

Cryptanalysis Of Symmetric Key Algorithms: A Comparative Study of RC4, 3DES and AES in an Ethical Hacking Context

Auyo S. G.^{1*}, Kamal S. W.², Yushau A.³, M. A. Jalo⁴, Ibrahim A. A.⁵

¹Department of Cyber Security
Sule Lamido University,
Kafin Hausa.

²Department of Computer Science
National Open University of Nigeria

³Department of Computer Science
Jigawa State Polytechnic,
Dutse.

⁴Department of Information Technology
Modibbo Adama University,
Yola.

⁵Department of Information Technology
Federal University Dutse

Email: salihuauyo@gmail.com

Abstract

During a period in which cyber-threats continue increasing, assessing the efficiency of cryptography algorithms became significant in protecting critical data in both organization and personal system. The speedy increase of data exchange and digital communication has strengthened the needs for a strong and effective cryptography mechanism to secure crucial data or information from unwanted access. This research depicts a cryptanalysis of the most and widely used key symmetric algorithms which are Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), and Rivest Cipher4 (RC4) in the context of ethical hacking. The study aims to assess and make comparison of the algorithms based upon their time efficiency when decryption and encryption processes. VB.Net was utilized in developing the simulation environment in which documents of 2MB was decrypted and encrypted through each algorithm and the execution time was assessed in millisecond. The results of the experiment showed that Advanced Encryption Standard proven to be the fastest algorithm runtime, with an average recording execution time of 62 milliseconds, making the algorithm most time efficient in this study. RC4 closely followed with 64 milliseconds, showing highest speed but due to its known vulnerabilities, has raised a serious concern. In comparison, 3DES depicted the slowest in performance at 107 milliseconds basically because of the algorithm triple round encryption process and high overhead processing. From the ethical hacking viewpoint, these results highlight the trade-off concerning security and speed, giving emphasis on performance only cannot decide the appropriateness of an encryption algorithm. This study determines that even though RC4 depicts quick execution, its weaknesses in security making it inappropriate for modern system security. AES shows potential as the most efficient and reliable choice for time critical and security application, 3DES is practically less in high

**Author for Correspondence*

performance environment. These contribute to better-informed decision-making when selecting cryptographic algorithms for information security.

Keywords: AES, Ethical Hacking, RC4, Time Efficiency, 3DES

INTRODUCTION

The rapid expansion of digital communication and data-driven systems has intensified global concerns about information security. As organizations increasingly rely on interconnected networks to store and transmit sensitive data, the need for robust cryptographic mechanisms has become more critical than ever.

Alguliyev *et al.*, (2021) noted that the widespread use of network systems, combined with the rapid advancement of digital technologies, has made information security a critical concern for governments, individuals, and organizations. Sensitive documents including personal information, financial records, industrial control as well as military communications are increasingly interconnected, stored and transmitted, thereby expanding their exposure to security vulnerabilities (Kumar and Ahmad, 2024). The roles of ciphering became significant and fundamentals in protecting sensitive data from unwanted access as well as malicious exploitations as cybercriminal activities continue to escalate (Gudepu and Jaladi 2022).

Symmetric key cryptography remains a core technique for securing electronic information due to its high efficiency and speed relative to asymmetric technique (Kapoor and Thakur, 2022). Sharma *et al.*, (2024) argued that Rivest Cipher2 (RC2), Triple Data Encryption Standard (3DES), Advance Encryption Standard (AES) and Rivest Cipher 4 (RC4) are also part of the symmetric algorithms that have been developed and implemented for the purpose of securing data. Various security applications have deployed these algorithms like database securing, communication protocol securing, and security network infrastructure as well as systems authentication (Omotunde and Ahmad, 2023).

However, cryptographic strength is not static; advancements in computational power and cryptanalytic techniques can render previously secure algorithms increasingly susceptible to cryptographic attacks, thereby necessitating continuous evaluation and standardization Ramakrishna *et al.*, (2024).

On the other hand, encryption strength algorithms are not always stable. As computing power increase and advanced, the algorithms that previously found to be secured vulnerable to modern attacks (Kshetri *et al.*, 2024). For example, RC4, has been found to suffer from statistical weaknesses and practical attack vectors (Singh *et al.*, 2024). While 3DES and RC2 face limitations in key strength and resistance to known cryptanalytic techniques. In comparison, AES remains widely accepted as a global cryptographic standard due to its resilience against practical attacks (Sarkar *et al.*, 2024).

Ethical hacking plays a crucial role in evaluating system security by simulating real-world attack scenarios to identify weaknesses in cryptographic implementations (Aslan *et al.*, 2023; Smith, 2024). Within this context, cryptanalysis serves not as an act of malicious intrusion, but as a proactive defensive technique for identifying vulnerabilities and promoting more secure alternatives (Onyema *et al.*, 2022; Gopalsamy & Dastageer, 2025).

Though, the efficiency of any symmetric cryptographic system is mostly determined by algorithm structures, resistance to cryptanalysis attacks, and key sizes. Ganesh *et al.*, (2025), as emphasized by the National Institute of Standards and Technology (NIST), stated that

insufficient key lengths as well as weak algorithm designs meaningfully increase vulnerabilities to statistical attacks and brute-force attempts, making numerous legacy algorithms inappropriate for modern security applications.

Numerous symmetric techniques or algorithms have been historically utilized, including RC4, RC2, AES, and 3DES (Sharma *et al.*, 2024). RC4 and RC2 were developed by Ronald Rivest and were globally accepted and utilized for their efficiency. However, these algorithms have subsequently been shown to contain structural vulnerabilities that make them susceptible to cryptanalytic practical attack. Perriello *et al.*, (2024) argued that 3DES presented as an improvement of DES, though its imperfect key strengths and low efficiency led to broken in numerous modern systems. Furthermore Buell (2021) argued that Rijndael was chosen by the NIST as the source for AES and presently considered among the most secured symmetric blocks cipher because of its robust linear resistance, brute-force attacks, and differential attacks.

There is an evident absence of practical comparative cryptanalysis conducted in the context of ethical hacking utilizing real-world document files, despite the availability of theoretical assessments of symmetric algorithms. Existing literature has mostly focused on automatically generated plaintext, which does not accurately imitate real deployment conditions. Additionally, there is limited attention given to evaluating time efficiency such as decryption and encryption time using uploaded documents from a computer such as TXT files, DOCX, and PDF. Weak encryption has been employed in many legacy systems because of compatibility requirements; however, there remains inadequate performance analysis, real-world risk exposure assessment, and empirical evidence to guide security professionals in identifying vulnerabilities.

Therefore, to address this gap, this study conducts a comparative cryptanalysis of AES, RC4, and 3DES within an ethical-hacking simulation environment using real uploaded document files. The performance of these algorithms is assessed based on time efficiency using a VB.NET-based simulation.

Research Questions

1. How does the time efficiency of RC4, AES, and 3DES compare when encrypting and decrypting real document files uploaded from a computer?
2. How does document size influence the encryption and decryption performance of RC4, AES, and 3DES?
3. Which algorithm demonstrates the best-case, average-case, and worst-case performance scenarios when processing different uploaded document types?

Methodology

A simulation-based approach using VB.NET was adopted to ensure controlled and repeatable testing conditions for evaluating the performance of AES, RC4, and 3DES. This approach aligns with prior empirical studies that evaluated symmetric encryption algorithms through controlled computational experiments in order to benchmark efficiency, execution time, and operational behavior under realistic workloads (Sharma *et al.*, 2024; Omotunde & Ahmad, 2023; Kapoor & Thakur, 2022). Performance-based evaluation of cryptographic algorithms has been widely adopted in the literature to complement theoretical security analysis and practical cryptanalytic assessments (Aslan *et al.*, 2023; Onyema *et al.*, 2022).

The approach was used in this study to measure encryption and decryption times for real document files because simulation environments enable researchers to model algorithmic behavior under multiple operating conditions without the logistical constraints of physical

deployment or live production systems (Alguliyev *et al.*, 2021; Gudepu & Jaladi, 2022). This supports controlled experimentation while maintaining relevance to real-world security applications.

A real uploaded document file, rather than synthetic plaintext, was selected to more accurately represent operational environments and to reflect how encryption algorithms behave under realistic workloads, consistent with applied cryptographic performance studies focusing on practical system behavior and deployment realism (Omotunde & Ahmad, 2023; Smith, 2024). The use of a 2 MB file size was chosen to balance computational manageability and practical relevance, reflecting the common document sizes encountered in business, academic, and communication systems (Kumar & Ahmad, 2024).

Each algorithm underwent 30 independent encryption-decryption cycles to minimize random variation and enhance reliability, in line with experimental rigor recommended in computational security evaluation studies (Aslan *et al.*, 2023; Gopalsamy & Dastageer, 2025). The VB.NET Stopwatch class was used to record time measurements in milliseconds with high precision. Repeated trials and controlled system conditions strengthen internal validity by reducing the influence of background processes, caching effects, and transient CPU states, thereby improving measurement consistency and reproducibility.

Simulation Environment

A standard personal computer running 64-bit Windows 10 Professional was used for all experiments. The system was equipped with an Intel® Core™ i5-7200U processor, 8 GB of RAM, and a 256 GB SSD. Visual Studio 2019 with the .NET Framework 4.8 was installed and used to develop and execute the encryption and decryption programs in VB.NET. The AES, RC4, and 3DES algorithms were implemented within a single VB.NET application, and a real document file of 2 MB was loaded into the application for encryption and decryption processing. For each experimental run, the application executed the selected algorithm, encrypted the input file, immediately decrypted the output, and recorded the execution time in milliseconds using the VB.NET Stopwatch class. This process was repeated for 30 independent cycles for each algorithm under the same hardware and software conditions. No additional applications were intentionally executed during testing in order to minimize background interference and maintain consistent system performance. The use of a 64-bit Windows 10 operating system, moderate hardware specifications, and a stable development environment ensured that all algorithms were evaluated under identical conditions. This controlled setup allowed performance differences observed in the results to be attributed primarily to algorithmic behavior rather than variations in hardware or software configuration, thereby supporting internal validity and practical interpretability of the findings.

Table 1 depicts the symmetric algorithms key assess based on time efficiency when decryption and encryption of document file from computer. It also depicts Cipher type, key sizes and specifications associated with each algorithm. This information provides an overview of the structural characteristics and operational parameters of AES, RC4, and 3DES, which are essential for understanding their performance differences in the subsequent analysis.

Algorithm	Key Sizes Tested	Type	Specification
AES	128-bit (Min), 256-bit (Max)	Block Cipher	FIPS PUB 197
RC4	40-bit (Min), 128-bit (Max)	Stream Cipher	RSA Security
3DES	112-bit (Min), 168-bit (Max)	Block Cipher	NIST FIPS PUB 46-3

Table 1: Evaluated Algorithms

Simulation Procedure

The simulation procedure was used to ensure that each algorithm was assessed under the same controlled conditions. Each test used a 2 MB plaintext file as the input to access algorithm performance. This keeps the evaluation consistent across the algorithms and to reflect a realistic document size commonly processed in practical environments. Using the same file size for all tests helps to avoid differences caused by file variation and allows the assessment to focus directly on the performance of the algorithms. Encryption Latency, Decryption Latency, and Total Runtime are the performance metrics that were assessed in this study. Encryption latency captures the time required to transform plaintext into ciphertext, while decryption latency measures the time needed to revert ciphertext back to plaintext. Evaluating both metrics independently provides insight into whether a given algorithm exhibits balanced performance across encryption and decryption tasks. The total runtime, calculated as the sum of both operations, offers a comprehensive measure of overall algorithmic efficiency during a full encryption decryption cycle.

Method of Time Measurement

- The diagnostic system timing measurements, recorded in milliseconds (ms), were obtained using the VB.NET Stopwatch class.
- Every cycle of encryption and decryption was carried out 30 times for every algorithm and key size to ensure consistency.
- After the completing the 30 trials, the average runtime was determined to represent the final performance value.

Test Execution Steps

The test execution steps were designed to ensure that each algorithm was evaluated under consistent, accurate, and controlled simulation conditions, as recommended for cryptographic performance evaluation studies (Sharma et al., 2024; Omotunde & Ahmad, 2023). The simulation environment was launched using the VB.Net cryptography simulation, which provides a stable platform for executing the encryption and decryption functions of the selected algorithms in a controlled software environment (Alguliyev et al., 2021; Aslan et al., 2023). Selecting the file directories for the encrypted file, decrypted file, and the document to be tested ensures that the system has correct access paths for all inputs and outputs. This step prevents file-handling errors and supports proper organization of the simulation outputs.

A document within the 2 MB size limit was uploaded from the computer to maintain uniformity across all tests. This file size reflects a realistic document type commonly used in business, academic, and communication environments while also ensuring computational manageability during repeated trials (Kumar & Ahmad, 2024; Omotunde & Ahmad, 2023). The algorithm to be tested (3DES, RC4, or AES) was then selected within the simulation environment. This selection allows the system to load the specific cryptographic routines associated with each algorithm and ensures that the correct encryption and decryption

procedures are executed. Clicking on the “Load File” button initiates the encryption or decryption process, and the stopwatch begins automatically. This automatic timing mechanism records the execution time in milliseconds with high precision, removing any possibility of manual measurement error and improving experimental reliability (Aslan et al., 2023; Onyema et al., 2022). These steps collectively ensure that every test cycle is executed systematically, accurately, and consistently, allowing reliable performance comparison across the algorithms.

Results

The cryptanalysis comparative analysis of AES, RC4, and 3DES through document files uploaded from a computer rather than automatically generated plaintext is depicted in the figures below. This research assesses their performance via time efficiency using a simulation technique. The simulation results in table 2, and Figure 1,2,3 show clear differences in performance among the evaluated algorithms. AES produced the fastest runtime, completing both encryption and decryption in 62 milliseconds. RC4 followed closely at 64 milliseconds, displaying only a minimal delay compared to AES. However, despite its speed, RC4s known structural vulnerabilities limit its applicability in secure systems. In contrast, 3DES recorded a significantly slower runtime of 107 milliseconds. This performance reduction is attributed to its triple encryption process, which increases computational workload. The wide gap between 3DES and the other algorithms is further reflected in the statistical summary, where 3DES disproportionately increases both the mean and standard deviation. Overall, AES demonstrates the most consistent and efficient performance, making it suitable for time-sensitive applications, while 3DES proves impractical for environments requiring rapid processing.

Table 2: Assessed/Evaluated Algorithms Observed Performance and Runtime

Algorithm	Runtime (Milliseconds)	Observed Performance
AES	62 milliseconds	Most time efficient and fastest
RC4	64 milliseconds	Slightly Slower, compared to AES but Very fast,
3DES	107 milliseconds	Slowest among the tested algorithms

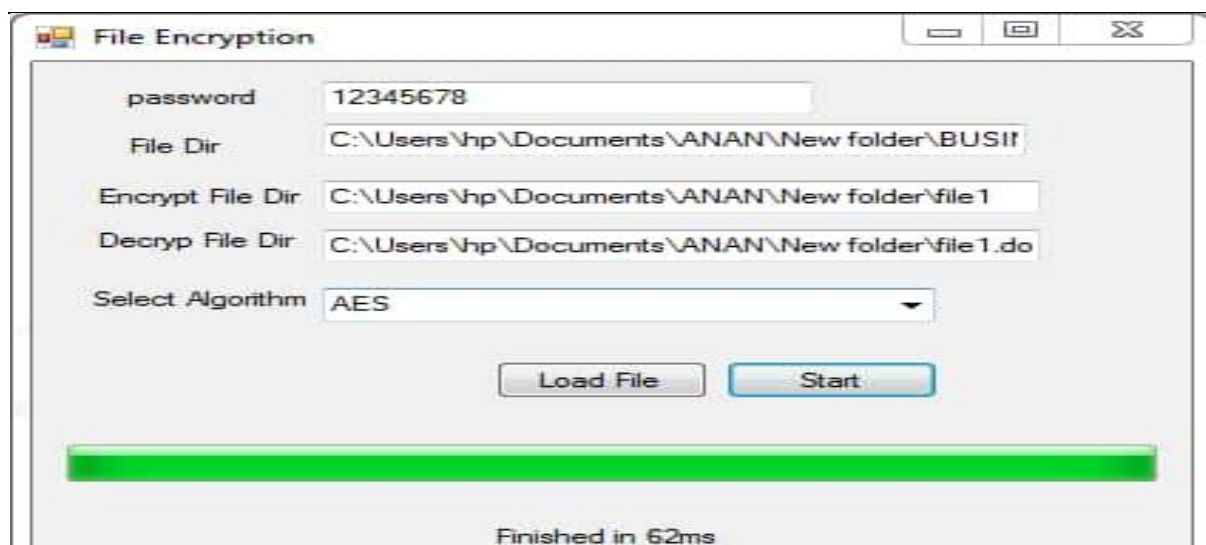


Figure 1: Simulation GUI of VB.Net for AES Algorithm time efficiency assessment

Figure 2: Simulation GUI of VB.Net for 3DES Algorithm time efficiency assessment

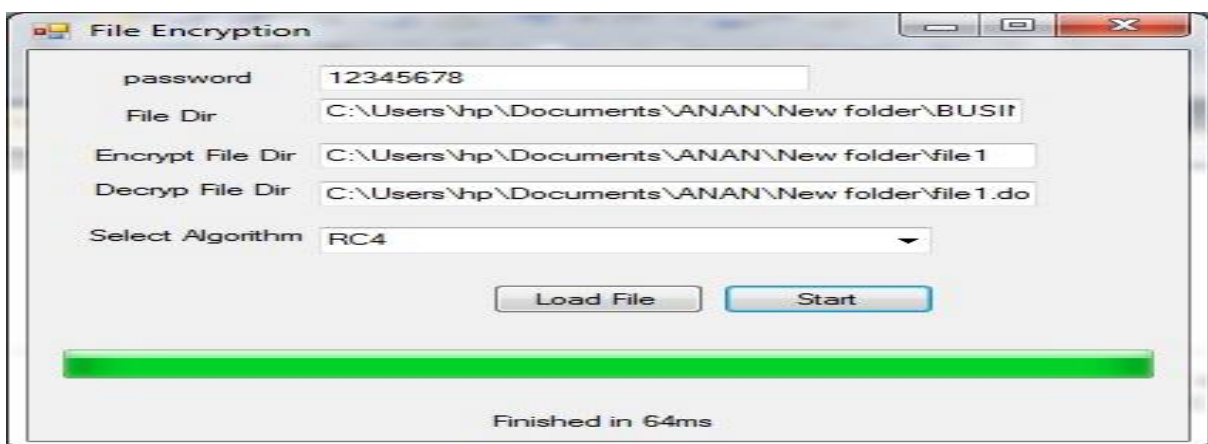
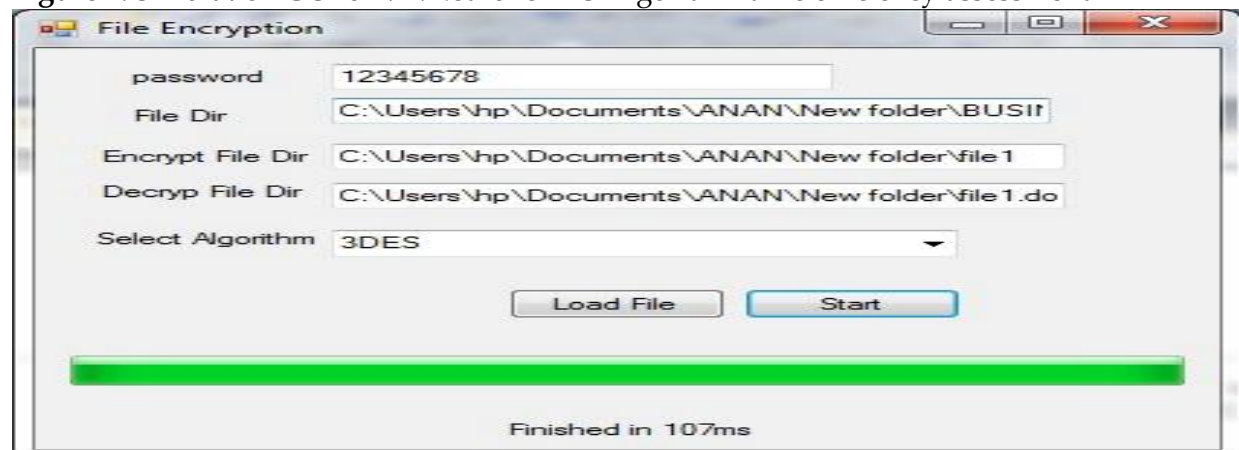


Figure 3: Simulation GUI of VB.Net for RC4 Algorithm time efficiency assessment

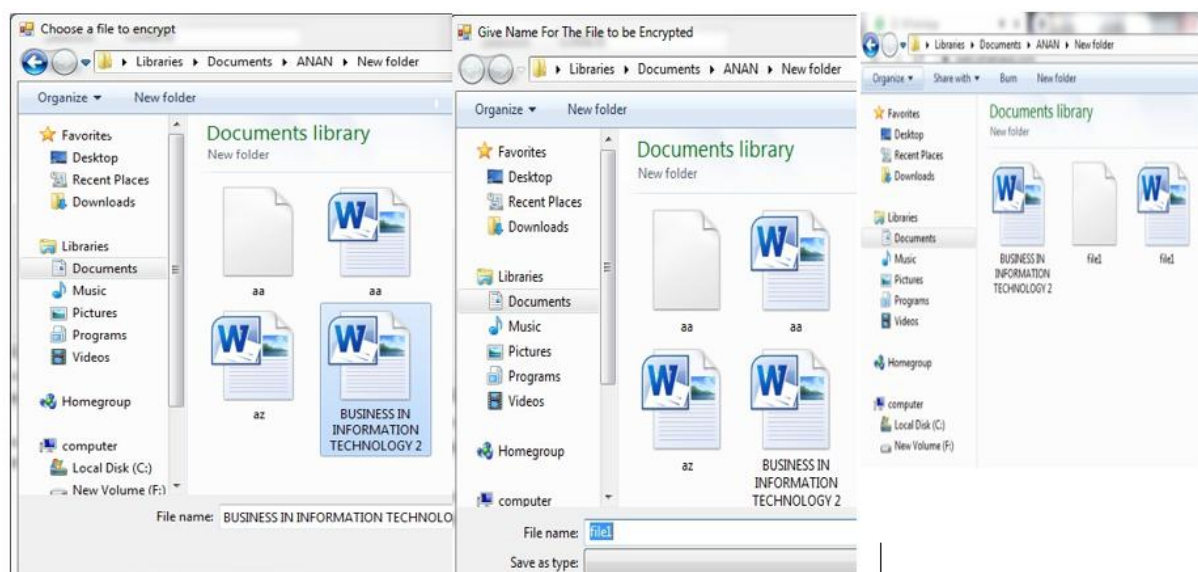


Figure 4: File to Encrypt (Business Information Technology2), renaming the file to be encrypted, and renamed file (File1)

Table 3 discusses the statistical summary of the results of this study, which clearly shows that the Advanced Encryption Standard (AES) finished the decryption and encryption procedures in 62 milliseconds, which is the lowest runtime recorded among the assessed algorithms. Rivest Cipher 4 (RC4) also finished the operation in 64 milliseconds, depicting a two-millisecond delay when compared to the Advanced Encryption Standard. In comparison, the Triple Data Encryption Standard (3DES) required 107 milliseconds, making it 45 milliseconds slower than AES and 43 milliseconds slower than Rivest Cipher 4. This difference is a direct result of Triple Data Encryption Standard executing three DES consecutive procedures for each data block, which essentially increases computational workload in the VB.Net simulation environment.

Due to the runtimes measured, the Advanced Encryption Standard depicts the highest time efficiency in processing document-uploaded files. In contrast, the Triple Data Encryption Standard depicts reduced efficiency for time-sensitive applications because of its high processing time. Although Rivest Cipher 4 performed close to AES in this assessment, its recognized cryptographic vulnerabilities limit its suitability for practical modern secured systems. As a result, for any application that requires both security and speed, the Advanced Encryption Standard is the most suitable algorithm among those assessed in this research. Figure 5 depicts the performance between the assessed symmetric algorithms while decrypting and encrypting of the document uploaded through the VB.Net simulation environment.

Table 3: Statistical Summary of Results

Statistic	Value in milliseconds
Mean which is the Average	77.67 milliseconds
Median	64 milliseconds
Minimum	62 milliseconds which is AES
Maximum	107 milliseconds which is 3DES
Range	45 milliseconds
Standard Deviation (The sample)	25.43 milliseconds
Standard Deviation (The population)	20.76 milliseconds

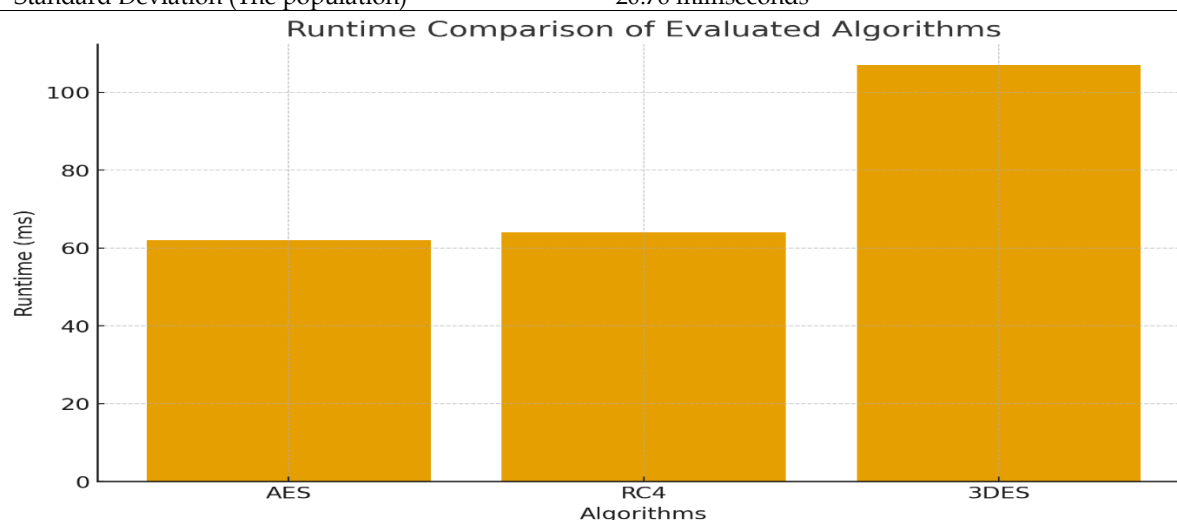


Figure 5: Runtime Comparison of valuated Algorithms

Performance Differences

Table 4 shows differences in performance among the assessed algorithms. Advanced Encryption Standard (AES) fastest recorded runtime of 62 milliseconds, stating the best-case scenario, while Triple Data Encryption Standard (3DES) depicts the slowest runtimes of 107

milliseconds stating the worst-case scenario. The overall processing time is averagely 77.67 milliseconds provided all the algorithms are measured together.

Table 4: Performance Differences

Scenarios	Algorithms	Runtime (milliseconds)	Interpretations
Best Case	AES	62 milliseconds	Most time efficient
Average Case	All combined	77.67 milliseconds	Largely mean runtime
Worst Case	3DES	107 milliseconds	Least efficient

Discussion

This research was carried out in the context of ethical hacking in which symmetric cryptography algorithms were exposed in a controlled cryptanalytic simulation to examine time efficiency and practical vulnerabilities (Aslan *et al.*, 2023; Onyema *et al.*, 2022). The assessed algorithms are 3DES, AES, and RC4, which represent diverse generations of security strength and cryptographic design, making them suitable comparative cryptanalysis candidates (Sharma *et al.*, 2024; Kapoor & Thakur, 2022). The assessment findings depict that AES recorded the fastest decryption and encryption time of 62 milliseconds, followed closely by RC4 at 64 milliseconds, while the Triple Data Encryption Standard (3DES) required the highest processing time of 107 milliseconds. Although Rivest Cipher 4 (RC4) was marginally slower than AES in this environment, the 2-millisecond difference is operationally insignificant in most computing scenarios, as similarly observed in symmetric performance benchmarking studies (Omotunde & Ahmad, 2023; Alguliyev *et al.*, 2021). However, cryptography extends beyond measuring speed; it also evaluates algorithm predictability, structural weaknesses, and resistance to attacks (Ganesh *et al.*, 2025; Kshetri *et al.*, 2024).

Rivest Cipher 4's performance benefit is explained through its stream-cipher structure, which operates by forming a pseudo-random keystream and integrating it with plain text data. RC4 tends to function faster than block ciphers due to this design (Singh *et al.*, 2024). However, Ramakrishna and Shaik (2024) point out that previous cryptographic attacks have revealed essential weaknesses in RC4, specifically in the key-scheduling algorithm, which produces biased outputs that can be exploited through known-plaintext, statistical, and chosen-plaintext attacks. In the ethical hacking context, this makes RC4 a high-risk algorithm regardless of its obvious speed (Aslan *et al.*, 2023). In comparison, research by Sarkar *et al.*, (2024) showed that the Advanced Encryption Standard has demonstrated both resilience and speed. As the standard successor of the Rijndael algorithm, AES utilizes a substitution-permutation network that is highly resistant to different cryptanalysis techniques, brute-force attacks, and linear cryptanalysis (Buell, 2021; Sarkar *et al.*, 2024). The robust performance recorded in this assessment confirms that high security does not necessarily require increased computational costs, which is consistent with earlier symmetric algorithm evaluations (Kapoor & Thakur, 2022). This makes AES a strong and appropriate candidate for protecting data in critical infrastructure environments where integrity, availability, and confidentiality are paramount (Alguliyev *et al.*, 2021).

The slow performance of 3DES is directly tied to its triple-round architecture, which applies the DES algorithm three times to each data block. Although this increases the key length compared to single DES, it does not provide security comparable to AES and instead introduces significant processing overhead (Periello *et al.*, 2024). Additionally, its 64-bit block size makes it vulnerable to birthday attacks in large-scale data environments, further limiting

its suitability for modern systems (Ganesh *et al.*, 2025). Within the ethical hacking framework utilized in this research, 3DES clearly demonstrates increased cryptographic obsolescence and reduced efficiency (Kshetri *et al.*, 2024). The outcome of this cryptanalytic assessment confirms that the Advanced Encryption Standard provides the best balance of speed and practical security, while 3DES and RC4 exhibit weaknesses that make them inappropriate for secure modern systems, in line with global cybersecurity recommendations and standardization guidance (Ganesh *et al.*, 2025; Sarkar *et al.*, 2024).

Conclusion

This research applied ethical hacking based cryptanalysis to assess time efficiency of 3DES, AES and RC4. The results depicts that AES is the most consistent runtime and scored fastest, closely followed by RC4 and 3DES significantly performed slower because of it is triple round processing. Despite the fact that RC4 speed, it is well known weaknesses makes it inappropriate for security application. Therefore, AES emerge as the most practical and reliable algorithm giving highest efficiency. The findings emphasize the essentials of ethical hacking simulation through generating evidence that is realistic in guiding encryption algorithms selection and outdated ciphers retirement.

References

- Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. S., & Aliguliyev, R. M. (2021): Information security as a national security component. *Information Security Journal: A Global Perspective*, 30(1), 1-18.
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023): A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
- Buell, D. (2021): Modern symmetric ciphers—Des and Aes. In *Fundamentals of Cryptography: Introducing Mathematical and Algorithmic Foundations* (pp. 123-147). Cham: Springer International Publishing.
- Ganesh, R., Khan, B. U. I., Khan, A. R., & Kamsin, A. B. (2025): A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges. *International Journal of Information Security*, 24(5), 1-45.
- Gopalsamy, M., & Dastageer, K. B. (2025): The Role of Ethical Hacking and AI in Proactive Cyber Defense: Current Approaches and Future Perspectives. *Int. J. Innov. Sci. Res. Technol*, 10(2).
- Gudepu, B. K., & Jaladi, D. S. (2022): Data Discovery and Security: Protecting Sensitive Information. *International Journal of Acta Informatica*, 1(1), 176-187.
- Kapoor, J., & Thakur, D. (2022): Analysis of symmetric and asymmetric key algorithms. In *ICT analysis and applications* (pp. 133-143). Singapore: Springer Nature Singapore.
- Kshetri, N., Rahman, M. M., Rana, M. M., Osama, O. F., & Hutson, J. (2024): algoTRIC: Symmetric and asymmetric encryption algorithms for Cryptography--A comparative analysis in AI era. *arXiv preprint arXiv:2412.15237*.
- Kumar, R., & Ahmad Khan, R. (2024): Securing military computing with the blockchain. *Computer Fraud & Security*, 2024(2).
- Omotunde, H., & Ahmed, M. (2023): A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of CyberSecurity*, 2023, 115-133.
- Onyema, E. M., Dinar, A. E., Ghouali, S., Merabet, B., Merzougui, R., & Feham, M. (2022): Cyber threats, attack strategy, and ethical hacking in telecommunications systems. In *Security and privacy in cyberspace* (pp. 25-45). Singapore: Springer Nature Singapore.

- Perriello, S., Barengi, A., & Pelosi, G. (2024, September): A Quantum Circuit to Execute a Key-Recovery Attack Against the DES and 3DES Block Ciphers. In *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)* (Vol. 1, pp. 1-12). IEEE.
- Ramakrishna, D., & Shaik, M. A. (2024): A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges. *IEEE Access*.
- Ramakrishna, D., & Shaik, M. A. (2024): A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges. *IEEE Access*.
- Sarkar, B., Saha, A., Dutta, D., De Sarkar, G., & Karmakar, K. (2024): A survey on the advanced encryption standard (AES): a pillar of modern cryptography. *International Journal of Computer Science and Mobile Computing*, 13(4), 68-87.
- Sarkar, B., Saha, A., Dutta, D., De Sarkar, G., & Karmakar, K. (2024): A survey on the advanced encryption standard (AES): a pillar of modern cryptography. *International Journal of Computer Science and Mobile Computing*, 13(4), 68-87.
- Sharma, P., Kumari, R., & Bansal, P. (2024, July): Cryptography: A Comparative Analysis of Symmetric and Asymmetric Techniques. In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* (pp. 1343-1348). IEEE.
- Sharma, P., Kumari, R., & Bansal, P. (2024, July): Cryptography: A Comparative Analysis of Symmetric and Asymmetric Techniques. In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* (pp. 1343-1348). IEEE.
- Singh, P., Dutta, S., & Pranav, P. (2024): A modified RC-4 cryptosystems to enhance security by using negative key schedule. *Security and Privacy*, 7(6), e438.
- Smith, A. (2024): Exploring the Use of Ethical Hacking Techniques in Strengthening Organizational Cybersecurity Defenses. *Global Research Perspectives on Cybersecurity Governance, Policy, and Management*, 8(12), 1-11.