

## Experiment 05

To understand how to Encrypt long messages using various modes of operation using AES

Roll No.	14
Name	Ishika Sanjay Devare
Class	D15-A
Subject	Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

**Aim:** To Encrypt long messages using various modes of operation using AES.

### **Introduction:**

AES stands for Advanced Encryption Standard and is a symmetric encryption algorithm. It is mainly used for encryption and protection of electronic data. It was used as the replacement of DES(Data Encryption Standard) as it is much faster and better than DES. AES consists of three block ciphers that are used to provide encryption of data.

### **History:**

AES was developed by NIST(National Institute of Standard and Technology) in 1997. It was developed to replace DES which was slow and vulnerable to various attacks. So, therefore a new encryption algorithm was made to overcome the shortcomings of DES. AES was published on 26th November 2001.

### **Characteristics:**

- AES has keys of three lengths which are 128, 192, 256 bits.
- It is flexible and has implementations for software and hardware.
- It provides high security and can prevent many attacks.
- It doesn't have any copyright so it can be easily used globally
- It consists of 10 rounds of processing for 128-bit keys.

### **Advantages:**

It can be implemented on both hardware and software.

It provides high security to the users.

It provides one of the best open source solutions for encryption.

It is a very robust algorithm.

### **Disadvantages:**

It requires many rounds for encryption.

It is hard to implement on software.

It needs much processing at different stages.

It is difficult to implement when performance has to be considered.

### **Block Cipher modes of Operation:**

Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher. Block Cipher algorithm is an encryption algorithm which takes fixed size of input i.e b bits and produces a ciphertext of b bits again. If input is larger than b bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

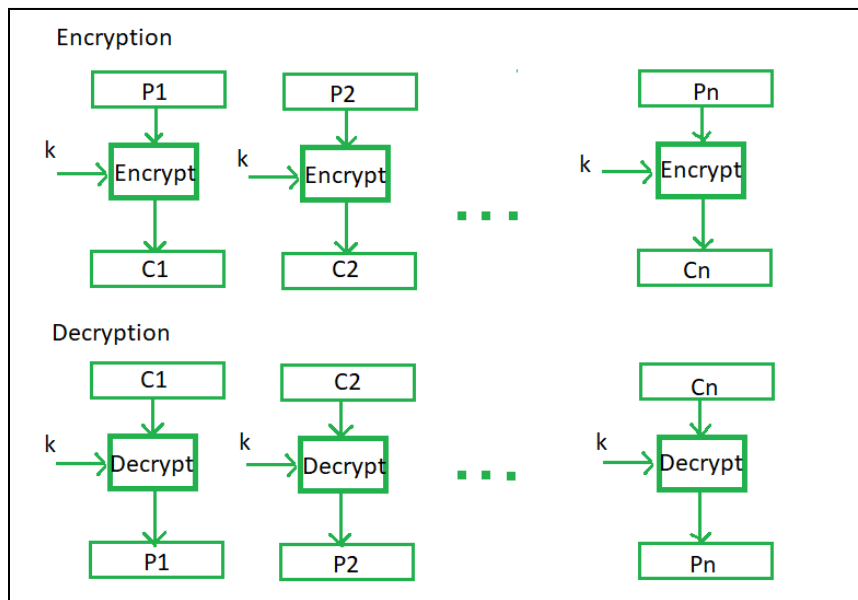
## Methods are:

Different methods of Block Cipher mode of Operation are:

### 1. Electronic Code Book (ECB)-

Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in the form of blocks of encrypted ciphertext. Generally, if a message is larger than  $b$  bits in size, it can be broken down into a bunch of blocks and the procedure is repeated.

Procedure of ECB is illustrated as-



### Advantages:

1. Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
2. Simple way of block cipher.

### Disadvantages:

1. Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

### Applications:

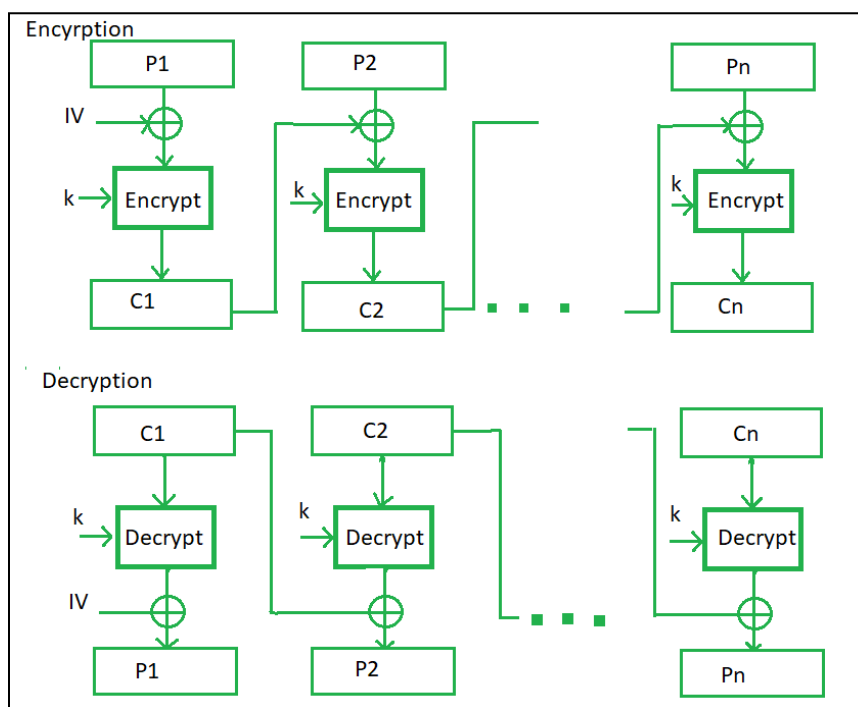
1. If a message is short enough to fit in one block, security issues and error propagation are tolerable.
2. It is useful where records need to be encrypted before they are stored in a database.

3. ECB allows parallel processing, if we want to create a very huge encrypted database.

## 2. Cipher Block Chaining (CBC)-

Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block. In a nutshell here, a cipher block is produced by encrypting an XOR output of the previous cipher block and present plaintext block.

Procedure of CBC is illustrated as-



### Advantages:

1. Cipher Block Chaining works well for input greater than  $b$  bits.
2. CBC is a good authentication mechanism.
3. Better resistive nature towards cryptanalysis than ECB.

### Disadvantages:

1. Parallel encryption is not possible as every encryption requires a previous cipher.

### Application:

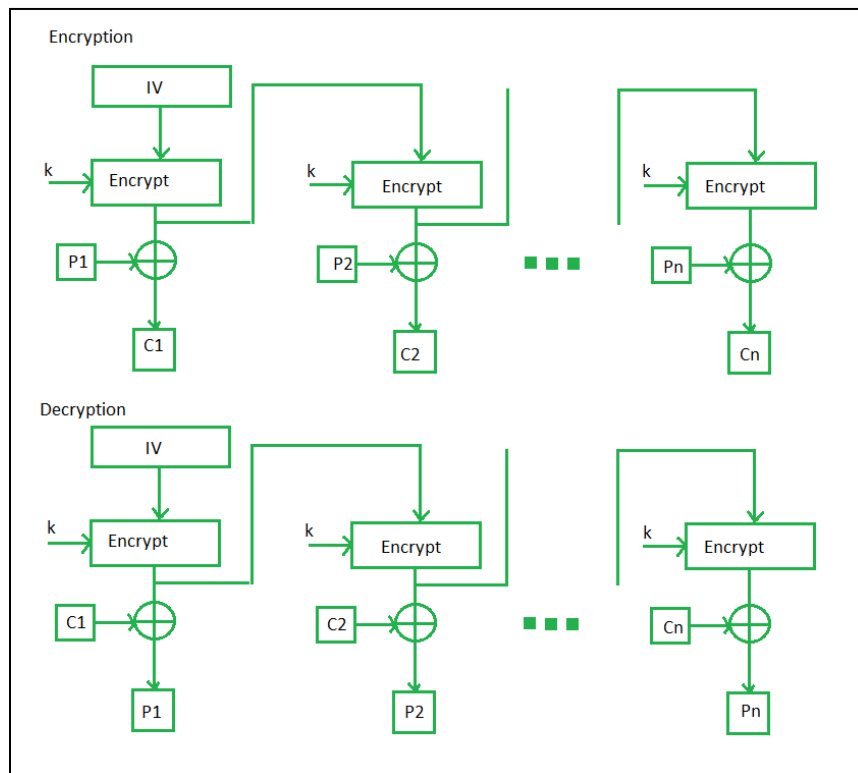
1. It is not used when we need parallel processing because it uses a chaining mechanism.

2. It is not used to encrypt and decrypt random-access files because encipherment here requires access to previous records.
3. It is used for authentication purposes.

### 3. Output Feedback Mode:

The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are sent instead of sending selected  $s$  bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.

Procedure of OFB is illustrated as-



#### Advantages:

In the case of CFB, a single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit errors in the plaintext block.

#### Disadvantages:

OFB is more vulnerable to a message stream modification attack than is CFB in the modes of operation.

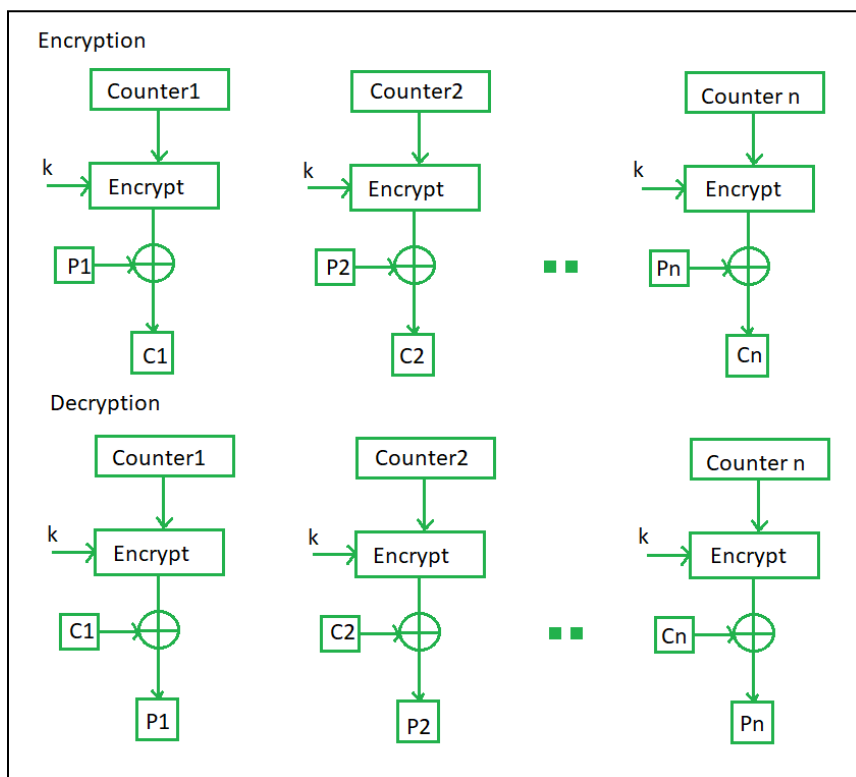
### Applications:

Can be used to encipher blocks of small size such as one character or bit at a time. No need for padding because the size of the plaintext block is normally fixed.

### 4. Counter Mode:

The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in a ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

Procedure of Counter Mode is illustrated as-



### Advantages:

1. Since there is a different counter value for each block, the direct plaintext and ciphertext relationship is avoided. This means that the same plaintext can map to different ciphertext.
2. Parallel execution of encryption is possible as outputs from previous stages are not chained as in case of CBC.

## Disadvantages:


1. It requires a synchronous counter at the sender and receiver in this mode. Decreases of synchronization lead to incorrect recovery of plaintext or original text.

## What is Vlab?

It provides remote-access to simulation-based Labs in various disciplines of Science and Engineering.

## Results:

### 1. Electronic Code Book (ECB)

AES and Modes of Operation

---

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

---

**PART II**  
Key size in bits: 128  

ec666cf5 3b01b352 fda0f0df 11a7007f  
9a47434f b12d2194 e21e7fc5 530357fe  
0b364926 9c986357 2befb269 996a1c34  
a79bdf1e 31399157 2a4df869 cbbd823c  
cf5cdc7d 5aba0ea1 a7fde3c1 127a98ec

Next Plaintext

Key: 12fb881c ee6efdde b1a1c351 3caf3620

Next Keytext

IV: 

Next IV

CTR: 

Next CTR

---

**PART III**  
Calculate XOR:  

Calculate XOR

XOR:

---

**PART IV**  
Key in hex: 12fb881c ee6efdde b1a1c351 3caf3620  
Plaintext in hex: a79bdf1e 31399157 2a4df869 cbbd823c  
Ciphertext in hex: 1fd71f3d b29a1e7b ab5149e8 55304d43  

Encrypt Decrypt Clear

---

**PART V**  
Enter your answer here:  

1223515d 37806f6b 58b69544 b98f7695 816ec71f b234bdda 541c9fb1 e547fde0 Check Answer!

## 2. Cipher Block Chaining

Virtual Labs

AES and Modes of Operation

**PART I**  
Choose your mode of operation: Cipher Block Chaining

**PART II**  
Key size in bits: 128  

075ac13d f43876f4 bd57661e 1196fbd7  
d9a5f85f ec87cad0 70d4377e f68e3e12  
0026dbbd b7f95a9e 75944704 269877aa  
705b0bdc 79102b82 d72345e0 7defa9e2  
555d7500 87cee18d 17b585c1 416bc7f9

Plaintext:  Next Plaintext Key: 70e2c265 ae782eda 587dab11 df33fbfb Next Keytext

IV: aedfdad7 48a6d181 da942d08 9ea110a2 Next IV

**PART III**  
Calculate XOR:  

0db5ca80 602646ef 4bc7096e 7134d127  
555d7500 87cee18d 17b585c1 416bc7f9 Calculate XOR

XOR: 58e8bf80 e7e8a762 5c728caf 305f16de

**PART IV**  
Key in hex: 70e2c265 ae782eda 587dab11 df33fbfb  
Plaintext in hex: 58e8bf80 e7e8a762 5c728caf 305f16de  
Ciphertext in hex: bd3ac87d 1c846e55 d0008081 ab6f5f19  
Encrypt Decrypt Clear

**PART V**  
Enter your answer here:  
aedfdad7 48a6d181 da942d08 9ea110a2 cfb84c3b 6166c8a6 77d2b36e 4a2494a Check Answer!

## 3. Output Feedback

Virtual Labs

AES and Modes of Operation

**PART I**  
Choose your mode of operation: Output Feedback

**PART II**  
Key size in bits: 128  

c120f21c d51c52d3 9ffac799 38ada0d7  
b14e4d10 b88eb319 e04c8086 e87ee163  
d2493543 c4cf61f9 fdbb71c0 1b019a1b  
d083a0ef 6a9f7b46 2d0e0180 88c02d0a  
af370a3a d2c08758 10a9c7a8 d0f22cb1

Plaintext:  Next Plaintext Key: 16e1ce42 9c4b68f0 7f208570 905fd590 Next Keytext

IV: d6d771c7 959e8d77 2fd29f31 eb63a152 Next IV

**PART III**  
Calculate XOR:  

3419d27e 503ac73b 821dcfda cff9809d  
af370a3a d2c08758 10a9c7a8 d0f22cb1 Calculate XOR

XOR: 9b2ed844 82fa4863 92b40872 1f9bac2c

**PART IV**  
Key in hex: 16e1ce42 9c4b68f0 7f208570 905fd590  
Plaintext in hex: 9b2ed844 82fa4063 92b40872 1f9bac2c  
Ciphertext in hex: 80e4a505 f6b7f0 4e0100e1 70f4050d  
Encrypt Decrypt Clear

**PART V**  
Enter your answer here:  
d6d771c7 959e8d77 2fd29f31 eb63a152 50143923 75044010 6d87addb 600d Check Answer!





## 4. Counter Mode

The screenshot displays a web application titled "AES and Modes of Operation" with a navigation menu on the left. The interface is divided into five parts:

- PART I:** A dropdown menu labeled "Choose your mode of operation:" is set to "Counter mode".
- PART II:** A section for key and plaintext input. It includes a "key size in bits:" dropdown set to "128". A large text area contains a list of hexadecimal values. Below this, there are input fields for "Plaintext:", "CTR:", "Next Plaintext", "Key:", "Next Keytext", and "Next CTR".
- PART III:** A section for calculating XOR. It includes input fields for "Calculate XOR:", "XOR:", and a "Calculate XOR" button.
- PART IV:** A section for encryption/decryption. It includes input fields for "Key in hex:", "Plaintext in hex:", and "Ciphertext in hex:". Below these are buttons for "Encrypt", "Decrypt", and "Clear".
- PART V:** A section for entering the answer. It includes a text input field and a "Check Answer!" button.

The bottom of the application shows a Windows taskbar with various icons and a system tray displaying "ENG US", "10:04 AM", and "8/22/2022".

**Conclusion:** Hence, we successfully understood how to Encrypt long messages using various modes of operation using AES.