Semester : VI Subject : CSS Academic Year: 2023-2024

## BLOCK CIPHER MODES OF OPERATION :-

There are 5 types of operations in block cipher modes:

* Electronic Code Book (ECB)
* Cipher Block Chaining (CBC)
* Cipher Feedback Mode (CFB).
* Output Feedback (OFB) Mode
* Counter Mode (CTR)

### (1) Electronic Code Book Mode:

→ It is the simplest mode of operation of block cipher:

→ The plain text is divided into blocks of 64bits each.

→ Each block is separately encrypted and decrypted

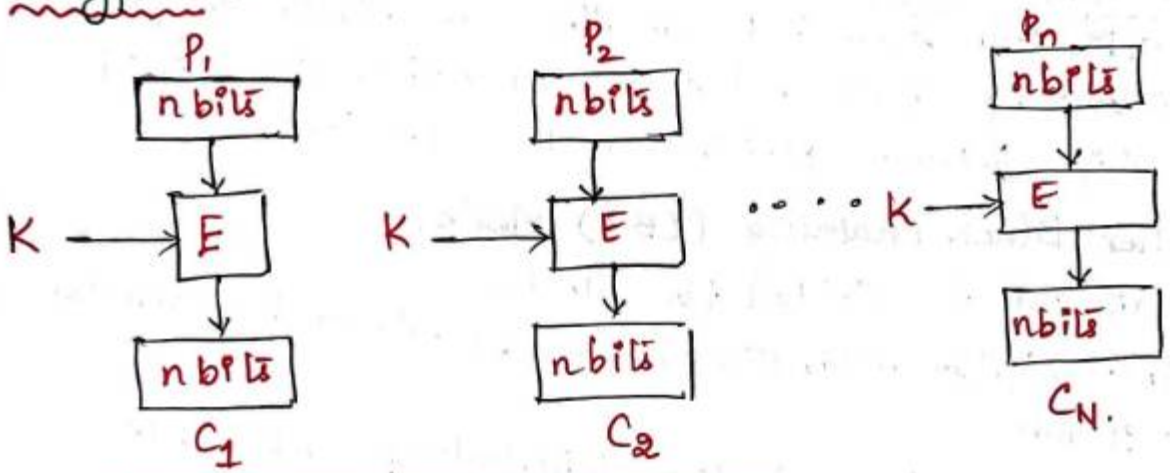
→ Each block is encrypted using the same key and makes the block of ciphertext

→ The ECB mode is deterministic, if the block of plain text is repeated in the original message, then its corresponding Cipher Text will also be repeated.

E → Encryption.
D → Decryption
$P_i$ → Plaintext block i
$C_i$ → Cipher Text block i
K → secret key.

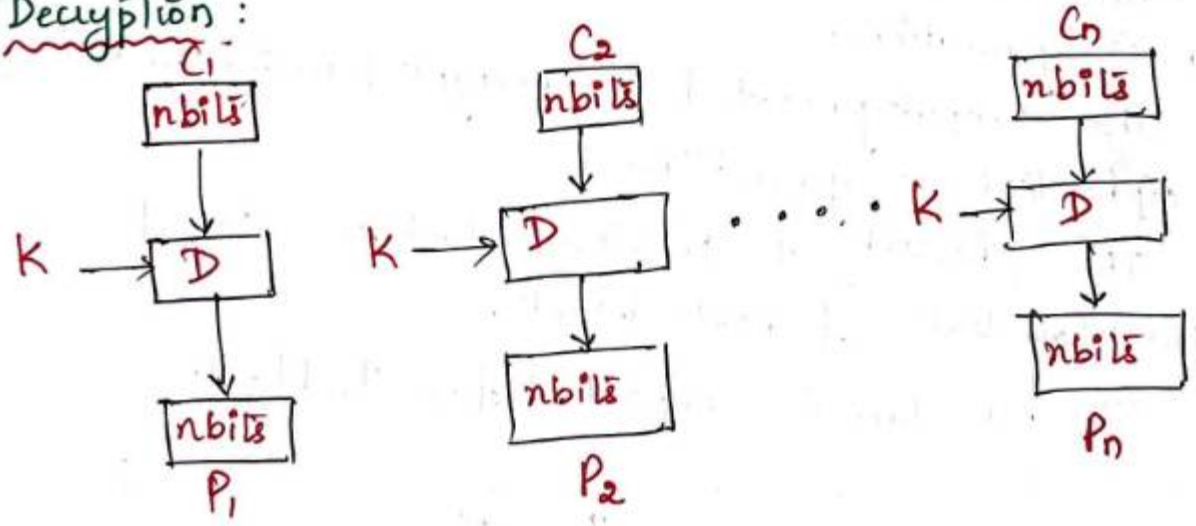
Semester: VI Subject: CSS Academic Year: 2023-2024

## Encryption :-




Encryption : $C_i = E_k(P_i)$
Decryption : $P_i = D_k(C_i)$
← Rules for encryption & Decryption.

## Decryption :




## Advantages of ECB:

* Simplest way of block ciphers.
* Faster ways of encryption as parallel encryption of blocks of bits are possible.

Semester: VI Subject: CSS Academic Year: 2023-2024

## Disadvantages of ECB:

* A cipher text from ECB can allow an attacker to guess the plaintext by trial-and-error since there is a direct relationship between plaintext and cipher text.

## (2) Cipher Block Chaining (CBC) Mode:

→ Plain text is divided into blocks.
→ Initialization Vector (IV) is used, which can be a random block of text.
→ IV is used to make the ciphertext of each block unique since the key used is same for encryption as we use for ECB.
→ Plain Text is XORed with IV and the resultant output is generation.
→ The output generated is encypted using the K and cipher text is generation.
→ The ciphertext of previous block is XORed with the plain text of next block.
→ The procedure is repeated for $P_n$ blocks.

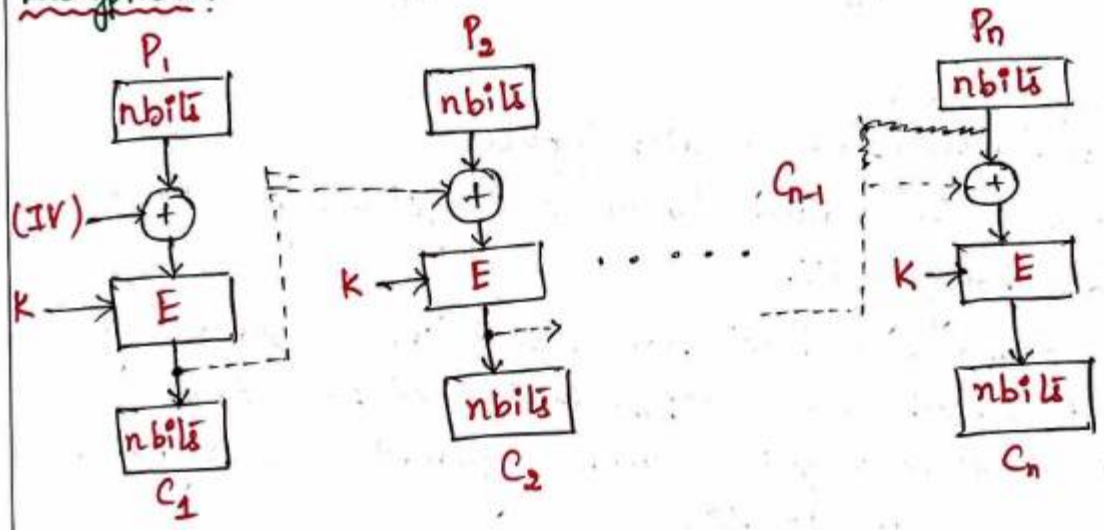
| Encryption | Decryption. |
|---|---|
| $C_0 = IV$ | $C_0 = IV$ |
| $C_i = E_k(P_i \oplus C_{i-1})$ | $P_i = D_k(C_i) \oplus C_{i-1}$ |
| $i = 0, 1, 2 \ldots n.$ | |

Semester: VI Subject: CSS Academic Year: 2023-2024

CBC is non-deterministic since even if the block of plain text is repeated in the original message, it will produce a different ciphertext for corresponding blocks.

E: Encryption
$P_i$: Plain Text block i
K: Secret Key.
D: Decryption.
$C_i$: Ciphertext block i
IV: Initial Vector ($C_0$).

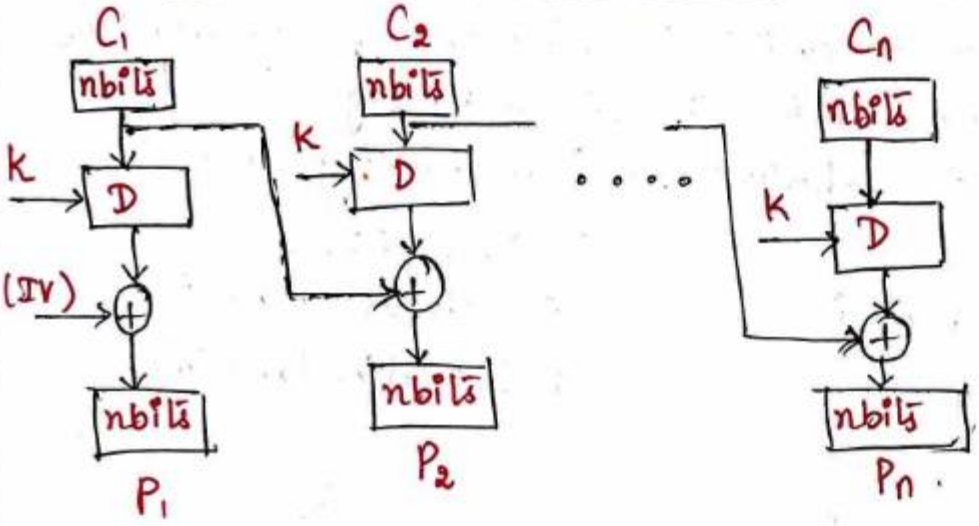
Encryption:-




Decryption:

→ Receiver side, the cipher text is divided into blocks.
→ The same key is used for decryption.
→ The resultant output is XORed with IV to get the plain text of first block.
→ The second block is also decrypted.
→ The decrypted output is XORed with the previous block Cipher text and the plain text is generated.

Semester : VI Subject : CSS Academic Year: 2023-2024




## Advantages of CBC.

* CBC works well for greater input.
* Better resistive nature towards cryptanalysis than ECB due to changing IV.
* CBC forms the basis for a well known data origin authentication mechanisms. Thus it is used for those applications that require both symmetric encryption and data origin authentication.

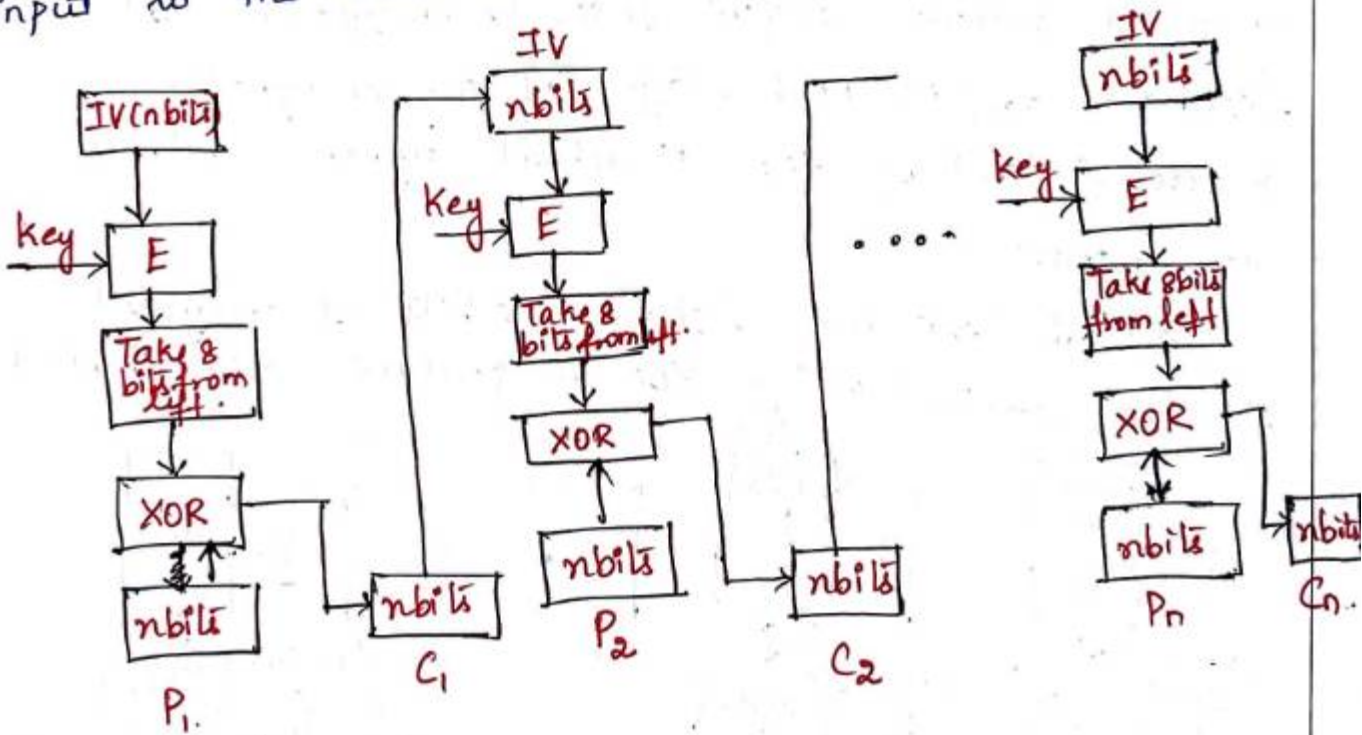
## Disadvantages of CBC:-

* Parallel encryption is not possible.
* Error in transmission gets propagated to few further blocks during decryption due to chaining effect.

Semester: VI Subject: CSS Academic Year: 2023-2024.

## (3) CIPHER FEEDBACK MODE:

→ An initialization vector (IV) is initialized.
→ It is encrypted using the key and forms the ciphertext.
→ The 8 bits from the left of output bits are are selected and are applied in XOR operation with plain text.
→ The resultant output is the cipher Text.
→ The cipher text of previous block is given as input to the next block.




### Advantages of CFB:

* It is difficult for applying cryptanalysis since there is some data loss due to use of shift register.
* It provides some of the advantageous properties of

of a stream cipher while retaining the advantageous properties of a block cipher too.

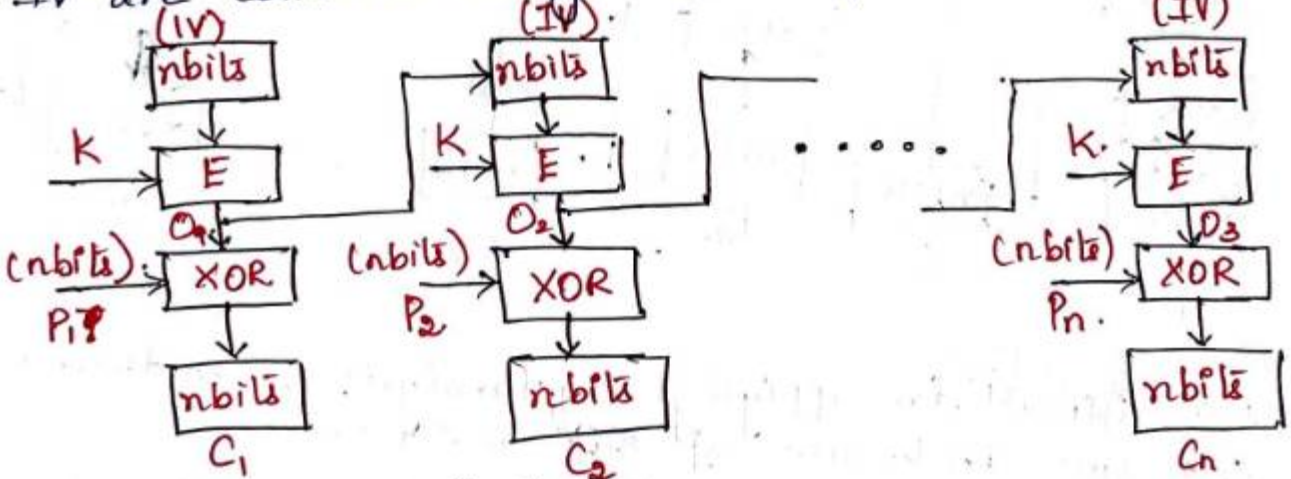
**Disadvantage of CFB:**

* The error of transmission gets propagated due to changing of blocks.

**Output Feedback Mode:**

* The OFB mode follows nearly same process as the Cipher Feedback mode except that it sends the encrypted output (output of the IV encryption) as feedback for the next stage of the encryption process instead of the 'actual cipher which is XOR output.

* Plain Text and leftmost 8 bits of encrypted IV are combined using XOR to produce the ciphertext.




E: Encryption C: Ciphes Text
O: Output K: Key:

Semester: VI Subject: CSS Academic Year: 2023-2024.

**Advantages of OFB:-**

*Hold great resistance towards bit-transmission errors.

*It decreases the dependency of cipher on plaintext.

**Disadvantages of OFB:-**

*Repeatedy encrypting the initialization vector may produce the same state that has occured before.

**COUNTER (CTR) Mode:**

**Encryption:**

→ The CTR is a simple counter based block cipher implementation. It uses the sequence of numbers as an input for the algorithm.

→ Every time a counter initiated value is encrypted and given as input to XOR with plaintext which results in Cipher Text.

→ When the block is encrypted, to fill the next register next counter value is used.

→ Everytime the counter value is incremented by 1 for next stage.

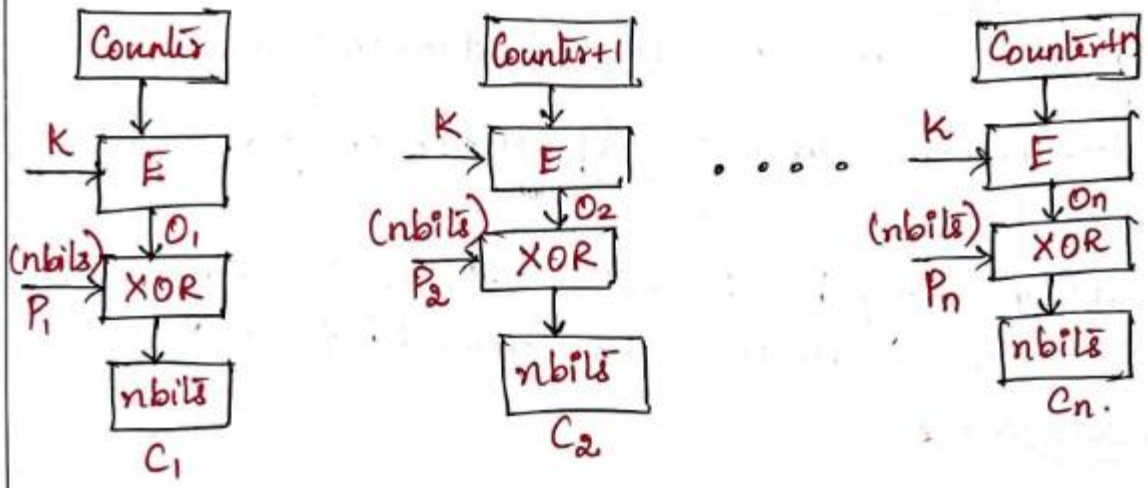
→ This process is continued until the last plaintext block has been encrypted.

E: Encryption K: Key.

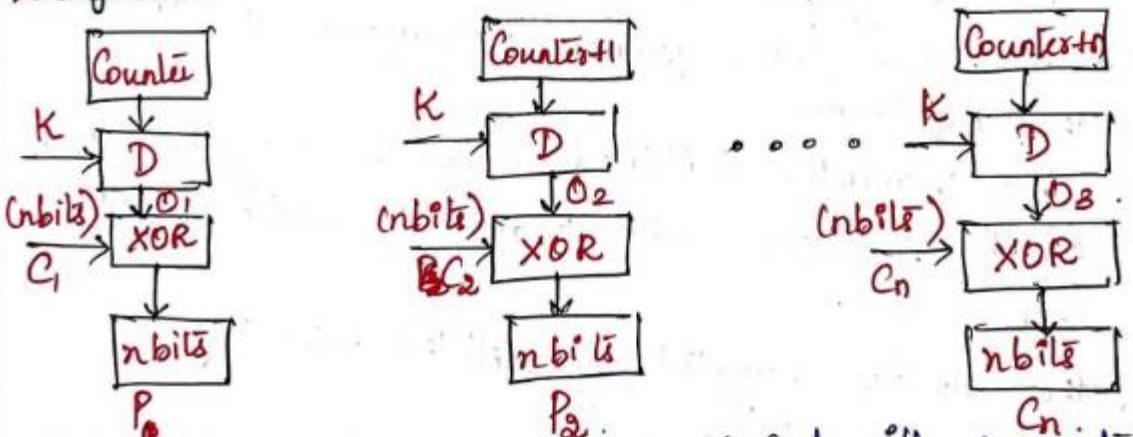
D: Decryption O: Output

Counter is incremented for each block.

Semester : IV Subject : CSS Academic Year: 2023-2024




Decryption :




→ For decryption the Ciphertext is XORed with the output of encrypted contents of counter value.
→ Sender and Receiver need to access to a reliable counter.

Advantages :
* It does not have message dependancy.
* Parallel encryption is possible.

Disadvantages :
* It requires synchronous counter at sender and receiver.
* Loss of synchronization leads to incorrect recovery of plaintext.