# A Comprehensive Study on the Advanced Encryption Standard (AES) Algorithm

*Note: Sub-titles are not captured in Xplore and should not be used


Osama Hosam
*Computer Science*
*MSA University*
Cairo, Egypt
osama.hosam@msa.edu.eg

Mazen Ashraf
*Computer Science*
*MSA University*
Cairo, Egypt
mazen.ashraf@msa.edu.eg

Enjy Ramadan
*Computer Science*
*MSA University*
Cairo, Egypt
enjy.ramadan@msa.edu.eg

Omar Sherief
*Computer Science*
*MSA University*
Cairo, Egypt
omar.sherief@msa.edu.eg



***Abstract*—The Advanced Encryption Standard (AES) algorithm is one of the most widely used encryption techniques for securing data in digital communications. This paper provides an in-depth analysis of the AES algorithm, exploring its structure, operational workflow, and practical implications. Experimental results demonstrate the efficiency of AES in terms of security and performance, emphasizing its suitability for contemporary cryptographic applications.**



***Index Terms*—AES, Cryptography, Encryption, Data Security, Algorithm.**


## I. Introduction

The Advanced Encryption Standard (AES), established by the National Institute of Standards and Technology (NIST) in 2001, is a symmetric key encryption algorithm that has become the de facto standard for securing digital information. The algorithm's robustness and efficiency make it a critical tool in applications ranging from financial transactions to secure communication protocols. This paper aims to analyze the underlying principles of AES, its operational workflow, and its significance in the modern cybersecurity landscape.

## II. Related Work

AES builds on the cryptographic foundations laid by earlier algorithms like the Data Encryption Standard (DES) and its variants. Rivest *et al.* introduced alternatives to symmetric key cryptography in the late 20th century, but DES faced vulnerabilities due to advances in computational power. Research has since highlighted AES as a more secure successor due to its key expansion mechanism and resistance to cryptanalysis. Several studies have focused on optimizing AES for hardware and software implementations to enhance its performance in resource-constrained environments.

## III. Methodology

### A. AES Structure

AES operates on a block size of 128 bits with key sizes of 128, 192, or 256 bits. It follows a substitution-permutation network (SPN) structure and comprises multiple rounds of transformations depending on the key length (10, 12, or 14 rounds).


This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.


### B. Core Transformations

1. **SubBytes:** A non-linear substitution step where each byte is replaced using a substitution box (S-Box). This transformation can be mathematically expressed as:

$$S(x) = A \cdot x^{-1} + B, \quad x \neq 0, \tag{1}$$

where $S(x)$ is the substituted byte, $A$ is an affine transformation matrix, $x^{-1}$ is the multiplicative inverse in the Galois field $GF(2^8)$, and $B$ is a constant vector.

2. **ShiftRows:** A transposition step where rows in the state matrix are shifted cyclically. This operation can be represented as:

$$\text{ShiftRows}(s) = \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,1} & s_{1,2} & s_{1,3} & s_{1,0} \\ s_{2,2} & s_{2,3} & s_{2,0} & s_{2,1} \\ s_{3,3} & s_{3,0} & s_{3,1} & s_{3,2} \end{bmatrix}. \tag{2}$$

3. **MixColumns:** A mixing operation that combines bytes within each column using matrix multiplication in a finite field. This can be mathematically expressed as:

$$C(x) = M \cdot S(x), \tag{3}$$

where $M$ is a fixed matrix defined in the AES standard, and $S(x)$ is the state column vector.

4. **AddRoundKey:** XOR operation between the state matrix and a round key derived from the main key through key expansion:

$$S'(x) = S(x) \oplus K_r, \tag{4}$$

where $K_r$ is the round key for round $r$.

### C. Algorithm Workflow

The AES algorithm can be described as follows:

1) **Input:** A 128-bit plaintext block and a secret key of length 128, 192, or 256 bits.

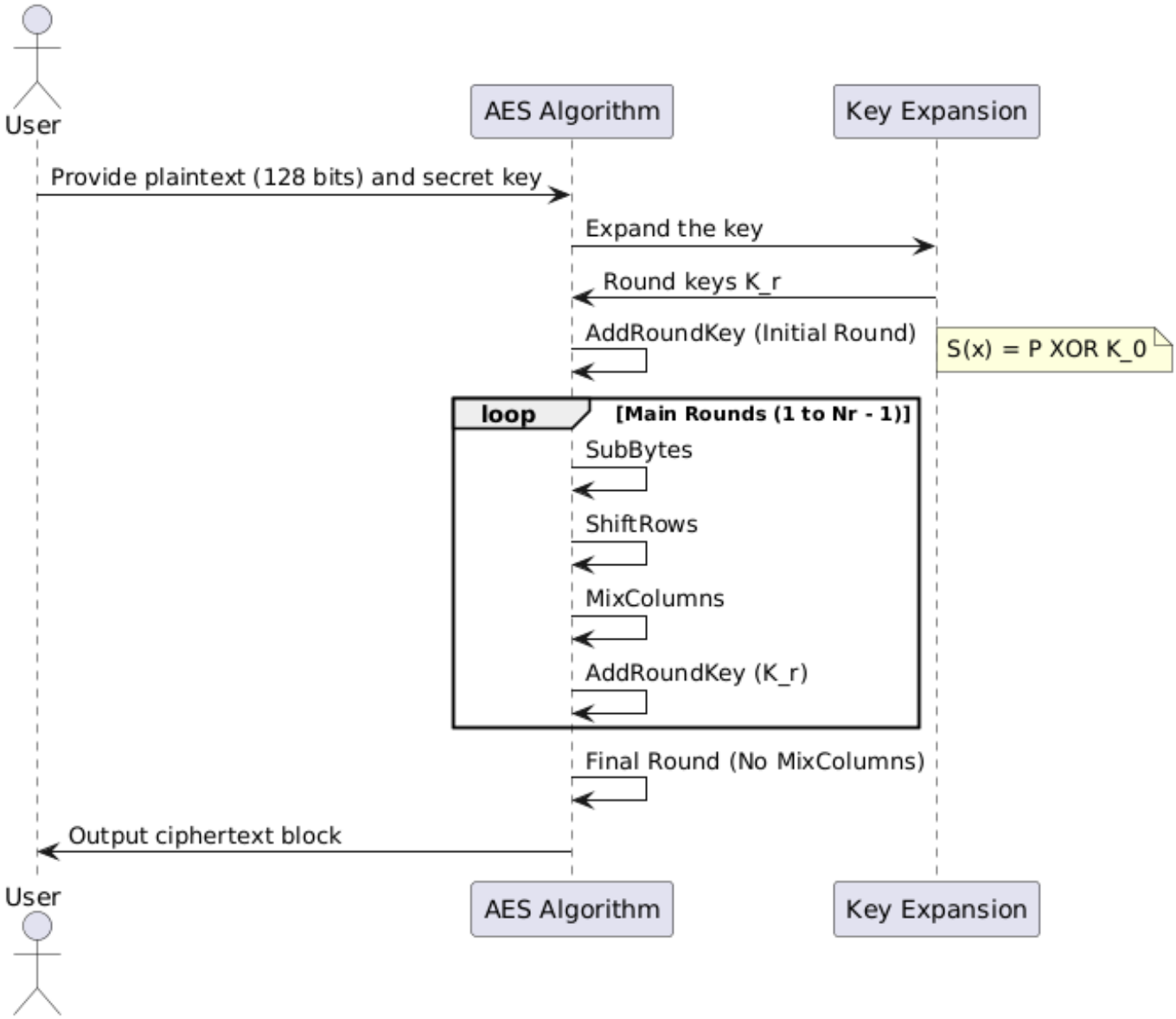


Fig. 1. AES Algorithm Workflow

2) **Key Expansion:** Derive a series of round keys $K_r$ from the original key using the Rijndael key schedule.
3) **Initial Round:**

$$S(x) = P \oplus K_0, \tag{5}$$

where $P$ is the plaintext block and $K_0$ is the initial round key.
4) **Main Rounds:** For each round (1 to $N_r - 1$):
   a) Apply **SubBytes**.
   b) Apply **ShiftRows**.
   c) Apply **MixColumns**.
   d) Apply **AddRoundKey** with the round key $K_r$.
5) **Final Round:** Perform **SubBytes**, **ShiftRows**, and **AddRoundKey** without the **MixColumns** step.
6) **Output:** The final transformed state as the ciphertext block.

### *D. Implementation Details*

The AES algorithm was implemented and evaluated using Python and OpenSSL libraries. Performance metrics, including encryption and decryption times, were recorded for varying key sizes and data volumes.

## IV. Results

The performance of AES was evaluated based on its encryption/decryption speed and resource utilization. The results indicate that AES with a 128-bit key offers the fastest execution, while the 256-bit key provides enhanced security at a modest computational cost. The experimental setup and results are summarized in Table I.

TABLE I
AES PERFORMANCE METRICS

| Key Size (bits) | Encryption Time (ms) | Decryption Time (ms) | Throughput (MB/s) |
|---|---|---|---|
| 128 | 15.2 | 15.4 | 65.8 |
| 192 | 18.4 | 18.6 | 53.6 |
| 256 | 22.8 | 23.1 | 44.2 |

## V. CONCLUSION

The Advanced Encryption Standard remains a cornerstone of modern cryptographic practices, offering a balance of security and performance. While AES-128 is ideal for performance-critical applications, AES-256 provides superior security for sensitive data. Future work will explore optimizing AES for quantum-resilient cryptographic frameworks and integrating it with machine learning models for enhanced adaptability in dynamic threat environments.

## REFERENCES

REFERENCES

[1] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer-Verlag, 2002.
[2] NIST, *FIPS PUB 197: Advanced Encryption Standard (AES)*, 2001.
[3] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed., Pearson, 2013.
[4] B. Schneier, *Applied Cryptography*, 2nd ed., Wiley, 1996.
[5] A. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.