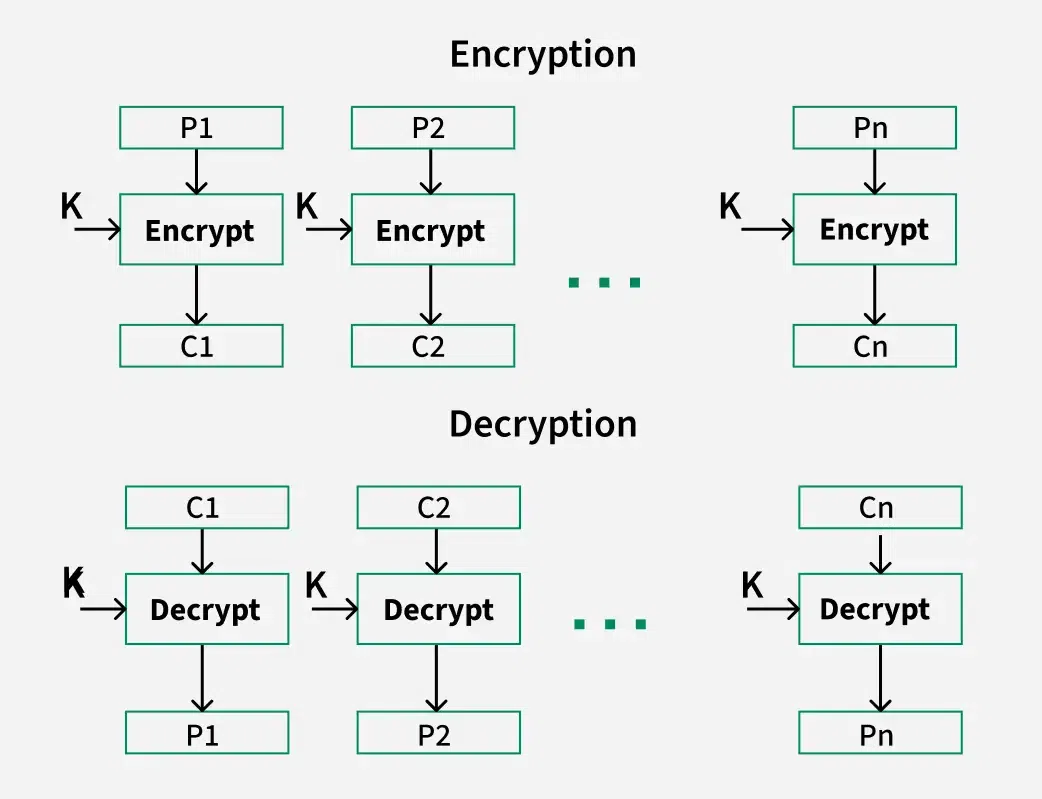
## ****What are Block Cipher Modes of Operation?****

Block Cipher Modes of Operation define how to securely encrypt and decrypt large amounts of data using a block cipher. A block cipher is an encryption algorithm that processes data in fixed-size blocks (e.g., 128 bits) rather than one bit at a time. However, to encrypt data larger than a single block, different modes of operation are used to ensure both security and efficiency. Here are a few common modes. **Here are a few common modes:**

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

The electronic codebook is the easiest block cipher mode of functioning. It is easier because of the 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.  
  
**The procedure of ECB is illustrated below:**

Electronic Code Book

### ****Advantages of using ECB****

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

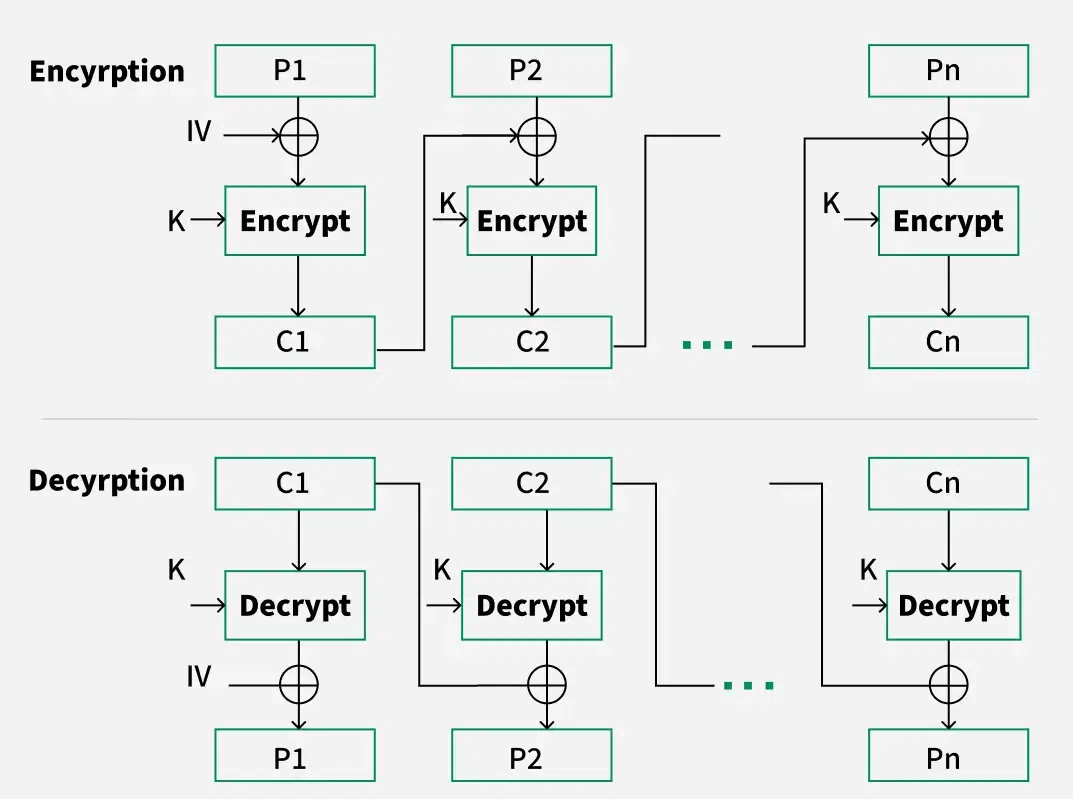
### ****Disadvantages of using ECB****

* Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.
* Identical plaintext blocks produce identical ciphertext blocks, which can reveal patterns.

## ****Cipher Block Chaining****

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.

**The process is illustrated here:**

Cipher Block Chaining

### ****Advantages of CBC****

* CBC works well for input greater than *b* bits.
* CBC is a good authentication mechanism.
* Better resistive nature towards cryptanalysis than ECB.
* More secure than ECB as it hides patterns.

### ****Disadvantages of CBC****

* Requires the previous ciphertext block for [encryption and decryption](https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/" \t "https://www.geeksforgeeks.org/ethical-hacking/block-cipher-modes-of-operation/_blank), making parallel processing difficult.