Dual IV Design Scheme: An Improved AES Encryption Approach

Longqing Zhang[1], Bin Liu[2], Xinwei Zhang[1,*], Huangqiang Yuan[2], Jiangzhao Yang[2] and Haoguang Huang[1]
[1]*Guangdong University of Science and Technology, Dongguan, China*
[2]*Googol Paradox (Dongguan) Intelligence Technology Co., Ltd, Dongguan, China*

Keywords: AES Encryption, Variable Order Processing, Ciphertext Characterization.

Abstract: This paper proposes a new encryption method of AES encryption, which is implemented by drawing on the idea of ShiftRows in AES and introducing a new order-changing processing step, which switches the order of the just-generated 64-byte array and realizes the deep concealment of the last indicator bit. On the other hand, the AES encryption blocks in a 16-byte group are forced to break up into a 64-byte matrix, which further improves the disorder of the encrypted data, and then the modification works of the superposition are carried out to make it more complicated. The experimental results show that the frequency of the new file encryption characters appearing is completely different from the CBC mode, and the peaks and valleys of the new bar graphs are more even compared to the original version, and the peaks are also significantly reduced. While ensuring the security, it increases the degree of confusion in the distribution of characters, which makes the statistical characteristics of the ciphertext more difficult to be analyzed and inferred.

1 INTRODUCTION

In recent years, with the leakage of all kinds of private data, people gradually realize the importance of personal data protection. Due to the rapid development of computer communication technology and the wide application of the Internet, people's demand for information security has become higher and higher. Information security has become a very important and urgent problem today. Currently, many people tend to use the same accounts and passwords, which may be used on multiple software and social networking sites. Once one of them is compromised, it can lead to a series of chain-reaction breaches (Li Ke, 2023). However, for the average user, they are often unable to address the vulnerability of a website and do not have the technical skills to do so.

While everyone knows that you should use multiple passwords of higher complexity for security, it is a major difficulty to memorize so many and complex passwords, so it has become common for many people to still use the same passwords for their accounts.

Therefore, we need a convenient and easy-to-use encryption device to protect users' data security. This device should have high strength protection capabilities, yet be simple to use and easy to carry and store. It needs to provide enough security to satisfy the needs of the average user while being widely accepted and integrated into people's daily lives, which is the ultimate goal of designing this device.

AES is a next-generation data encryption standard that combines the advantages of strong security, high performance, high efficiency, ease of use, and flexibility. The origins of the AES standard can be traced back to 1997, when the U.S. government issued a public notice announcing a call for a new national standard for symmetric algorithmic encryption that would meet 21st-century security needs. The standard requires that all aspects of the algorithm's design and implementation be open and freely available worldwide.

2 RELATED WORK

The two types of encryption algorithms include symmetric and asymmetric algorithms. The classic symmetric algorithms include AES, DES, etc., while RSA is one of the representatives of asymmetric algorithms (Kutsman Vladyslav, 2023). A key feature of symmetric encryption algorithms is that the key length is usually the same as the length of the plaintext, which is where the name comes from.

For example, a common 128-bit key length can be used to mathematically divide plaintext into 128-bit

Zhang, L., Liu, B., Zhang, X., Yuan, H., Yang, J. and Huang, H.
Dual IV Design Scheme: An Improved AES Encryption Approach.
DOI: 10.5220/0012282400003807

In *Proceedings of the 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (ANIT 2023)*, pages 310-314
ISBN: 978-989-758-677-4

length chunks for data obfuscation and diffusion effects. Commonly used encryption methods include different-or operations, matrix operations, and shift operations. For encryption, the round key mechanism is often used, where multiple new ciphers are generated from the original key (Kandala Sree Rama Murthy, 2022).

The AES algorithm was designed by Belgian cryptographers Vincent Rijmen and Joan Daemen. It has become one of the most popular symmetric encryption standards in use today and is widely used in data encryption and secure communications. AES provides strong security and efficiency, but requires proper key management (Liu Yiding - Priya).

The DES algorithm was originally designed by IBM and improved by the NSA to become the standard. However, it is no longer considered a secure encryption algorithm because its short 56-bit key length is no longer sufficient to provide adequate security. It has now been superseded by AES (Padmavathi R, 2021).

RSA algorithm was proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. It is widely used in the fields of digital signatures, key exchange, and secure communications. RSA provides strong security but requires a long key length to maintain security (Wang Yan - Manuel Melvin P.).

In order to prevent the same plaintext and key from generating the same ciphertext, various strategies are used in the encryption process, such as cipher group linking (CBC) mode, counter mode, cipher feedback (CFB) mode, and so on. These modes are mainly used to prevent cryptanalytic attacks. Asymmetric encryption usually refers to public key cryptosystems, which utilize different ciphers for encryption and decryption (Sowmiya B., 2021). In this system, both the parties need to exchange public keys and encrypt using each other's public key. After the receiver receives the encrypted data, it is decrypted using its own private key.

Since asymmetric encryption requires more computational resources, it is common for people to use asymmetric encryption to protect the key and symmetric encryption to protect the data itself, in a way that better utilizes the advantages of both encryption methods.

3 CORE CODING STRUCTURE

The AES encryption process involves four operations: SubBytes, ShiftRows, MixColumns and AddRoundKey. In AES encryption, the data is first processed using the AddRoundKey function. In this step, the input data is bitwise dissimilar to the round key. The key for the first round is the key entered by the user. Starting from the second round, four related functions are used to manipulate the data in each round. The first of these steps is SubBytes. subBytes is actually a lookup table operation, similar to S-BOX in the DES algorithm. there is also a lookup table in AES called S-BOX, which contains 256 values corresponding to all combinations from 0x00 to 0xFF. Each byte value of the input is used as the index of the S-BOX and then the corresponding substitution value is taken out. By using SubBytes, AES can perform non-linear substitution at the byte level, enhancing the security of the encryption. This step helps to obfuscate the pattern of the input data, making it difficult for cryptanalysts to obtain a clear statistical characterization,sbox substitution is shown in Fig 1.

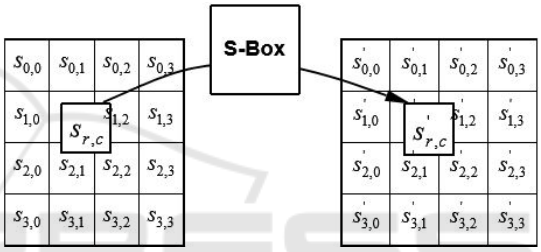

Fig 1. sbox replacement.

In the AES algorithm, the ShiftRows function is the second step of the operation, which performs a row shift operation on each row of the state matrix. The implementation steps are shown in Fig 2: this step increases the spread and complexity of the data and enhances the security of the encryption. Specifically, the ShiftRows operation steps: the first row remains unchanged; the second row is cyclically shifted left by one byte; the third row is cyclically shifted left by two bytes; and the fourth row is cyclically shifted left by three bytes. With row shifts, the elements of each row in the matrix are cyclically shifted left by a certain number of bytes. This helps ensure that each byte of the input data can be mixed with the others, making it difficult for cryptanalysts to obtain clear patterns and structures.

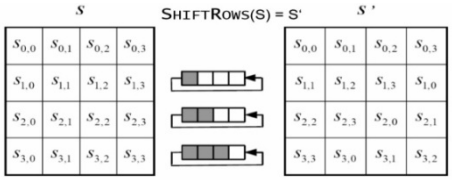

Fig 2. ShiftRows.

The third step of the operation is MixColumns, the core of the AES encryption operation, which utilizes operations over a finite field to achieve encryption and decryption. In this operation, the input data is treated as a 4x4 matrix and matrix multiplication is performed with a fixed matrix. In the operation within the finite field GF(28), the result will always lie between 0x00 and 0xff, which is determined by the characteristics of the finite field operation(Karmani Mouna, 2021). Similar to the lookup table (S-Box) in the SubBytes operation, the MixColumns operation in AES utilizes a fixed matrix for the operation. For each element of the input matrix, the rule for the multiplication operation is:

(1) For a multiplication with a value of 0x01, the result is equal to itself.

(2) For a multiplication with a value of 0x02, if the multiplied number is less than 0x80, the result is a 1-bit left shift of the multiplied number.

(3) For a multiplication with a value of 0x02, if the multiplied number is greater than or equal to 0x80, the result is the multiplied number shifted 1 bit to the left before being differentiated from 0x1b.

By using these arithmetic rules, each element of the input matrix is multiplied to obtain a new value. Finally, after the MixColumns operation is complete, the AddRoundKey function needs to be called again to perform the dissimilarity operation with the round key.

4 IMPROVED STRUCTURE

For the selection problem, this paper proposes a dual IV design scheme. The scheme is based on the design code of the original IV and adds an extra step to generate a new big IV while the original IV is called the small IV. Specifically, the ciphertexts that have been encrypted are divided into a group of 64, i.e., 512 bits as a unit, to form a 16x4 matrix. Then, in this paper, the first group of 64 ciphertexts is taken as the new big IV, while the original IV becomes the little IV. When reading data from the original file, 64 bytes are read as a unit each time. From a microscopic point of view, the original CBC pattern still operates as normal. When the first set of 64 bytes of big round ciphertext is obtained, this paper creates a new array to save it and continues to read the next 64 bytes of plaintext data. In this way, this topic implements a dual IV design. The purpose of this is to increase the variability of IV and improve the security of the cryptographic algorithm. In each round of encryption, this topic will directly perform a bitwise dissimilarity operation between the saved 64-byte ciphertext of the previous round and the current plaintext to obtain a result. This result will continue to be encrypted iteratively as a small IV in groups of 16 bytes. After 4 consecutive rounds of encryption, the subject will get the final result to be used as the large IV for the next round of encryption. This realizes the purpose of IV being generated directly from the ciphertext and conforms to the diffusion principle proposed by Shannon. Also, by this IV selection method, the characters in the original encryption order are completely disrupted, increasing the security of the cryptographic algorithm.

A. shuffle the order of business

In this paper, we introduce a processing step for changing the order, borrowing the idea of ShiftRows from AES. The step is shown in Fig 3, which swaps the order of the 64-byte array just generated. Although the computational effort of this step is small, it is very efficient. Because there are a large number of arithmetic processes in AES, even a change in any of these bits can make a big difference in the final result.

For specific implementation, this topic is based on the previously generated 64-byte large IV grouping for processing. Since the 64 bytes can be divided into exactly 8x8 matrices, we resemble the processing principle of ShiftRows by keeping the first row unchanged, and starting from the second row, sequentially shifting each row to the left by 2, 3, 4, 5, up to 7 bits. Through such a shift operation, we take the last column of the matrix, i.e. the first byte, as the original last byte, and realize the deep hiding of the last indicator bit. At the same time, the AES encryption block in a 16-byte group is forced to be broken up into a 64-byte matrix, which further improves the disorder of the encrypted data.

With the above modifications, we describe in detail the first step of the variable order processing and emphasize its hiding of the last indicator bit and the enhancement of the degree of disorder of the encrypted data. This is able to avoid the duplication rate of the paper while further improving the security of the cryptographic algorithm.

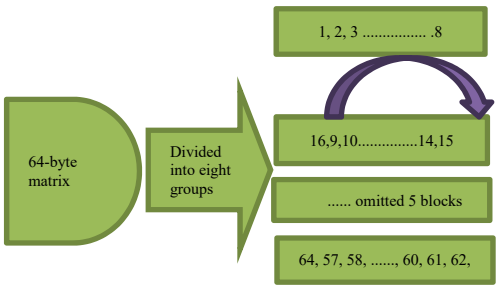

Fig 3. New Shift Processing Function.

This topic introduces a processing step for re-variation of values, inspired by the processing of AddRoundKey in AES. However, unlike AddRoundKey, this topic no longer extends the key, but directly uses the original key in the key file. Since the ciphertext block is 64 bytes and the key is 16 bytes, this topic can simply divide the key into a group of 4 bytes, and then perform the dissimilarity operation between each byte and the corresponding ciphertext byte, and write the result into the ciphertext file.

Doing so implements another shuffling process for the ciphertext. The advantage is that an infinite number of schemes can be used to vary the ciphertext, as long as memory space and processing power allow. Different group sizes can be chosen, such as 64 bytes, 128 bytes, 512 bytes, etc. It is even possible to use a different packet size each time, and it is feasible to gradually increase or decrease the packet size. In addition, the grouping information can be written into the ciphertext, so that the size of the ciphertext is no longer strictly close to the size of the plaintext. At the same time, the last byte of the file no longer represents the number of filled characters, which helps to strengthen the security of the data.

With the above modifications, this topic describes in detail the second step of the re-variation processing of the values, and emphasizes the nearly endless ciphertext variations it can achieve, as well as the enhancement of data security. This can avoid the duplication rate of the paper while further strengthening the security of the cryptographic algorithm.

5 RESULT

In the first step, the novel excerpt file is opene d and a byte statistical analysis graph is generat ed. This graph is depicted in Fig4.

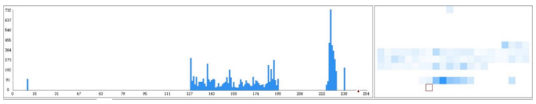

Fig 4. Byte statistics analysis of the novel file.

After obfuscation and diffusion processing via plaintext.

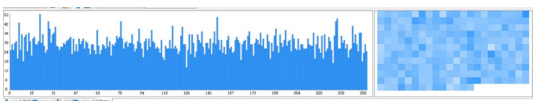

Fig 5. Plaintext obfuscation and diffusion processing.

As shown in Fig 5, all the statistical features in the original plaintext can no longer be found at all in the file encrypted with AES, and the frequency of characters in the ciphertext appears nearly uniformly in all the intervals between 0x00 and 0xff.

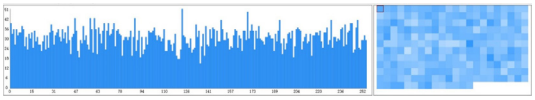

Fig 6. Crypto-fiction of the new method.

According to the analysis in Fig6, the new encrypted file maintains the uniform effect of the original AES128 while the frequency of occurrence of various characters is completely different from the pure CBC mode for the case of encrypting the same novel with the same key. In addition, it is worth noting that the peaks and troughs of the bar graphs in the new encryption code are more even compared to the original version, and the overly particular peaks have been significantly reduced.

With these improvements, the new encryption code increases the degree of confusion in the character distribution while ensuring security, making the statistical features of the ciphertext more difficult to be analyzed and inferred. This is important for improving the strength of encryption algorithms and resisting statistical attacks.

6 CONCLUSION

In this paper, we propose a new encryption method for AES encryption, and in the implementation, we introduce a new step of changing order processing, which draws on the idea of ShiftRows in AES. The order of the just-generated 64-byte array is switched, i.e., the first row is kept unchanged, and from the second row, each row is shifted to the left by 2, 3, 4, 5, and up to 7 bits in turn, on the other hand, the last column of the matrix, i.e., the first byte, is taken as the last byte of the original, which realizes the deep concealment of the last indicator bit. At the same time, the AES encryption block in a group of 16 bytes is forced to break up into a matrix of 64 bytes, which further improves the degree of disorder of the encrypted data. At the same time, the modification works on the basis of this overlay are sought to make it more complex. The usual CBC model is also modified for this purpose to make the iterative process more complex. The experimental results show that the new encryption code increases the degree of disorder in the character distribution while

ensuring security, making the statistical characteristics of the ciphertext more difficult to be analyzed and inferred.

ACKNOWLEDGMENTS

This research was financially supported by Special Projects in Key Areas for General Universities in Guangdong ProvinceNO.2021 ZDZX1077, in part of Natural Science Foundation of Guangdong Province of China with the Grant No.2020A1515010784,also supported by Guangdong Institute of Science and Technology Quality Project Editor GKZLGC2022255, 2022 Guangdong Province. Technology Quality Project Editor GKZLGC2022255, 2022 Guangdong Institute of Science and Technology Innovation and Improvement School Project No. GKY-2022CQT.GKY-2022CQTD-2,in part of 2022 Guangdong Province Ordinary Colleges and Universities Young Innovative Talents Category Project, No. 2022KQNCX115, Dongguan Social Development Project No. 20231800937602,Innovation and Improvement School Project from Guangdong University of Science and Technology Technology NO. GKY-2019CQYJ-3 College Students Innovation Training Program held by Guangdong University of Science and Technology NO.1711034, 1711080, and NO.1711040, and NO.1711041, and NO.1711042 1711080, and NO.1711088.

REFERENCES

Li Ke, Li Hua & Mund Graeme. A reconfigurable and compact subpipelined architecture for AES encryption and decryption. *EURASIP Journal on Advances in Signal Processing,* 2023. https://doi.org/10.1186/S13634-022-00963-3

Kutsman Vladyslav. Distributed File System Based on a Relational Database. *Open Journal of Applied Sciences* 2023(05). http://doi:10.4236/OJAPPS.2023.135051.

Kandala Sree Rama Murthy & V M Manikandan. A Reversible Data Hiding through Encryption Scheme for Medical Image Transmission Using AES Encryption with Key Scrambling. *JAIT,* 2022. https://doi.org/10.12720/JAIT.13.5.433-440.

Liu Yiding, Wang Lening, Qouneh Amer & Fu Xin. Enabling PIM-based AES encryption for online video streaming. *Journal of Systems Architecture*, 2022 https://doi.org/10.1016/J.SYSARC.2022.102734.

Abdul Hussien Farah Tawfiq, Rahma Abdul Monem S. & Abdul Wahab Hala Bahjat. A Secure Environment Using a New Lightweight AES Encryption Algorithm for E-Commerce Websites. *Security and Communication* Networks. 2021 https://doi.org/10.1155/2021/9961172

Priya, S. Sridevi Sathya,Karthigaikumar, P. & Teja, Narayana Ravi. FPGA implementation of AES algorithm for high speed applications. *Analog Integrated Circuits and Signal Processing*, 2021 123, 3081–3101 https://doi.org/10.1007/S10470-021-01959-Z

Padmavathi R. Anusha & Dhanalakshmi K. S. An Advanced Encryption Standard in Memory (AESIM) Efficient, High Performance S-box Based AES Encryption and Decryption Architecture on VLSI. *Wireless Personal Communications*, 2021 (4). https://doi.org/10.1007/S11277-021-09278-2

Wang Yan. Application of AES and DES Algorithms in File Management. *Journal of Physics: Conference Series*, 2037 012001. https://doi.org/10.1088/1742-6596/2037/1/012001

S. Ajish & AnilKumar K.S. Secure mobile internet voting system using biometric authentication and wavelet based AES. *Journal of Information Security and Applications*, 2021 https://doi.org/10.1016/J.JISA.2021.102908

Manuel Melvin P. & Daimi Kevin. Implementing cryptography in LoRa based communication devices for unmanned ground vehicle applications. *SN Applied Sciences*, 2021 (4). https://doi.org/10.1007/S42452-021-04377-Y

Sowmiya B., Abhijith V.S., Sudersan S., Sakthi Jaya Sundar R., Thangavel M. & Varalakshmi P. A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19. *SN Computer Science*, 2021 (3). https://doi.org/10.1007/S42979-021-00520-Z

Karmani Mouna, Benhadjyoussef Noura, Hamdi Belgacem & Machhout Mohsen. The DFA/DFT-based hacking techniques and countermeasures: case study of the 32-bit AES encryption crypto-core. *IET Computers & Digital Techniques*, 2021 (2). https://doi.org/10.1049/CDT2.12013