Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

Proposed new modification of AES algorithm for data security

Baydaa Jaffer Al-Khafaji [1,*] and Abdul Monem S Rahma [2]

[1] *Iraqi Commission for Computers and Informatics, Informatics institute for postgraduate studies, Baghdad, Iraq.*
[2] *Department of Computer Science, Al-Maarif University College, Iraq.*

Global Journal of Engineering and Technology Advances, 2022, 12(03), 117–122

Publication history: Received on 19 August 2022; revised on 24 September 2022; accepted on 26 September 2022

Article DOI: https://doi.org/10.30574/gjeta.2022.12.3.0165

Abstract

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as cipher text. Ideally, only authorized parties can decipher a cipher text back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

In this research, a method has been suggested using the encryption algorithm multiple and serially since it was used (4 - AES) implemented serially. The proposed algorithm is faster because it encrypts 64 bytes together. It encrypts all kinds of data and the number of files that are encrypted (2048) file and in one as it is possible to encrypt several files or one file at the same time.

The performance of this technique has been done by computer using mathlab package.

Keywords: DES; AES algorithm; Encryption; Decryption; Key; Cipher text; Plaintext

1. Introduction

The Advanced Encryption Standard (AES), also known by its original name Rijndael (Dutch pronunciation ['rɛinda:l]),[1] is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.[2]

AES is a variant of the Rijndael block cipher[3] developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal[3] to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been adopted by the U.S. government. It supersedes the Data Encryption Standard (DES),[7] which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. .[2] .[4]

* Corresponding author: Baydaa Jaffer Al-Khafaji
Iraqi Commission for Computers and Informatics, Informatics institute for postgraduate studies, Baghdad, Iraq.

Copyright © 2022 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

In the United States, AES was announced by the NIST as U.S. FIPS PUB 1970 on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable (see Advanced Encryption Standard process for more details). .[6] .[1]

AES is included in the ISO/IEC 18033-3 standard. AES became effective as a U.S. federal government standard on May 26, 2002, after approval by the U.S. Secretary of Commerce. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the U.S. National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module (see Security of AES, below). [3]

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware.[9] Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael *per se* is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits. .[7] .[8]

The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. Fig(1)

The number of rounds are as follows:

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as cipher text. Ideally, only authorized parties can decipher a cipher text back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. Fig (2)

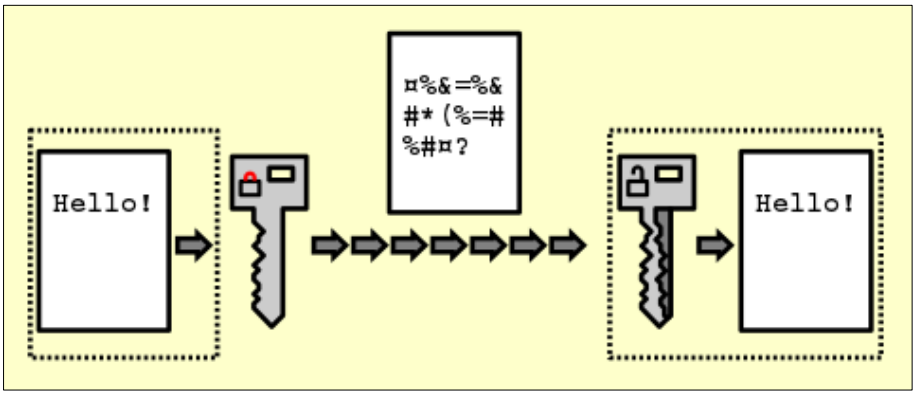

Figure 1 Use the same key in symmetric (encryption, decryption)

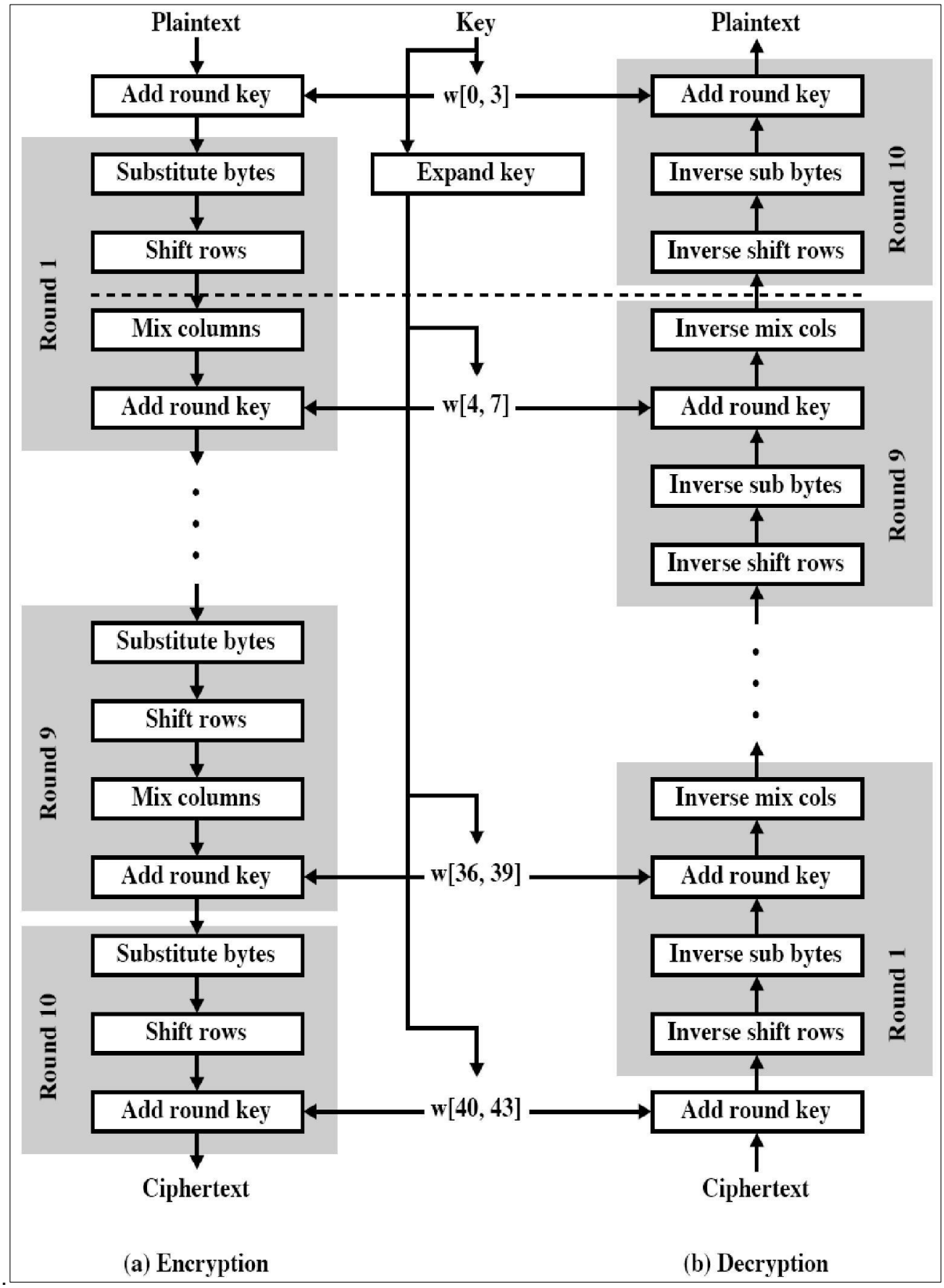

Figure 2 AES algorithm

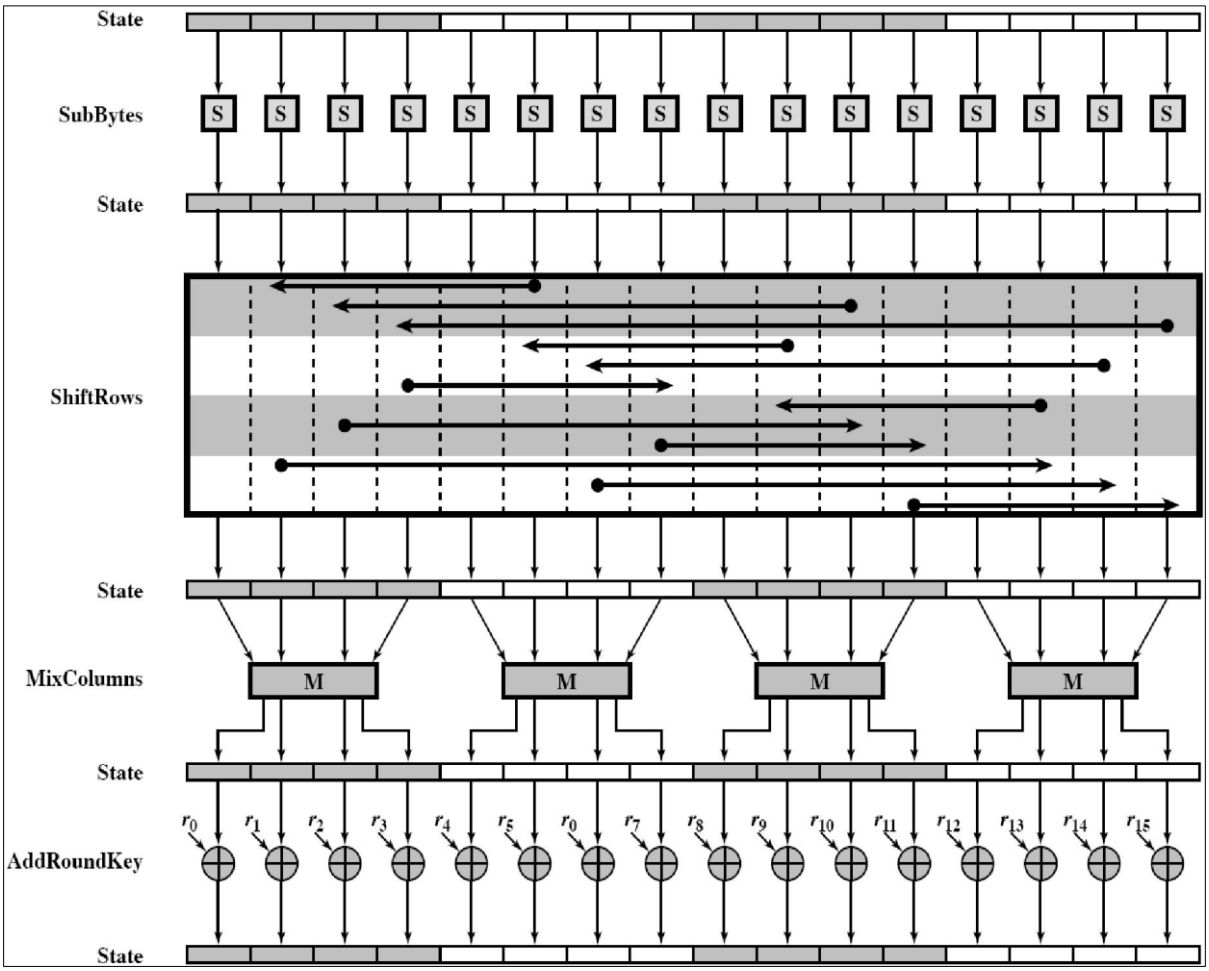

Figure 3 The process of AES

2. Propose new algorithm

- Input data
- Read a 512-bit block-sized file
- Transformed into a single matrix the size of a mass 2048 bit
- The data is converted into four single arrays, each 128 bits.
- All arrays are integrated into a 2048-bit mass-sized single matrix
- Data release with 512 bit mass external file
- The process continues until the end of the data,

2.1. Flow chart of new algorithm fig (4)

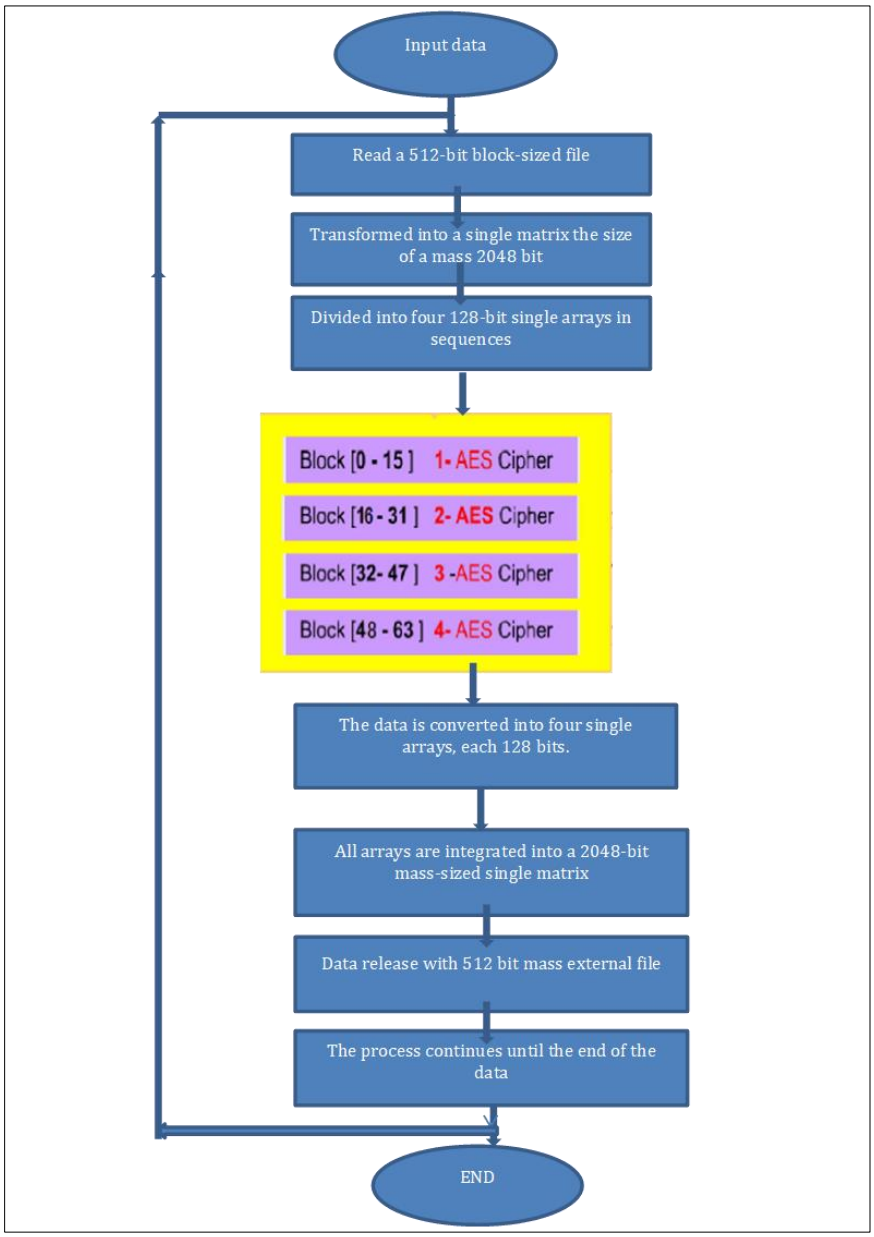

Figure 4 Flow chart of new algorithm

3. Result and discussion

Table 1 Computational time for encryption vs. File size in

File in KB	Proposed(modify AES)	AES
20	26	28
35	35	58
140	215	216
90	435	466
300	435	466
512	450	501

Here from the table (1), we can see that, we take different file size of 20, 35, 140,90, 300 and 512. And for 20kb we get the execution time 26, 35, 215, 435,435 and 450.

4. Conclusion

This paper proposed a modification to the AES algorithm is faster because it encrypts 64 bytes together. It encrypts all kinds of data and the number of files that are encrypted (2048) file and in one as it is possible to encrypt several files or one file at the same time through the evaluation of, the results show that it provides a better security level when a comparison was made with AES. Therefore, is highly secure and is suitable for color image encryption In future, this system will be devolved to the image encryption standard based with 3timensional process. Up Next task of this system would be adding the authentication part for data security over cloud computing. At that stage the system will be concerned about the performance.

Compliance with ethical standards

Acknowledgments

I would like to express my gratitude to all my colleagues and faculty members who made the completion of this paper successful.

Disclosure of conflict of interest

The authors certify that they have no conflict of interest in the subject matter or materials discussed in this manuscript.

References

[1] RAHMA AMS, RAHMA MAS, RAHMA MAS. Automated analysis for basketball free throw. In: Proceedings of the 7th International Conference on Intelligent Computing and Information Systems, Cairo, December 2015. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers. 2015, 447-453.

[2] BJ AlKhafaji, M Salih, S Shnain, Z Nabat, improved technique for hiding data in a colored and a monochrm images. Periodicals of Engineering and Natural Sciences. 2020, 8(2): 1000-1010.

[3] Li Nan, Sun Caixin, Li Jian, Du Lin, Wang Youyuan. Chaos and Its Application Research Progress in Electric Power Engineering. Journal of Chongqing University (natural science edition). 2005, 28(6): 30-36.

[4] BJ AlKhafaji, M Salih, S Shnain, Z Nabat. Segmenting video frame images using genetic algorithms. Periodicals of Engineering and Natural Sciences. 2020, 8(2): 1106-1114

[5] Akhavan A, Samsudin A, Akhshani A. Cryptanalysis of an improvementover an image encryption method based on total shuffling. Optics Communications. 2015,-09-01; 350:

[6] BJ AlKhafaji, MA Salih, SAH Shnain, OA Rashid, AA Rashid, MT Hussein, Applying the Artificial Neural Networks with Multiwavelet Transform on Phoneme recognition, Journal of Physics: Conference Series. 2021, 1804.

[7] Kaur H, Mehla, R. Image Encryption Using AES with Modified Transformation, International Journal of Science and Research (IJSR). 2014; 3(7): 360-363.

[8] Vaidehi M, Rabi BJ. Enhanced Mix Columns Design for AES Encryption, Indian Journal of Science and Technology. 2015; 8(35): 1-7.

[9] Alabaichi A, Salih AI. Enhance Security of Advance Encryption Standard Algorithm Based on Key-Dependent S-box, In 5th International Conference on Digital Information Processing and Communications (ICDIPC), IEEE. 2015; 44-53.

[10] Riyaldhi R, Kurniawan A, Improvement of Advanced Encryption Standard Algorithm With Shift Row And S. Box Modification Mapping In Mix Column," Procedia Computer Science. 2017; 116: 401-407.