Partners Universal Innovative Research Publication (PUIRP)
Volume: 02 Issue: 05 | September-October 2024 | ISSN: 3048-586X | www.puirp.com

Performance Evaluation for AES, Blowfish, DES, and 3DES Cryptography Algorithms

Ebtihal Abdulrahman AL-Maqtari[1], Elham Abdulrahman AL-Maqtari[2]

[1,2]Software College, Northeastern University, China.

Abstract - Protecting data over the network is one of the biggest challenges in the information security field. Cryptography is one of the most important solutions for protecting data. Many algorithms can encrypt data. This paper compares the performance of four encryption algorithms: AES, Blowfish, DES, and 3DES. Testing the performance of these algorithms by using several text file sizes (10 MB, 30 MB, 50 MB, 70 MB, and 100 MB) shows that the fastest algorithm is AES.

Keywords: Encryption, AES, Blowfish, DES, 3DES, Security.

1.INTRODUCTION

Over the years, the need for security has increased. Cryptography is the method used to protect data. During the years, the cryptography methods have been developed from the easiest to the most complex ones in order to provide more security for data. This data is varying according to the field that it is used in, so this data can be personal, medical, financial, and so on. Many terms are included in cryptography: encryption, decryption, plaintext, ciphertext, key, and block size. Before moving deeply into the main purpose of this paper, we will explain the cryptography terms briefly.

Encryption is a branch of mathematics that presents the principle of guaranteeing the security of sensitive information. The encryption procedure happens by transforming the plaintext into ciphertext using varying algorithms so the information is unreadable. In other words, encryption is the process of converting readable data into unreadable data. The decryption operation is completely reversed of the encryption, so it is converting the unreadable data into readable data (the original data). Plaintext is the data before it gets encrypted. Otherwise, the ciphertext is the data after getting encrypted. The key term is the keyword that the sender and the receiver know and use to encrypt and decrypt the data. On the other hand, the block size is the size that is used to divide the data during the encryption and decryption processes as well. Cryptography has two categories: symmetric and asymmetric. For symmetric encryption, both encryption and decryption use the same key. On the other hand, asymmetric has two keys: a public key and a private key.

- **Data Encryption Standard (DES):** In 1975, DES was developed by IBM. It is a symmetric key algorithm with a 64-bit block size and the same 56-bit key.
- **Triple Data Encryption Standard (3DES):** 3DES was published in 1998. It is an enhancement of the DES algorithm by using it three times with separate 64-bit keys used each time. 3DES is used to enhance the security of DES.
- **Blowfish:** Blowfish was designed by Bruce Schneider in 1993. It is a symmetric key algorithm that uses a 64-bit block size, and the key can range from 32 to 448 bits.

- **Advanced Encryption Standard (AES):** AES is a symmetric key algorithm. It was published in 2001 by the National Institute of Standard Technology (NIST). It can use 128, 192, or 256-bit keys for encryption.

2. RELATED WORK

According to the increase of the encryption algorithms, much of the recent research compares the performance of these algorithms from different aspects. We will highlight the recent papers that present these comparisons.

The authors in [4] applied the DNA cryptography techniques to three different symmetric cryptographic algorithms, which are DES, AES, and Blowfish. The comparison is tested based on average encryption time, average decryption time, and the effect of length of plaintext on encryption time and decryption time. The results show that the DES-based DNA algorithm has the least encryption time, while the Blowfish has the least decryption time.

In [5], the study focuses on testing the optimal times and throughputs (speeds) for data encryption and decryption operations. They chose AES, Blowfish, Twofish, Salsa20, and ChaCha20 for this experiment. According to the final results, the ChaCha20 has the best average time for encryption and decryption. The Twofish algorithm has the lowest throughput.

The authors of [6] made an experiment by using Python programming to test the performance of AES, Blowfish, and Twofish. The main criteria they considered were encryption and decryption time, throughput, and 128-key size. AES is the fastest algorithm in terms of time and speed of encryption and decryption. Otherwise, Blowfish is near AES in encryption and decryption speed.

In [7], the authors evaluated the performance of five encryption algorithms, which are DES, 3DES, Blowfish, Twofish, and Threefish. They tested the performance by using the Python programming language. For evaluating the performance, they used text files of sizes 1, 5, 10, 50, and 100 MB for testing the speed of the encryption with different key sizes. For 3DES, Blowfish and Twofish used 128 key sizes, while 64 key sizes were used for DES and 256 key sizes were used for the Threefish algorithm, and Blowfish was the fastest.

3. THE MECHANISM

3.1 Data Encryption Standard

DES belongs to the symmetric key algorithm category. Using 16 Feistel rounds, DES encrypts and decrypts data, and two permutations (P Boxes) are initial and final permutations, as shown in Figure 1.

Partners Universal Innovative Research Publication (PUIRP)
Volume: 02 Issue: 05 | September-October 2024 | ISSN: 3048-586X | www.puirp.com

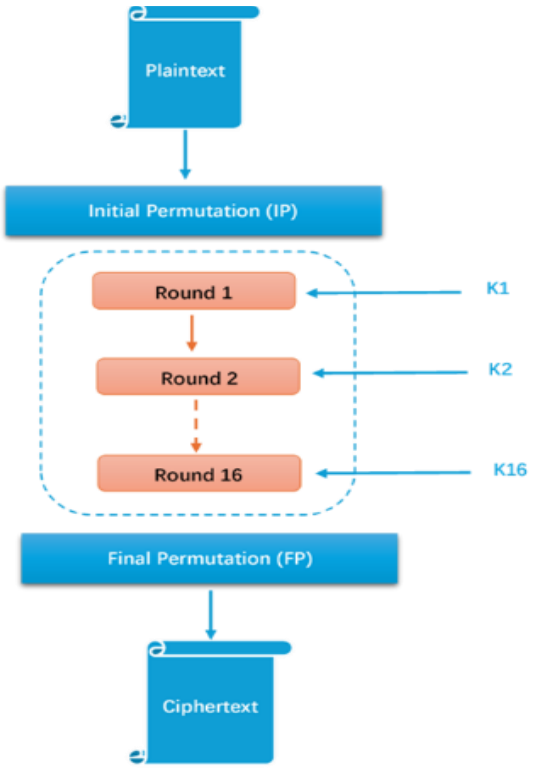

Fig -1: The Structure of the DES Algorithm

To encrypt and decrypt data, DES uses a block of 64-bit data using the same 56-bit key (the actual length of the key that is used is only 56 bits). The initial permutation overwrites the first bit with the 58th bit, the second bit with the 50th of the input data, and so on. The initial permutation is the inverse of the final permutation. Both are keyless operations. Figure 2 shows the round in the DES algorithm.

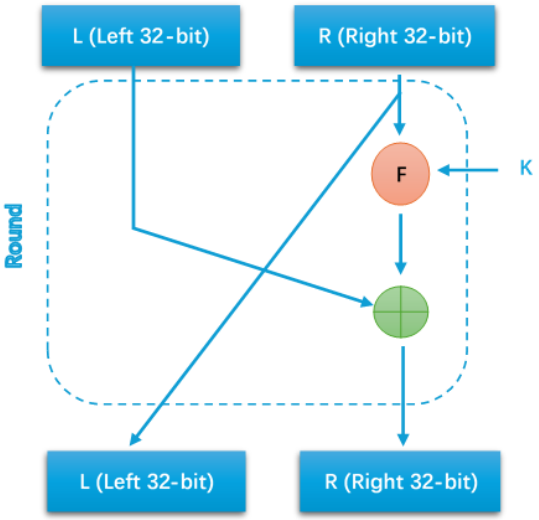

Fig -2: The Round in the DES Algorithm

The 64-bit block is divided into two sub-blocks left and right after the initial permutation. The size of each sub-block is 32-bits. The rule of the DES function is to take the right part of the 32-bit data and convert it to 48-bit for XORing with a 48-bit key. Then the result of XORing a 48-bit insert into the S-Box produces a 32-

bit output. Swap the left part 32-bit of the data with the right one after each round. This process is repeated 16 times in the DES algorithm. After finishing the last round, the final permutation combines the left and right parts into one 64-bit block.

3.2 Triple Data Encryption Standard

The main purpose of the 3DES algorithm is to increase the protection and security of the data. Although 3DES is more difficult to crack than DES, it needs more time consumption than DES in the encryption process. Figure 3 presents the structure of the 3DES algorithm.

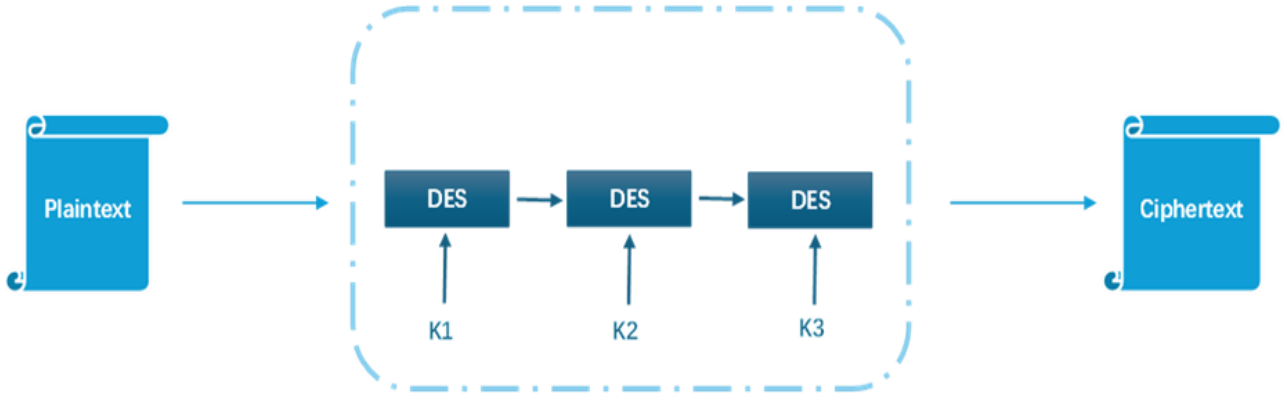

Fig -3: The 3DES Algorithm Structure

The mechanism of the 3DES algorithm is to encrypt the plaintext three times using the DES algorithm, each time with a different key. According to that, 3DES has three keys. Key 1 and Key 2 are different, but Key 1 and Key 3 are the same.

3.3 Blowfish

To encrypt data, Blowfish divides the block of 64-bit data into left (L) and right (R), 32-bit for each. The Blowfish operates through 16 iterations (i = 0 to 16). At each round, L and Pi are XORed, then the output passes to the blowfish function (F), which contains 4 key-dependent substitution boxes. The output from the function and R are XORed. After that, the left part and the right part are swapped. This process repeats 16 times. Pi is an array that contains 18 sub-keys; each sub-key is 32-bit. The Blowfish algorithm encryption process is shown in Figure 4.

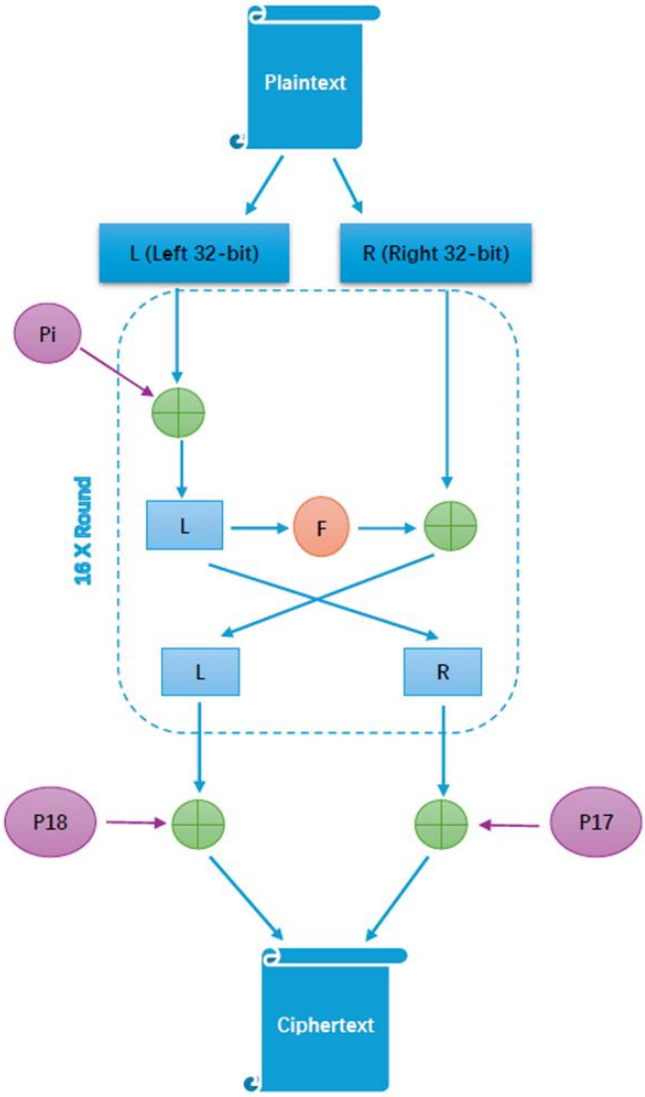

Fig -4: The Blowfish Algorithm Encryption

After 16 rounds are finished, the last step is swapping between L16 and R16 and XORing them with P18 and P17, respectively, and finally combining them to produce the ciphertext. Decryption is the same process as encryption but reversed.

3.4 Advanced Encryption Standard

The AES algorithm, which is a symmetric key algorithm, has different size keys, 128, 192, and 256, and the rounds in the AES depend on the size keys 10, 12, and 14 rounds, respectively. Figure 5 presents the encryption operation for the AES algorithm.

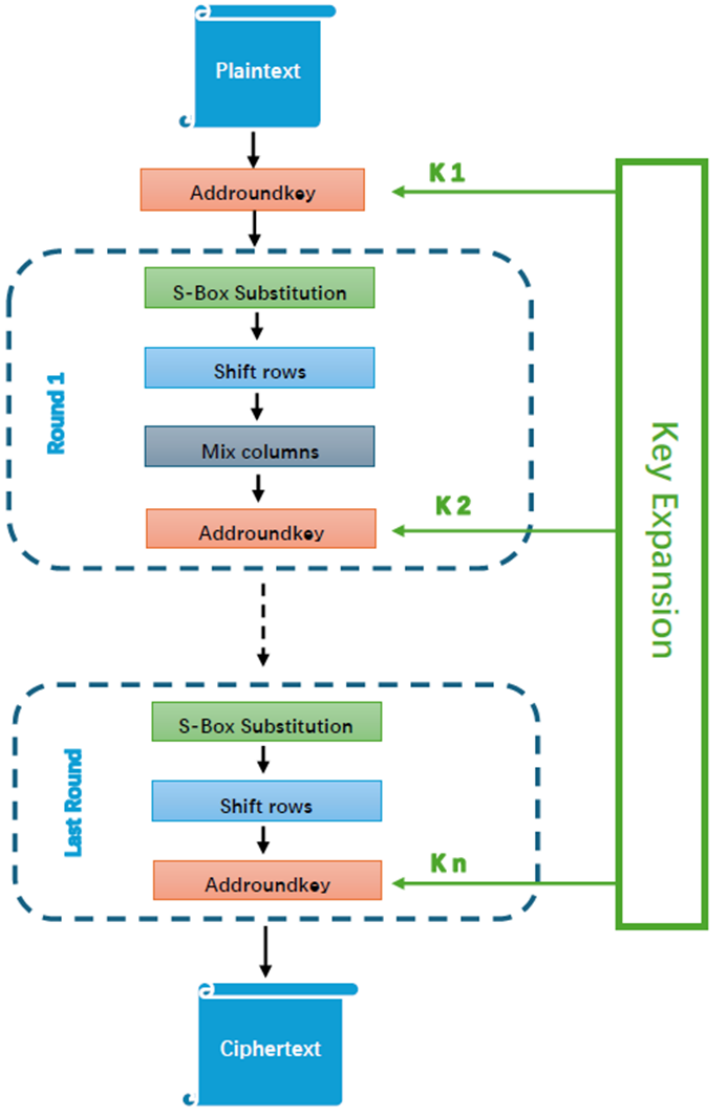

Fig -5: The AES Algorithm Encryption

The AddRoundKey process is added before starting each round. Each round has the same process: S-box substitution, shift rows, and Mix columns, except for the last round, which has no Mix columns process. AddRoundKey is the process of XORing the round key with the block of data. S-box substitution is the process of replacing each byte of the input with another byte from the S-box table. Shiftrows is the process of shifting the bytes in the rows to the left; the first row is fixed with no shifting, but from the second row to the fourth row is shifting increasingly by the row. Multiplying each column in the matrix by a fixed polynomial matrix is the process of mixing columns.

4. PERFORMANCE EVALUATION

4.1 Implementation

The experiment was done by running a Python code for each algorithm to test the speed of encryption of text files. The sizes for the files are 10 MB, 30 MB, 50 MB, 70 MB, and 100 MB. The experiment was on Microsoft Windows 11, a 64-bit operating system, and an Intel Core i7 13th Gen processor.

4.2 Results

The experiment results showed that the fastest algorithm is AES, followed by Blowfish, then DES, and the last was 3DES. Chart 1 presents the encryption speed for the four algorithms applied to five files of different sizes.

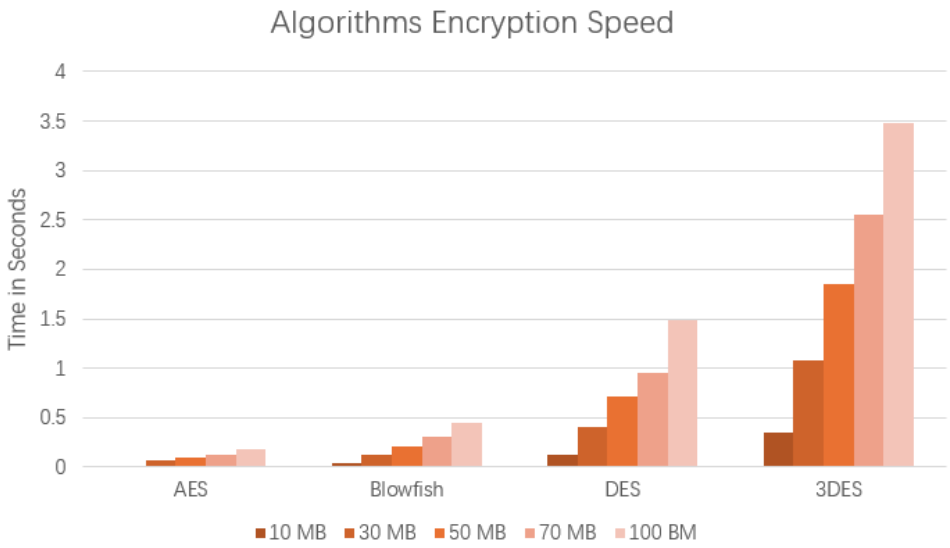

Chart -1: Algorithms Encryption Speed

Chart 2 shows the chart for the encryption speed for the algorithms after calculating the mean value for the speed of the five files that were used for the encryption process.

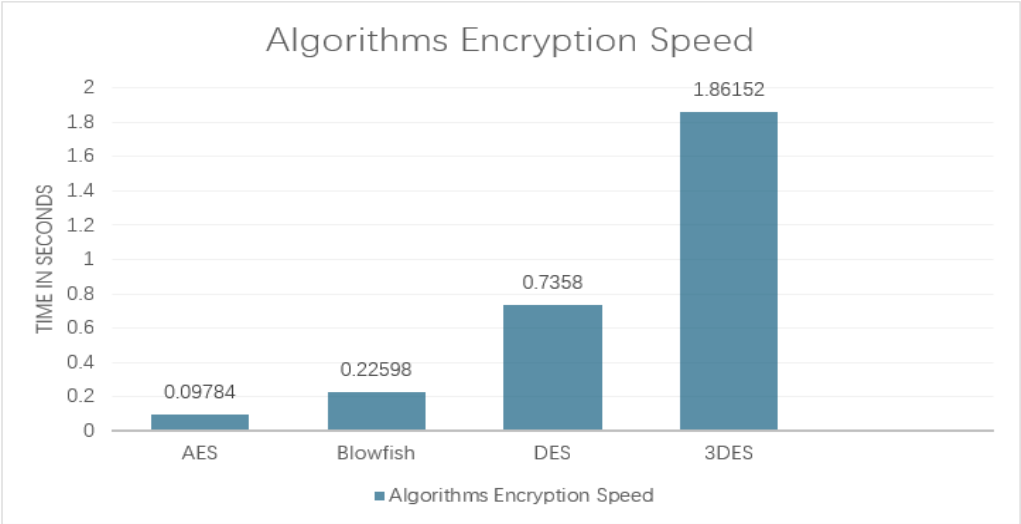

Chart -2: The Mean Value for Encryption Speed

The final results of testing the four algorithms are summarized in Table 1. The time in the table is calculated in seconds.

Table -1: Summary of Encryption Speed

File size	Algorithms			
	AES	Blowfish	DES	3DES
10 MB	0.0126	0.0458	0.1314	0.3459
30 MB	0.0652	0.1287	0.4053	1.0861
50 MB	0.1021	0.2093	0.7095	1.8459
70 MB	0.1271	0.3043	0.9487	2.5511
100 MB	0.1822	0.4418	1.4841	3.4786

Another way to check the performance of the algorithms is by testing the throughput. As shown in Chart 3, the AES algorithm provides the highest throughput, which means this algorithm has the best performance among the four algorithms.

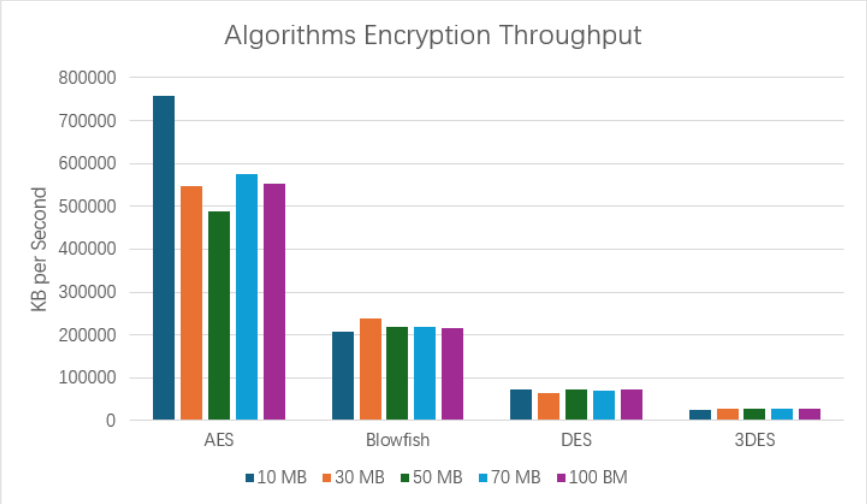

Chart -3: Algorithms Encryption Throughput

Table 2 represents how many kilobytes of data are encrypted per second for the four algorithms.

Table -2: Algorithms throughput

File size	Algorithms throughput (kilobytes per second)			
	AES	Blowfish	DES	3DES
10 MB	758170.54	208343.24	73536.45	26487.16

30 MB	545993.12	237281.81	65528.79	29090.97
50 MB	489384.80	218684.92	73136.51	28813.61
70 MB	574121.64	219661.09	70465.49	28971.46
100 MB	553857.41	216097.85	72468.63	28809.73

5. CONCLUSIONS

The speed of encryption is one of the most critical measures to evaluate the performance of the algorithm. This paper shows a comparison between DES, 3DES, Blowfish, and AES to test the performance of the encryption speed of five different sizes of text files: 10 MB, 30 MB, 50 MB, 70 MB, and 100 MB. The results show that the fastest algorithm is AES, followed by Blowfish, then DES, and the slowest one is 3DES.

REFERENCES

[1] Akoh Atadoga et al, "A comparative review of data encryption methods in the USA and Europe", Computer Science & IT Research Journal 5.2, February 2024, pp. 447–460, doi: https://doi.org/10.51594/csitrj.v5i2.815

[2] Khalid M Hosny et al, "Multimedia security using encryption: A survey", IEEE Access 11, June 2023, pp. 63027–63056, doi: 10.1109/ACCESS.2023.3287858

[3] Roopali Sood and Harpreet Kaur, "A literature review on rsa, des and aes encryption algorithms", Emerging Trends in Engineering and Management, September 2023, pp. 57–63, doi: https://doi.org/10.56155/978-81-955020-3-5-07

[4] Narayan Dhamala and Krishna Prasad Acharya, "A Comparative Analysis of DES, AES and Blowfish Based DNA Cryptography", Adhyayan Journal 11.11, June 2024, pp. 69–80, doi: https://doi.org/10.3126/aj.v11i11.67080

[5] Rebwar Khalid Muhammed et al, "Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption", Kurdistan Journal of Applied Research 9.1, June 2024, pp. 52–65, doi: https://doi.org/10.24017/science.2024.1.5

[6] Kwame Assa-Agyei and Funminiyi Olajide, "A Comparative study of Twofish, Blowfish, and advanced encryption standard for secured data transmission". In: International Journal of Advanced Computer Science and Applications 14.3, Jan 2023, doi: 10.14569/IJACSA.2023.0140344

[7] Haneen Alabdulrazzaq and Mohammed N Alenezi, "Performance Analysis and Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 14 No. 1, April 2022, pp. 51-61.

[8] Ms S Selvakumari, "Comparative Study on Blowfish & Twofish Algorithms in Iot Applications", Journal of Engineering Research and Application 10.02, February 2020, pp 64-69, doi: 10.9790/9622-1002036469

[9] [9] Archisman Ghosh, "Comparison of encryption algorithms: AES, Blowfish and Twofish for security of wireless networks", International Research Journal of Engineering Technology, June 2020, pp. 4656–4658.

[10] [Hasan Dibas and Khair Eddin Sabri, "A comprehensive performance empirical study of the symmetric algorithms: AES, 3DES, Blowfish and Twofish", 2021 International Conference on Information Technology (ICIT). IEEE, July 2021, pp. 344–349, doi: 10.1109/ICIT52682.2021.9491644

[11] Suha Husam Jasim, Haider Kadhim Hoomod, and Khalid Ali Hussein, "Image Encryption Based on Hybrid Parallel Algorithm: DES-Present Using 2D-Chaotic System.", International Journal of Safety & Security Engineering 14.2, April 2024, pp. 633-646, doi: https://doi.org/10.18280/ijsse.140229

[12] Udit Hasija et al, "Cryptographic foundations: A Comprehensive review of block cipher and stream cipher concepts", 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, April 2024, pp. 1302–1306, doi: 10.23919/INDIACom61295.2024.10498260

[13] Siti Munirah Mohd et al, "THE PERFORMANCE OF THE 3DES AND FERNET ENCRYPTION IN SECURING DATA FILES", Journal of Theoretical and Applied Information Technology 102.3, February 2024, pp. 812-820

[14] Anis Putma Cahyani and Ajib Susanto, "A Good Result for Blowfish Image Encryption Based on Stepic", Advance Sustainable Science, Engineering and Technology 6.1, January 2024, pp. 0240107-01-0240107-08, doi: https://doi.org/10.26877/asset.v6i1.17332

[15] Hamed Shawky Zied, Ahmed Gamal Abdellatif, and Adham Ahmed Elmahallawy, "An optimized implementation of the Blowfish encryption algorithm", 2024 International Telecommunications Conference (ITC-Egypt). IEEE, August 2024, pp. 55–59, doi: 10.1109/ITC-Egypt61547.2024.10620572

[16] Zahraa A Mohammed et al, "Advancing cloud image security via AES algorithm enhancement techniques", Engineering, Technology & Applied Science Research 14.1, February 2024, pp. 12694–12701, doi: https://doi.org/10.48084/etasr.6601

[17] M Santhanalakshmi, Ms Lakshana, and Ms Shahitya GM, "Enhanced AES-256 cipher round algorithm for IoT applications", The Scientific Temper 14.01, March 2023, pp. 184–190, doi: https://doi.org/10.58414/SCIENTIFICTEMPER.2023.14.1.22

[18] Wahyu Ady Putra, Suyanto Suyanto, and Muhammad Zarlis, "Performance Analysis Of The Combination Of Advanced Encryption Standard Cryptography Algorithms With Luc For Text Security", Sinkron: jurnal danpenelitian teknik informatika 7.2, April 2023, pp. 890–897, doi: https://doi.org/10.33395/sinkron.v8i2.12202

[19] Taniya Hasija et al, "A survey on performance analysis of different architectures of AES algorithm on FPGA", Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021, February 2023, pp. 39–54, doi: https://doi.org/10.1007/978-981-19-6383-4_4