# An Empirical Evaluation of Encryption and Decryption Times on Block Cipher Techniques

Funminiyi Olajide[1]
Department of Computer Science
Nottingham Trent University
Nottingham
United Kingdom
Email: funminiy.olajide@ntu.ac.uk

Kwame Assa-Agyei[1]
Department of Computer Science
Nottingham Trent University
Nottingham
United Kingdom
Email: kwame.assa-agyei@ntu.ac.uk

Christopher Edo [2]
Department of Information Systems
Auburn University
Alabama
United State of America
Email: oedo@aum.edu

***Abstract*—The significant majority of individuals in today's technology environment use the Internet for various purposes. Most often, data sent via the Internet contains private or confidential information that people desire to keep private. As a result, a variety of encryption techniques are extensively used and accessible in information security. Encryption techniques are used to handle different file types or formats over the Internet. This study examines the encryption and decryption times of 3DES, Twofish, and AES utilizing various file formats and constant block sizes of 128 bits. Moreover, the study examined the effectiveness of Blowfish by analyzing its performance with varying key sizes of 128, 192, and 256 bits, while maintaining a fixed block size of 64 bits. However, no study has examined various key bit sizes utilizing a constant block size on these algorithms with diverse file types in more depth up to this point. Cryptographic methods have the drawback of using a lot of computational resources, including CPU time, memory, and battery power. The study analyzed various symmetric encryption algorithms, namely AES, Twofish, 3DES, and Blowfish, and their performance for encrypting and decrypting data files with fixed block sizes. AES's 256 key bit size was determined to be the best for encrypting while using key sizes of 192 and 256 bits can enhance decryption speed. In the case of Blowfish, the 256-key-bit size was found to be more efficient than its 128 and 192-bit counterparts, particularly when dealing with a block size of 64 bits. To enhance the speed of both encryption and decryption processes, the study recommends the utilization of key bit sizes of 192 and 256. The results show that Blowfish can match the encryption and decryption speeds of AES.**

***Keywords*— Cryptography, Twofish, Blowfish, AES, 3DES, data encryption, decryption**

## I. INTRODUCTION

Securing information is a challenge in the modern digital age, as terabytes of data are generated daily on the Internet and online transactions occur virtually every second [1]. The only way to secure data transmitted over the Internet is by using encryption methods. Data is scrambled via encryption so that it cannot be decoded even if it is intercepted. The ultimate focus of encryption is to make data access by unauthorized users extremely difficult or impossible. When sending data via a network, such as the local area network or the Internet, encryption is a possibility. Accessing encrypted data legitimately is known as decryption [2]. Depending on the kind of security keys used to encrypt/decrypt the data, there are two primary categories of cryptography. Asymmetric and symmetric encryption algorithms fall under these two groups [3]. A single key is used to encrypt and decrypt data in symmetric key encryption or secret key encryption. Two keys are utilized in asymmetric keys: private and public keys. Both the public key and the private key are used for encryption and decryption respectively (e.g. RSA and ECC) [4]. Unfortunately, the strong encryption scheme requires extensive computation time and is very complex [5]. Typically, an implementation of cryptography is comprised of computationally intensive algorithms which are used for securing data within applications. As a result, these complex cryptographic algorithms have performance issues on general-purpose systems. They consume a lot of computer resources while executing encryption techniques. The aim of this study is to compare the performance of AES, Twofish, and 3DES symmetric encryption algorithms with respect to their encryption and decryption speed. The analysis is based on the variation of AES, Twofish, and 3DES key bit sizes while using a consistent block size of 128 bits. The research is conducted using two different approaches: (1) evaluating the simulation of 128, 192, and 256 key bit sizes of AES, Twofish, and 3DES with different file extensions and a block size of 128 bits, and (2) assessing the performance of Blowfish with 128, 192, and 256 key bit sizes and a block size of 64 bits. Many cryptographic algorithms have been analyzed and published, but none of these previous works have conducted an empirical analysis based on key bits comparisons of AES, Twofish, and 3DES using constant block sizes to ascertain how well they perform in terms of process time and other factors.

979-8-3503-2759-5/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCE60160.2023.00386

This paper analyzes and compares the performance of selected algorithms, namely: AES (Rijndael), Twofish, and 3DES. This study addresses the following research questions.
RQ1: Which key bit sizes of the algorithms AES, Twofish, and 3DES work best in terms of encryption and decryption times when using a consistent block size of 128 bits?
RQ2: How does the performance of the Blowfish algorithm vary with different key bit sizes and a fixed block size of 64 bits?
RQ3: Which key bit size performs better with different file extensions? Hence, the current study makes the following contributions.

i. To perform an extensive evaluation of the encryption and decryption times of AES, Twofish and 3DES using a block size of 128 bits
ii. To analyze the performance of AES, Twofish, and 3DES using varying key bit sizes of 128, 192 and 256.
iii. To further analyse the performance of Blowfish with key bit sizes of 128, 192, and 256, while maintaining a fixed block size of 64 bits

The rest of the paper is organized as follows: Section II presents the related work. The experimental setup is also presented in Section III. Section IV and V present the performance results and discussion of this research respectively. Finally, the conclusion is presented in section VI.

## II. RELATED WORK

AES, 3DES, Blowfish, and Twofish were the focus of an empirical investigation by Dibas and Sabri. The outcome demonstrated that, in terms of execution time, AES is the most effective encryption and decryption algorithm. In terms of encryption and decryption, Blowfish performed far better than 3DES. The findings obtained by Twofish were the worst. The authors found that, in terms of memory usage for encryption, AES and 3DES used less memory whereas Blowfish and Twofish used more memory and had the largest ciphertext sizes [6]. Nema and Rizvi [7] examined different symmetric key cryptographies to determine their plusses and minuses. The main goal was to inform the audience on the right cryptographic algorithm to adopt in their applications or solutions. The examination revealed that Blowfish performed the best among all encryption algorithms in terms of security, adaptability, memory utilisation, and encryption speed. Tyagi and Ganpati [8] investigated the encryption and decryption times and throughput of Blowfish, DES, 3DES, and AES. The DES, 3DES, and AES symmetric key encryption techniques are all slower than the blowfish algorithm. Finally, it was determined that Blowfish outperformed DES, 3DES, and AES in terms of throughput, encryption time, and decryption time. 3DES has the least performance among all mentioned algorithms. Anand Kumar and Karthikeyan [9] conducted a comparison study on the effectiveness of the Blowfish and Rejindael (AES) algorithms for the chosen cryptographic algorithms in terms of energy consumption, changing data types like text or documents and images, power consumption, changing packet size, and changing key size. The simulation findings revealed that Blowfish surpasses AES in almost all of the test scenarios. The study found that while AES is better for image encryption, blowfish is better for text-based encryption. It is also shown that performance changes when the AES algorithm's key size is altered. Overall, the study found that AES can be used in circumstances needing a high level of security. Blowfish, however, is a performance-wise viable option. Gautam et al. [10] conducted an experiment on cryptographic algorithms to analyze their performance and usage. The outcomes of the research on AES and TWOFISH are regarded as the two top candidates for achieving the aims of the study focus. These two outperform the other encryption methods in terms of speed, entropy, and optimal encoding, however, AES still has an advantage over TWOFISH due to its higher efficiency. The authors in [11] analysed the parameters of various cryptographic techniques, including AES and Blowfish, for performance, including encryption speed, CPU usage over time, and battery consumption. The outcomes showed that in terms of processing speed and throughput, the Blowfish approach performed better than the AES algorithm. The algorithm has a higher throughput while running more quickly and with less energy. According to the study, blowfish is the best option. In 2020, Gosh conducted a side-by-side comparison of the three algorithms AES, Blowfish, and Twofish while taking into account various factors like speed and computation time. Conclusion: In terms of the evaluated evaluation measures, such as encryption time, decryption time, and throughput, Twofish clearly outperformed AES and Blowfish [2]. The study conducted a comparative analysis of five symmetric key cryptographic algorithms namely: DES, 3DES, Blowfish, Twofish, and Threefish. The results indicated that Blowfish outperformed the other algorithms examined. The study emphasizes the need to select an appropriate algorithm that meets specific performance and security requirements. The paper offers valuable insights into the advantages and drawbacks of various encryption algorithms and their practical applications [12]. Mota et al. [13] evaluated the various encryption methods for secure data transmission. The study came to the conclusion that Blowfish outperformed AES, DES, and 3DES in terms of encryption and decryption times, power use, memory utilisation, latency, jitter, and security level. A fair comparison of the four most popular encryption algorithms—AES, DES, 3DES, and Blowfish in terms of security and power consumption was presented by Singh et al. The outcomes of the simulation demonstrated that AES performed better than other popular algorithms [14]. Singh and Supriya [15] reviewed in-depth the well-known encryption methods such as RSA, DES, 3DES, and AES. They added that a variety of encryption techniques are available and that the advantages and disadvantages of each algorithm will determine which method is optimal for encrypting plain text. Each method is effective for real-time encryption. Each technique is distinctive in its own way, may

be appropriate for various purposes, and has advantages and disadvantages of its own. The AES algorithm has been shown to be the most effective in terms of speed, time, throughput, and the avalanche effect, according to studies and a literature review. Ramesh and Suruliandi [16] evaluated the efficacy of some few particular symmetric algorithms in 2013. The experimental findings and input text file size led to the conclusion that the Blowfish method generates higher throughput while requiring less execution time and memory. In comparison to AES and DES, B1owfish performed around four times faster. Comparing Blowfish to AES and DES, memory usage is lower. Since AES required more computing resources than other algorithms, its performance results were subpar. Blowfish is not only the quickest encryption algorithm, but it also offers excellent security because of its large key size, making it suitable for usage in a wide range of applications, including packet encryption, random bit generation, internet-based security, and many more. The most popular encryption method, particularly in financial applications, is DES. AES is helpful for objects that are used in games or anything that involves financial transactions and is perfect for encrypting communications transferred between objects via chat channels. To determine which method was superior, the authors in [3] analyzed the performance of the three most popular symmetric cryptography algorithms: DES, AES, and Blowfish. The simulation results demonstrated that Blowfish performs better than other widely used encryption techniques. Blowfish is a strong candidate to be used as a standard encryption method because it currently has no known security vulnerabilities. Since AES required more computing resources than other algorithms, its performance results were subpar. Even though using CBC mode added some processing time, it was generally inconsequential, especially for applications that need to encrypt reasonably big data blocks with more secure encryption. Raigoza and Jituri [17] evaluated the performance of symmetric encryption algorithms. The aim of this paper is to assess and contrast the performance of the Blowfish algorithm and the widely used Advanced Encryption Standard (AES). The AES algorithm outperformed Blowfish in terms of speed. And, when the data size was altered, there were minor changes between the methods evaluated, such that the encrypted data for the AES and Blowfish algorithms tended to be roughly the same length. When the authors changed the ASCII value range, both the AES and the Blowfish algorithms increased overall execution time as the ASCII value increased. It is important to mention here that the regression line slope for the Blowfish also increased. Given the same rising ASCII values, the encrypted data from the Blowfish algorithm tended to be greater in size than the AES encrypted data. A comparison of the symmetric cryptographic algorithms AES, MARS, DES, and 3DES was presented by Nurgaliyev and Wang. This paper's main aim is to assess the efficiency of various elements utilized in current symmetric key algorithms. It was determined that symmetric approaches are effective for delivering large amounts of encrypted data. Most frequently, symmetric algorithms are built from a collection of elements that can be transformed mathematically. According to this analysis, AES (Rijndael) performs the best in terms of security, flexibility, memory usage, and encryption performance [18]. Abood et al. investigated the cryptographic techniques used in smart grids to maintain privacy and security. The algorithms DES, TDES, E-DES, RSA, and BLOWFISH were selected for this study. This study proved that the overall performance of symmetric algorithms is superior to that of asymmetric algorithms. The findings showed that some algorithms, including BLOWFISH, can encrypt and decrypt data at rates that are competitive with AES. The aggregate results show that the DES algorithm is second to the AES method as the most secure approach. It is recommended that the smart grid employ the AES algorithm to keep the sensitive data as secure as possible [19]. In reference to [20], the authors scrutinize a study that examines eight of the most frequently used symmetric cryptographic algorithms, which are DES, 3DES, Blowfish, Twofish, RC2, RC5, RC6, and AES. The comparative analysis is based on the algorithm's structure, encryption and decryption times, throughput, and memory utilization. The analysis shows that Twofish and Blowfish are the fastest performing algorithms, while 3DES and RC2 perform the worst. Regarding memory usage, 3DES requires significantly more memory than the other algorithms. AES is considered the most secure algorithm, but Twofish and Blowfish are the fastest schemes for both encryption and decryption. Devasia and Visakh [21] incorporated encryption methods into the multicast protocol authentication for ad-hoc networks in 2013. The following symmetric encryption techniques were the main emphasis of the paper: AES, DES, 3DES, and Blowfish. The following conclusions were made: Blowfish encrypts and decrypts data more quickly than all other algorithms, and the results showed that Blowfish uses less CPU power. AES, ARC2, Blowfish, CAST, and 3DES were all thoroughly evaluated for standalone systems by [22]. The results of the investigation supported the following conclusions: Although Blowfish is the fastest approach, it demonstrates unfavorable throughput volatility for smaller plaintext sizes. Plaintext must be compressed to maximize memory efficiency before being provided into any symmetric key technique. AES delivers a performance that is generally consistent and only slightly better than the others, with the exception of Blowfish. Additionally, while Blowfish has a block size of 64 bits, AES has a block size of 128 bits, making it more resistant to birthday attacks. Advani and Gonsai [23] conducted a survey on AES, DES, DESede, Blowfish and Twofish on files of different sizes. The researchers concluded that both AES and blowfish appear to be more effective for all kinds of files.

The analysis of the aforementioned studies on the performance of 3DES, AES, *Blowfish, and Twofish schemes on general-purpose systems shows that there are still experimental challenges and research gaps. This current research aims to address these experimental challenges or gaps in terms of encryption and decryption times using varying key bit sizes for all the selected block cipher

encryption techniques while maintaining their respective block sizes.

## III. EXPERIMENTAL DESIGN

The symmetric algorithms AES, Twofish, and 3DES are used as the basis for the performance evaluation in terms of encryption and decryption times. In addition, the study further conducted performance analysis on 128, 192 and 256 key bits sizes on Blowfish using a block size of 64. This is because Blowfish has a 64-bit block size. The simulations were run on a laptop with an Intel® CoreTM i5-10210U CPU running at 2.40 GHz and 16 GB of RAM. Version 21H2 of Windows 11 Pro for Workstations was used. In this experiment, key sizes of 128, 192, and 256 bits were used to provide reliable values for comparing the performance of the AES, Blowfish, 3DES, and Twofish cryptographic algorithms. The experiment was run twelve (12) times and the average execution time in seconds was recorded. Table 1 also summarizes the various block-cipher techniques: AES, Blowfish, Twofish and 3DES.

**TABLE I. KEY BITS AND BLOCK SIZES**

| Factors | AES | *Blowfish | Twofish | 3DES |
|---|---|---|---|---|
| Key sizes | 128, 192 and 256 bits | 128, 192 and 256 bits | 128, 192 and 256 bits | 128 and 192 bits |
| Block size | 128 bits | 64 bits | 128 bits | 128 bits |

* Please note that the analysis of Blowfish was not included in the comparative study.

## IV. PERFORMANCE EVALUATION

The algorithms were compared based on their processing speeds, block sizes, and key bit sizes. Table II to VII shows the times in seconds for both encryption and decryption.

**TABLE II. 128 KEY SIZE - AVERAGE ENCRYPTION TIMES**

| File format | Size in Kb | AES Average time | *Blowfish Average time | Twofish Average time | 3DES Average time |
|---|---|---|---|---|---|
| ***Txt*** | 9 | 0.057 | 0.04 | 0.25 | 0.053 |
| ***PDF*** | 1,018 | 1.862 | 1.782 | 26.34 | 2.169 |
| ***MP3*** | 5,166 | 9.105 | 9.545 | 131.5 | 10.928 |
| ***MP4*** | 9,610 | 17.529 | 17.75 | 244.11 | 20.144 |
| ***DOCX*** | 1,003 | 1.918 | 1.951 | 25.39 | 2.115 |
| ***XLS*** | 657 | 1.088 | 1.278 | 16.59 | 1.519 |
| ***PPT*** | 243 | 0.52 | 0.529 | 6.2 | 0.573 |
| ***JPG*** | 2,446 | 4.342 | 4.812 | 63.02 | 5.252 |

**TABLE III. 192 KEY SIZE - AVERAGE ENCRYPTION TIMES**

| File format | Size in Kb | AES Average time | *Blowfish Average time | Twofish Average time | 3DES Average time |
|---|---|---|---|---|---|
| ***Txt*** | 9 | 0.049 | 0.04 | 0.246 | 0.178 |
| ***PDF*** | 1,018 | 1.737 | 1.58 | 23.859 | 1.678 |
| ***MP3*** | 5,166 | 8.876 | 7.954 | 120.319 | 8.453 |
| ***MP4*** | 9,610 | 15.995 | 15.193 | 225.117 | 15.746 |
| ***DOCX*** | 1,003 | 1.739 | 1.625 | 23.771 | 1.665 |
| ***XLS*** | 657 | 1.091 | 1.051 | 15.821 | 1.083 |
| ***PPT*** | 243 | 0.426 | 0.471 | 5.96 | 0.417 |
| ***JPG*** | 2,446 | 4.316 | 3.957 | 59.714 | 4.011 |

**TABLE IV. 256 KEY SIZE - AVERAGE ENCRYPTION TIMES**

| File format | Size in Kb | AES Average time | *Blowfish Average time | Twofish Average time |
|---|---|---|---|---|
| ***Txt*** | 9 | 0.038 | 0.033 | 0.228 |
| ***PDF*** | 1,018 | 1.5 | 1.485 | 24.198 |
| ***MP3*** | 5,166 | 7.611 | 7.383 | 124.065 |
| ***MP4*** | 9,610 | 14.115 | 13.704 | 230.228 |
| ***DOCX*** | 1,003 | 1.432 | 1.439 | 23.953 |
| ***XLS*** | 657 | 0.94 | 0.945 | 15.563 |
| ***PPT*** | 243 | 0.378 | 0.366 | 5.779 |
| ***JPG*** | 2,446 | 3.485 | 3.498 | 58.084 |

**TABLE V. 128 KEY SIZE - AVERAGE DECRYPTION TIMES**

| File format | Size in Kb | AES Average time | *Blowfish Average time | Twofish Average time | 3DES Average time |
|---|---|---|---|---|---|
| ***Txt*** | 9 | 0.035 | 0.054 | 0.244 | 0.046 |
| ***PDF*** | 1,018 | 1.889 | 1.868 | 25.6 | 2.022 |
| ***MP3*** | 5,166 | 9.068 | 9.722 | 135.491 | 10.832 |
| ***MP4*** | 9,610 | 17.643 | 18.074 | 245.67 | 20.364 |
| ***DOCX*** | 1,003 | 1.866 | 1.983 | 25.333 | 2.091 |
| ***XLS*** | 657 | 1.138 | 1.303 | 16.628 | 1.433 |
| ***PPT*** | 243 | 0.504 | 0.498 | 6.151 | 0.561 |
| ***JPG*** | 2,446 | 4.559 | 4.415 | 62.013 | 5.27 |

**TABLE VI. 192 KEY SIZE - AVERAGE DECRYPTION TIMES**

| File format | Size in Kb | AES Average time | *Blowfish Average time | Twofish Average time | 3DES Average time |
|---|---|---|---|---|---|
| ***Txt*** | 9 | 0.032 | 0.046 | 0.246 | 0.046 |
| ***PDF*** | 1,018 | 1.422 | 1.464 | 23.922 | 1.698 |
| ***MP3*** | 5,166 | 7.115 | 7.349 | 118.859 | 8.471 |
| ***MP4*** | 9,610 | 13.236 | 13.651 | 228.702 | 15.724 |
| ***DOCX*** | 1,003 | 1.413 | 1.447 | 23.862 | 1.678 |
| ***XLS*** | 657 | 0.924 | 0.956 | 15.563 | 1.103 |
| ***PPT*** | 243 | 0.366 | 0.378 | 5.755 | 0.416 |
| ***JPG*** | 2,446 | 3.363 | 3.486 | 58.655 | 4.041 |

**TABLE VII. 256 KEY SIZE - AVERAGE DECRYPTION TIMES**

| File format | Size in Kb | AES Average time | *Blowfish Average time | Twofish Average time |
|---|---|---|---|---|
| ***Txt*** | 9 | 0.027 | 0.031 | 0.255 |
| ***PDF*** | 1,018 | 1.44 | 1.473 | 24.514 |
| ***MP3*** | 5,166 | 7.201 | 7.366 | 124.713 |
| ***MP4*** | 9,610 | 13.401 | 13.733 | 231.95 |
| ***DOCX*** | 1,003 | 1.43 | 1.506 | 23.931 |
| ***XLS*** | 657 | 0.949 | 0.968 | 15.653 |
| ***PPT*** | 243 | 0.356 | 0.383 | 5.84 |
| ***JPG*** | 2,446 | 3.482 | 3.475 | 59.243 |

## V. DISCUSSION OF RESULTS

The analysis presented is based on two methods utilized during the experiment. The first approach involved conducting a comparative analysis of Advanced Encryption Standard, Triple DES (3DES), and Twofish with key sizes of 128, 192, and 256 bits, using various file extensions and maintaining a constant block size of 128 bits. The second method involved analyzing Blowfish with key sizes of 128, 192, and 256 using a block size of 64 bits.

Table II (128-bit key size) shows that the Twofish algorithm generally performs slower than the other two algorithms across all file formats. For example, for a PDF file of size 1,018 Kb, the Twofish algorithm took 26.34 seconds on average, while the AES and 3DES algorithms took 1.862 and 2.169 seconds, respectively. In contrast, the Twofish algorithm showed slightly improved performance with a speed of 0.25 seconds when processing a 9 Kb TXT file. The AES algorithm generally performs the fastest except for small text file (9 Kb), 128-key bits 3DES has the fastest encryption time of 0.053 seconds, while 128-key bits AES is slightly slower with an average encryption time of 0.057 seconds. Table III displays distinct trends in contrast to Table II, with the 192 key bits of 3DES algorithm being generally the fastest, and Twofish being the slowest across all file formats except for text file where 192 key bit of AES outperform 3DES with a speed of 0.049 seconds. Table IV (256-bit key size) shows that the AES algorithm is generally the fastest for all file formats, followed by Twofish. Tables IV and VII do not include any values for the 256 key bit size for either the encryption or decryption timeframes data on 3DES because it has no 256 key bit size. Table V presents the average decryption times for a 128-bit key size for AES, Twofish, and 3DES encryption algorithms. The data in this table indicates that Twofish takes the longest time to decrypt all file formats compared to AES and 3DES. The AES algorithm takes the least amount of time to decrypt all file formats. Table VI shows the average decryption times for a 192-bit key size for the same encryption algorithms and file formats. The results show that AES remains the fastest algorithm for all file formats, with Twofish still taking the longest time to decrypt. The decryption time for all algorithms has decreased for all file formats with the increase in key size. Table VII presents the average decryption times for a 256-bit key size for the same encryption algorithms and file formats. The data shows that Twofish still takes the longest time to decrypt compared to AES.

Tables II to VII also include the average encryption and decryption times of the Blowfish algorithm with different key sizes for various file formats using a fixed block size of 64 bits. Comparing tables II to VII, it can be observed that increasing the key size from 128 bits to 192 bits and then to 256 bits leads to a decrease in the encryption and decryption times. Overall, the 256-bit key size of Blowfish outperforms the 128-bit and 192-bit key sizes in both encryption and decryption times.

In summary, the 256 key bit size of AES has the highest encryption time compared to the 128 and 192 key bit sizes of AES. On average, AES algorithm outperforms Twofish and 3DES in terms of encryption times. During the decryption process, on average, the 192-bit key size of AES showed slightly superior performance compared to the 256-bit key size in restoring data to its original form.

During the analysis, it is observed that Blowfish's 256 key bit size had the fastest encryption and decryption times on 128 and 192 key bit sizes of Blowfish.

## VI. CONCLUSION

Based on the length of the key bits, four (4) block cipher algorithms—AES, Blowfish, Twofish, and 3DES—were thoroughly investigated in this paper. The processing times for each symmetric approach were tested using a variety of file types. When it comes to encryption and decryption speeds, 192 and 256 key bit sizes of AES both produce extremely comparable results. During the analysis, it was found that AES's 256 key bit size had the fastest encryption times. In terms of decryption time, AES with a key size of 192 bits outperformed the 256-bit key size of AES. It can also be observed that with a fixed block of 64 bits, Blowfish's 256 key-bit size presented the quickest encryption and decryption timings than 128 and 192 key bit sizes of Blowfish. The findings further demonstrate that Blowfish can compete with AES in terms of encryption and decryption speed.

## REFERENCES


[1] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[2] A. Ghosh, "Comparison of Encryption Algorithms : AES , Blowfish and Twofish for Security of Wireless Networks," *Int. Res. J. Eng. Technol.*, no. June, pp. 4656–4659, 2020, doi: 10.13140/RG.2.2.31024.38401.

[3] N. Kumar, J. Thakur, and A. Kalia, "Performance Analysis of Symmetric Key Cryptography Algorithms: DES, AES and Blowfish," *Anu Books*, vol. 1, no. 2, pp. 28–37, 2011, [Online]. Available: www.tropsoft.com.

[4] D. S. Abd Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms," *Int. J. Netw. Secur.*, vol. 10, no. 3, pp. 213–219, 2010.

[5] B. Soewito, F. Gunawan E., Diana, and A. Antonyová, "Power Consumption for Security on Mobile Devices," *2016 11th Int. Conf. Knowledge, Inf. Creat. Support Syst.*, pp. 4–7, 2016.

[6] H. Dibas and K. E. Sabri, "A comprehensive performance empirical study of the symmetric algorithms:AES, 3DES, Blowfish and Twofish," *2021 Int. Conf. Inf. Technol. ICIT 2021 - Proc.*, pp. 344–349, 2021, doi: 10.1109/ICIT52682.2021.9491644.

[7] P. Nema and M. A. Rizvi, "Critical Analysis of Various Symmetric Key Cryptographic Algorithms," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 3, no. 6, pp. 4301–4306, 2015.

[8] N. Tyagi and A. Ganpati, "Comparative Analysis of Symmetric Key Encryption Algorithms," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 6, pp. 94–99, 2014.

[9] M. Anand Kumar and S. Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms," *Int. J. Comput. Netw. Inf. Secur.*, vol. 4, no. 2, pp. 22–28, 2012, doi: 10.5815/ijcnis.2012.02.04.

[10] S. Gautam, S. Singh, and H. Singh, "A Comparative Study and Analysis of Cryptographic Algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH," *Int. J. Res. Electron. Comput. Eng.*, vol. 7, no. 1, 2019, [Online]. Available: https://www.researchgate.net/publication/334724160.

[11] C. Haldankar and S. Kuwelkar, "Implementation of Aes and Blowfish Algorithm," *Int. J. Res. Eng. Technol.*, vol. 03, no. 15, pp. 143–146, 2014, doi: 10.15623/ijret.2014.0315026.

[12] H. Alabdulrazzaq and M. N. Alenezi, "Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish," *Int. J. Commun. Networks Inf. Secur.*, vol. 14, no. 1, 2022, doi: 10.17762/ijcnis.v14i1.5262.

[13] A. V. Mota, A. Sami, K. C. Shanmugam, Bharanidharan Yeo, and K. Krishnan, "Comparative Analysis of Different Techniques of Encryption for Secured Data Transmission," *IEEE Int. Conf. Power, Control. Signals Instrum. Eng.*, vol. 54, no. 4, pp. 847–860, 2017.

[14] G. Singh, A. Kumar, and K. S. Sandha, "A Study of New Trends in Blowfish Algorithm," *Int. J. Eng. Res. Appl. www.ijera.com*, vol. 1, no. 2, pp. 321–326, 2015, [Online]. Available: www.ijera.com.

[15] G. Singh and S. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 33–38, 2013, doi: 10.5120/11507-7224.

[16] A. Ramesh and A. Suruliandi, "Performance analysis of encryption algorithms for information security," *Proc. IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT 2013*, pp. 840–844, 2013, doi: 10.1109/ICCPCT.2013.6528957.

[17] J. Raigoza and K. Jituri, "Evaluating Performance of Symmetric Encryption Algorithms," *Proc. - 2016 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2016*, pp. 1378–1379, 2017, doi: 10.1109/CSCI.2016.0258.

[18] A. Nurgaliyev and H. Wang, "Comparative study of symmetric cryptographic algorithms," *Proc. - 2021 Int. Conf. Netw. Netw. Appl. NaNA 2021*, pp. 107–112, 2021, doi: 10.1109/NaNA53684.2021.00026.

[19] O. G. Abood, M. A. Elsadd, and S. K. Guirguis, "Investigation of cryptography algorithms used for security and privacy protection in smart grid," *2017 19th Int. Middle-East Power Syst. Conf. MEPCON 2017 - Proc.*, vol. 2018-Febru, no. December, pp. 644–649, 2018, doi: 10.1109/MEPCON.2017.8301249.

[20] E. Elgeldawi, M. Mahrous, and A. Sayed, "A Comparative Analysis of Symmetric Algorithms in Cloud Computing: A Survey," *Int. J. Comput. Appl.*, vol. 182, no. 48, pp. 7–16, 2019, doi: 10.5120/ijca2019918726.

[21] T. Devasia and R. Visakh, "Integrating encryption technique in authentication of multicast protocol for Ad-hoc networks," *Proc. - 2013 3rd Int. Conf. Adv. Comput. Commun. ICACC 2013*, pp. 423–426, 2013, doi: 10.1109/ICACC.2013.90.

[22] A. Kubadia, D. Idnani, and Y. Jain, "Performance evaluation of AES, ARC2, BlowFish, CAST and DES3 for standalone systems," in *Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019*, 2019, no. Iccmc, pp. 118–123, doi: 10.1109/ICCMC.2019.8819729.

[23] N. A. Advani and A. M. Gonsai, "Performance analysis of symmetric encryption algorithms for their encryption and decryption time," in *Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development, INDIACom 2019*, 2019, pp. 359–362.