iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46619

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Image Encryption using AES Algorithm: Study and Evaluation

Pratiksha Shete[1], Surekha Kohle[2]
Master in computer Application(MCA) 2nd year, Department of computer science, Veermata Jijbai Technological Institude(VJTI), Matunga, Mumbai-400019

Abstract: ***Image security is important these days as data is increasing a lot. These data can be images, videos, text, audio, etc. so to protect these images from attackers who can destroy the image quality or modify the images, some technologies like AES, DES, RSA, etc. have been invented. With the generation, data security has also become an essential issue. Considering these issues, the proposed technique ensures confidentiality, integrity, and authentication. Using these techniques, the host can encrypt and decrypt the image and can keep the digital images safe. When AES was chosen 16 years ago, digital technology was completely different from today and the scale of challenges was smaller, so with recent advanced technology and the emergence of new applications such as Big Data applications, in addition to applications running with 64-bit and many other applications have become necessary to design a new current algorithm for current requirements. Advanced Encryption Algorithm (AES) is a symmetric algorithm, which we will further discuss in detail in our research, and in addition to new recommendations for future work, a list of shortcomings and vulnerabilities of the internal structure of the AES algorithm will be diagnosed.***
Keywords: AES Algorithm, Image Encryption, Image Decryption, Symmetric Cipher

I. INTRODUCTION

Internet communication plays an important role in transferring a large amount of data to many users every day. Over the years, with the increase in data security, it becomes a problem that data is sent through insecure channels that are exposed to manipulation or attack by malicious users. Various security technologies have been put in place to ensure that data or messages reach only those who are authorized to receive them. Cryptography has been one of the main techniques deployed to secure data through the processes of encryption and decryption. Encryption involves encoding information to secure data from attackers so that they cannot easily access it. This process involves turning "images" into invisible "cipher images" using keys, substitutions, and permutations. In the decryption process, we intend to convert the encrypted image back to the original plain image without missing any pixel from the original image. Carrying out both processes involves the use of mathematical calculations and certain algorithms. The main concern of cryptography is to provide confidentiality, integrity, non-repudiation, and authentication through encryption and decryption algorithms. There are various cryptographic techniques symmetric, asymmetric, and hashing. In this article, we will discuss the AES algorithm which is symmetric cryptography technique.

II. PREVIOUS WORK

In paper [3] This gives low complexity architecture and easily achieves low latency as well as high throughput. The design used an iterative looping approach with a block and key size of 128-bit, lookup table implementation of S-box. Kamali S.H et. [4] used the modified advanced encryption algorithm to reflect a high level of security and better image encryption. The modification is done by adjusting the ShiftRow Transformation. The author has compared the results of the previous AES algorithm and the modified AES algorithm.

III. PROPOSED WORK

A. AES Algorithm

AES is a data encryption algorithm introduced by the US National Institute of Standards and Technology (NIST) in 2001. The AES algorithm, also known as the Rijndael algorithm, is a symmetric block cipher algorithm that uses 128,192 or 256 bits. Keys to transform a 128-bit message block into 128-bit ciphertext. This method makes it strong, secure, and exponentially stronger than DES, which uses a 56-bit key.

The AES algorithm uses a substitution permutation or SP network with several rounds to generate the ciphertext. The length of the key used will determine the number of rounds.

The number of rounds shown in Figure 2, 10, applies to the case where the encryption key is 128 bits long. The number of cycles is 12 when the key is 192 bits, and 14 when the key is 256. Before any cycle-based encryption processing can begin, they converted the digital images into a binary matrix to process it through the AES encryption algorithm. It is divided into 4*4 matrix for each unit of 8 bits to form the plain text of the algorithm. The input state field is XORed with the first four bytes of the key schedule.
The same thing happens during decryption - except now we XOR the state field of the ciphertext with the last four words of the key schedule.

Byte 00	Byte 01	Byte 02	Byte 03
Byte 04	Byte 05	Byte 06	Byte 07
Byte 08	Byte 09	Byte 10	Byte 11
Byte 12	Byte 13	Byte 14	Bye 15

Figure 1: 4*4 Matrix

For encryption, in each round following 4 steps are performed:
1) Replace bytes, 2) Shift rows, 3) Shuffle columns, and 4) Add round key.
In the last step XOR the output of the previous three steps with four words from the key schedule.

For decryption, in each round following four steps are performed:
1) Inverse row shift, 2) Inverse spare bytes, 3) Round key addition, and 4) Inverse column mix.
In the third step XOR the output of the previous two steps with four words from the key schedule.
The last round for encryption doesn't contain the "Mix columns" step. The last round for decryption doesn't contain the "Inverse mix columns" step.

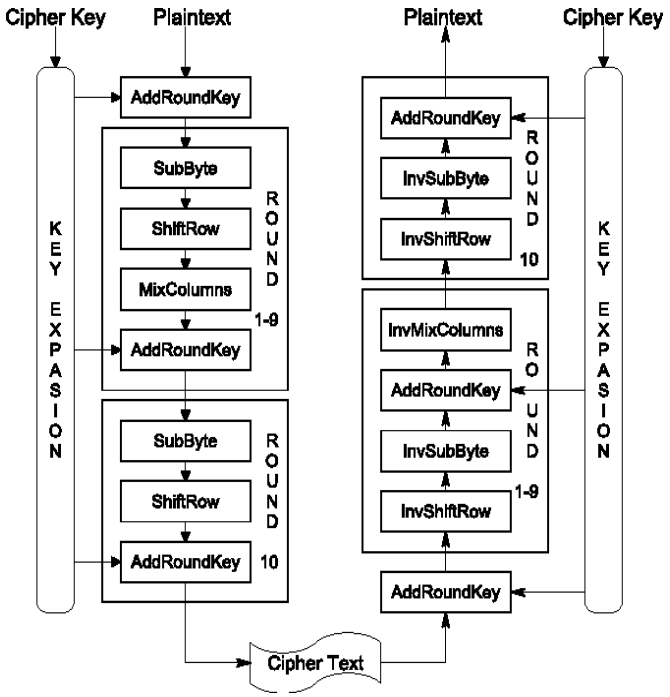


Figure 2: Block diagram AES Encryption and Decryption

Figure 2: shows the various steps performed in each round.

1) *Step 1:* This step is named **SubBytes** for byte-by-byte substitution during the encryption process. During decryption, the corresponding substitution step is performed it is called **as InvSubBytes**. In the subtype step, it is divided into two equal parts and converts each byte into hexadecimal of the state array. These parts are the row mapped with a substitution box (S-Box) to generate new values for the final state array.

2) *Step 2:* Next step is named ShiftRows for shifting the rows of the state array during the encryption process. The corresponding transformation during decryption is called InvShiftRows for Inverse Shift-Row Transformation. It swaps the row elements among each other. No shift within the first row. In the second row, it shifts element to one position left It also shifts the elements from the third row two consecutive positions to the left, and it turns the last row three positions to the left.
3) *Step 3:* Next step is named as MixColumns for mixing up the bytes in each column separately during the encryption process. The corresponding transformation during decryption is called InvMixColumns and stands for inverse mix column transformation. In the state array, it multiplies a constant matrix with each column to get a new column for the subsequent state array. We will get the state array for the next step, once all the columns are multiplied with the same constant matrix. This particular step is not to be done in the last round.
4) *Step 4:* the last step is called AddRoundKey for adding the round key to the output of the previous step during the encryption process. The corresponding step during decryption is named aInvAddRoundKey for inverse add round key transformation. With the first key generated (K0), we pass the block data stored in the state array through an XOR function. It passes the output of the previous state array on as input to the next step.

B. Analysis And Justifications For The Drawbacks Of The Aes Algorithm

After a study and analysis of the internal structure and the algebraic foundation of the AES cipher, there is evidence that the AES algorithm has many suspicious aspects and it has suffered from several vulnerabilities from the design term that is listed below:

1) Most of the development methods of the previous studies for improvement of AES, focus on increasing the number of rounds or increasing the block size to increase the security level, but this is not considered the best solution for development experiments.
2) In AES encryption, In the process of encryption and decryption unbalanced structure observed. AES decryption is comparatively slower than encryption process.
3) When the accumulator repeats thousands of rounds then encryption process for thousands of bits will provide an obvious time difference between the encryption and decryption process, so the difference will be clearly visible.
4) AES cipher with secure 128-bit may not be appropriate for big data applications and other modern big applications like secure cloud storage. Therefore, these applications with huge data may need a larger algorithm with a larger order of mathematical and structure foundations.
5) In the last round mixcolumn has no effective role in the security factor whether it is added or not as it was mentioned by the authors of the AES algorithm.

C. Recommendations

After this deep study, there are several important recommendations for future work that are summarized here:

1) Need to make the improvements in algorithm for balanced in encryption and decryption process.
2) Model with higher irreducible polynomial and higher mathematical order of finite field should be implemented to increase security.
3) Eliminate the use of constant values. Use of constant values may increase risk and can easily get attacked.
4) Key generation technique needs to implement with the real length for the long keys that comprise 192-bits, 256-bits, and upper that increase the guessing probability effectively

IV. CONCLUSIONS

The As mentioned above, the Advanced Encryption Standard (AES) algorithm is one of the most efficient algorithms and is widely supported and adopted on hardware and software. Another notable thing about the AES algorithm is that the encryption and decryption processes are very similar except for a few differences. The basic aim of this study is to point out weak points and vulnerable points, in addition to explaining the gaps in the structural elements that can be used in the AES structure. This paper discussed the properties of the AES algorithm that are the best alternatives by providing a set of basic diagnostic factors for negative aspects from the perspective of scientific researchers around the world. In addition to basic solutions for the development of a modern algorithm, the mentioned research also includes some future recommendations for designers and academic specialists. The AES algorithm certainly has some weaknesses, but they are minimal compared to its strengths.

V. ACKNOWLEDGEMENT

I would like to express my great appreciation to Dr. Surekha Kohle for her valuable and constructive suggestions during the research paper.

REFERENCES

[1] Bhargav, S., Majumdar, A., & Ramudit, S. (2008, Spring). 128-bit AES decryption. Retrieved November 21, 2020, from http://www.cs.columbia.edu/~sedwards/classes/2008/4840/reports/AES.pdf

[2] Clark, A. (2018, August 2). How much encryption is too much: 128,, 256 or 512-bit? Retrieved November 21, 2020, from https://discover.realvnc.com/blog/how-much-encryption-is-too-much-128-256-or-512-bit

[3] Hoang Trang and Nguyen Van Loi, "An Efficient FPGA Implementation of The Advanced Encryption Standard algorithm", IEEE International Conference on Computing and Communication Technology, page 1-4, Ho Chi Minh city, 2012.

[4] Kamali S.H, Shakerian R, Hedayati M and Rahmani M, "A new modied version of Advanced Encryption Standard based algorithm for image encryption", (ICEIE) International Conference On Electronics and Information Engineering, volume 1, page 1250-1255, Aug 2010

[5] AES Encryption: study and Evaluation
(PDF) AES Encryption: Study & Evaluation (researchgate.net)

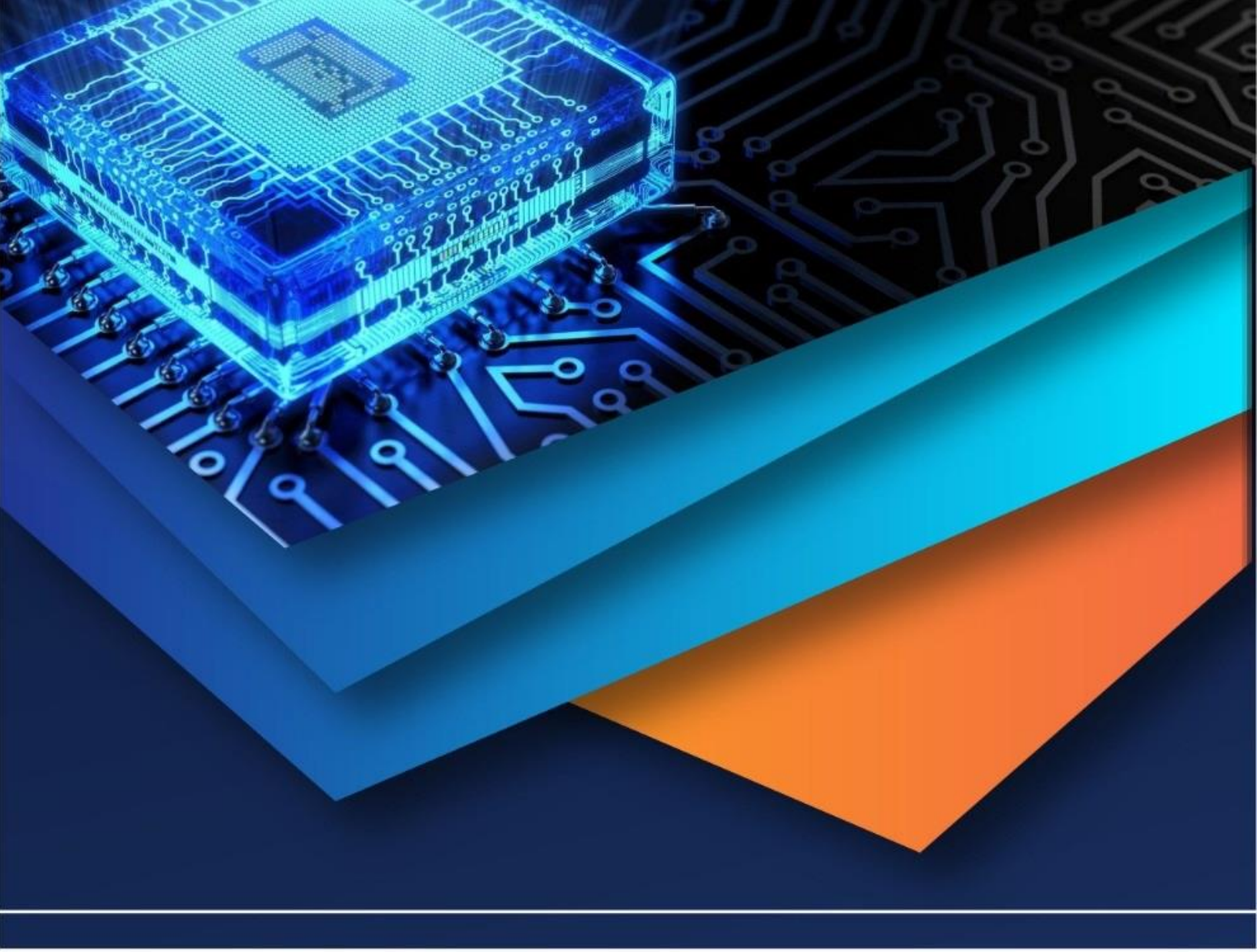
[6] Thakkar, J. (2020, June 2). DES vs. AES: Everything to Know About AES 256 and DES Encryption. Retrieved November 21, 2020, from https://sectigostore.com/blog/des-vs-aes-everything-to-know-about-aes-256-and-des-encryption/

[7] Townsend Security. (2020, June 1). AES vs. DES Encryption: Why AES has replaced DES, 3DES, and TDEA. Retrieved November 21, 2020, from https://www.precisely.com/blog/data-security/aes-vs-des-encryption-standard-3des-tdea

[8] Mustafeez, A. Z. (n.d.). What is the AES algorithm? Retrieved November 20, 2020, from https://www.educative.io/edpresso/what-is-the-aes-algorithm

[9] M. Y. Rhee, "Internet Security Cryptographic Principles, Algorithms and Protocols", John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, England, 2003.

[10] O. A. Dawood, A. S. Rahma and A. J. Abdul Hossein, "The New Block Cipher Design (Tigris Cipher)", I.J.Computer Network and Information Security (IJCNIS).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY