Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a highly trusted **encryption algorithm** used to secure data by converting it into an unreadable format without the proper key. It is developed by the National Institute of Standards and Technology (NIST) in 2001. It is is widely used today as it is much stronger than DES and triple DES despite being harder to implement. **AES encryption** uses various **key lengths** (128, 192, or 256 bits) to provide strong protection against unauthorized access. This **data security** measure is efficient and widely implemented in securing **internet communication**, protecting **sensitive data**, and encrypting files. AES, a cornerstone of modern cryptography, is recognized globally for its ability to keep information safe from cyber threats.

- AES is a Block Cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text. AES relies on the substitution-permutation network principle, which is performed using a series of linked operations that involve replacing and shuffling the input data.

Working of The Cipher

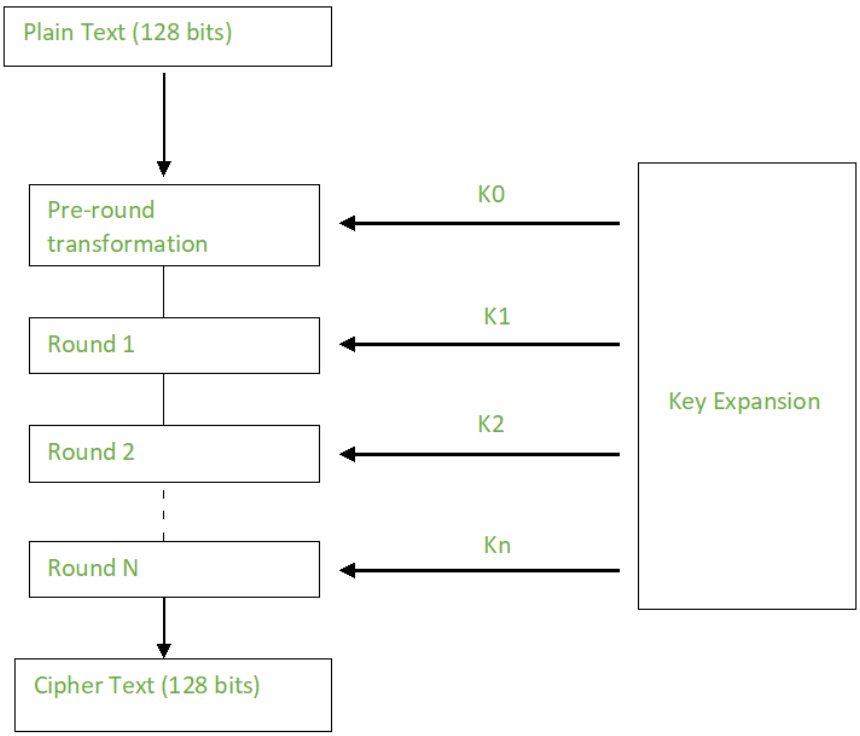
AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows :

N (Number of Rounds)	Key Size (in bits)
10	128
12	192
14	256

Creation of Round Keys

A Key Schedule algorithm calculates all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

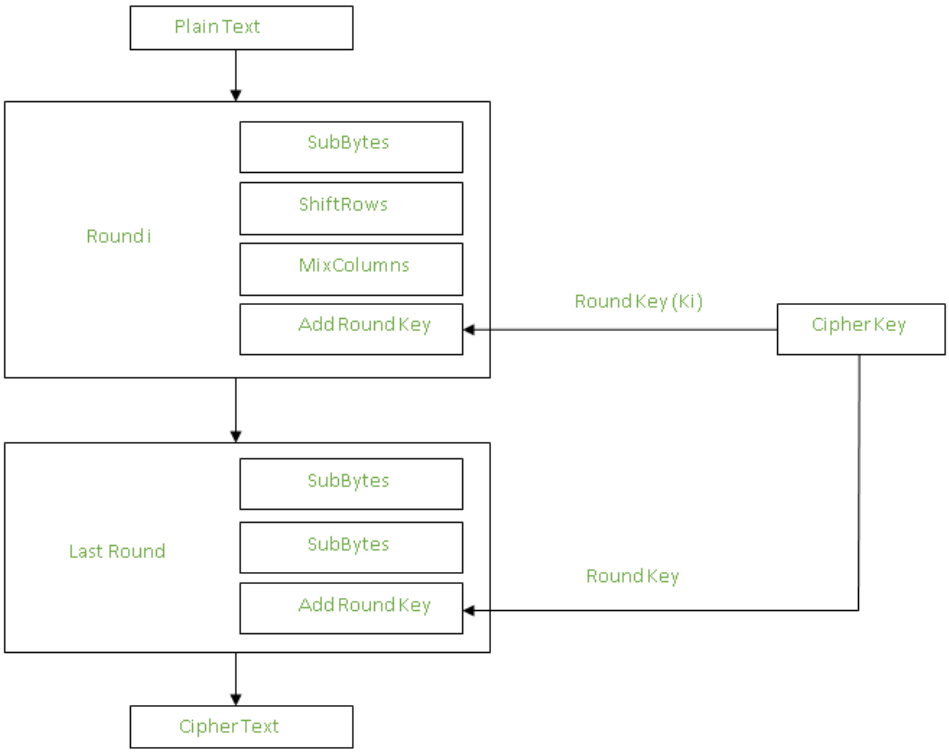


Creation of Round Keys (AES)

Encryption

AES considers each block as a 16-byte (4 byte x 4 byte = 128) grid in a column-major arrangement.

[b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]



Added Round Keys (AES)

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

Step1. Sub Bytes

This step implements the substitution.

In this step, each byte is substituted by another byte. It is performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16-byte (4 x 4) matrix like before.

The next two steps implement the permutation.

Step2. Shift Rows

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)
[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]
| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |
| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |
[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

Step 3: Mix Columns
This step is a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.
This step is skipped 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]

Step 4: Add Round Keys

- Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes are not considered as a grid but just as 128 bits of data.
- After all these rounds 128 bits of encrypted data are given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption
The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes. Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
The stages of each round of decryption are as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so I will explain the steps with notable differences.
Inverse MixColumns

- This step is similar to the Mix Columns step in encryption but differs in the matrix used to carry out the operation.
- Mix Columns Operation each column is mixed independent of the other.
- Matrix multiplication is used. The output of this step is the matrix multiplication of the old values and a

constant matrix
[b0] = [14 11 13 9] [c0]
[b1]=[9 14 11 13] [c1]

[b2] =[13 9 14 11] [c2]
[b3]=[11 13 9 14] [c3]

Inverse SubBytes

- Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.
- Function Substitute performs a byte substitution on each byte of the input word. For this purpose, it uses an S-box.

Applications of AES

AES is widely used in many applications which require secure data storage and transmission. Some common use cases include:

- **Wireless security:** AES is used in securing wireless networks, such as Wi-Fi networks, to ensure data confidentiality and prevent unauthorized access.
- **Database Encryption:** AES can be applied to encrypt sensitive data stored in databases. This helps protect personal information, financial records, and other confidential data from unauthorized access in case of a data breach.
- **Secure communications:** AES is widely used in protocols such as internet communications, email, instant messaging, and voice/video calls. It ensures that the data remains confidential.
- **Data storage:** AES is used to encrypt sensitive data stored on hard drives, USB drives, and other storage media, protecting it from unauthorized access in case of loss or theft.
- **Virtual Private Networks (VPNs):** AES is commonly used in VPN protocols to secure the communication between a user's device and a remote server. It ensures that data sent and received through the VPN remains private and cannot be deciphered by eavesdroppers.
- **Secure Storage of Passwords:** AES encryption is commonly employed to store passwords securely. Instead of storing plaintext passwords, the encrypted version is stored. This adds an extra layer of security and protects user credentials in case of unauthorized access to the storage.
- **File and Disk Encryption:** AES is used to encrypt files and folders on computers, external storage devices, and cloud storage. It protects sensitive data stored on devices or during data transfer to prevent unauthorized access.

Difference between AES and DES ciphers

- Advanced Encryption Standard (AES) is a highly trusted encryption algorithm used to secure data by converting it into an unreadable format without the proper key while Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security. In this article, we are going to discuss the differences between AES and DES.
- What is AES?
- AES stands for Advanced Encryption Standard and is a widely used encryption algorithm designed to secure data, developed in 2001. As triple-DES was found to be slow, AES was created and is six times faster than the triple-DES. It is one of the most widely used symmetric block cipher algorithms used nowadays. It works on bytes rather than bits. It encrypts information using a symmetric key, meaning the same key is used for both encryption and decryption.
- AES is known for its high speed and strong security, making it ideal for protecting sensitive data in various applications, such as online banking, file encryption, and wireless security. Understanding AES and its importance in cybersecurity helps ensure that your data remains safe from unauthorized access and cyber threats.
- Applications of AES
- Wireless Security : AES is widely used in securing wireless networks, including Wi-Fi networks . It ensures data confidentiality and prevents unauthorized access.
- Data Storage and Transmission : AES is employed for secure data storage and transmission. It’s commonly used in applications where sensitive information needs protection.
- VPN (Virtual Private Network) : AES secures VPN connections , allowing users to access private networks securely over the internet.
- Disk Encryption : AES encrypts data on hard drives, USB drives , and other storage devices.
- Secure Messaging Apps : Many messaging apps use AES to encrypt chat messages and attachments.
- What is DES?
- DES stands for Data Encryption Standard, is an encryption algorithm used to secure data by converting it into unreadable code, developed in 1977. It is a multi-round cipher that divides

the full text into 2 parts and then works on each part individually. It includes various functionality such as Expansion, Permutation, and Substitution, XOR operation with a round key. It uses a symmetric key, meaning the same key is used for both encryption and decryption.

- Although DES was widely used for many years, it has since been deemed less secure due to its shorter key length, making it vulnerable to brute-force attacks. Despite this, understanding DES is important as it laid the groundwork for more advanced encryption methods like AES, helping to shape modern data security practices.
- Applications of DES
- Triple DES (3DES) : A more secure variant of DES, 3DES applies DES encryption three times sequentially. It's still used in legacy systems.
- Financial Transactions : DES was once used for securing financial transactions, but it has largely been replaced by AES.
- Legacy Systems : Some older systems still rely on DES for compatibility reasons.
- Difference Between AES and DES

S.No	AES	DES
1.	AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
2.	The date of creation is 2001.	The date of creation is 1977.
3.	Byte-Oriented.	Bit-Oriented.
4.	Key length can be 128-bits, 192-bits, and 256-bits.	The key length is 56 bits in DES.

S.No	AES	DES
5.	Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations
6.	The structure is based on a substitution-permutation network.	The structure is based on a Feistel network .
7.	The design rationale for AES is open.	The design rationale for DES is closed.
8.	The selection process for this is secret but accepted for open public comment.	The selection process for this is secret.
9.	AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
10.	The rounds in AES are: Byte	The rounds in DES are:

• S.No	• AES	• DES
	Substitution, Shift Row, Mix Column and Key Addition	Expansion, XOR operation with round key, Substitution and Permutation
• 11.	• AES can encrypt 128 bits of plaintext.	• DES can encrypt 64 bits of plaintext.
• 12.	• It can generate Ciphertext of 128, 192, 256 bits.	• It generates Ciphertext of 64 bits.
• 13.	• AES cipher is derived from an aside-channel square cipher.	• DES cipher is derived from Lucifer cipher.
• 14.	• AES was designed by Vincent Rijmen and Joan Daemen.	• DES was designed by IBM.
• 15.	• No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attacks have better	• Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis.

• S.No	• AES	• DES
	complexity than brute force but still ineffective.	
• 16.	• It is faster than DES.	• It is slower than AES.
• 17.	• It is flexible.	• It is not flexible.
• 18.	• It is efficient with both hardware and software.	• It is efficient only with hardware.

- Conclusion
- In conclusion, while both AES and DES are important encryption algorithms, AES leads DES in terms of speed, security, and versatility. AES, created in 2001, has longer key lengths and a more complex structure, making it more secure and frequently used in modern applications. In contrast, DES, which was introduced in 1977, has shorter key lengths and recognized errors, hence it has been replaced by AES in most security applications.
-