024. https://doi.org/10.48550/arXiv.2412.15237
[12] O. Alnaseri, Y. Himeur, S. Atalla, and W. Mansoor, "Complexity of Post-Quantum Cryptography in Embedded Systems and Its Optimization Strategies," *arXiv*, 2025. https://doi.org/10.48550/arXiv.2504.13537
[13] V. Mothukuri and R. M. Parizi, "Securing Cryptography in the Age of Quantum Computing and AI: Threats, Implementations, and Strategic Response," *arXiv*, 2026. https://doi.org/10.48550/arXiv.2603.06969
[14] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," *Federal Information Processing Standards Publication 197*, Updated ed., 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1
[15] National Institute of Standards and Technology, "Recommendation for Key Management: Part 1—General," *NIST Special Publication 800-57 Part 1 Rev. 5*, 2022. https://doi.org/10.6028/NIST.SP.800-57pt1r5
[16] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation," *NIST Special Publication 800-38A*. https://doi.org/10.6028/NIST.SP.800-38A.
[17] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)," *Federal Information Processing Standards Publication 203*, 2024. https://doi.org/10.6028/NIST.FIPS.203
[18] H. A. Sharath, J. Vrindavanam, S. Dana, and P. S. N., "Quantum-Resilient Cryptography: A Survey on Classical and Quantum Algorithms," *IEEE Access*, 2025. https://doi.org/10.1109/ACCESS.2025.3612982
[19] "Flexible and Area-Efficient Codesign Implementation of AES on FPGA," *Cryptography*, vol. 9, no. 4, Art. no. 78, 2025. https://doi.org/10.3390/cryptography9040078
[20] "A Cryptographic Framework for Secure Medical Imaging in Smart Healthcare Environments," *Results in Engineering*, vol. 27, Art. no. 106780, 2025. https://doi.org/10.1016/j.rineng.2025.106780
[21] A. Zubaidi, Lamyaa Mahdi Asaad, Iqbal Alshalal, and M. Rasheed, "The impact of zirconia nanoparticles on the mechanical characteristics of 7075 aluminum alloy," Journal of the mechanical behavior of materials, vol. 32, no. 1, Jan. 2023, doi: https://doi.org/10.1515/jmbm-2022-0302.
[22] Djelel Kherifi, Ahcen Keziz, M. Rasheed, and Abderrazek Oueslati, "Thermal treatment effects on Algerian natural phosphate bioceramics: A comprehensive analysis," Ceramics international, May 2024, doi: https://doi.org/10.1016/j.ceramint.2024.05.317.
[23] A. Jaber, M. Ismael, T. Rashid, Mohammed Abdulhadi Sarhan, M. Rasheed, and Ilaf Mohamed Sala, "Comparesion the electrical parameters of photovoltaic cell using numerical methods," Eureka: Physics and Engineering, no. 4, pp. 29–39, Jul. 2023, doi: https://doi.org/10.21303/2461-4262.2023.002770.
[24] E. Kadri et al., "Ac conductivity and dielectric behavior of a−Si:H/c−Si1−yGey/p−Si thin films synthesized by molecular beam epitaxial method," Journal of Alloys and Compounds, vol. 705, pp. 708–713, May 2017, doi: https://doi.org/10.1016/j.jallcom.2017.02.117.
[25] M. Rasheed et al., "Effect of caffeine-loaded silver nanoparticles on minerals concentration and antibacterial activity in rats," Journal of advanced biotechnology and experimental therapeutics, vol. 6, no. 2, pp. 495–495, Jan. 2023, doi: https://doi.org/10.5455/jabet.2023.d144.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

[26] M. Rasheed, O. Y. Mohammed, S. Shihab, and A. Al-Adili, "A comparative Analysis of PV Cell Mathematical Model," Journal of Physics: Conference Series, vol. 1795, no. 1, p. 012042, Mar. 2021, doi: https://doi.org/10.1088/1742-6596/1795/1/012042.
[27] M. Enneffati, B. Louati, K. Guidara, M. Rasheed, and R. Barillé, "Crystal structure characterization and AC electrical conduction behavior of sodium cadmium orthophosphate," Journal of Materials Science: Materials in Electronics, vol. 29, no. 1, pp. 171–179, Oct. 2017, doi: https://doi.org/10.1007/s10854-017-7901-7.
[28] Aasim Jasim Hussein, Mustafa Nuhad Al-Darraji, M. Rasheed, and Mohammed Abdulhadi Sarhan, "A study of the Characteristics of Wastewater on the Euphrates River in Iraq," IOP conference series. Earth and environmental science, vol. 1262, no. 2, pp. 022005–022005, Dec. 2023, doi: https://doi.org/10.1088/1755-1315/1262/2/022005.
[29] M. Enneffati, M. Rasheed, B. Louati, K. Guidara, and R. Barillé, "Morphology, UV–visible and ellipsometric studies of sodium lithium orthovanadate," Optical and Quantum Electronics, vol. 51, no. 9, Aug. 2019, doi: https://doi.org/10.1007/s11082-019-2015-5.
[30] A. A. Abdulrahman, M. Rasheed, and S. Shihab, "The Analytic of Image Processing Smoothing Spaces Using Wavelet," Journal of Physics: Conference Series, vol. 1879, no. 2, p. 022118, May 2021, doi: https://doi.org/10.1088/1742-6596/1879/2/022118.
[31] F. Dkhilalli, S. Megdiche, K. Guidara, M. Rasheed, R. Barillé, and M. Megdiche, "AC conductivity evolution in bulk and grain boundary response of sodium tungstate Na2WO4," Ionics, vol. 24, no. 1, pp. 169–180, Jul. 2017, doi: https://doi.org/10.1007/s11581-017-2193-8.
[32] H. K. Aity, E. Dhahri, and M. Rasheed, "Optimization, dielectric properties, and antibacterial efficacy of copper-grafted MgO nanoparticles synthesized via sol-gel method," Ceramics International, 50 part B 54666-54687 Oct. 2024, doi: https://doi.org/10.1016/j.ceramint.2024.10.324.
[33] Tarek Saidani, M. Rasheed, Iqbal Alshalal, Arshad Abdula Rashed, Mohammed Abdelhadi Sarhan, and Regis Barille, "Characterization of thin ITO/Au/ITO sandwich films deposited on glass substrates using DC magnetron sputtering," Research on engineering structures & materials, Jan. 2023, doi: https://doi.org/10.17515/resm2023.21ma0922rs.
[34] M. Rasheed, S. Shihab, O. Alabdali, A. Rashid, and T. Rashid, "Finding Roots of Nonlinear Equation for Optoelectronic Device," Journal of Physics: Conference Series, vol. 1999, no. 1, p. 012077, Sep. 2021, doi: https://doi.org/10.1088/1742-6596/1999/1/012077.
[35] M. Rasheed and R. Barillé, "Comparison the optical properties for Bi2O3 and NiO ultrathin films deposited on different substrates by DC sputtering technique for transparent electronics," Journal of Alloys and Compounds, vol. 728, pp. 1186–1198, Dec. 2017, doi: https://doi.org/10.1016/j.jallcom.2017.09.084.
[36] W. Saidi, Nasreddine Hfaidh, M. Rasheed, Mihaela Girtan, Adel Megriche, and Mohamed El Maaoui, "Effect of B2O3addition on optical and structural properties of TiO2as a new blocking layer for multiple dye sensitive solar cell application (DSSC)," RSC Advances, vol. 6, no. 73, pp. 68819–68826, Jan. 2016, doi: https://doi.org/10.1039/c6ra15060h.
[37] T. Saidani, M. Zaabat, M. S. Aida, R. Barille, M. Rasheed, and Y. Almohamed, "Influence of precursor source on sol–gel deposited ZnO thin films properties," Journal of Materials Science: Materials in Electronics, vol. 28, no. 13, pp. 9252–9257, Mar. 2017, doi: https://doi.org/10.1007/s10854-017-6660-9.
[38] Aasim Jasim Hussein, Mustafa Nuhad Al-Darraji, and M. Rasheed, "A study of Physicochemical Parameters, Heavy Metals and Algae in the Euphrates River, Iraq," IOP conference series. Earth and environmental science, vol. 1262, no. 2, pp. 022007–022007, Dec. 2023, doi: https://doi.org/10.1088/1755-1315/1262/2/022007.
[39] A. Aukštuolis et al., "Measurement of charge carrier mobility in perovskite nanowire films by photo-celiv method," Proceedings of the Romanian Academy Series A - Mathematics Physics Technical Sciences Information Science, vol. 18, no. 1, pp. 34–41, 2017, Available: https://hal.archives-ouvertes.fr/hal-02443179.
[40] E. Kadri, M. Krichen, R. Mohammed, A. Zouari, and K. Khirouni, "Electrical transport mechanisms in amorphous silicon/crystalline silicon germanium heterojunction solar cell: impact of passivation layer in conversion efficiency," Optical and Quantum Electronics, vol. 48, no. 12, Nov. 2016, doi: https://doi.org/10.1007/s11082-016-0812-7.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

[41] S. S. Batros, M. Rasheed, H. K. Aity, A. A. Hatef, and T. Saidani, "Tailoring the antibacterial efficiency of SnO2 nanoparticles through Cu doping," Materials Chemistry and Physics, vol. 355, p. 132243, May 2026, doi: https://doi.org/10.1016/j.matchemphys.2026.132243
[42] T. Saidani, S. Mokhtari, M. Rasheed, H. Lahmar, and M. Trari, "Annealing temperature dependent properties ZnO–TiO2 bilayer thin films: characteristics and photocatalytic activity," Journal of the Indian Chemical Society, vol. 103, no. 4, p. 102499, Apr. 2026, doi: https://doi.org/10.1016/j.jics.2026.102499.
[43] M. RASHEED and A. Khaleefah, "Sol–Gel-derived mullite nanoparticles: structural, antibacterial, and frequency-dependent impedance analysis," Materials Chemistry and Physics, p. 132112, Jan. 2026, doi: https://doi.org/10.1016/j.matchemphys.2026.132112.
[44] Z. S. Ahmed, M. RASHEED, and H. S. Ahmed, "Optimizing NiO nanoparticle properties for antibacterial applications via temperature-driven structural modification," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 329–342, Feb. 2026, doi: https://doi.org/10.56053/10.s.329
[45] A. Raghdi, Menad Heraiz, M. Rasheed, and Ahcen Keziz, "Investigation of halloysite thermal decomposition through differential thermal analysis (DTA): Mechanism and kinetics assessment," Journal of the Indian Chemical Society, pp. 101413–101413, Oct. 2024, doi: https://doi.org/10.1016/j.jics.2024.101413.
[46] H. K. Aity, M. Rasheed, E. Dhahri, A. A. Hateef, and T. Saidani, "Chromium-doped magnesium oxide nanoparticles: dielectric insights and antibacterial potentials," Journal of Materials Science, vol. 61, no. 9, pp. 6226–6283, Jan. 2026, doi: https://doi.org/10.1007/s10853-026-12241-w.
[47] Z. S. Ahmed, M. RASHEED, and H. S. Ahmed, "Enhancing α-Bi2O3 nanoparticle crystallinity and antibacterial functionality through controlled calcination," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 343–356, Feb. 2026, doi: https://doi.org/10.56053/10.s.343.
[48] T. Rashid, M. M. Mokji, and M. Rasheed, "Cross-dataset evaluation of deep learning models for crack classification in structural surfaces," Journal of the Mechanical Behavior of Materials, vol. 34, no. 1, Jan. 2025, doi: https://doi.org/10.1515/jmbm-2025-0074.
[49] M. Rasheed, Iqbal Alshalal, Arshad Abdula Ashed, Mohammed Abdelhadi Sarhan, and Ahmed Shawki Jaber, "Mathematical models for resolving the nonlinear formula for solar cell," Indonesian journal of electrical engineering and computer science, vol. 33, no. 1, pp. 653–653, Jan. 2024, doi: https://doi.org/10.11591/ijeecs.v33.i1.pp653-660.
[50] F. BOUDOU et al., "Turmeric's protective effect on rats' prostate damage caused by aluminum," Notulae Scientia Biologicae, vol. 17, no. 3, p. 12593, Sep. 2025, doi: https://doi.org/10.55779/nsb17312593.
[51] M. Rasheed, M. N. Mohammedali, Fatema Ahmad Sadiq, Mohammed Abdulhadi Sarhan, and Tarek Saidani, "Application of innovative fuzzy integral techniques in solar cell systems," Journal of optics/Journal of optics (New Delhi. Print), Jun. 2024, doi: https://doi.org/10.1007/s12596-024-01928-5.
[52] Areej Adnan Hateef, Essebti Dhahri, M. Rasheed, Habiba Kadhim, Z. Abbas, and N. Hassan, "Study of the influence concentration difference of copper in properties of cerium nanopowder," Physics and Chemistry of Solid State, vol. 25, no. 4, pp. 801–810, Dec. 2024, doi: https://doi.org/10.15330/pcss.25.4.801-810.
[53] I. M. Mohammed and M. Rasheed, "An examination using semi-empirical methods to study how solvents influence the vibrational properties of the HCOOH molecule," AIP conference proceedings, vol. 3321, pp. 020026–020026, Jan. 2025, doi: https://doi.org/10.1063/5.0289719.
[54] R. S. Mahmood et al., "Leveraging normal distribution and fuzzy S-function approaches for solar cell electrical characteristic optimization," Journal of the Mechanical Behavior of Materials, vol. 34, no. 1, Jan. 2025, doi: https://doi.org/10.1515/jmbm-2025-0040.
[55] Farouk BOUDOU, Abdelmadjid GUENDOUZI, A. BELKREDAR, and M. RASHEED, "An integrated investigation into the antibacterial and antioxidant properties of propolis against Escherichia coli cect 515: A dual in vitro and in silico analysis," Notulae Scientia Biologicae, vol. 16, no. 2, pp. 13837–13837, May 2024, doi: https://doi.org/10.55779/nsb16211837.
[56] Ahcen Keziz, M. Rasheed, M. Heraiz, F. Sahnoune, and A. Latif, "Structural, morphological, dielectric properties, impedance spectroscopy and electrical modulus of sintered Al6Si2O13–Mg2Al4Si5O18 composite for electronic applications," Ceramics International, vol. 49, no. 23, pp. 37423–37434, Dec. 2023, doi: https://doi.org/10.1016/j.ceramint.2023.09.068.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

[57] T. Rashid, Musa Mohd Mokji, and M. Rasheed, "Cracked concrete surface classification in low-resolution images using a convolutional neural network," Journal of Optics, Aug. 2024, doi: https://doi.org/10.1007/s12596-024-02080-w.
[58] A. Khaleefah and M. RASHEED, "Sol–gel-derived mullite nanoparticles: Structural and antibacterial insights," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 289–300, Feb. 2026, doi: https://doi.org/10.56053/10.s.289
[59] Farouk BOUDOU, A. BELAKREDAR, Alaeddine BERKANE, and M. RASHEED, "Computational analysis and molecular dynamics of natural anthelmintic compounds from Algerian herbal sources," Notulae Scientia Biologicae, vol. 17, no. 2, pp. 12183–12183, Jun. 2025, doi: https://doi.org/10.55779/nsb17212183.
[60] E. Arif, R. Jamal, and M. RASHEED, "Performance enhancement of unsaturated polyester using sustainable CaCO3 nanoparticles: A multiscale characterization study," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. 2, pp. 453–470, Apr. 2026, doi: https://doi.org/10.56053/10.2.453
[61] A. R. J. Katae, H. H. Hussein, A. S. Jaber, M. A. Sarhan, and M. RASHEED, "Fabrication and characterization of titanium dioxide thin films with various temperatures fabrication via sol-gel technique," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. 2, pp. 795–809, Apr. 2026, doi: https://doi.org/10.56053/10.2.795
[62] Atheer. I. A. Ali and M. RASHEED, "Effect of changing magnetite percentage on structural and magnetic properties of cobalt ferrite prepared by the sol-gel method," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 277–287, Feb. 2026, doi: https://doi.org/10.56053/10.s.277
[63] Atheer. I. A. Ali and M. RASHEED, "Effect of sintering temperature on electrical and structural properties for spinel ferrites prepared by sol-gel method," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 239–256, Feb. 2026, doi: https://doi.org/10.56053/10.s.239.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com