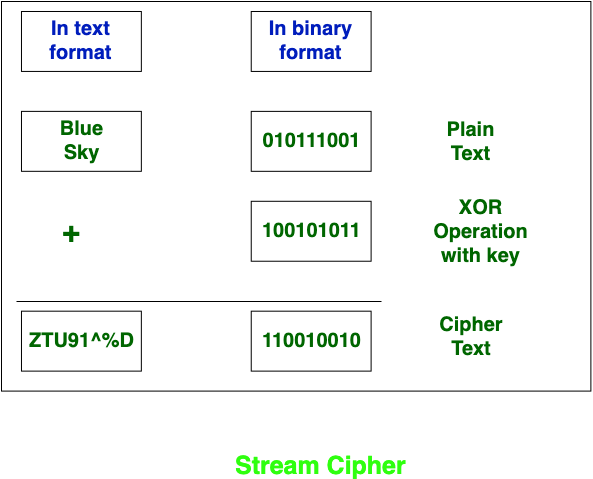
**Block Cipher** and **Stream Cipher** belongs to the symmetric key cipher. These two block ciphers and stream cipher are the methods used for converting the plain text into ciphertext.

The main difference between a **Block cipher** and a **Stream cipher** is that a block cipher converts the plain text into cipher text by taking plain text’s block at a time. While stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.

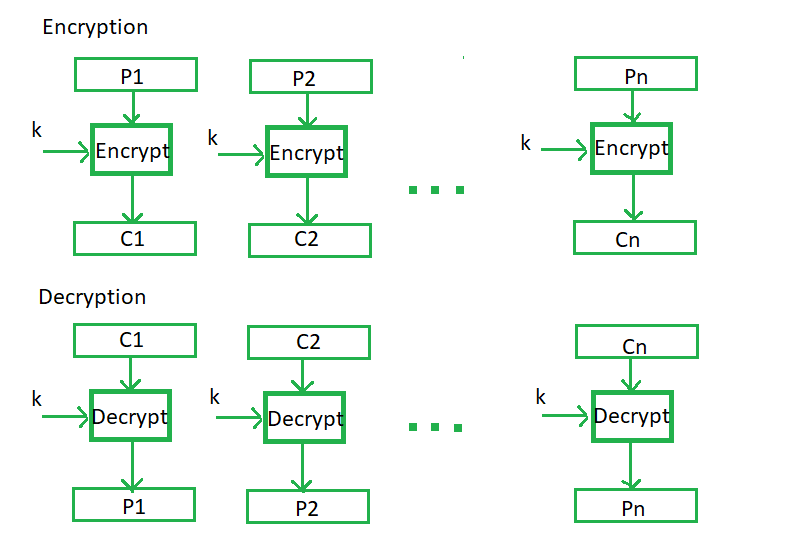


* Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
* Block Cipher Converts the plain text into cipher text by taking plain text’s block at a time.
* While stream cipher uses 8 bits.
* Block cipher uses either 64 bits or more than 64 bits.
* The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (Output Feedback).
* The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).
* While stream cipher is fast in comparison to block cipher.

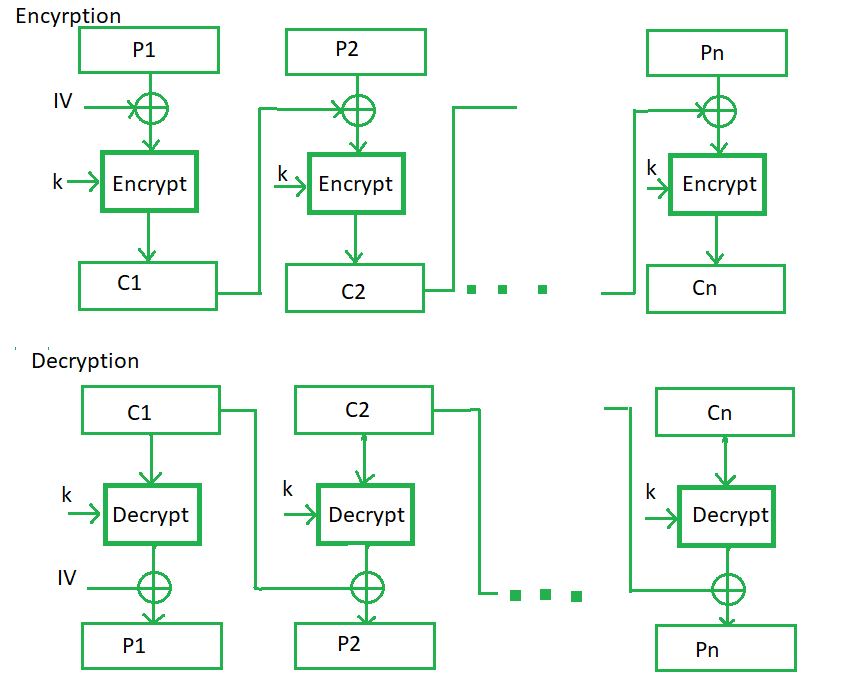
Block cipher is slow as compared to a stream cipher.

**Block Cipher modes of Operation**

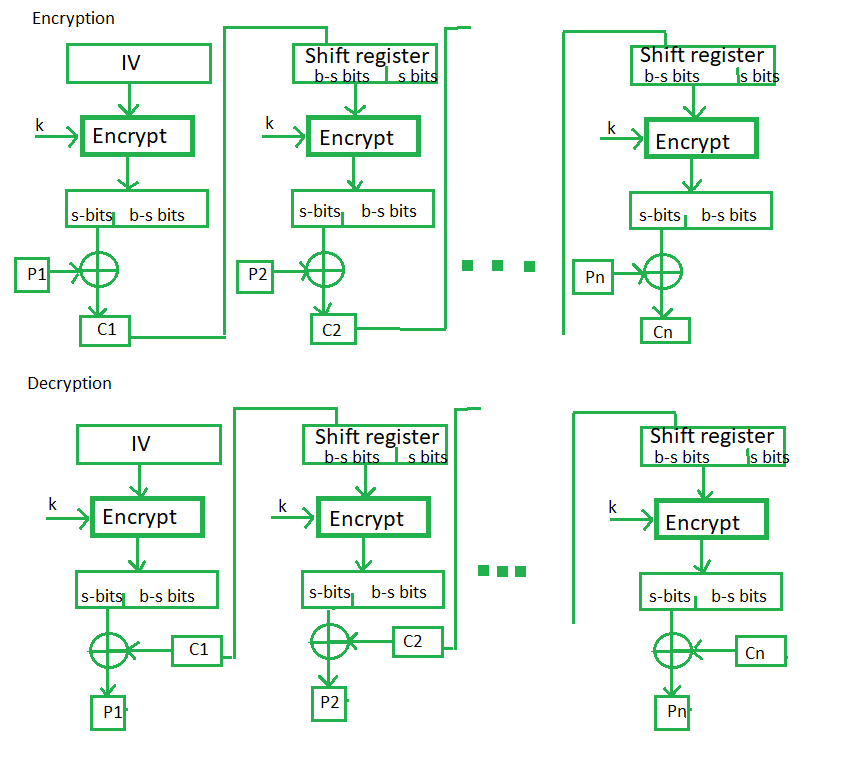
**Electronic Code Book (ECB) –**   
Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted cipher text. The term codebook is used because, for a given key, there is a unique ciphertext for every b-bit block of plaintext. Therefore, we can imagine a gigantic codebook in which there is an entry for every possible b-bit plaintext pattern showing its corresponding ciphertext.



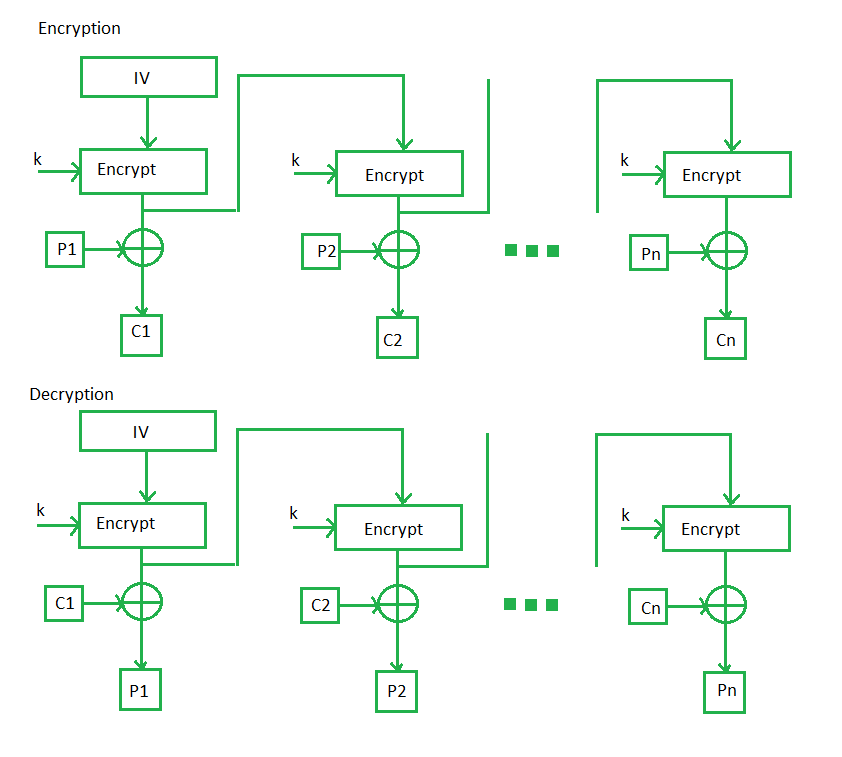
**Cipher Block Chaining –**   
Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block. In a nutshell here, a cipher block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



**Cipher Feedback Mode (CFB) –**   
In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used for first encryption and output bits are divided as a set of *s*and*b-s* bits the left-hand side *s*bits are selected and are applied an XOR operation with plaintext bits. The result is given as input to a shift register and the process continues. The encryption and decryption process for the same is shown below, both of them use encryption algorithms.



**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.



**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 cipher text block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

