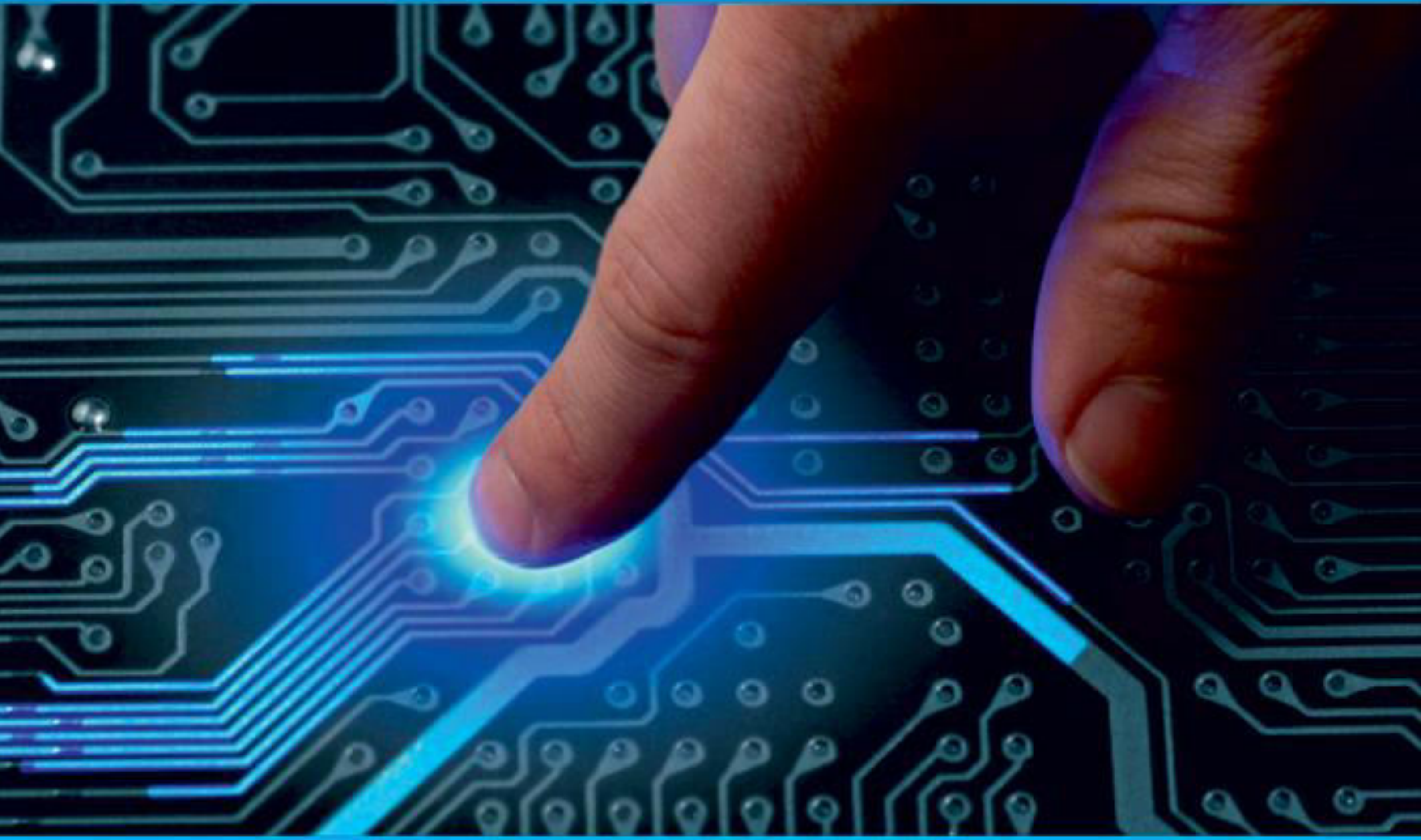
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 10, October 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Analysis of AES-Advance Encryption Standards

Dr. Susil Kumar Sahoo, Mr. Sevanth P, Mr. Ngampai Yanlem

Professor & Head, Department of Computer Science and Applications, The Oxford College of Science, Bangalore, India

MSC Student, Department of Computer Science and Application, The Oxford College of Science, Bangalore, India

ABSTRACTS: Symmetric encryption is a method of Cryptography that uses a key for both encryption and decryption, for faster and easier operation and within Symmetric Encryption there is a method called Advance Encryption Standards (AES) which is the widely used algorithm of Symmetric Encryption replacing the older algorithms like RSA(Rivest-Shamir-Adleman) and DES (Data Encryption Standard) due to its faster,better and easier used. AES employs key length of 128, 192,256 bits, offering high security and robustness against brute-force attacks. Due to the stronger encryption, AES is used instead of DES, as DES's 56-bit key is vulnerable to modern computational attacks. And since RSA is a method of asymmetric encryption, it is primarily used for key exchange and digital signatures; AES excels in speed and scalability, making it ideal for encrypting large volumes of data. While RSA is secure for small data and critical for secure key distribution. It is computationally expensive and inefficient for bulk data encryption. AES's efficient block cipher structure and hardware optimization have made it the de facto standard for securing communication, storage, and various cryptographic applications.[1]

KEYWORDS: Symmetric encryption, Cryptography, Encryption, Decryption, Faster and Easier operation, Advance Encryption Standards (AES), Key Length of 128,192,256 bits, High Security and Robustness against Brute-Force Attack, Speed and Scalability, Key Exchange, Digital Signatures, Block Cipher Structure, Hardware Optimization, de facto standard.

I. INTRODUCTION

With the increase in modern society and advancement in technology, the need to secure our data has become more important as almost everything are being exchanged digitally, and the risk to lose everything depends on a virtual software, which can be hack, endangering our personal data and information, so to avoid or prevent such disaster, Encrypting the data became more secure. Encryption algorithms play a pivotal role in protecting this information from unauthorized access and malicious attacks. Among the most prominent encryption algorithms are the Advanced Encryption Standard (AES), the Data Encryption Standard (DES), and the Rivest-Shamir-Adleman (RSA) algorithm.

The Advanced Encryption Standard (AES), also known by its original name Rijndael, a specification for the encryption of electronic data established by the in 2001. AES is a variant of the Rijndael block cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, Who submitted a proposal to NIST during the AES selection three members of the Rijndeal family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.[1] [2]

AES, a symmetric key encryption algorithm, was developed in response to the vulnerabilities of DES, an older encryption standard that had become susceptible to brute-force attacks due to advancements in computational power. AES was selected by the U.S. National Institute of Standards and Technology (NIST) in 2001 as the encryption standard for securing sensitive data, replacing DES. Its adoption was driven by its strong security properties, efficiency in handling large datasets, and its ability to resist cryptographic attacks. AES supports key sizes of 128, 192, and 256 bits, offering flexibility in balancing security and performance.[2]

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

The significant challenges in symmetric encryption is Key Distribution. Since both parties must have access to the same encryption key, the key must be securely shared before encrypted communication can begin. This presents a problem when the parties are communicating over an insecure channel. Various approach has been taken to address the issue.[3]

- **Pre-shared Keys (PSK)**:

A pre-shared key is a secret key that is manually distributed and shared between parties before secure communication begins. The parties use this key for encryption and decryption of messages, ensuring confidentiality.

- **Key Exchange Protocols:**

Key exchange protocols enable two or more parties to generate and share secret keys securely. These keys are essential for encrypting and decrypting messages to ensure confidentiality and integrity.

- **Key Management Systems(KMS):**

In large-scale systems, automated systems are used to manage keys, including generating, distributing, storing, and revoking keys. Cloud services such as AWS and Google Cloud provide KMS services to their users to ensure secure key management.

III. STRUCTURE AND METHODOLOGY

AES (Advanced Encryption Standard) is a symmetric block cipher that encrypts and decrypts data in fixed blocks of 128 bits (16 bytes) using keys of varying lengths (128,192,256 bits)[4]

- **Structure of AES algorithm:**

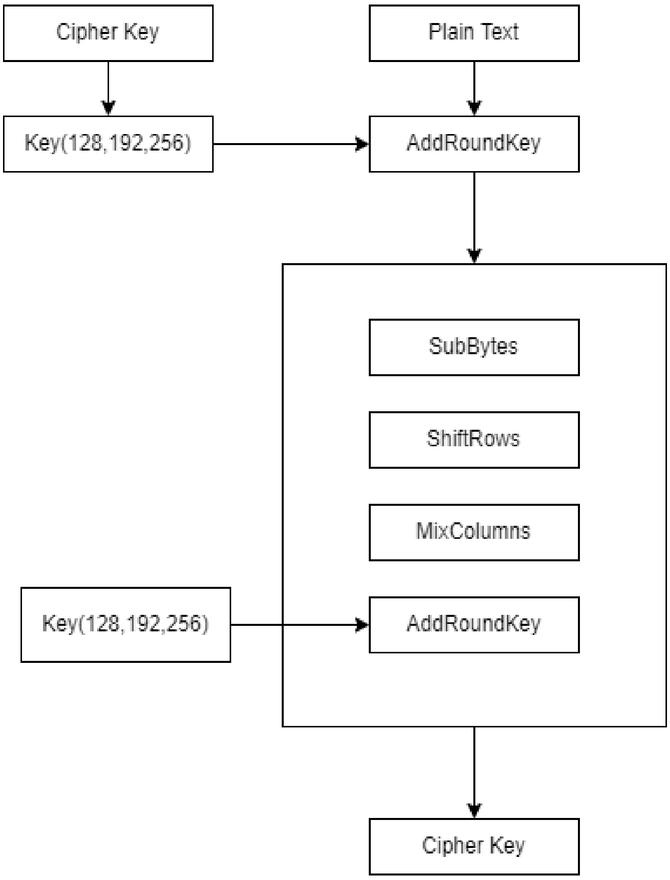
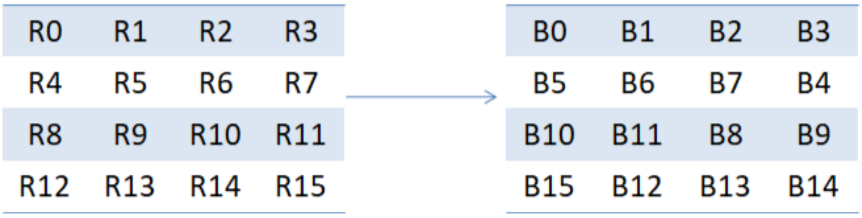


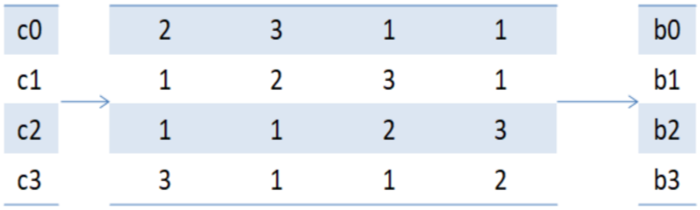
Figure 1: Structure of AES Encryption Algorithm

- **Key Components:**
  - **Plain Text:** This is the input data or information that is to be encrypted.
  - **Cipher Key**: Cipher key is the secret key or lock that will used for encryption, varying in key length (128, 192, 256 bits)
  - **Round**: The encryption process involves multiple rounds depending on the key size:
    - 10 rounds for 128 bit keys
    - 12 rounds for 192 bit keys
    - 14 rounds for 156 bit keys
- **Steps for AES Encryption:**
  - **Key Expansion:** AES begins by expanding the cipher key into several round keys, which are required for each round of encryption. In other words, the initial key is divided into words and apply substitution and rotation to the key based on the round constants to generate new round key.
  - **Initial Round:** Before the main encryption round starts, AES apply an initial AddRoundKey. That XORed the PlainText Block with the first round key**.**
  - **Main Rounds:** This repeats for each round except of the last
    - **Byte Subsitution(SubBytes):** The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.
    - **ShiftRows:** Each of the four rows of the matrix is shifted to the left. Any entries that 'Fall off' are re-inserted on the right side of the rows. Shift is carried out as follows:
      - First row is not shifted
      - Second row is shifted one (byte) position to the left.
      - Third row is shifted two positions to the left.
      - Fourth row is shifted three positions to the left. The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.



R0	R1	R2	R3	B0	B1	B2	B3
R4	R5	R6	R7	B5	B6	B7	B4
R8	R9	R10	R11	B10	B11	B8	B9
R12	R13	R14	R15	B15	B12	B13	B14

- **MIxColumn:** Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. This result is another new matrix consisting of 16 new bytes. It should be noted that this steps is not performed in the last round.



c0	2	3	1	1	b0
c1	1	2	3	1	b1
c2	1	1	2	3	b2
c3	3	1	1	2	b3

- **AddRoundKey:** This 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.
- **Final round:** This round is similar to the main round but without MixColumn:
  - **SubBytes:**
  - **ShiftRows:**
  - **AddRoundKey:**

- **Steps for AES Decryption:**

Decryption process occurs in the reverse manner to the AES Encryption process. I.e. in the following order:

- AddRoundKey
- MixColumn
- ShiftRows
- Byte Substitution(SubBytes)

IV. COMPARISM BETWEEN AES AND DES ENCRYPTION

The Advance Encryption Standard (AES) is the successor of The Data Encryption Standard (DES) as the advancement in the industries the security provided by the Data Encryption Standard (DES) were unable to keep up to with the technology as the encrypted message provided by DES was easily broken within 22 hours and 15 minutes in 1999 by Electronic Frontier Foundation's Deep Crack computer and Distributed.net's computer network, as a result in 2000 the National Institute of Standards and Technology(NIST) primary objective was to search for a replacement for DES as a result ,NIST announced a Rijndael as the proposed Advanced Encryption Standard(AES).

Key Difference between AES and DES which lead to AES becoming more favored by the industries are as follows[5]

Data Encryption Standard(DES)	Advanced Encryption Standard(AES)
1. The data block in DES is split into two halves.	1. The entire block in AES is processed as a single matrix.
2. It works on Feistel Cipher structure.	2. It works in substitution and permutation method.
3. It was designed by IBM in 1976.	3. It was designed by Vincent Rijmen and Joan Daeman in 1999.
4. It had only 16 rounds.	4. The number of rounds depends on the key size: • 10 rounds for 128-bit algorithm • 12 rounds for 192-bit algorithm • 14 rounds for 256-bit algorithm
5. It is slower than AES.	5. AES is faster than DES.
6. Since DES uses a smaller key, it was less secure.	6. Since AES uses a larger secret key, it is more secure.
7. The PlainText can be only 64 bits.	7. PlainText can be of 128.192 or 256 bits.
8. Brute force would force the text to be decrypted.	8. At This moment there is no identified attack.
9. The block size is 128-bits.	9. The block size is 64-bits.
10. DES originated from Lucifer cipher	10. AES originates from square cipher.

V. RESULT

AES Encryption is used to encrypt our data to keep it private; it is used to make it difficult to for other to view our data. This is the reason why many industries implement this feature in their software. At the same time it is faster and optimal because of it being symmetric encryption (i.e. uses a single key for encryption and decryption) it is easier to learn and use and provides more security then DES encryption.

Software companies like facebook, watapps, etc implement Encryption to keep the users data secure to keep them away from cyber bullying, blackmail etc.

VI. CONCLUSION

AES Encryption is more favored by most of the industries and also are in an increase in demand in the modern society. This paperhighlights a very small portion of Cryptography, with the aim to show the importance of Encryption as it is a very common in-name but in reality only few knows how it actually works and why it has replaced DES encryption.

REFERENCES

1. Joan Daemen and Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard", Springer- Verlag Berlin Heidelberg 2002.
2. William Stallings ," Cryptography and Network Security : Principle and Practices 4th edition" Published by Dorling Kindersley (India) Pvt. Ltd, licenses by Pearson Education in South Asia 2011.
3. Neigel p Smart," Cryptography made Simple" Springer International Publishing Switzerland 2016.
4. F. Weissbaum and T. Lugrin," Symmetric Cryptography" Research of National Institute of Standards and Technology in 1999
5. Eil Biham, Adi Shamir. "Differential Cryptanalysis of DES" Springer Verlag, New York 1993

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details