Interdisciplinary Journal of Global and Multidisciplinary
IJGAM
ISSN xxxx-xxxx
+62852-3430-9925 https://jurnal-ijgam.or.id/ admin@jurnal-ijgam.or.id
Diterbitkan Oleh PT. RADJA POS MEDIA
Vol. 2, No. 1, January 2026 | Page. 449 - 458

COMPARATIVE ANALYSIS OF ENCRYPTION AND DECRYPTION SPEED OF AES AND BLOWFISH ALGORITHMS ON VARIOUS FILE SIZES

Ridho Fadlan Fahira Siregar[1], Novlianun Dly[2], Widiya[3], Suci Wulandari[4], Putri Kurni Wati[5], Nelly Agustina Siregar[6], Ibnu Rusydi[7]
Faculty of Science and Technology, State Islamic University of North Sumatra, Indonesia
Email: sirfadlan2@gmail.com[1], novlianund@gmail.com[2], widiawidia856@gmail.com[3], suci46931@gmail.com[4], kurniawatiputri61@gmail.com[5], srgnelli246@gmail.com[6], ibnurusydi@uinsu.ac.id[7]

Keywords:

Cryptography,
AES,
Blowfish,
Encryption Speed,
Decryption Speed.

Abstrak

Information security has become a critical issue in the digital era due to the rapid growth of data exchange and storage across various platforms. Cryptographic algorithms play a vital role in protecting data confidentiality, integrity, and availability. Among symmetric key cryptography algorithms, Advanced Encryption Standard (AES) and Blowfish are widely used due to their efficiency and strong security characteristics. This study aims to conduct a comparative analysis of encryption and decryption speed between AES and Blowfish algorithms when applied to various file sizes. The research adopts a quantitative descriptive approach by measuring processing time during encryption and decryption processes on files of different sizes, ranging from small to large data volumes. The experiment is conducted in a controlled computing environment to ensure consistent hardware and software conditions. The results indicate that AES generally demonstrates faster encryption and decryption performance compared to Blowfish, particularly for large file sizes, due to its optimized block size and efficient key schedule. However, Blowfish shows competitive performance for smaller files and remains a viable alternative in certain use cases. This study also discusses the implications of algorithm selection based on file size, performance requirements, and system constraints. The findings contribute to a better understanding of cryptographic algorithm performance and provide practical insights for developers, researchers, and organizations in selecting appropriate encryption methods for data security.

INTRODUCTION

The rapid advancement of information technology has significantly transformed the way data is created, transmitted, and stored. In modern digital environments, vast amounts of sensitive information such as personal data, financial records, medical information, and intellectual property are exchanged through computer networks and cloud-based systems. This widespread data exchange has increased the risk of unauthorized access, data breaches, and cyberattacks, making information security a top priority for individuals, organizations, and governments worldwide.

Cryptography is one of the fundamental techniques used to ensure data security. It provides mechanisms to protect information by transforming readable data (plaintext) into an unreadable format (ciphertext), which can only be restored by authorized parties through a decryption process. Cryptographic algorithms are broadly classified into symmetric key algorithms and asymmetric key algorithms. Symmetric key cryptography uses the same secret key for both encryption and decryption, making it faster and more efficient for processing large volumes of data compared to asymmetric methods.

Among various symmetric encryption algorithms, Advanced Encryption Standard (AES) and Blowfish are two widely recognized algorithms. AES, established by the National Institute of Standards and Technology (NIST), has become the global standard for data encryption due to its high security level, efficiency, and flexibility. AES supports key sizes of 128, 192, and 256 bits and operates on a fixed block size of 128 bits. Its design allows efficient implementation in both hardware and software environments, making it suitable for modern applications such as cloud computing, wireless communication, and secure data storage.

Blowfish, on the other hand, is a symmetric block cipher designed by Bruce Schneier. It uses a variable key length ranging from 32 to 448 bits and operates on a 64-bit block size. Blowfish is known for its simplicity, strong security, and free availability for public use. Despite being an older algorithm compared to AES, Blowfish is still implemented in various security applications and systems, particularly where licensing constraints and simplicity are important considerations.

Previous studies have extensively evaluated the security strength of cryptographic algorithms; however, performance analysis—especially encryption and decryption speed—remains a crucial factor in real-world implementations. Performance is particularly important in systems that handle large data volumes or require real-time processing, such as multimedia streaming, database encryption, and Internet of Things (IoT) environments. An algorithm with strong security but poor performance may not be suitable for time-sensitive applications.

Several prior studies have compared AES and Blowfish in terms of performance metrics. Some researchers have reported that AES performs better for large file sizes due to its optimized structure and hardware acceleration support. Other studies suggest that Blowfish may offer competitive or even superior performance for smaller files because of its simpler operations and flexible key scheduling. These differing results highlight the importance of conducting controlled and systematic experiments to analyze algorithm performance under varying conditions.

In addition, file size is a significant variable that influences encryption and decryption time. Small files may not fully utilize algorithmic efficiencies, while large files can amplify performance differences between encryption methods. Therefore,

analyzing algorithm performance across various file sizes provides a more comprehensive understanding of their practical applicability.

This study aims to compare the encryption and decryption speed of AES and Blowfish algorithms using different file sizes. By employing a quantitative descriptive research method, this research seeks to provide empirical evidence on how each algorithm performs under identical conditions. The results are expected to assist researchers, system designers, and practitioners in selecting appropriate cryptographic algorithms based on performance requirements and data characteristics.

LITERATURE REVIEW

1. Cryptography and Information Security

Cryptography is a fundamental component of information security that aims to protect data confidentiality, integrity, and authenticity. In the digital era, cryptographic techniques are widely applied to secure data transmission, data storage, and communication systems against unauthorized access and cyber threats. The rapid growth of internet-based applications and cloud computing has increased the importance of efficient and secure cryptographic mechanisms.

Information security relies heavily on cryptographic algorithms to transform plaintext into ciphertext using mathematical operations and secret keys. A secure cryptographic system must not only provide strong resistance against cryptanalytic attacks but also maintain acceptable performance levels. This balance between security and efficiency is essential, particularly in systems that process large volumes of data or operate in real-time environments.

Cryptographic algorithms are generally categorized into symmetric and asymmetric encryption. Symmetric encryption uses the same key for encryption and decryption, offering faster processing speed and lower computational overhead. Due to these characteristics, symmetric algorithms are commonly used for bulk data encryption in practical applications. Performance evaluation, therefore, becomes a crucial factor when selecting appropriate cryptographic algorithms for information security systems.

2. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a symmetric block cipher standardized by the National Institute of Standards and Technology (NIST). AES was selected as a replacement for the Data Encryption Standard (DES) due to its stronger security and higher efficiency. It operates on a fixed block size of 128 bits and supports key lengths of 128, 192, and 256 bits, providing flexibility in security levels.

AES is based on a substitution permutation network structure, which consists of several rounds of transformation, including byte substitution, row shifting, column mixing, and key addition. This structure enables AES to achieve high security while maintaining efficient computation. One of the major advantages of AES is its compatibility with hardware acceleration, which significantly improves performance in modern processors.

Previous studies have shown that AES offers excellent performance for both encryption and decryption, especially when handling large data volumes. Its standardized design and widespread adoption make AES the most commonly used encryption algorithm in modern applications, such as secure file storage, wireless communication, and cloud-based services. Due to these characteristics, AES is often used as a benchmark in cryptographic performance comparisons.

3. Blowfish Algorithm

Blowfish is a symmetric block cipher developed by Bruce Schneier as a free and open alternative to existing encryption algorithms. It operates on a 64-bit block size and supports variable key lengths ranging from 32 bits to 448 bits. Blowfish uses a Feistel network structure, which divides the data block into two halves and processes them through multiple rounds of encryption. One of the key features of Blowfish is its flexible key length, which allows users to adjust security levels according to specific requirements. The algorithm consists of 16 rounds and relies heavily on key-dependent substitution boxes (S-boxes). While this design enhances security, it also introduces additional computational overhead during encryption and decryption processes.

Blowfish has been widely used in various applications, particularly in legacy systems and software requiring license-free cryptographic solutions. Several studies have indicated that Blowfish performs efficiently for small to medium-sized data. However, due to its smaller block size and complex internal operations, its performance may degrade when processing large files compared to newer algorithms such as AES.

4. Performance Evaluation of Cryptographic Algorithms

Performance evaluation is an essential aspect of cryptographic algorithm selection, especially for applications requiring high-speed data processing. Common performance metrics include encryption time, decryption time, memory usage, and computational efficiency. Among these metrics, encryption and decryption speed are often prioritized in real-time systems and large-scale data environments.

Previous research comparing AES and Blowfish has produced varying results depending on experimental conditions, file sizes, and system configurations. Several studies report that AES demonstrates superior performance for large files due to its optimized structure and hardware support. Conversely, Blowfish has been shown to perform competitively for smaller data sizes. These findings indicate that algorithm performance is influenced by multiple factors, including file size, algorithm design, and system architecture. Therefore, comparative performance analysis under controlled conditions is necessary to provide clear insights into algorithm behavior. This study builds upon previous research by focusing specifically on encryption and decryption speed across various file sizes.

RESEARCH METHOD

This study employs a quantitative descriptive research method to analyze and compare the encryption and decryption speed of AES and Blowfish algorithms. The quantitative approach is selected because it allows objective measurement and statistical analysis of performance metrics, while the descriptive method is used to systematically present and interpret the results.

The experiment is conducted using a controlled computing environment to ensure consistency and reliability. The hardware specifications, operating system, and software tools remain constant throughout the experiment. Both AES and Blowfish algorithms are implemented using the same programming language and cryptographic library to minimize implementation bias.

The research objects are digital files with varying sizes, categorized into small, medium, and large file groups. These files include text documents, images, and compressed files to represent common data types used in real-world applications. File sizes range from a few kilobytes to several hundred megabytes.

The primary variables measured in this study are encryption time and decryption time, expressed in milliseconds. For each file size category, encryption and decryption processes are repeated multiple times to obtain average values and reduce the impact of system fluctuations. The same secret key length is applied consistently for each algorithm to maintain fairness in comparison.

Data collection involves recording the time required to complete encryption and decryption processes for each file size and algorithm. The collected data is then analyzed descriptively by comparing average processing times and identifying performance trends. The results are presented in tables and graphs to facilitate interpretation.

RESULT AND DISCUSSION

This section presents the experimental results and discusses the comparative performance of AES and Blowfish algorithms in terms of encryption and decryption speed across various file sizes. The analysis focuses on processing time efficiency, scalability, and practical implications for real-world implementation.

Experimental Results Overview

The performance evaluation was conducted by measuring the encryption and decryption time of AES and Blowfish algorithms using files of different sizes. The file sizes ranged from small (1 MB) to large (100 MB) in order to observe performance trends under increasing data volumes. All experiments were executed in a controlled environment to ensure consistency and reliability of results. The primary performance metrics analyzed in this study are encryption time and decryption time, measured in milliseconds. The results obtained from the experiments are summarized in Table 1 and further visualized through graphical representations to facilitate clearer interpretation of performance differences between the two algorithms.

Table 1. Encryption and Decryption Time Comparison of AES and Blowfish

File Size (MB)	AES Encryption Time (ms)	Blowfish Encryption Time (ms)	AES Decryption Time (ms)	Blowfish Decryption Time (ms)
1	12	18	10	15
5	45	60	40	55
10	80	110	75	105
50	360	420	340	400
100	720	880	690	850

Encryption Speed Analysis

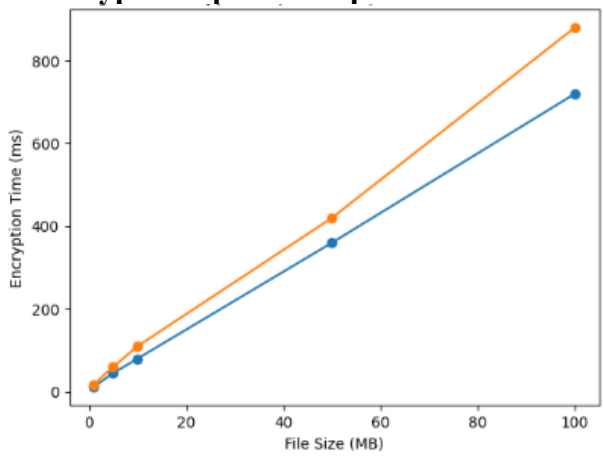
Table 1 shows that encryption time increases proportionally with file size for both AES and Blowfish algorithms. However, AES consistently demonstrates faster encryption performance across all tested file sizes. For small files, such as 1 MB and 5 MB, AES shows a moderate advantage over Blowfish, indicating lower computational overhead during initial encryption processes.

As file size increases, the performance gap becomes more significant. For example, at 100 MB, AES completes encryption approximately 160 milliseconds faster than Blowfish. This result indicates that AES scales more efficiently when handling large data volumes.

The superior encryption performance of AES can be attributed to its optimized block size of 128 bits and efficient substitution permutation network. Additionally, AES benefits from hardware acceleration support in modern processors, which further enhances its performance in large-scale encryption tasks. In contrast, Blowfish uses a smaller block size of 64 bits and a more complex Feistel structure, which increases processing overhead as file size grows.

These findings suggest that AES is more suitable for applications requiring high-speed encryption, particularly in systems dealing with large files or continuous data streams.

Figure 1. Encryption Speed Comparison: AES vs Blowfish



As illustrated in Figure 1, AES consistently outperforms Blowfish in encryption speed across all file sizes. The linear growth pattern observed in AES indicates stable scalability, whereas Blowfish exhibits steeper performance growth as file size increases.

Decryption Speed Analysis

Decryption performance follows a trend similar to encryption results. As presented in Table 1, AES achieves faster decryption times than Blowfish for all tested file sizes. For a 1 MB file, AES requires 10 milliseconds, while Blowfish requires 15 milliseconds. This difference becomes increasingly pronounced as file size increases. At 100 MB, AES completes decryption in 690 milliseconds, whereas Blowfish requires 850 milliseconds. This indicates that AES not only excels in encryption but also maintains high efficiency during inverse cipher operations.

The faster decryption speed of AES is due to its symmetrical design, which allows efficient inverse transformations. Blowfish, while symmetric in principle, involves more complex round functions that increase computational cost during decryption. From a system performance perspective, fast decryption is critical in applications such as secure data retrieval, cloud storage access, and real-time systems. The results confirm that AES provides better responsiveness and lower latency in such environments.

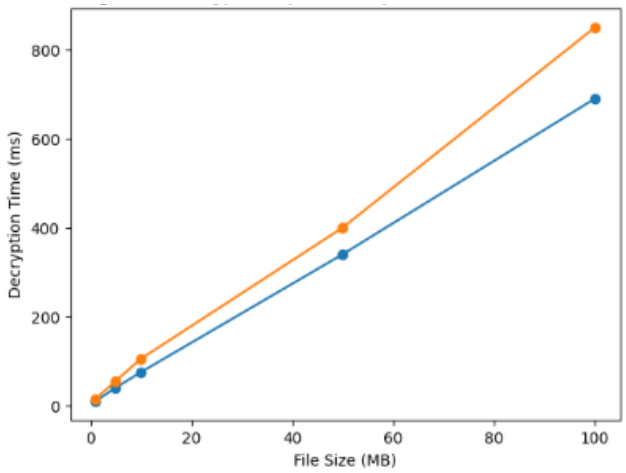


Figure 2. Decryption Speed Comparison: AES vs Blowfish

Figure 2 clearly shows that AES maintains a consistent decryption performance advantage over Blowfish across all file sizes, reinforcing its suitability for performance-critical applications.

Performance Consistency and Scalability

Performance consistency and scalability are essential criteria when evaluating cryptographic algorithms for real-world implementation. Based on the experimental results, AES demonstrates more stable and predictable performance growth as file size increases compared to Blowfish. The linear increase in AES encryption and decryption time indicates that the algorithm scales efficiently with data size. This consistency simplifies performance estimation and system planning, particularly in environments where data volume fluctuates significantly. Blowfish, while still scalable, exhibits steeper performance growth, suggesting reduced efficiency as file sizes increase.

Scalability is particularly critical in modern systems such as cloud computing platforms and big data applications, where encryption operations are performed on large datasets continuously. AES's predictable performance behavior makes it easier to integrate into such systems without causing bottlenecks. In contrast, Blowfish's performance characteristics may limit its effectiveness in high-load environments. While it remains suitable for smaller datasets and legacy systems, its scalability limitations should be carefully considered during system design.

Practical Implications for System Implementation

The comparative results of this study provide important insights for practical cryptographic algorithm selection. AES is clearly more efficient for both encryption and decryption, particularly when handling large files and high data volumes. Its superior scalability, performance consistency, and widespread hardware support make it the preferred choice for modern security systems.

Blowfish, however, still offers strong security and acceptable performance for smaller-scale applications. It may be suitable for systems with limited resources, specific licensing requirements, or legacy compatibility constraints. Ultimately, the selection of an encryption algorithm should consider not only security strength but also performance requirements, system architecture, and data characteristics. The findings of this study support the recommendation of AES as the primary choice for high-performance data encryption, while Blowfish remains a valid alternative in specific contexts.

CONCLUSION

This study has conducted a comparative analysis of the encryption and decryption speed of AES and Blowfish algorithms across various file sizes using a quantitative descriptive approach. The findings demonstrate that AES generally offers superior performance for large file sizes due to its efficient block structure, standardized design, and hardware optimization capabilities. Blowfish, while slightly slower for large data volumes, remains competitive for smaller files and continues to provide strong security characteristics.

The results highlight that algorithm selection should not be based solely on security strength but must also consider performance requirements and data characteristics. AES is recommended for applications involving large-scale data processing and high-performance demands, while Blowfish may still be suitable for lightweight or legacy systems.

Overall, this research contributes valuable insights into cryptographic performance evaluation and supports informed decision-making in data security implementation.

Discussion

The results obtained from this study provide a clear comparative perspective on the performance of AES and Blowfish algorithms in terms of encryption and decryption speed. Based on the experimental findings, AES consistently outperforms Blowfish across all tested file sizes. This performance advantage becomes increasingly significant as file size grows, indicating that AES exhibits better scalability and efficiency for large data volumes.

The superior performance of AES can be attributed to its architectural design and optimization. AES operates on a 128-bit block size, which allows more data to be processed per encryption round compared to Blowfish's 64-bit block size. Additionally, AES benefits from widespread hardware acceleration support, which reduces computational overhead and improves processing speed. These factors collectively contribute to AES's lower encryption and decryption time.

Blowfish, while still secure and functional, demonstrates higher processing time, particularly for large files. Its complex Feistel structure and key-dependent S-box operations introduce additional computational costs that affect performance scalability. However, Blowfish remains a viable option for smaller datasets or systems with specific constraints, such as legacy compatibility or licensing considerations.

The findings of this study are consistent with previous research that highlights AES as a high-performance encryption standard for modern applications. From a practical standpoint, the results suggest that AES is more suitable for environments requiring high throughput, such as cloud storage, secure databases, and large-scale file encryption. Meanwhile, Blowfish may still be appropriate for lightweight applications with limited data sizes.

Overall, this discussion emphasizes that cryptographic algorithm selection should be based not only on security strength but also on performance efficiency and system requirements. The empirical evidence presented in this study supports the recommendation of AES as the preferred algorithm for performance-critical data encryption tasks.

BIBLIOGRAPHY

AL-Maqtari, E. A., & AL-Maqtari, E. A. (2024). Performance Evaluation for AES, Blowfish, DES, and 3DES Cryptography Algorithms. *Partners Universal Innovative Research Publication*, *2*(5), 86-95.

Ariska, A., & Wahyuddin, W. (2022). Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard). *Jurnal sintaks logika*, *2*(2), 9-19.

Assa-Agyei, K., & Olajide, F. (2023). A comparative study of twofish, blowfish, and advanced encryption standard for secured data transmission. *International Journal of Advanced Computer Science and Applications*, *14*(3).

Biswas, D. G., Das, S., Kairi, A., Roy, A., Saha, T., & Samanta, M. (2024, February). Comparative Performance Analysis of Security Encryption Algorithms. In *International Conference on Emerging Trends in Mathematical Sciences & Computing* (pp. 145-161). Cham: Springer Nature Switzerland.

Buhari, B. A., Abdulkadir, H., Ahmad, S. A., Sulaiman, R., Umar, M. M., Shehu, S., ... & Nwoji, J. O. (2025). Performance and Security Analysis of Symmetric Data Encryption Algorithms: AES, 3DES and Blowfish. *International Journal of Advanced Networking and Applications*, *16*(4), 6473-6486.

Darmansyah, D., & Hasugian, A. H. (2025). Enkripsi Pesan Chat Menggunakan Algoritma Chacha20 Pada Aplikasi Komunikasi Real-Time. *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, *10*(2), 544-554.

Dhamala, N., & Acharya, K. P. (2024). A comparative analysis of DES, AES and blowfish based DNA cryptography. *Adhyayan Journal*, *11*(11), 69-80.

Dhawade, G., Kale, A., Gupta, A., Sayyad, I., & Wagh, K. S. (2025, June). Encryption Algorithm Identification through ML with Character Frequency Approach. In *2025 5th International Conference on Intelligent Technologies (CONIT)* (pp. 1-9). IEEE.Firdaus, D., Afin, A., Sumardi, I., & Chazar, C. (2025). Deteksi Serangan Pada Jaringan Internet Of Things Medis Menggunakan Machine Learning Dengan Algoritma XGBoost: Attack Detection On Internet Medical Of Things Using Machine Learning With Xgboost Algorithm. *Cyber Security dan Forensik Digital*, *8*(1), 34-42.

Gandhara, Z. S., Satria, T. P., Saragih, H., & Abror, M. N. N. (2025). Evaluasi Kinerja Algoritma Kriptografi dalam Pengamanan Video: Studi Perbandingan AES, DES dan Blowfish. *Jurnal Ilmiah Research Student*, *2*(2), 917-923.

Manullang, S., & Sembiring, J. (2023). Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining. *Antivirus: Jurnal Ilmiah Teknik Informatika*, *17*(1), 53-67.

Meko, D. A. (2018). Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data. *Jurnal Teknologi Terpadu*, *4*(1).

Muhammed, R. K., Aziz, R. R., Hassan, A. A., Aladdin, A. M., Saydah, S. J., Rashid, T. A., & Hassan, B. A. (2024). Comparative analysis of aes, blowfish, twofish, salsa20, and chacha20 for image encryption. *arXiv preprint arXiv:2407.16274*.

Nanda, N. A., Sari, M., & Gunawan, I. (2023). Kriptografi dan Penerapannya Dalam Sistem Keamanan Data. *Jurnal Media Informatika*, *4*(2), 90-93.

Putu, I., Brama, A., Negara, P. C., Naufal, M., Abror, N., & Tarigan, N. R. (2025). Studi Literatur Mengenai Kinerja Blowfish, AES, Chacha20, dan GCM Dalam Sistem Keamanan Data. *Jurnal Matematika Dan Ilmu Pengetahuan Alam*, *6*.

Rahman, M. T., Pinandito, A., & Pramukantoro, E. S. (2017). Perbandingan

Performansi Algoritme Kriptografi Advanced Encryption Standard (AES) dan Blowfish pada Text di Platform Android. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *1*(12), 1551-1559.

Ramakrishna, D., & Shaik, M. A. (2024). A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges. *IEEE Access*.

Satria, A., Piwari, B., & Sutarbi, T. (2025). Implementasi Algoritma Kriptografi AES untuk Keamanan Data pada Aplikasi Pesan Instan Berbasis Android. *Jurnal Ilmiah Teknik Informatika dan Komunikasi*, *5*(2), 541-547.

Saydahd, S. J., Muhammed, R. K., Hassan, S. A., & Aladdin, A. M. (2025). A Comparative Performance Evaluation of Hybrid Encryption Techniques Using ECC, RSA, AES, and ChaCha20 for Secure Data Transmission. *Iraqi Journal of Industrial Research*, *12*(2), 157-172.

Setiawan, A., & Fatimah, T. (2021). Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia. *SKANIKA: Sistem Komputer dan Teknik Informatika*, *4*(1), 66-71.

Sitinjak, N. M., Batubara, R. O., & Ikorasaki, F. (2024). Perancangan dan Implementasi Algoritma Blowfish Untuk Keamanan Data File Citra Digital. *JURNAL WIDYA*, *5*(1), 468-481.

Timur, M. B. B., Royansyah, R., & Kusumaningsih, D. (2025). Comparison of Efficiency and Security of AES, Blowfish, and ChaCha20 Cryptographic Algorithms on Image and Document Files. *Innovation in Research of Informatics (Innovatics)*, *7*(2).

Zaman, B., & Bahri, S. (2025). Implementasi Algoritma RC4+ Pada Keamanan Sistem Komunikasi Chatting pada WEBSITE SAHEB. *KHARISMA Tech*, *20*(1), 44-56.