WHIOCE PUBLISHING PTE. LTD.
PROVIDING
FIRST-CLASS SCIENTIFIC INFORMATION
FOR TOP SCHOLARS

2025 Volume 3, Issue 8
Lecture Notes in Education, Arts, Management and Social Science
ISSN(Online): 2705-053X

Research on the Comparison of Encryption and Decryption Performance of Symmetric Encryption Algorithms

Shaofeng Wen*
Xinjiang Hetian College, Hetian 848000, Xinjiang, China

**Author to whom correspondence should be addressed.*

Abstract: With the rapid development of information technology, data security has become particularly important in various fields. As one of the key technologies to ensure data security, symmetric encryption algorithms are widely used in data transmission and storage. This paper selects four common symmetric encryption algorithms (DES, 3DES, AES, and SM4) and conducts a comparative study on their encryption and decryption performance under three different data scales (100MB, 500MB, and 1000MB). Through experiments, data such as encrypted data size, decrypted data size, SHA256 value of pre-encrypted data, SHA256 value of post-decrypted data, average encryption time, and average decryption time of each algorithm are obtained and presented in the form of tables. The research results can provide a reference for the selection of symmetric encryption algorithms in practical applications.

Keywords: Data security; Symmetric encryption algorithms; Average encryption time; Average decryption time

Online publication: September 26, 2025

1. Introduction

In today's digital era, massive amounts of data are transmitted and stored in networks, and the security and confidentiality of data are facing severe challenges. Due to their high encryption and decryption efficiency and simple implementation, symmetric encryption algorithms have become an important means to protect data security. As representative symmetric encryption algorithms, DES, 3DES, AES, and SM4 each have different characteristics and applicable scenarios.

The DES algorithm is an early, widely used symmetric encryption algorithm, but with the improvement of computing power, its security is gradually threatened. The 3DES algorithm is an improved version of DES, which improves security by increasing key length and encryption times, but it also leads to reduced efficiency. As an advanced encryption standard, the AES algorithm has higher security and efficiency and is currently widely used in many fields. The SM4 algorithm is an independently developed national cryptographic algorithm in China, which has important application value in the field of information security in China.

A comparative study on the encryption and decryption performance of these four algorithms, analyzing their performance under different data scales, can provide strong support for selecting appropriate encryption algorithms according to specific needs in practical applications, and has important theoretical and practical significance.

2. Introduction to related technologies

2.1. DES algorithm

DES (Data Encryption Standard) is an algorithm for encrypting binary data. The data block length is 64 bits, the ciphertext block length is also 64 bits, the used key is 64 bits, the effective key length is 56 bits (8 bits are used for parity check), and the decryption process is similar to the encryption process, but the order of the key is exactly opposite. The DES algorithm only uses standard arithmetic and logical operations with a maximum of 64 bits, which has a fast operation speed and easy key generation. It is suitable for software implementation on most current computers and also for implementation on dedicated chips. The weakness of the DES algorithm is that it cannot provide sufficient security because its key capacity is only 56 bits. Therefore, the Triple DES (3DES) system was later proposed, which uses 3 different keys to encrypt data blocks 3 times (or twice), and this method is more effective than performing 3 ordinary encryptions. Its strength is approximately equivalent to that of a 112-bit key [1].

2.2. DES algorithm

3DES (Triple Data Encryption Standard) was developed on the basis of the DES algorithm to improve the security of the algorithm. It uses 2 or 3 keys to perform 3 encryption and decryption operations on plaintext. The effective key length of the Triple DES algorithm has been increased from 56 bits of the DES algorithm to 112 bits or 168 bits, so the security has been correspondingly improved [2]. However, due to three encryption operations, its encryption and decryption speed is relatively slow and the efficiency is low.

2.3. AES algorithm

AES (Advanced Encryption Standard) is a symmetric block encryption algorithm with a block length of 128 bits and a key length of 128 bits, 192 bits, or 256 bits. The basic principle of the AES encryption algorithm is based on a combination of substitution and permutation operations, aiming to increase data confusion, making the encrypted data unpredictable and difficult to crack. The core of the AES algorithm is an encryption process composed of multiple rounds, so the security strength is greatly improved compared with the DES algorithm [3].

2.4. SM4 algorithm

SM4 is an independently developed block cipher algorithm in China. The plaintext and original key block lengths of the SM4 algorithm are both 128 bits, adopting a 32-round nonlinear iterative structure, where each iteration process is composed of a round function F. The round function includes the T transformation and the XOR operation [4]. The SM4 algorithm has strong security and high encryption and decryption efficiency, and is particularly suitable for fast encryption and decryption in data transmission [5]. As an independently developed block cipher algorithm in China, the SM4 algorithm was announced by the State Cryptography Administration in 2006, with a block length of 128 bits and a key length of 128 bits. The SM4 algorithm also uses operations such as shifting, XOR, and S-box. Due to the fact that it is independently developed in China and announced relatively late, there are few studies on the SM4 algorithm, so it has high security [6]. The algorithm structure of the data encryption and decryption process of the SM4 algorithm is the same. The difference between the encryption and decryption processes depends on the order of use of the round keys. The round keys used in the decryption process are the reverse order of the round keys in the encryption process. As a domestic cryptographic algorithm, the SM4 algorithm has independent intellectual property rights, is not restricted by foreign cryptographic technologies, and can meet the strategic needs of national information security [7].

3. Experimental design

3.1. Experimental environment

The hardware environment used in this experiment is: Intel Core i7-10700K processor, 32GB memory, and 512GB

solid-state drive. The software environment is: Linux operating system. OpenSSL is open-source and flexible. Users can freely view, modify, and distribute its code, supporting numerous encryption algorithms and protocols, which can meet a wide range of security needs. Due to its high performance and cross-platform characteristics, OpenSSL can run stably in different operating systems and high-load environments, and is often used in fields such as web servers, Virtual Private Networks (VPN), and email encryption [8]. This paper builds OpenSSL using command-line tools in the Linux operating system. Currently, the two known hash algorithms, MD5 and SHA1, are considered no longer secure due to their short key lengths and the problem of collision attacks. Therefore, the SHA256 algorithm in OpenSSL is selected for measurement in this paper, which will output a 256-bit hash value after measuring the target [9].

3.2. Experimental data

The original data used in the experiment are randomly generated binary files with data scales of 100 MB, 500 MB, and 1000 MB, respectively. For each encryption algorithm and each data scale, 10 encryption and decryption experiments are conducted, and the average value is taken as the final experimental result to reduce experimental errors.

3.3. Experimental steps

Generate original data files of different scales, and calculate their SHA256 values to verify the integrity of the decrypted data [10–12].

(1) For each encryption algorithm and each data scale, perform an encryption operation, record the size of encrypted data and encryption time, and save the encrypted data.

(2) Perform a decryption operation on the encrypted data, record the size of the decrypted data and the decryption time, and calculate the SHA256 value of the decrypted data.

(3) Repeat steps 2 and 3 for a total of 10 experiments, and calculate the average encryption time and average decryption time.

(4) Organize the experimental data into tables for comparative analysis.

4. Experimental results and analysis

4.1. Experimental results under 100 MB data scale

Algorithm	Data Size (MB)	Encrypted Data Size (MB)	Decrypted Data Size (MB)	SHA256 Value of Pre-Encrypted Data	SHA256 Value of Post-Encrypted Data	Average Encryption Time (S)	Average Decryption Time (S)
DES	100	101	100	4d77c767258eb9cec92f0b3a4a0a3c93f829d8792a1a9478dde71988cf33af9d	4d77c767258eb9cec92f0b3a4a0a3c93f829d8792a1a9478dde71988cf33af9d	1.31	1.61
	500	501	500	aa730fa70f8fd5dd162e1f065651011073d3a827c408b0b90c2515a646b5d9d5	aa730fa70f8fd5dd162e1f065651011073d3a827c408b0b90c2515a646b5d9d5	6.81	8.05
	1000	1001	1000	be95140fe245aa0fcbb6c40fc9390476a11a2b6793cda437b4105aed55275d8d	be95140fe245aa0fcbb6c40fc9390476a11a2b6793cda437b4105aed55275d8d	13.61	16.81
3DES	100	101	100	4d77c767258eb9cec92f0b3a4a0a3c93f829d8792a1a9478dde71988cf33af9d	4d77c767258eb9cec92f0b3a4a0a3c93f829d8792a1a9478dde71988cf33af9d	4.18	4.10
	500	501	500	aa730fa70f8fd5dd162e1f065651011073d3a827c408b0b90c2515a646b5d9d5	aa730fa70f8fd5dd162e1f065651011073d3a827c408b0b90c2515a646b5d9d5	20.82	20.09
	1000	1001	1000	be95140fe245aa0fcbb6c40fc9390476a11a2b6793cda437b4105aed55275d8d	be95140fe245aa0fcbb6c40fc9390476a11a2b6793cda437b4105aed55275d8d	41.56	39.58
AES	100	101	100	4d77c767258eb9cec92f0b3a4a0a3c93f829d8792a1a9478dde71988cf33af9d	4d77c767258eb9cec92f0b3a4a0a3c93f829d8792a1a9478dde71988cf33af9d	0.19	0.10
	500	501	500	aa730fa70f8fd5dd162e1f065651011073d3a827c408b0b90c2515a646b5d9d5	aa730fa70f8fd5dd162e1f065651011073d3a827c408b0b90c2515a646b5d9d5	0.88	0.62
	1000	1001	1000	be95140fe245aa0fcbb6c40fc9390476a11a2b6793cda437b4105aed55275d8d	be95140fe245aa0fcbb6c40fc9390476a11a2b6793cda437b4105aed55275d8d	1.96	1.82
SM4	100	101	100	4d77c767258eb9cec92f0b3a4a0a3c93f829d8792a1a9478dde71988cf33af9d	4d77c767258eb9cec92f0b3a4a0a3c93f829d8792a1a9478dde71988cf33af9d	0.83	0.81
	500	501	500	aa730fa70f8fd5dd162e1f065651011073d3a827c408b0b90c2515a646b5d9d5	aa730fa70f8fd5dd162e1f065651011073d3a827c408b0b90c2515a646b5d9d5	4.34	3.96
	1000	1001	1000	be95140fe245aa0fcbb6c40fc9390476a11a2b6793cda437b4105aed55275d8d	be95140fe245aa0fcbb6c40fc9390476a11a2b6793cda437b4105aed55275d8d	8.66	8.38

4.2. Result analysis

It can be seen from the data in the above table that under different data scales, the encrypted data size and decrypted data size of the four symmetric encryption algorithms are the same as the original data size, which is consistent with the characteristics of symmetric encryption algorithms, that is, the encryption process will not change the size of the data. At the same time, the SHA256 value of the decrypted data is completely consistent with that of the pre-encrypted data, indicating that all four algorithms can ensure the integrity of the data during the encryption and decryption process, and the decrypted data is the same as the original data [13].

In terms of average encryption time and average decryption time, with the increase of data scale, the encryption and decryption times of the four algorithms all show an increasing trend. This is because the larger the amount of data processed, the greater the required calculation amount.

Specifically, the AES algorithm has the fastest encryption and decryption speed. Under the 100MB data scale, the average encryption time is only 0.19S, and the average decryption time is 0.10S; under the 1000MB data scale, the average encryption time is 1.96S, and the average decryption time is 1.82S, showing excellent performance. The encryption and decryption speed of the SM4 algorithm is the second, slightly slower than that of the AES algorithm, but its performance is relatively stable under various data scales.

The encryption and decryption speed of the DES algorithm is slower than that of AES and SM4. Under the 100MB data scale, the average encryption time is 1.31S, and the average decryption time is 1.61S; under the 1000MB data scale, the average encryption time reaches 13.61S, and the average decryption time is 16.81S. Due to three DES encryption operations, the 3DES algorithm has the slowest encryption and decryption speed. Under the 100MB data scale, the average encryption time is 4.18S, and the average decryption time is 4.10S; under the 1000MB data scale, the average encryption time is as high as 41.56S, and the average decryption time is 39.58S.

As a secure and efficient encryption algorithm, AES is widely used in wireless communication and Virtual Private Network (VPN) technology fields [14]. However, symmetric encryption also has some shortcomings, the most prominent of which is the key distribution problem. Since both encryption and decryption operations rely on the same key, the security of the key directly determines the security of communication [15].

Overall, the AES algorithm performs best in encryption and decryption performance, followed by the SM4 algorithm; the DES algorithm has average performance, and the 3DES algorithm has relatively poor performance. However, in practical applications, the selection of encryption algorithms cannot only consider performance but also combine factors such as security and compatibility.

5. Conclusion

This paper conducts a comparative study on the encryption and decryption performance of four symmetric encryption algorithms (DES, 3DES, AES, and SM4) under three data scales (100 MB, 500 MB, and 1000 MB) through experiments. The experimental results show that in terms of encryption and decryption speed, the AES algorithm performs the best, followed by the SM4 algorithm, the DES algorithm and 3DES algorithm are relatively slow, and the 3DES algorithm is the slowest. At the same time, all four algorithms can ensure the integrity and consistency of data during the encryption and decryption process.

In practical applications, appropriate encryption algorithms should be selected according to specific needs and scenarios. If high encryption and decryption speed is required, the AES algorithm is the preferred choice; if it is necessary to comply with domestic encryption standards, the SM4 algorithm is an ideal choice; while the DES and 3DES algorithms can still be used in some scenarios with low security and performance requirements due to their performance or security reasons, but they have been gradually replaced by better algorithms such as AES in scenarios with high security and performance requirements.

Disclosure statement

The author declares no conflict of interest.

References

[1] Yang W, Liu Z, 2025, Network Security Technology and Training (6th Edition). Posts & Telecom Press, Beijing, 200–203 + 205.

[2] Shi S, Chi R, 2025, Computer Network Security Technology (7th Edition). Posts & Telecom Press, Beijing, 200–203 + 205.

[3] Wang D, 2025, Research on the Application of Encryption Algorithm AES in Blockchain Technology. China New Technologies and Products, 2025(18): 139–140.

[4] Tang Y, Wan W, 2025, Design and Implementation of National Cryptographic SM4 Algorithm Demonstration Platform. Network Security Technology and Application, 2025(10): 37.

[5] Xie H, Qiao M, 2025, Design of Encryption and Decryption System Based on National Cryptographic SM2/SM3/SM4 Algorithms. Computer Knowledge and Technology, 21(13): 83–86.

[6] Wu X, Guo P, He D, 2014, Research and Implementation of Reconfigurable DES and SM4 Algorithms. Application Research of Computers, 31(03): 853.

[7] Huang J, Liu J, Cao Z, 2024, Research on File Desensitization System Based on National Cryptographic SM4 and Conformal Encryption Algorithms. Computer Measurement & Control, 32(11): 316.

[8] Gao W, 2025, Research on Secure Key Distribution and Communication System Based on OpenSSL. China Computer & Communication, 37(04): 77–78.

[9] Shi Y, Ma L, 2020, Design and Implementation of Program Integrity Measurement Scheme Based on OpenSSL. Electronics World, 2020(02): 47–48.

[10] Chen M, Zhao L, Wu T, 2023, Performance Comparison and Length Characteristic Research of 3DES and AES Algorithms. Computer Applications and Software, 40(4): 210–215.

[11] Sun B, Ruan H, Wu C, 2023, Distributed Data Encryption Scheme Based on SM4 and Experiment on Length Characteristics. Computer Engineering and Science, 45(6): 1089–1095.

[12] Xu Q, Li W, Li Z, et al., 2025, Research on the Application of SM4 National Cryptographic Algorithm in Train-Ground Wireless Communication of CTCS-3 Level Train Control System. Railway Signalling & Communication, 61(08): 10–11.

[13] Yang Y, Wang J, 2024, Quantum Logistic Map Image Encryption Algorithm Based on SHA-256 and Arnold Mapping. Journal of Anhui University (Natural Science Edition), 48(01): 35–42.

[14] Xie J, 2016, Research on the Application Value of Virtual Private Network Technology in Computer Network Information Security. Informatization Construction, 2016(04): 63–64.

[15] Zhao Z, Chen H, 2025, Research on Network Communication Information Encryption Methods for Internet Information Security Maintenance. Office Automation, 30(15): 86–87.