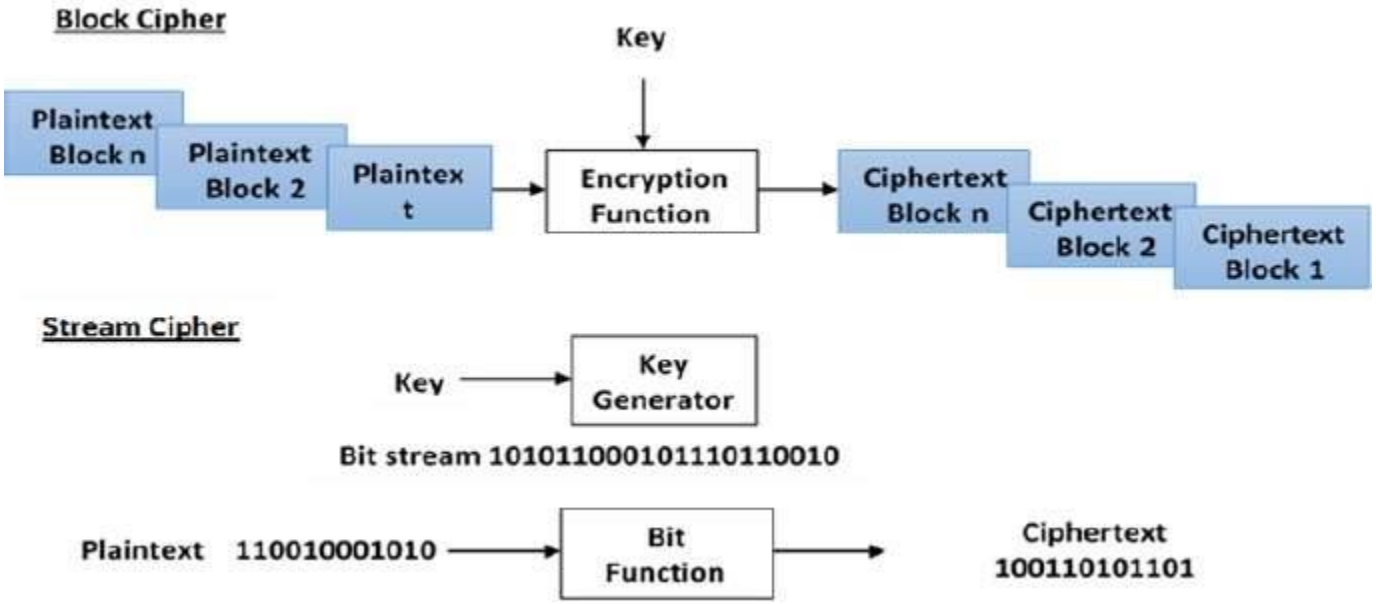
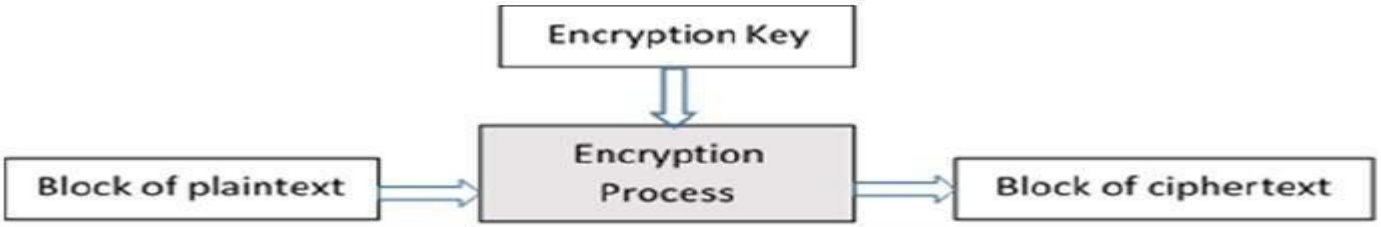
Modern Symmetric Key Encryption

- Digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process this binary strings to convert in to another binary string. Based on how these binary strings are processed, a symmetric encryption schemes can be classified in to −
- Block Ciphers
- In this scheme, the plain binary text is processed in blocks (groups) of bits at a time; i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits. The number of bits in a block is fixed. For example, the schemes DES and AES have block sizes of 64 and 128, respectively.
- Stream Ciphers
- In this scheme, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of ciphertext. Technically, stream ciphers are block ciphers with a block size of one bit.


Block Cipher
Key
Plaintext Block n
Plaintext Block 2
Plaintex t
Encryption Function
Ciphertext Block n
Ciphertext Block 2
Ciphertext Block 1
Stream Cipher
Key
Key Generator
Bit stream 101011000101110110010
Plaintext 110010001010
Bit Function
Ciphertext 100110101101

- The basic scheme of a block cipher is depicted as follows −



A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size. The size of block is fixed in the given scheme. The choice of block size does not directly affect to the strength of encryption scheme. The strength of cipher depends up on the key length.

Block Cipher modes of Operation

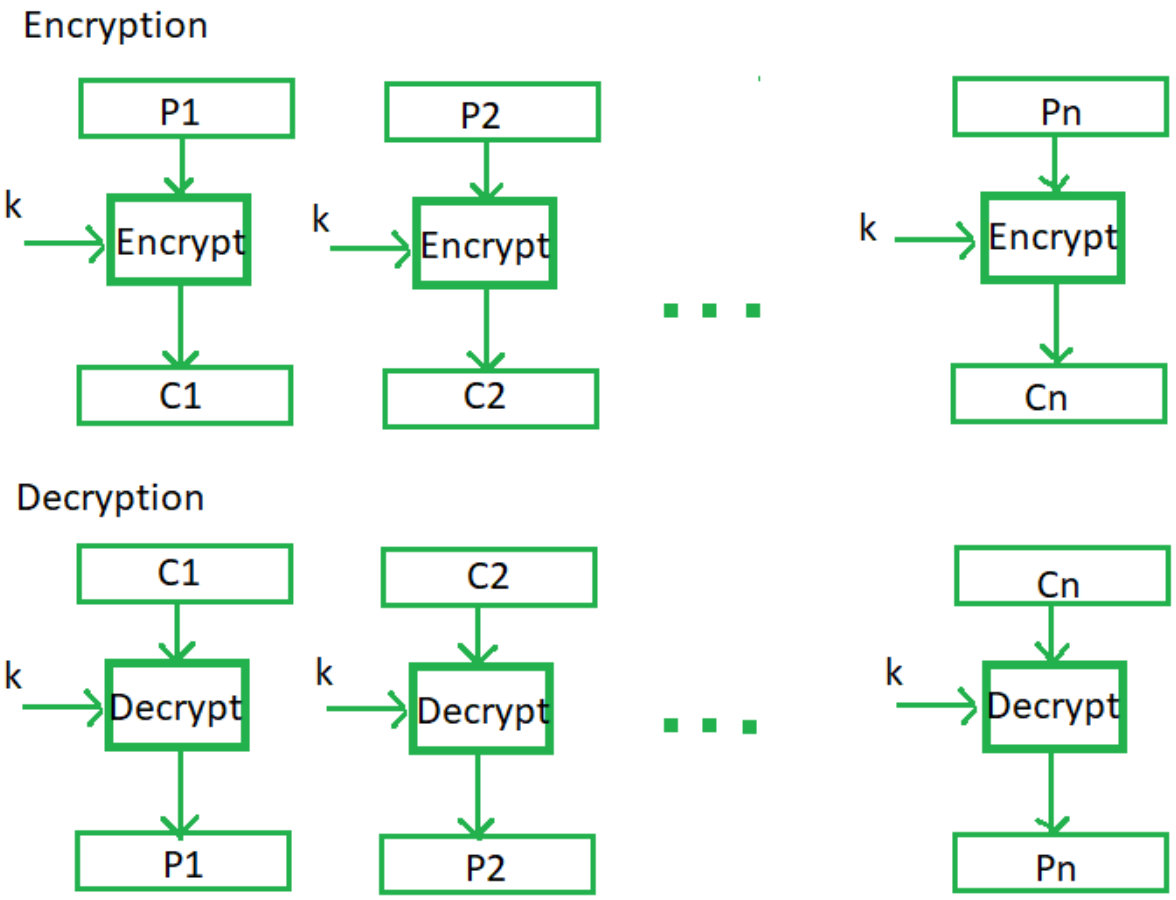
- **Block cipher** is an encryption algorithm which takes fixed size of input say *b* bits and produces a ciphertext of *b* bits again. If input is larger than *b* bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

- Block Size
- Though any size of block is acceptable, following aspects are borne in mind while selecting a size of a block.
- **Avoid very small block size** − Say a block size is m bits. Then the possible plaintext bits combinations are then 2^m. If the attacker discovers the plain text blocks corresponding to some previously sent ciphertext blocks, then the attacker can launch a type of 'dictionary attack' by building up a dictionary of plaintext/ciphertext pairs sent using that encryption key. A larger block size makes attack harder as the dictionary needs to be larger.
- **Do not have very large block size** − With very large block size, the cipher becomes inefficient to operate. Such plaintexts will need to be padded before being encrypted.
- **Multiples of 8 bit** − A preferred block size is a multiple of 8 as it is easy for implementation as most computer processor handle data in multiple of 8 bits.

- Padding in Block Cipher
- Block ciphers process blocks of fixed sizes (say 64 bits). The length of plaintexts is mostly not a multiple of the block size. For example, a 150-bit plaintext provides two blocks of 64 bits each with third block of balance 22 bits. The last block of bits needs to be padded up with redundant information so that the length of the final block equal to block size of the scheme. In our example, the remaining 22 bits need to have additional 42 redundant bits added to provide a complete block. The process of adding bits to the last block is referred to as **padding**.
- Too much padding makes the system inefficient. Also, padding may render the system insecure at times, if the padding is done with same bits always.

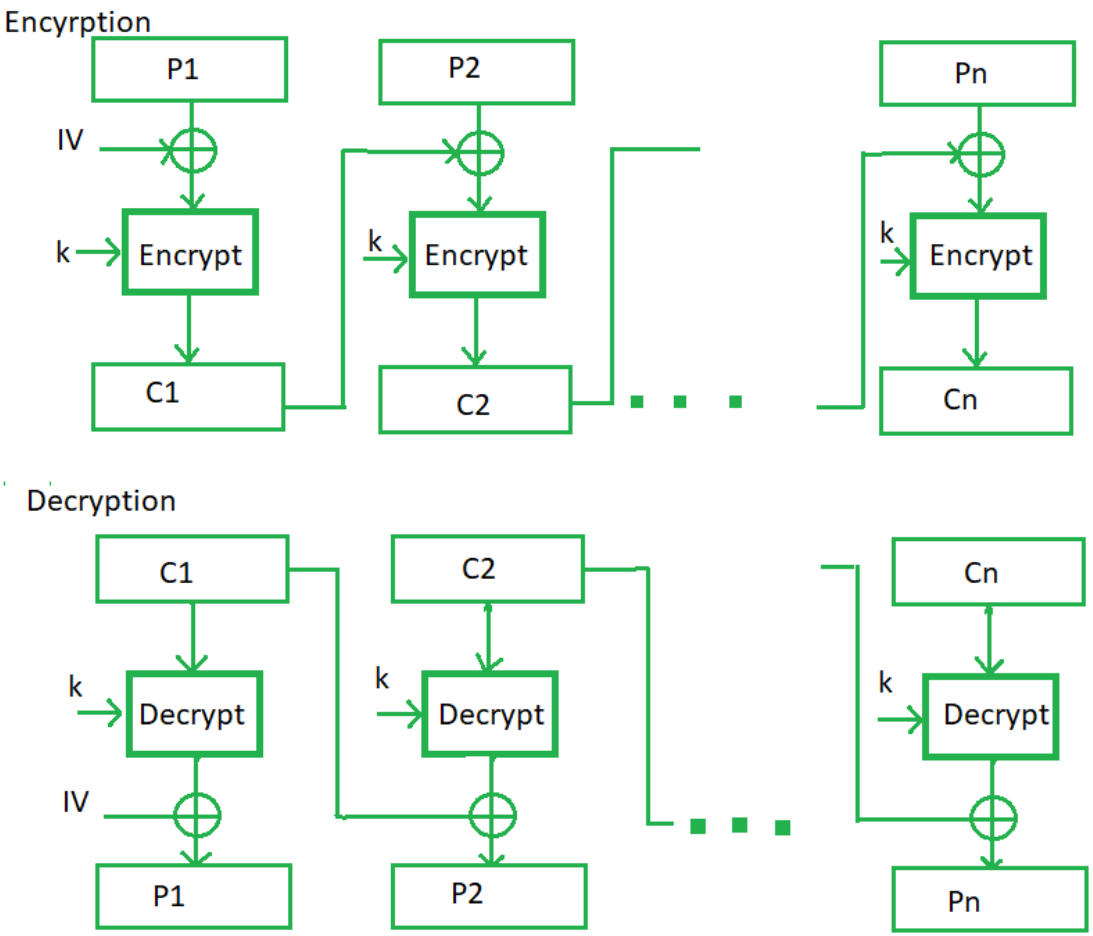
- Block Cipher Schemes
- There is a vast number of block ciphers schemes that are in use. Many of them are publically known. Most popular and prominent block ciphers are listed below.
- **Digital Encryption Standard (DES)** − The popular block cipher of the 1990s. It is now considered as a 'broken' block cipher, due primarily to its small key size.
- **Triple DES** − It is a variant scheme based on repeated DES applications. It is still a respected block ciphers but inefficient compared to the new faster block ciphers available.
- **Advanced Encryption Standard (AES)** − It is a relatively new block cipher based on the encryption algorithm **Rijndael** that won the AES design competition.

- **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 ciphertext. Generally, if a message is larger than *b* bits in size, it can be broken down into bunch of blocks and the procedure is repeated.


Encryption
P1
P2
Pn
k
Encrypt
k
Encrypt
k
Encrypt
C1
C2
Cn
Decryption
C1
C2
Cn
k
Decrypt
k
Decrypt
k
Decrypt
P1
P2
Pn

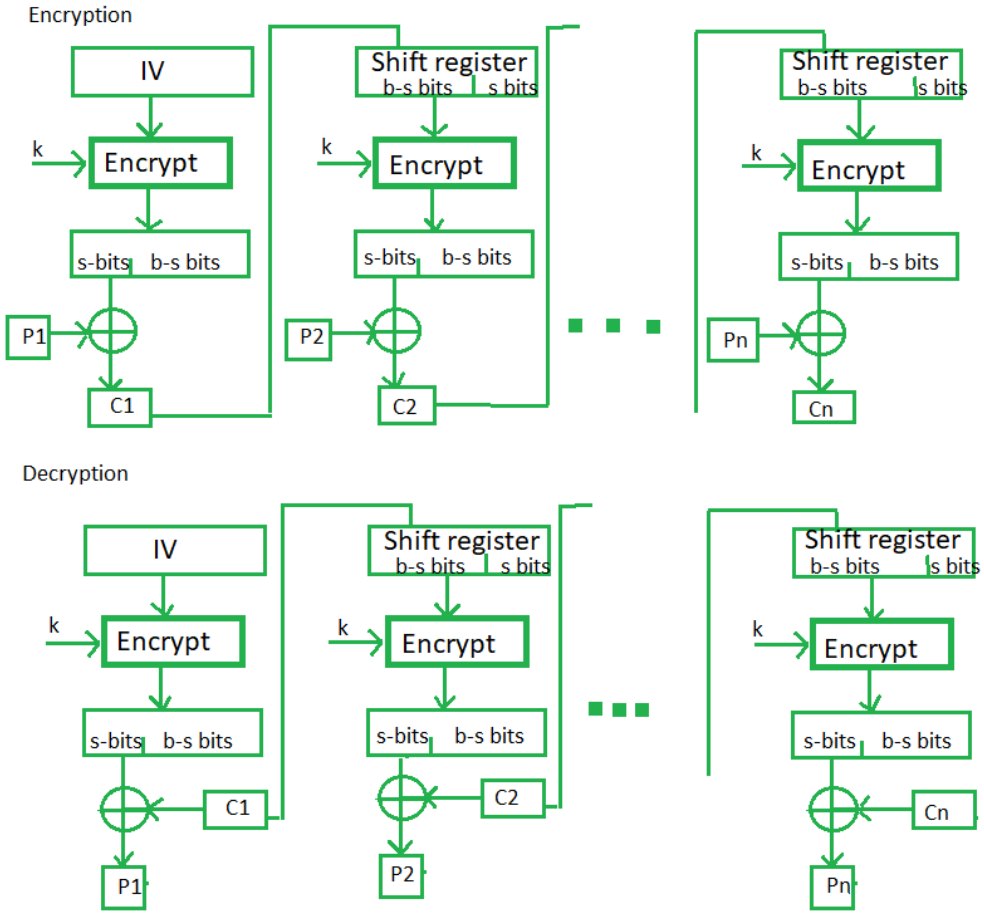
- **Advantages of using ECB –**
- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of block cipher.
- **Disadvantages of using ECB –**
- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

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


Encyrption
P1
P2
Pn
IV
k
Encrypt
k
Encrypt
k
Encrypt
C1
C2
Cn
Decryption
C1
C2
Cn
k
Decrypt
k
Decrypt
k
Decrypt
IV
P1
P2
Pn

- **Advantages of CBC –**
- CBC works well for input greater than *b* bits.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalsis than ECB.
- **Disadvantages of CBC –**
- Parallel encryption is not possible since every encryption requires previous cipher.

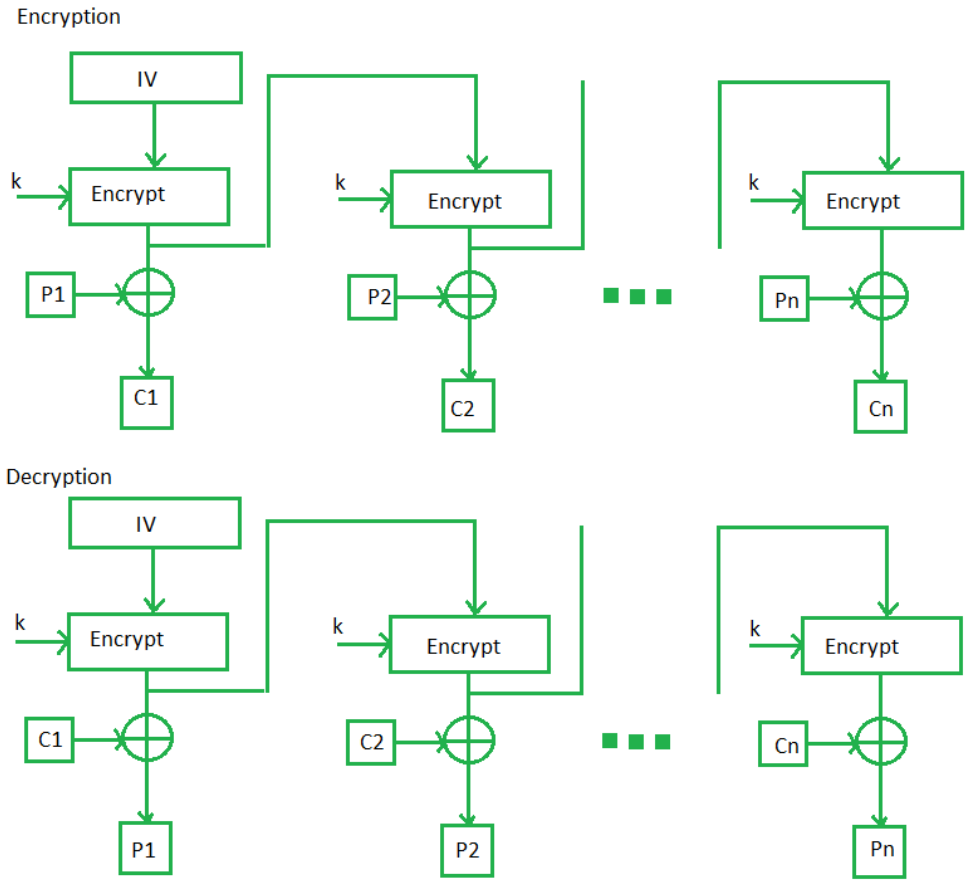
- **Cipher Feedback Mode (CFB) –**
  In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first an initial vector IV is used for first encryption and output bits are divided as set of *s*and*b-s* bits the left hand side *s*bits are selected and are applied an XOR operation with plaintext bits. The result 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 algorithm.



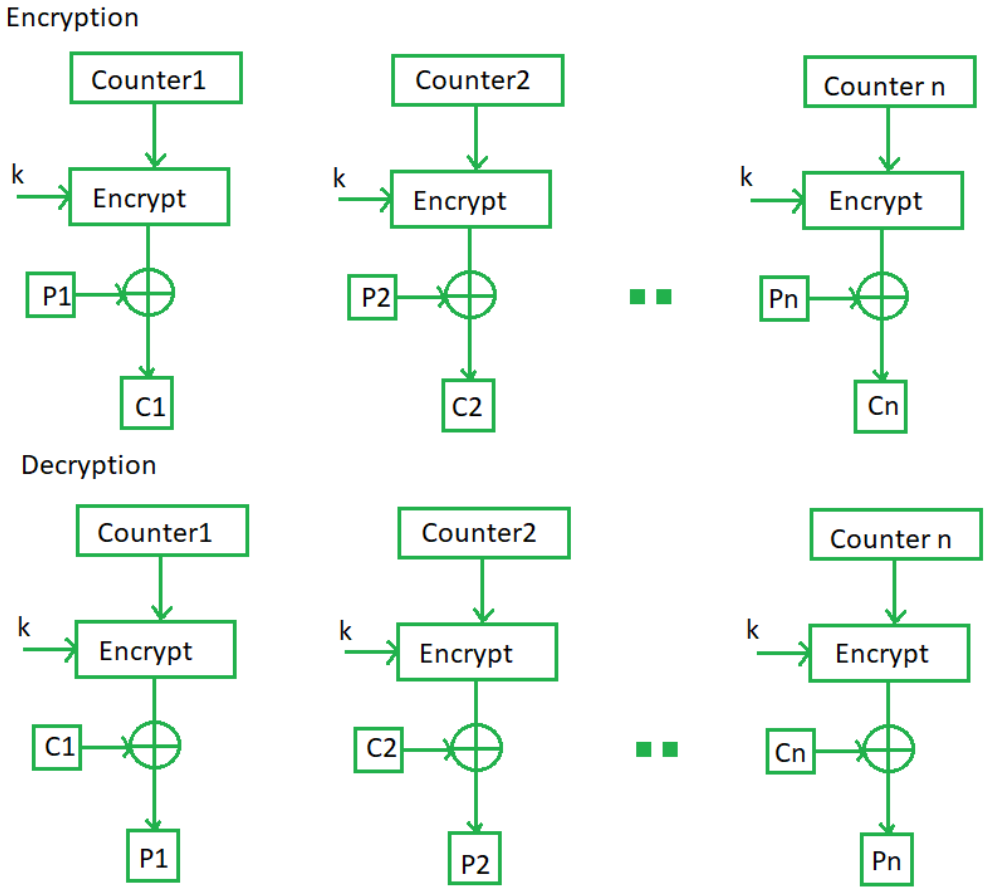
Advantages of CFB –

Since, there is some data loss due to use of shift register, thus it is difficult for applying cryptanalysis.

- **Output Feedback Mode –**
  The output feedback mode follows nearly 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 send instead of sending selected *s* bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases dependency or relationship of cipher on plaintext.
-

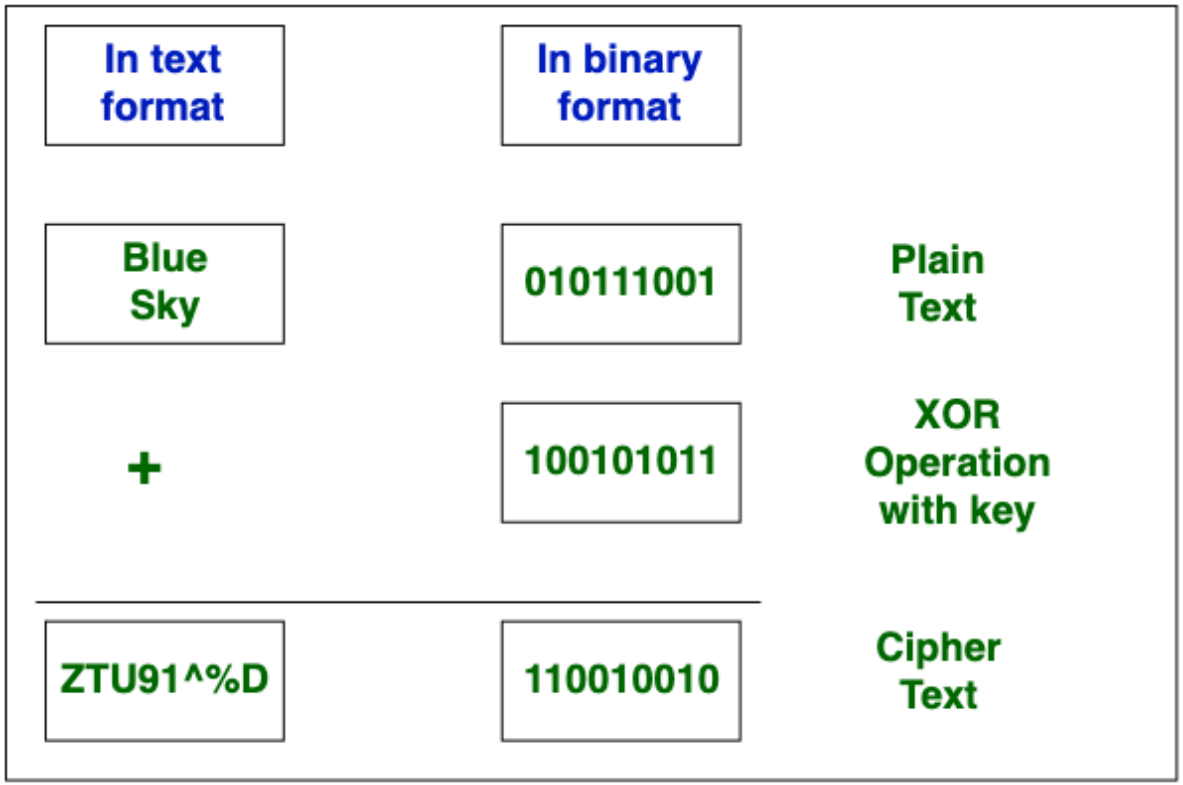

Encryption
IV
k
Encrypt
P1
C1
k
Encrypt
P2
C2
k
Encrypt
Pn
Cn
Decryption
IV
k
Encrypt
C1
P1
k
Encrypt
C2
P2
k
Encrypt
Cn
Pn

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


Encryption
Counter1
k
Encrypt
P1
C1
Counter2
k
Encrypt
P2
C2
Counter n
k
Encrypt
Pn
Cn
Decryption
Counter1
k
Encrypt
C1
P1
Counter2
k
Encrypt
C2
P2
Counter n
k
Encrypt
Cn
Pn

Difference between Block Cipher and Stream Cipher

- Both **Block Cipher** and **Stream Cipher** are belongs to the symmetric key cipher. These two block cipher and stream cipher are the methods used for converting the plain text into cipher text.
- The main difference between **Block cipher** and **Stream cipher** is that block cipher converts Converts the plain text into cipher text by taking plain text's block at a time. While stream cipher Converts the plaint text into cipher text by taking 1 byte of plain text at a time.



Stream Cipher

S.NO	BLOCK CIPHER	STREAM CIPHER
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plaint text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5.	In block cipher, reverse encrypted text is hard.	While in stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used in block cipher are: ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are: CFB (Cipher Feedback) and OFB (Output Feedback).