Image Encryption and Decryption Using AES

Mayank Singh [*1] Er. Shivam Dixit[*2]

[*1,2] Computer Science And Engineering Shri Ramswaroop College Of Engineering And Management Lucknow, Uttar Pradesh India.

ABSTRACT

Every day, the utilization of various devices like PCs, laptops, and others for communication and data transfer has evolved, leading to a wider customer base. However, with this expansion comes the heightened risk of unauthorized access and data breaches, emphasizing the importance of data security. Images, often containing sensitive information, are transmitted through various channels, necessitating protection from potential attacks. To address this challenge, we employ AES encryption for image encoding and decoding, rendering the encrypted data unintelligible to unauthorized users. This encrypted information is securely transmitted over networks and can be decrypted at the intended destination using AES, ensuring the safe transmission of images.

Keywords: AES, Information Security, Cryptography.

I. INTRODUCTION

The US government has adopted the Advanced Encryption Standard (AES) as a symmetric block cipher to safeguard collected data. AES is widely utilized for encrypting sensitive data across devices and networks globally, a crucial aspect of CEO concerns regarding PC, network, and electronic data security. In response to vulnerabilities in the Data Encryption Standard (DES), identified by the National Institute of Standards and Technology (NIST) in 1997, AES was developed to provide robust protection against various attack methods. NIST emphasized the importance of AES, stating it should remain effective for securing government information well into the 21st century. AES was designed to be versatile, capable of running on various computing platforms, including limited environments like smart cards, while offering strong security against potential threats. Initially developed for government use, AES encryption, also known as the Rijndael algorithm, employs 128-bit symmetric block encryption. It operates by encoding these blocks and combining them to generate ciphertext, relying on a Substitution-Permutation network. The number of rounds varies depending on the key length, with 10 rounds for a 128-bit key, 14 for a 192-bit key, and 256-bit key specified.

II. LITERATURE SURVEY

1. Performance analysis of encryption and decryption algorithm by Pronika, S. S. Tyagi, In this article, by comparing the time it takes for various encryption and decryption calculations of different log sizes, we also found that there is a trade-off between security and time. The two elements of safety and time play a fundamental role in choosing a calculation, as this could affect the representation of the framework in terms of safety and productivity if we divide thedifference by either of these two.

2. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Ako Muhamad Abdullah. This document is coordinated as follows: Section 2 presents a brief history of AES computation. Related work is examined in segment 3. In segment 4, the AES calculus evaluation rules are given. The basic structure of the AES calculation is described in Section 5. The encryption cycle of the AES calculation is presented in Section
6. In segment 7, the AES Extended Key makes sense. The decryption process is presented in Section 8. Section 9 covers AES launchpads. Finally, there is an ending in segment 10.

3. An image encryption method based on chaos system and AES algorithm.Shahid Bahonar,Mohammad Javad Rostami & Behnam Ghavami. In this article, an intelligent calculation of the image encryption in terms of the combination of disordered packing and transformed AES estimate is proposed. In this method, the encryption key is created using the Amold unordered sequence. The main image is then encrypted using the transformed AES computation and execution of

the round keys provided using mob system. The suggested approach not only reduces the ephemeral complexity of the computation, but also adds diffusivity to the proposed computation , making the images encoded by the proposed computation secure for differential attacks. The crucial space of the proposed method is large enough to neutralize the attacks of the creature's power. This technique is so sensitive to the basic elements and data of the image that small changes to these highlights can cause large changes to the encoded image. Using quantifiable tests, we show how this approach

can safeguard the image from real attacks. The side effects of the entropy test show that the entropy values are almost high and therefore the proposed estimate is secure against entropy attacks. The game results make it clear that small changes are not available for the main shell and big results are gigantic changes to the code schema and mainschema.

4. An Efficient Side-Channel Protected AES Implementation with Arbitrary Protection Order Hannes Gross, Stefan Mangard & Thomas Korak. In this article, Actual idle raids, such as control scans, pose a serious threat to the security of computer circuits. In this white paper, they present a side- channel production team plan protected by Progressed Encryption Standard (AES) that is extremely versatile in terms of security requirements. We show how to mitigate high-demand, multivariate attacks in the face of errors at similar random costs as sensitive circuits. Although our AES setup is adaptable, it is more modest, faster and requires fewer irregularities than the protected AES running on the opposite side channel. For example, our First Request-Secure-AES tariff takes only 18 pieces of randomness for each S-Box activity and 6 KGE of chip area. We show the adaptability of our AES run by combining it with guaranteed requirement fifteen.

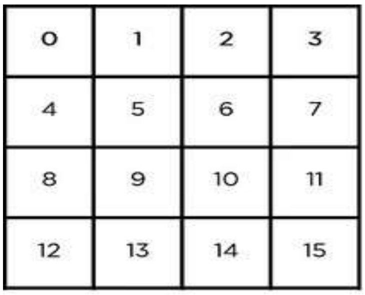
5. Advanced encryption standard (AES) security enhancement using hybrid approach Publisher: IEEE. Flevina Jonese D'souza; Dakshata Panchal Security is an important issue when dealing with data, correspondence, information and electronic commerce in an open partnership. Cryptography (secrecy agreement) is the combination of encrypting exchanges of messages to protect information and make it impregnable. AES is the symmetric encryption standard proposed by NIST. AES became an extraordinarily strong, faster and more profound encryption calculation. AES is commonly used because of its unimaginable power and competence. Recently, however, advanced attacks have been on the rise, keeping security researchers occupied in the lab coming up with improved designs to keep attackers at bay. Potential attacks in symmetric estimation can be Creature Power Attack, Differential Attack, Logarithmic Attack and Direct Attack. Therefore, in order to provide strong security in communicating message , an AES calculation with a combined method of dynamic key age and dynamic S-box age is proposed. In the hybrid methodology, after a while, we will first add more complexity to mess up and propagate code text with Dynamic Key Age, and then make it harder for the attacker to perform static design checks with Dynamic S-Boxage.

6. Rijndael's plan: AES: The provider's high-level encryption standard. In October 2000, the US Public Policy and Innovation Organization chose the Rijndael block cipher as the high-level encryption standard (AES). AES is intended to gradually replace the current Information Encryption Standard (DES) as the most widespread information encryption innovation. This book from the creators of the block character presents Rijndael without any preparation. Hidden Mathematics and the broad-path technique as basic planning thinking are comprehensively explained, and practical aspects of direct and differential cryptanalysis are adapted. The resulting parts check all known attacks on the Rijndael build and manage execution and progression issues. Finally, various codes related to Rijndael are introduced. This volume is THE definitive handbook for Rijndael and AES calculus. Experts, scientists, and students interested in dynamics or data encryption will find an important source of data and references here. Introduced calculation of AES key age; the deficiencies of the AES key age plan were investigated. Based on the main interest, a kind of new thinking plan was developed, and thisplanning technique was created, which can be used to furtherdevelop the AES key age calculation.

7. Research shows how such an improvement can improve the comfort of the first stone without compromising its effectiveness.

III. METHODOLOGY

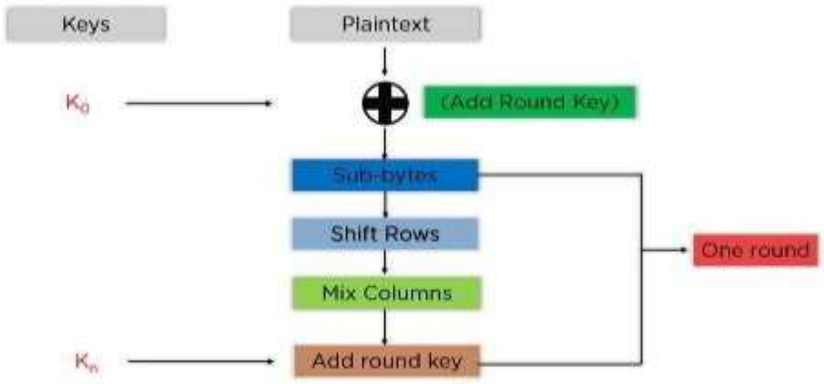
To understand how AES works, you first need to figure out how it sends data between different media. Since a lone block is 16 bytes, a 4x4 frame contains the information in a lone block, and each cell contains one byte of data.



0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Figure 1 - State Array

A state array is the network shown in the figure above. Essentially, the first key is expanded to (n+1) keys, where n is the number of rounds to use in the encryption cycle. For a 128-digit key, the number of turns is 16 and the number of keys to craft is 10+1, 11 keys.

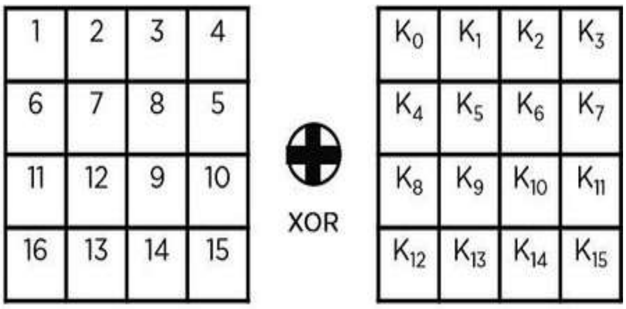


Each Round Steps –

Figure 2 – AES one round process

The referenced progressions are followed successively for each block. By effectively encrypting each block, they are consolidated to frame the final ciphertext. The means are as follows:

Add-round-key: Passes the block information stored in the state indicator via an XOR ability with the generated primary key (K0). Passes the resulting state cluster as a contribution to the next stage.



1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

K_0	K_1	K_2	K_3
K_4	K_5	K_6	K_7
K_8	K_9	K_{10}	K_{11}
K_{12}	K_{13}	K_{14}	K_{15}

Figure 3 – Add Round Key

Sub-bytes: In this step, you change each byte in the status cluster to hexadecimal, with a space in the middle. These parts are the lines and sections, planned with a replacement box (S-Box) to create new qualities for the last national exhibition.

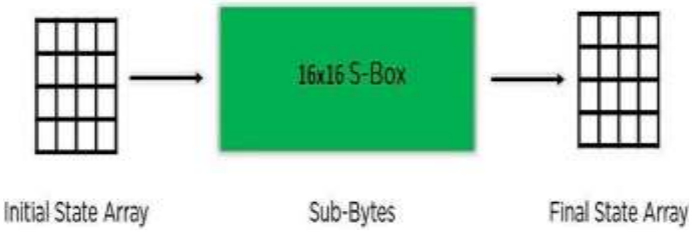
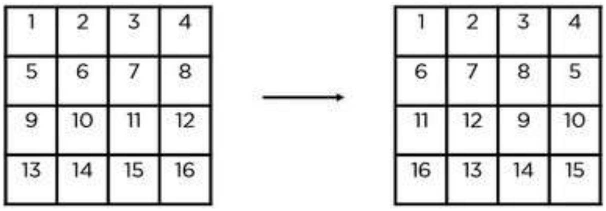


Figure 4 – Sub Bytes

Shift-rows: Swaps the column components among themselves. Avoid the main column. Move the components from the next column, one situation to the side. Also, move the components in the third column two consecutive positions to the side, and move the last row three positions to the side.

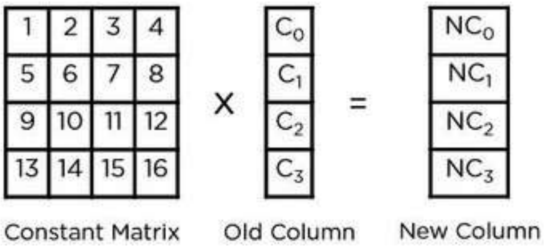


1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

Figure 5 – Shift Row

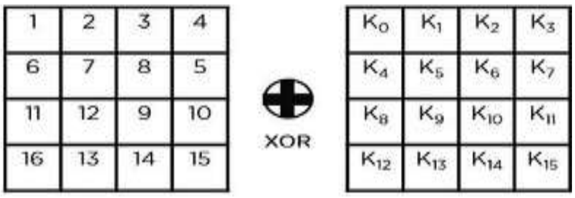
Mix-Column: Duplicates a frame consistent with each segment in the status group to get another segment for the subsequent status display. Expanding each of the sections with a similar consistent grid will earn its state exhibit for the next level. This step should not be completed in this mood round.



$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix} \times \begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} NC_0 \\ NC_1 \\ NC_2 \\ NC_3 \end{bmatrix}$$

Figure 6 – Mix-Column

Add-Round-Key: The key for the lap is XORed with the health indicator captured in the preceding step. If this is the final round, the resulting status indicator becomes the ciphertext for the block; otherwise, it is passed as a new status cluster entry for the following round.

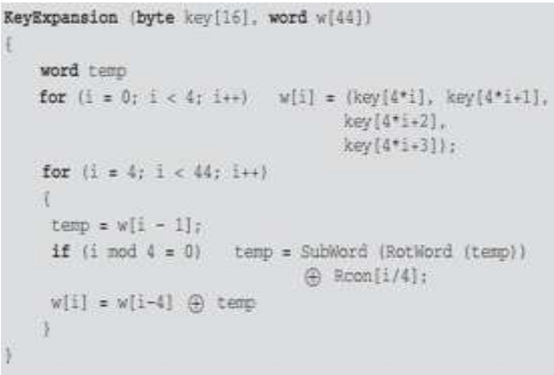


1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

K_0	K_1	K_2	K_3
K_4	K_5	K_6	K_7
K_8	K_9	K_{10}	K_{11}
K_{12}	K_{13}	K_{14}	K_{15}

Figure 7 – Add Round Key

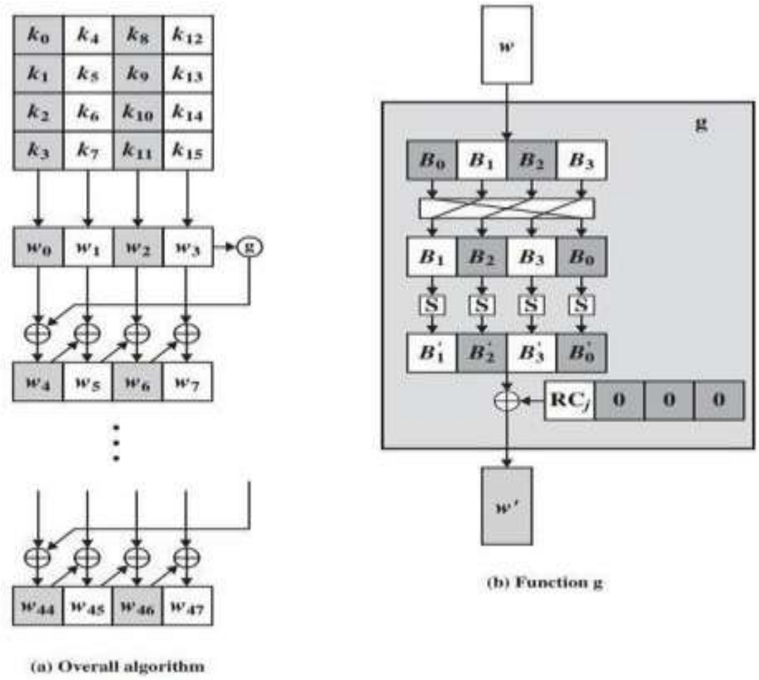
AES Key Distribution: The AES key extension algorithm takes a four-word (16 bytes) key as data and performs an immediate 44-word (176 byte) confirmation. This is enough to provide a 4 word round key for the hidden Add-Round-Key stage and each of the 10 code rounds. The pseudocode on the figure 8 shows the extension. The key is duplicated on the first 4 terms of the extended key. The rest of the long key is loaded four words at a time. Each additional work w[i] depends on the previous word w [i - 1]. likewise, the word 4 positions backwards, in 3 out of 4 cases a direct XOR is used. For a word whose position in group w is a variable number of 4, an impressive extra capacity is used. Figure 9 frames the age of the augmented key, using the g-picture to address this overwhelming ability. The ability g consists of the associated sub-abilities.



```
KeyExpansion (byte key[16], word w[44])
{
    word temp
    for (i = 0; i < 4; i++)   w[i] = (key[4*i], key[4*i+1],
                                      key[4*i+2],
                                      key[4*i+3]);

    for (i = 4; i < 44; i++)
    {
     temp = w[i - 1];
     if (i mod 4 = 0)   temp = SubWord (RotWord (temp))
                               ⊕ Rcon[i/4];
     w[i] = w[i-4] ⊕ temp
    }
}
```

Figure 8 – AES Algorithm



(a) Overall algorithm

(b) Function g

Figure 9 - AES Key Expansion Procedure

IV. RESULTS

1. After running our system, GUI looks like this, and we haveto select Image for encryption.

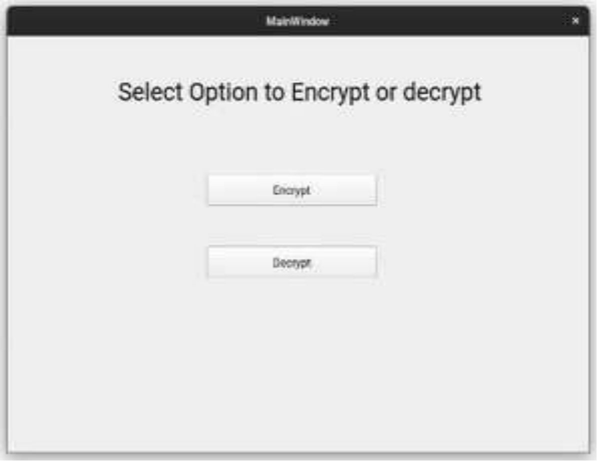
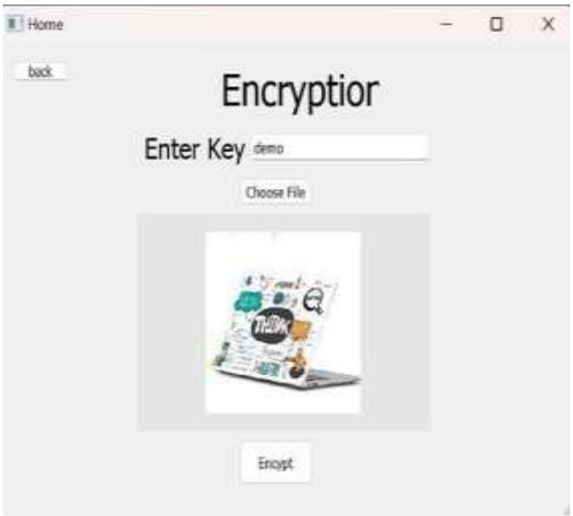


Figure 10 – GUI

2. Now we select Image for encryption and enter key



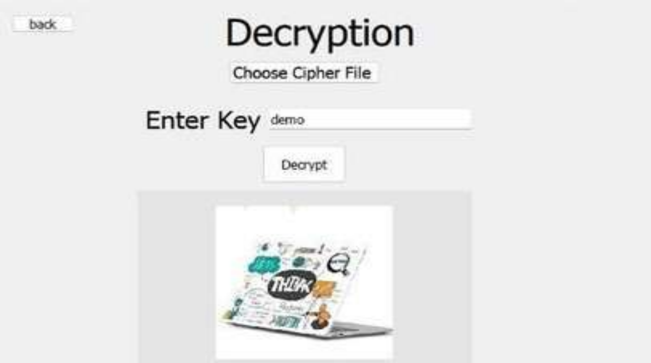
Enter Key demo

Figure 11 – Encryption

3. After Encryption a base 64 conversion of file is obtained –cipher.txt

Figure 12 – Cipher.txt

4. After entering key our Image is decrypted



demo

Figure 13 – Decryption

V. CONCLUSION

We've successfully developed a program that precisely encodes and decodes image documents, which can help reduce the risk of data theft and breaches of sensitive information. The resulting encoded file is highly secure, ensuring no unauthorized access. Thus, it can be transmitted within a company without worry. Our solution, though modest, is highly beneficial for military or medical fields. Utilizing AES encryption for image data effectively protects it from unauthorized access. Implementing AES symmetric key encryption is one of the notable encryption features available. Using Python, AES computation is adapted for image processing. Crucial images can be fully transformed even without optimization. The algorithms boast significant security capabilities, resisting common attacks like brute force, cipher, and plaintext attacks.

Improving key size and data block size could enhance security, though this may require additional resources. Thus, algorithms offering high security and throughput are ideal, particularly for media communications.
Future research should focus on optimizing systems for customizable key lengths and operation modes.

Techniques demonstrated with AES 192- and 256-bit configurations can be extended, and fast universal AES processors could be developed. Future AES designs could consider 8-bit data transmission, incorporating S- BOX configurations and pipelining techniques. Other cryptographic algorithms, especially those utilizing loop unrolling, could benefit from these advancements, ensuring robust security and efficient processing.

VI. REFERENCES

Pronika & Tyagi, S. (2021). Performance analysis of encryption and decryption algorithm. Indonesian Journalof Electrical Engineering and Computer Science. 23. 1030. 10.11591/ijeecs.v23.i2.pp1030-1038.

Abdullah, Ako Muhamad. "Advanced encryption standard (AES) algorithm to encrypt and decrypt data." Cryptography and Network Security 16 (2017): 1-11.

Arab, Alireza, Mohammad Javad Rostami, and Behnam Ghavami. "An image encryption method based on chaossystem and AES algorithm." The Journal of Supercomputing 75.10 (2019): 6663-6682.

Y. Yuan, Y. Yang, L. Wu and X. Zhang, "A High- Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," 2018 IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC), 2018, pp. 1-2, doi: 10.1109/EDSSC.2018.8487056.

Groß, Hannes, Stefan Mangard, and Thomas Korak. "An efficient side-channel protected AES implementation with arbitrary protection order." Cryptographers' Track at the RSA Conference. Springer, Cham, 2017.

F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 647-652, doi: 10.1109/CCAA.2017.8229881.

Daemen, Joan & Rijmen, Vincent. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. 10.1007/978-3-662-04722-4.

Nechvatal J, Barker E, Bassham L, Burr W, Dworkin M, Foti J, Roback E. Report on the Development of the Advanced Encryption Standard (AES). J Res Natl Inst Stand Technol. 2001 Jun 1;106(3):511-77. doi: 10.6028/jres.106.023. PMID: 27500035; PMCID: PMC4863838.