

### **LAB ASSIGNMENT NO:03**

**Aim:** Block cipher modes of operation using Advanced Encryption Standard (AES).

**Lab Outcome Attained:** Demonstrate Key management, distribution and user authentication.

#### **Theory:**

> Briefly explain AES algorithm (What type of cipher it is?, number of rounds, keysize, block size, operations in each round)

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that falls under the category of block ciphers. AES operates on fixed-size blocks of data and employs a substitution-permutation network (SPN) structure. It was selected by the National Institute of Standards and Technology (NIST) as the encryption standard in 2001, replacing the older Data Encryption Standard (DES).

Number of Rounds: AES operates with different numbers of rounds based on the key size:

128-bit key: 10 rounds

192-bit key: 12 rounds

256-bit key: 14 rounds

Key Size: AES supports key sizes of 128, 192, and 256 bits.

Block Size: AES operates on blocks of data, and the block size for AES is fixed at 128 bits.

#### Operations in Each Round:

**SubBytes:** Byte substitution using a fixed substitution table (S-box). Each byte in the block is replaced with a corresponding byte from the S-box.

**ShiftRows:** Byte shifting within rows of the block. The first row remains unchanged, the second row shifts by one byte to the left, the third row shifts by two bytes, and the fourth row shifts by three bytes.

**MixColumns:** Column-wise mixing operation. Each column is treated as a polynomial and is transformed through a matrix multiplication operation. This step provides diffusion and helps achieve confusion.

**AddRoundKey:** A bitwise XOR operation where each byte of the block is combined with the corresponding byte of the round key. The round key is derived from the original encryption key using a key expansion algorithm.

These operations are performed for the specified number of rounds based on the key size. The additional security of AES stems from its key expansion algorithm, which generates a set of round keys from the original encryption key. Each round key is used in the AddRoundKey step, adding a layer of complexity and security.

Overall, AES is a highly secure and efficient encryption algorithm that offers strong protection for sensitive data. Its adoption as a standard encryption mechanism in various applications demonstrates its robustness and reliability.

> With diagram explain in brief block cipher modes of operation

1. ECB mode
2. CBC mode
3. OFB mode
4. Counter mode

A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time.

### **Electronic Code Book (ECB) Mode**

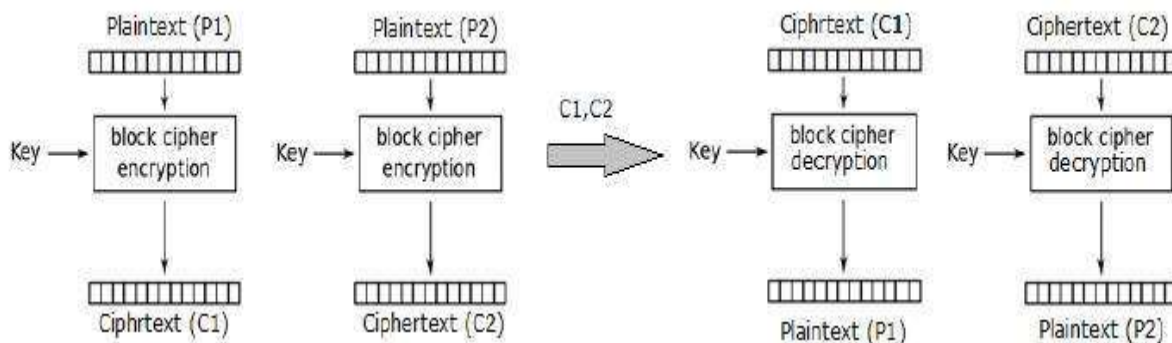
This mode is a most straightforward way of processing a series of sequentially listed message blocks.

#### **Operation**

- The user takes the first block of plaintext and encrypts it with the key to produce the first block of ciphertext.
- He then takes the second block of plaintext and follows the same process with same key and so on so forth.

The ECB mode is deterministic, that is, if plaintext block  $P_1, P_2, \dots, P_m$  are encrypted twice under the same key, the output ciphertext blocks will be the same.

In fact, for a given key technically we can create a codebook of ciphertexts for all possible plaintext blocks. Encryption would then entail only looking up for required plaintext and select the corresponding ciphertext. Thus, the operation is analogous to the assignment of code words in a codebook, and hence gets an official name – Electronic Codebook mode of operation (ECB). It is illustrated as follows –



### Analysis of ECB Mode

In reality, any application data usually have partial information which can be guessed. For example, the range of salary can be guessed. A ciphertext from ECB can allow an attacker to guess the plaintext by trial-and-error if the plaintext message is within predictable.

For example, if a ciphertext from the ECB mode is known to encrypt a salary figure, then a small number of trials will allow an attacker to recover the figure. In general, we do not wish to use a deterministic cipher, and hence the ECB mode should not be used in most applications.

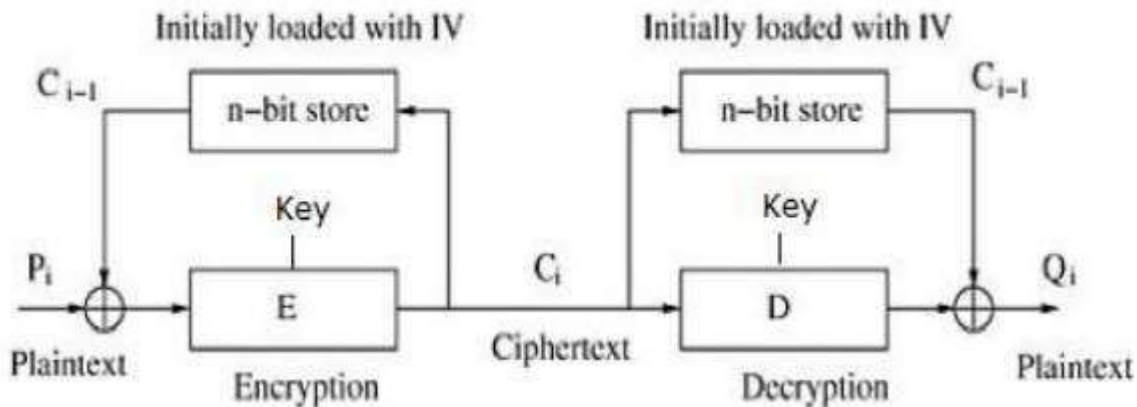
### **Cipher Block Chaining (CBC) Mode**

CBC mode of operation provides message dependence for generating ciphertext and makes the system non-deterministic.

#### **Operation**

The operation of CBC mode is depicted in the following illustration. The steps are as follows –

- Load the n-bit Initialization Vector (IV) in the top register.
- XOR the n-bit plaintext block with data value in top register.
- Encrypt the result of XOR operation with underlying block cipher with key K.
- Feed ciphertext block into top register and continue the operation till all plaintext blocks are processed.
- For decryption, IV data is XORed with first ciphertext block decrypted. The first ciphertext block is also fed into to register replacing IV for decrypting next ciphertext block.



### Analysis of CBC Mode

In CBC mode, the current plaintext block is added to the previous ciphertext block, and then the result is encrypted with the key. Decryption is thus the reverse process, which involves decrypting the current ciphertext and then adding the previous ciphertext block to the result.

Advantage of CBC over ECB is that changing IV results in different ciphertext for identical message. On the drawback side, the error in transmission gets propagated to few further block during decryption due to chaining effect.

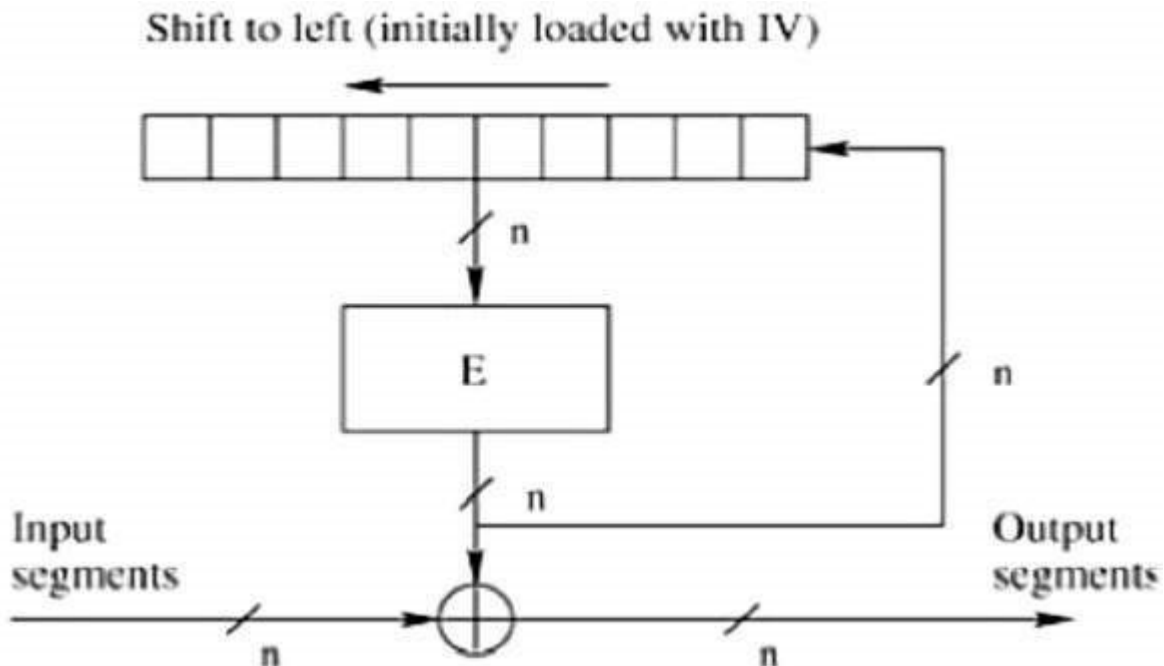
It is worth mentioning that CBC mode forms the basis for a well-known data origin authentication mechanism. Thus, it has an advantage for those applications that require both symmetric encryption and data origin authentication.

### **Output Feedback (OFB) Mode**

It involves feeding the successive output blocks from the underlying block cipher back to it. These feedback blocks provide string of bits to feed the encryption algorithm which act as the key-stream generator as in case of CFB mode.

The key stream generated is XOR-ed with the plaintext blocks. The OFB mode requires an IV as the initial random  $n$ -bit input block. The IV need not be secret.

The operation is depicted in the following illustration –



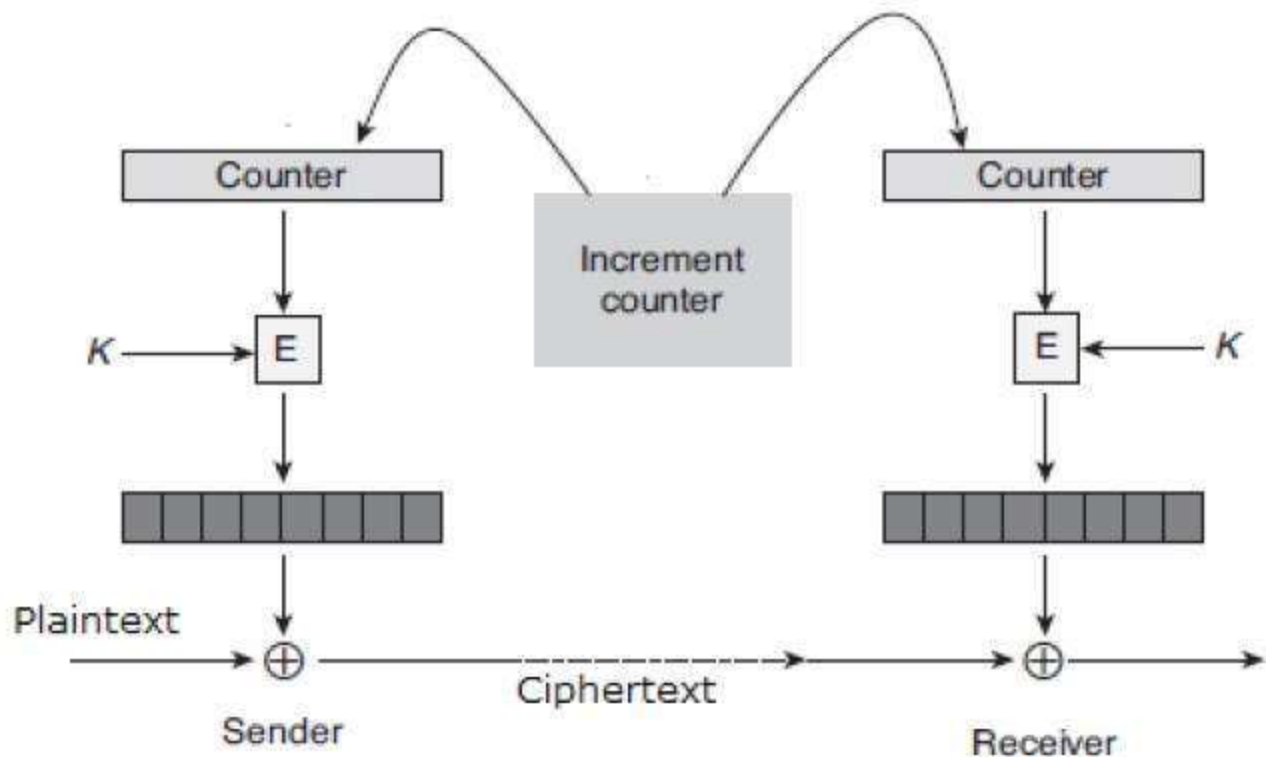
### Counter (CTR) Mode

It can be considered as a counter-based version of CFB mode without the feedback. In this mode, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a ciphertext block is exchanged. This shared counter is not necessarily a secret value, but challenge is that both sides must keep the counter synchronized.

#### Operation

Both encryption and decryption in CTR mode are depicted in the following illustration. Steps in operation are –

- Load the initial counter value in the top register is the same for both the sender and the receiver. It plays the same role as the IV in CFB (and CBC) mode.
- Encrypt the contents of the counter with the key and place the result in the bottom register.
- Take the first plaintext block  $P_1$  and XOR this to the contents of the bottom register. The result of this is  $C_1$ . Send  $C_1$  to the receiver and update the counter. The counter update replaces the ciphertext feedback in CFB mode.
- Continue in this manner until the last plaintext block has been encrypted.
- The decryption is the reverse process. The ciphertext block is XORed with the output of encrypted contents of counter value. After decryption of each ciphertext block counter is updated as in case of encryption.



### Analysis of Counter Mode

It does not have message dependency and hence a ciphertext block does not depend on the previous plaintext blocks.

Like CFB mode, CTR mode does not involve the decryption process of the block cipher. This is because the CTR mode is really using the block cipher to generate a key-stream, which is encrypted using the XOR function. In other words, CTR mode also converts a block cipher to a stream cipher.

The serious disadvantage of CTR mode is that it requires a synchronous counter at sender and receiver. Loss of synchronization leads to incorrect recovery of plaintext.

However, CTR mode has almost all advantages of CFB mode. In addition, it does not propagate error of transmission at all.

Roll No: 09  
Name: Shreya Bagade  
Date: 18/08/2023

### Output Screenshots:

Virtual Labs

cse29-iith.vlabs.ac.in/exp/aes/simulation.html

## AES and Modes of Operation

9e02b6c4 6dad8409 a3dc592c 5f49e9c9  
5ae4a80a 05c15647 f2b7af22 47dab354  
21c25393 4db0a87d 36f79572 f70bc208  
5efe9ed6 dd24c2ed 7c941112 9c521b47  
b1be277f 63340766 2818260b 135894a9

Plaintext:  Next Plaintext Key:  Next Keytext

IV:  Next IV

CTR:  Next CTR

### PART III

Calculate XOR:

Calculate XOR

XOR:

### PART IV

Key in hex:

Plaintext in hex:

Ciphertext in hex:

### PART V

Enter your answer here:

CORRECT!!

Virtual Labs

Virtual Labs

Virtual Labs

Virtual Labs

←

→

↺

[cse29-iith.vlabs.ac.in/exp/aes/simulation.html](https://cse29-iith.vlabs.ac.in/exp/aes/simulation.html)

🔍

🔖


⚙️

🔴

🔵

⋮

☰



Virtual Labs

AES and Modes of Operation

PART I

Choose your mode of operation: Output Feedback

PART II

Key size in bits: 128

efbf09b5 16be4bf5 3f4a32ae 18225641

a28e6b05 f9dd5d0e 2ceb4ac6 42e0bc60

4f4fda79 55b7567c bde310c 3fceeaa7

5b7befac 25904cc9 e8246988 e1c02e51

4f6a92c1 6607fca4 a1682d56 fbf0b537

Next Plaintext

Key: 969827e3 18d136da cce9794a 9fe9911c

Next Keytext

Plaintext: d7d68add bc0a6bad 4b16082b 8a62c28a

Next IV

PART III

Calculate XOR:

4f6a92c1 6607fca4 a1682d56 fbf0b537

1f6b8715 33427730 88c30c37 954c1685

Calculate XOR

XOR: 500115d4 55458b94 29ab2161 6ebca3b2

PART IV

Key in hex: 969827e3 18d136da cce9794a 9fe9911c

Plaintext in hex: 0183e3a3 5b614f98 eac112d1 16dana81

Ciphertext in hex: 1f6b8715 33427730 88c30c37 954c1685

Encrypt

Decrypt

Clear

Virtual Labs Virtual Labs Virtual Labs

cse29-iiith.vlabs.ac.in/exp/aes/simulation.html

### AES and Modes of Operation

Key size in bits: 128

Plaintext: efbfd9b5 10be4bf5 3fa32ae 18225641  
a29eb05 f9d650e 2ceb4ac6 43eb0cb0  
4f4fda79 5b7567c bde510c 3fcedea7  
5b7befac 25904c9 e8246988 e1c02e51  
4f6a92c1 6607fca4 a1682d56 fbf0b537

Next Plaintext Key: 969827e3 18d136da cce9794a 9fe9911c Next Keytext

IV: d7d68add bc0a6bad 4b16082b 8a62c28a Next IV

#### PART III

Calculate XOR:

4f6a92c1 6607fca4 a1682d56 fbf0b537  
1f6b8715 33427730 88c30c37 954c1685 Calculate XOR

XOR: 500115d4 55458b94 29ab2161 6ebca3b2

#### PART IV

Key in hex: 969827e3 18d136da cce9794a 9fe9911c  
Plaintext in hex: 0183e3a3 5b614f9b eac112d1 16daea81  
Ciphertext in hex: 1f6b8715 33427730 88c30c37 954c1685

Encrypt Decrypt Clear

#### PART V

Enter your answer here:

d7d68add bc0a6bad 4b16082b 8a62c28a 74fb98c8 11cd008d cddedba0 a29 Check Answer!

CORRECT!!

Type here to search

14:56 78-08-2023

Virtual Labs Virtual Labs Virtual Labs

cse29-iiith.vlabs.ac.in/exp/aes/simulation.html

### AES and Modes of Operation

Choose your mode of operation: Electronic Code Book (ECB)

#### PART II

Key size in bits: 128

Plaintext: 9e02b6c4 6dad0409 a3dc592c 5f49e0c9  
5ae4a8ba 65c15647 f2b74f22 47dab354  
21e25393 4b0a087d 36f79572 f70e32b8  
5efe9e6d d024c2ed 7c941112 9c521b47  
b1be277f 63340766 2818260b 135894a9

Next Plaintext Key: 9d8c0789 a9a3fede 99b87128 a85c7ee1 Next Keytext

IV: Next IV

CTR: Next CTR

#### PART III

Calculate XOR:

Calculate XOR

XOR:

#### PART IV

Key in hex: 9d8c0789 a9a3fede 99b87128 a85c7ee1  
Plaintext in hex: b1be277f 63340766 2818260b 135894a9  
Ciphertext in hex: 44b4ae8b c72b19ac 9f56206a aa0cbe4d

Encrypt Decrypt Clear

Type here to search

15:01 78-08-2023



Virtual Labs Virtual Labs Virtual Labs

← → ↺ cse29-iiith.vlabs.ac.in/exp/aes/simulation.html

**AES and Modes of Operation**

**PART I**

Choose your mode of operation: [Cipher Block Chaining]

**PART II**

Key size in bits: [128]

Plaintext: [c096db76 bc084d51 a0dc9fe9 b3c2f4b8  
5eed2064 08029863 59b71c0c b06e91c1  
66e3a8fd 4a183dc8 d2b75f18 dc305e0f  
8c03d450 12880f54 03469256 ab884d88  
67c2648a e98d960b 7e0110ac e8e31045]

Next Plaintext Key: [9c9fe223 03d2f6e2 88c441e5 0b58ed7d] Next Keytext

IV: [e747d10b c355ccff c80ae504 06a3e645] Next IV

**PART III**

Calculate XOR:

[67c2648a e98d960b 7e0110ac e8e31045]

[728527d5 c5d3ef1e 14561029 310f1652] Calculate XOR

XOR: [1547435f 2c5e7915 6a570085 d9ec0617]

**PART IV**

Key in hex: [9c9fe223 03d2f6e2 88c441e5 0b58ed7d]

Plaintext in hex: [1547435f 2c5e7915 6a570085 d9ec0617]

Ciphertext in hex: [85c0eed1 06502ed7 7b1e1877 9c441b3c]

Encrypt Decrypt Clear

Virtual Labs Virtual Labs Virtual Labs

← → ↺ cse29-iiith.vlabs.ac.in/exp/aes/simulation.html

**AES and Modes of Operation**

Key size in bits: [128]

Plaintext: [c096db76 bc084d51 a0dc9fe9 b3c2f4b8  
5eed2064 08029863 59b71c0c b06e91c1  
66e3a8fd 4a183dc8 d2b75f18 dc305e0f  
8c03d450 12880f54 03469256 ab884d88  
67c2648a e98d960b 7e0110ac e8e31045]

Next Plaintext Key: [9c9fe223 03d2f6e2 88c441e5 0b58ed7d] Next Keytext

IV: [e747d10b c355ccff c80ae504 06a3e645] Next IV

**PART III**

Calculate XOR:

[67c2648a e98d960b 7e0110ac e8e31045]

[728527d5 c5d3ef1e 14561029 310f1652] Calculate XOR

XOR: [1547435f 2c5e7915 6a570085 d9ec0617]

**PART IV**

Key in hex: [9c9fe223 03d2f6e2 88c441e5 0b58ed7d]

Plaintext in hex: [1547435f 2c5e7915 6a570085 d9ec0617]

Ciphertext in hex: [85c0eed1 06502ed7 7b1e1877 9c441b3c]

Encrypt Decrypt Clear

**PART V**

Enter your answer here:

[e747d10b c355ccff c80ae504 06a3e645 1e3ad250 9e5d7584 99966612 5927] Check Answer!

CORRECT!!

The screenshot shows the Virtual Labs AES simulation interface. A 'Page Unresponsive' error message is displayed in the top right corner, stating 'You can wait for it to become responsive or exit the page.' The interface includes a key size selector set to 128 bits, a plaintext input field containing a 16-byte hex string, and a CTR input field. Below these, there are sections for 'PART III' (Calculate XOR) and 'PART IV' (Key in hex, Plaintext in hex, Ciphertext in hex). The bottom section is 'PART V' (Enter your answer here).

The screenshot shows the Virtual Labs AES simulation interface with the title 'AES and Modes of Operation'. The key size is set to 128 bits. The plaintext input field contains a 16-byte hex string. The CTR input field is set to 'f24d9cb5 e987b0d9 56d7d23e d043426e'. The key input field is set to '2967c5fd 926fa06d 9c87ab27 8890f660'. Below these, there are sections for 'PART III' (Calculate XOR) and 'PART IV' (Key in hex, Plaintext in hex, Ciphertext in hex). The bottom section is 'PART V' (Enter your answer here).

**Conclusion:** This experiment focused on the study of the Advanced Encryption Standard (AES) algorithm and its application in Cipher Block Chaining (CBC) mode has provided valuable insights into modern symmetric encryption techniques. Through this experiment, we gained a deeper understanding of how AES operates and how different modes of operation, such as CBC, contribute to enhancing security and confidentiality.