VANTAGES of STREAM:-

speed of Transformation :- Algo's are linear in Time & Constant in Space

Low Error Propagation :- An Error in Encrypting 1 Symbol likely will not affect Subsequent Symbols.

Disadvantages :-

(i) Low Diffusion – Hide info in Plaintext between Ciphertext.

(ii) Susceptibility to insertions/Modifications :- Tampering of info or Msg.

BLOCK CIPHERS.

- Block Ciphers is one in which a block of Plaintext is treated as a whole & used to produce a ciphertext block of equal length.
- Typically, a block size of 64 or 128 bits is used.
- Same Symmetric Encryption key
- Eg:- DES where blocks of 64 bit are encrypted using 56 bit key.
- MOST Symmetric Block Ciphers are based on a feistel Cipher Structure.

ormal Definition of Block Cipher

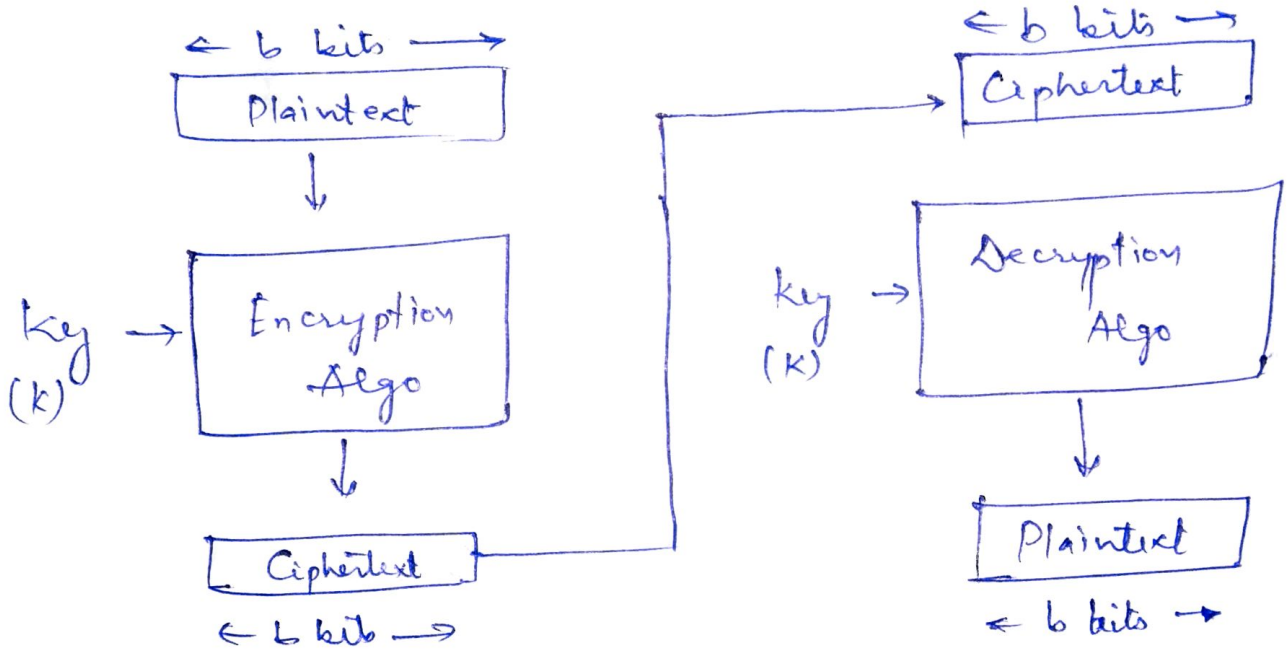
Let E be an encipherment algo & Let $E_K(b)$ be the encipherment of the message b with key K.

Let a Msg $m = b_1 b_2 \ldots$ where b_i is of a fixed Length.

A block Cipher is a cipher for which

$$E_K(m) = E_K(b_1)\, E_K(b_2) \ldots$$

$E_K(b_1)$: Keystream; E_K: Keystream; b_2: Block



(b) Block Ciphers.

Block Cipher.

JVANTAGES :-

(i) High Diffusion :- Info from One Plain Text Symbol is diffused into several Ciphertext Symbols.

(ii) Immunity To Tempering :- Difficult to insert Symbols without Detection

Disadvantages

(i) Slowness of Encryption

(ii) Error Propagation :- Error in one symbol may corrupt the entire Block

Stream v/s Block Ciphers.

Stream Ciphers	Block Ciphers
Stream Cipher Combines in Text bits with a Pseudorandom Cipher bits stream using XOR Op^n.	Block Ciphers encrypt fixed length blocks of bits.
i) Stream Ciphers use varying transformation based on the state of engine.	Block Ciphers use the same Transformations.
iii) Stream Ciphers Execute faster.	Block Ciphers execute slowly
(iv) Stream Ciphers are less Complex.	Block Ciphers are more Complex
(v) They are used when the Plain Text is Available in varying quantities, ∵ block ciphers cannot operate directly on blocks shorter than the block size.	Using certain modes of Op^n, a block Cipher can be used to act as a stream Cipher by allowing it to encrypt the smallest unit of data available.