Algorithm Modes

ECB,
CBC,
CFB,
OFB

Two Key Aspects of Algorithm

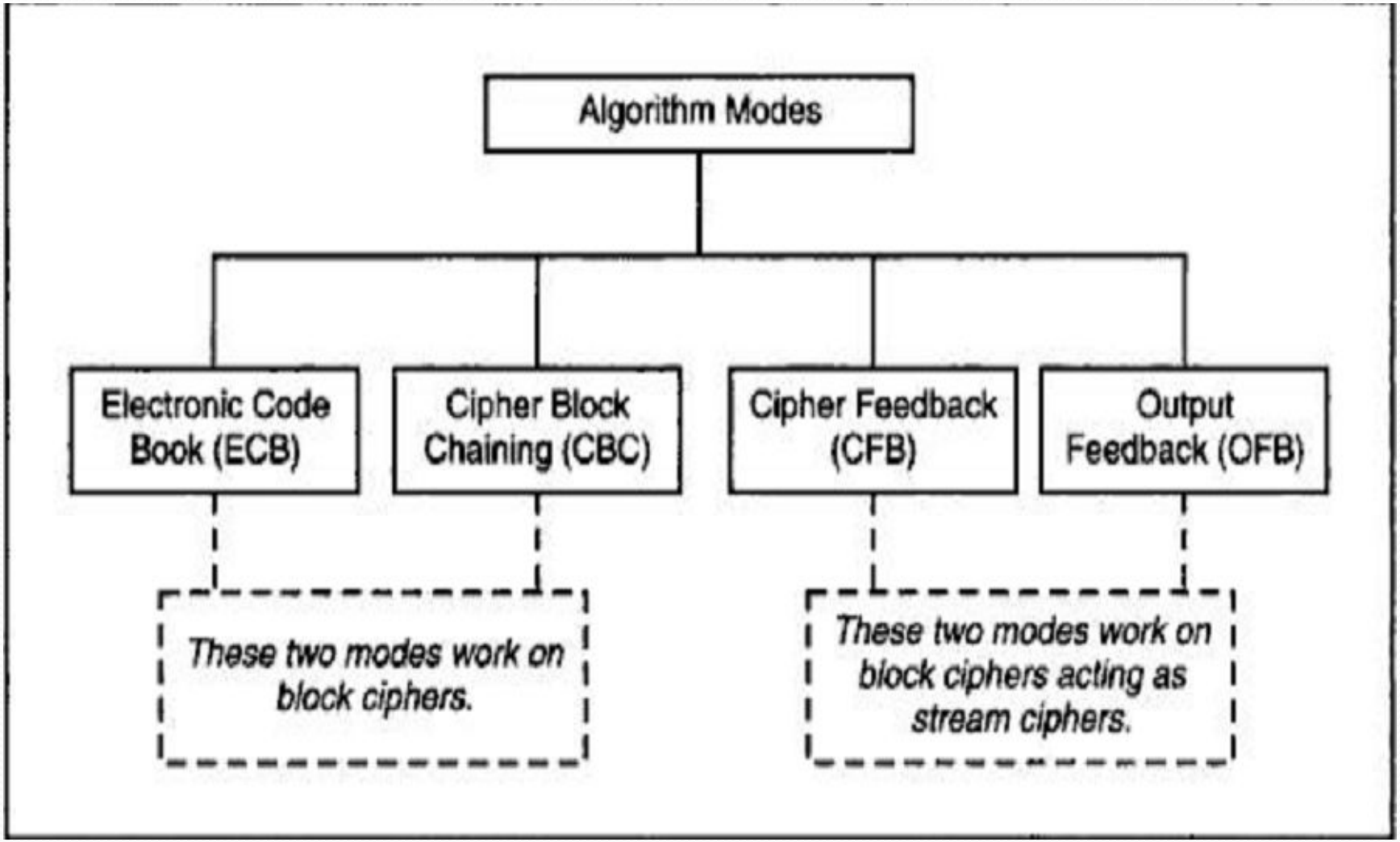
1. Algorithm type :- It defines what should be the size of PT.

   - ✔ Stream
   - ✔ Block

2. Algorithm Modes:- It defines the *details* of the cryptographic Algorithm.

   - ✔ It is a combination of the basic steps on block cipher & some kind of feedback from previous step

Algorithm Modes



1.ECB

- ✔ Encryption Process:-
  - PT divided 64 bits each.
  - Encrypted Independently
  - Same key
- ✔ Decryption Process:-
  - Divide
  - Same Key
  - PT
- ✔ Limitation:-
  - If Repeated PT Then Repeated CT
  - Small Messages where the scope of repeating quite less.

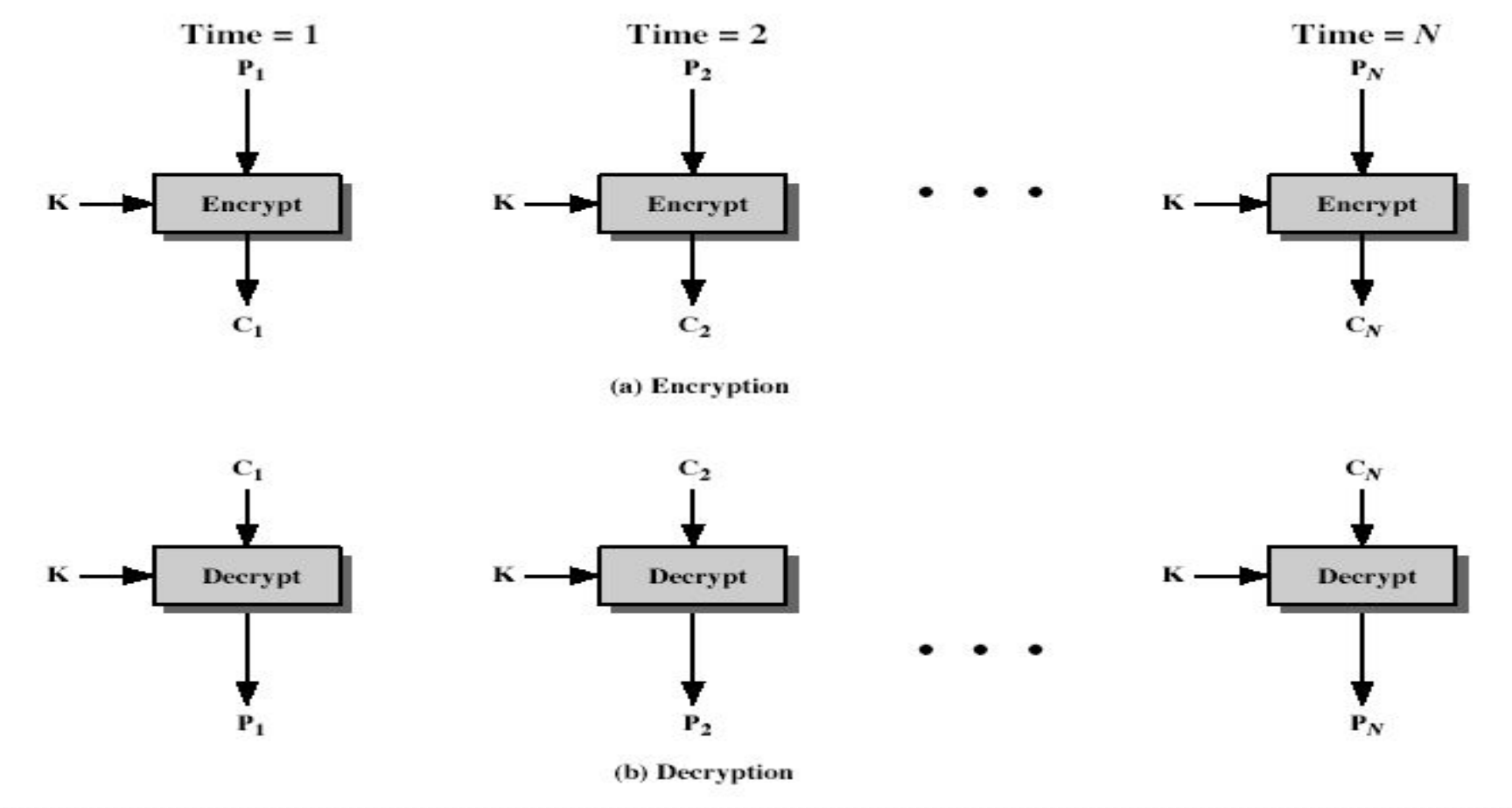
Electronic Codebook Book (ECB)

- Message is broken into independent blocks which are encrypted
- *Each block is a value which is substituted, like a codebook, hence name*
- Each block is encoded independently of the other blocks

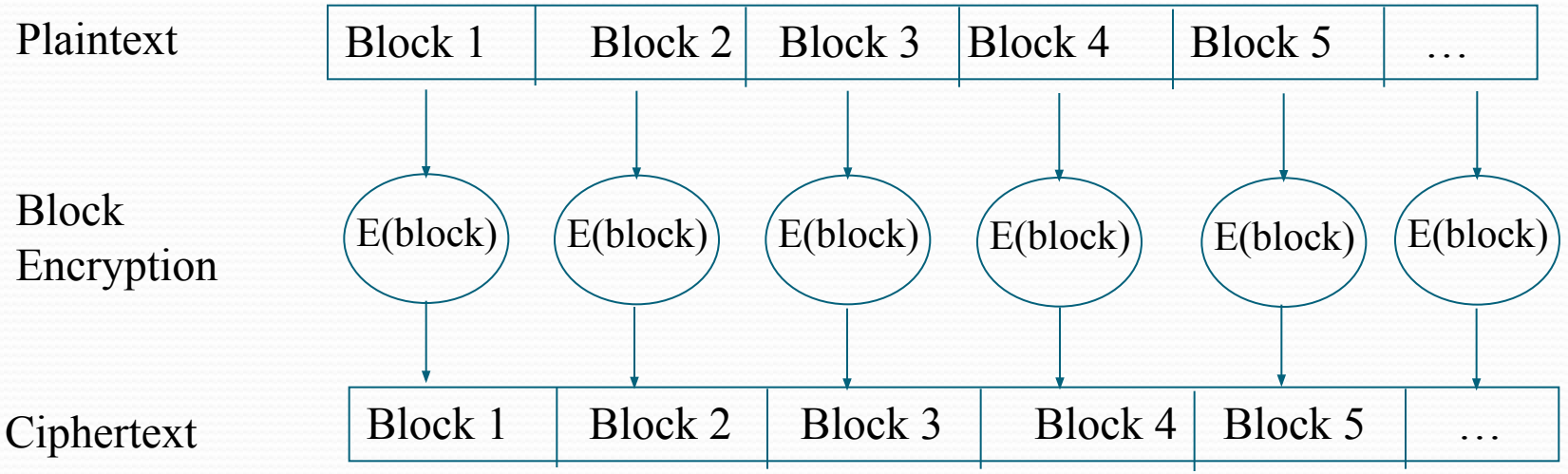
$$C_i = E_{K1}(P_i)$$

- Uses: transmission of single values.(i.e;-PW or key for E/D) in secure fashion.
  - E=Encryption , D= Decryption

Electronic Codebook Book (ECB)



Electronic Code Book (ECB) Mode



- Pad last block, if necessary

Advantages and Limitations of ECB

- Repetitions in message may show in cipher text
  - if aligned with message block
  - particularly with data such graphics
  - Or with messages that change very little, which become a *code-book analysis problem .*
- weakness due to encrypted message blocks being independent.
- main use is sending a few blocks of data.

2.CBC

- Different CT for every PT including identical/repeat PT.
- Feed back Mechanism used(i.e: Chaining).
- **Initialization Vector(IV)** for creating unique message.
- Random Block called IV can be XOR with plain text in First step.
- *Not a secret – just prevents a codebook. Often times a timestamp.*
- I/O-> IV XOR PT Block 1 = CT Block 1<- we can call it as New IV for next step.
- Same key
- Dependent on previous one.

Cipher Block Chaining (CBC)

- Message is broken into blocks
- But these are linked together in the encryption operation
- *Each previous cipher blocks is chained with current plaintext block, hence name*
- Use Initial Vector (IV) to start process (Block 1)

$$C_{-1} = IV$$

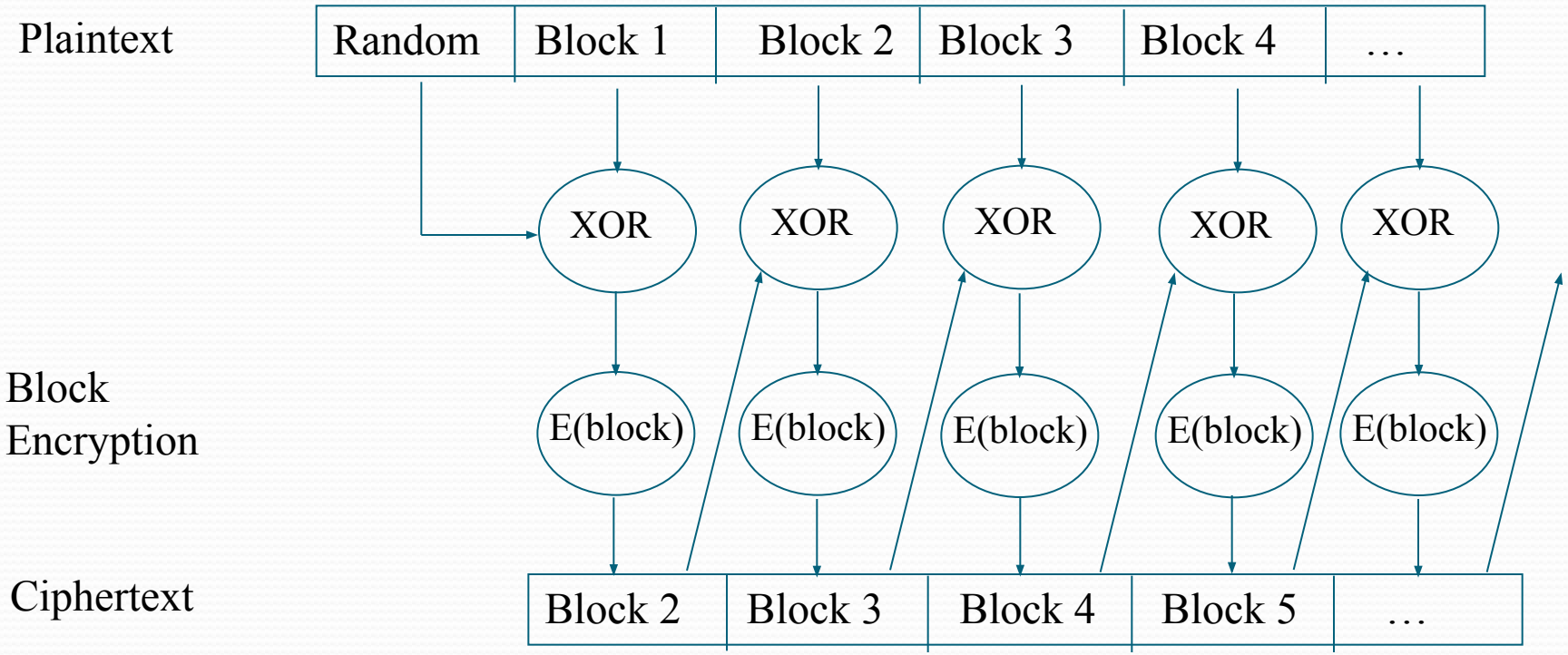
$$C_i = E_{K1}(P_i \text{ XOR } IV)$$

- From block 2

$$C_i = E_{K1}(P_i \text{ XOR } C_{i-1})$$

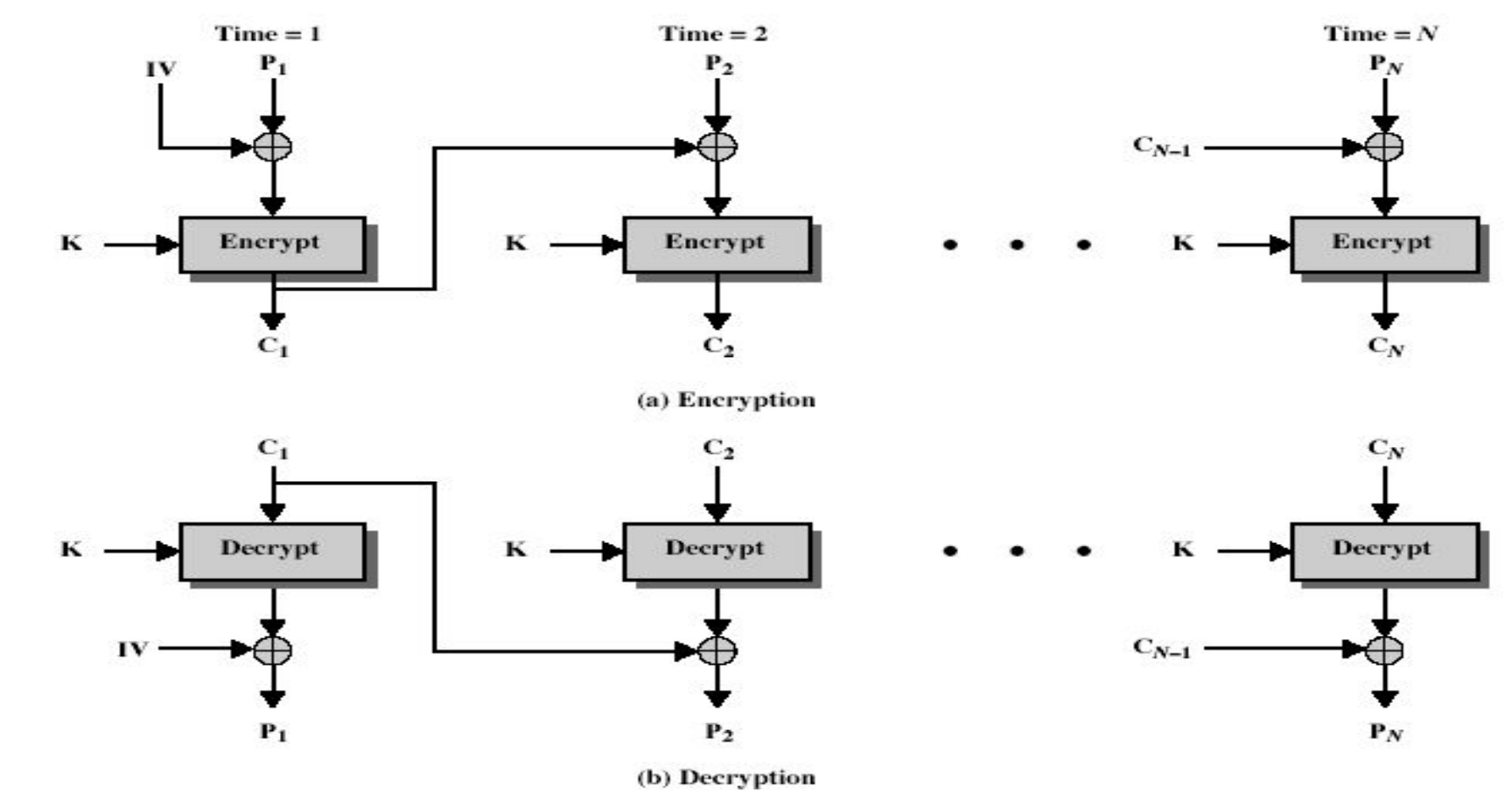
- Uses: bulk data encryption, authentication

Cipher Block Chaining (CBC) Mode



- Pad last block, if necessary
-

Cipher Block Chaining (CBC)



Advantages and Limitations of CBC

- Each cipher text block depends on **all** message blocks
- Thus a change in the message affects all cipher text blocks after the change as well as the original block
- Need **Initial Value** (IV) known to sender & receiver
  - However if IV is sent in the clear, an attacker can change bits of the first block, and change IV to compensate
  - Hence either IV must be a fixed value or it must be sent encrypted in ECB mode before rest of message
- At end of message, handle possible last short block
  - By padding either with known non-data value (eg nulls)
  - Or pad last block with count of pad size
    - eg. [b1 b2 b3 0 0 0 0 5] <- 3 data bytes, then 5 bytes pad+count

CFB

- Where Stream Cipher must be used?
- *An operator typing keystrokes at a terminal, which need to be immediately transmitted across communication link in a secure manner.*
- *Max Size of unit is 8.*

Cipher Feed Back (CFB)

- Message is treated as a stream of bits
- Added to the output of the block cipher
- Result is feed back for next stage (hence name)
- Standard allows any number of bit (1,8 or 64 or whatever) to be feed back
  - denoted CFB-1, CFB-8, CFB-64 etc
- Is most efficient to use all 64 bits (CFB-64)

$$C_i = P_i \text{ XOR } {}_{K1}(C_{i-1})$$
$$C_{-1} = IV$$

- Uses: stream data encryption, authentication

Step 1

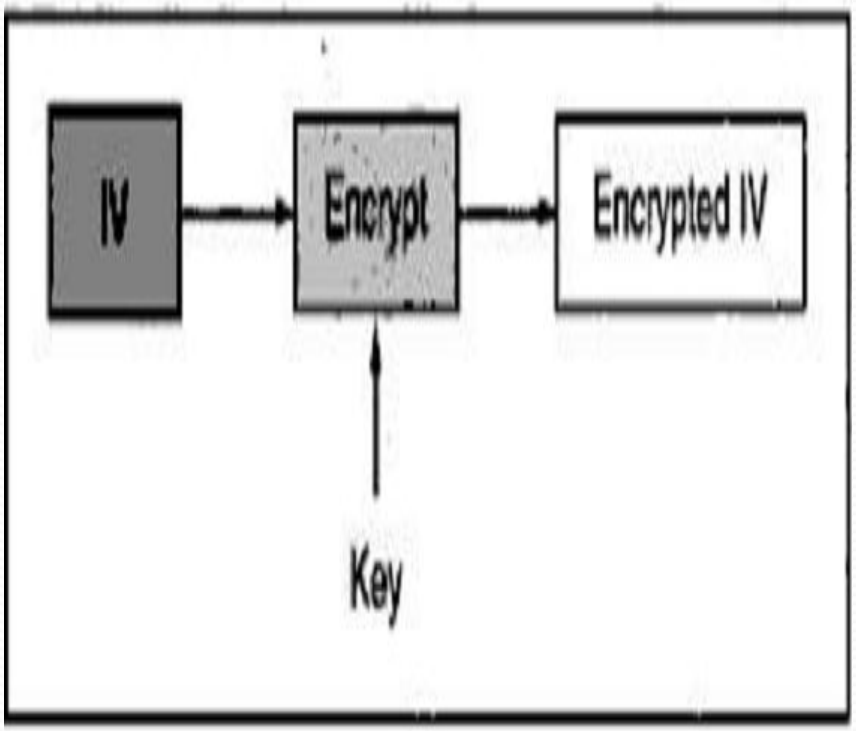


Fig. 3.10 CFB—Step I

- 64 bit IV PT
- Kept in Shift Register
- Encrypted
- 64 bit IV CT

Step 2

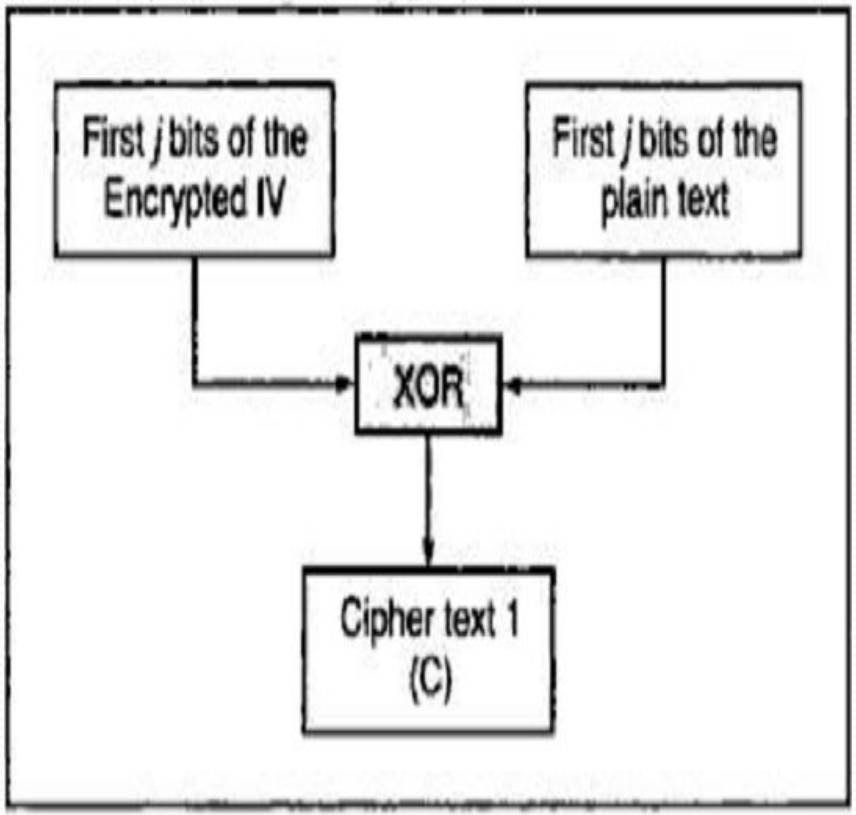
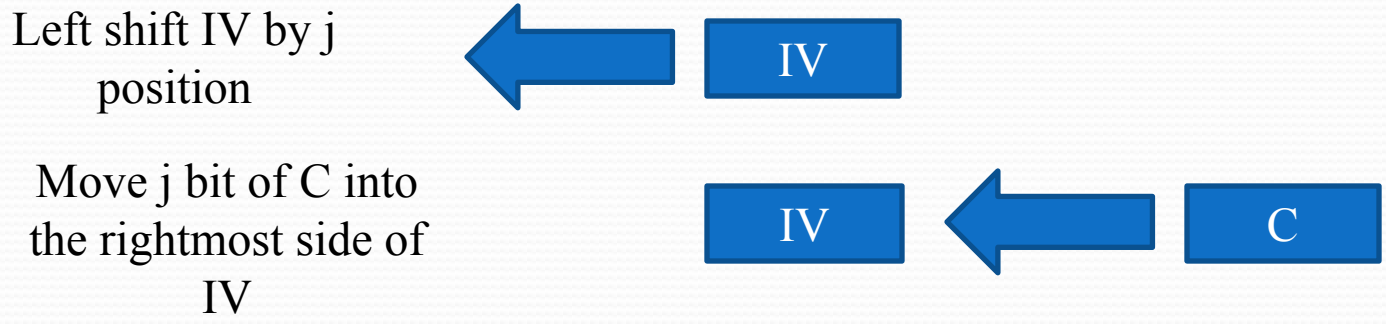


Fig. 3.11 CFB—Step 2

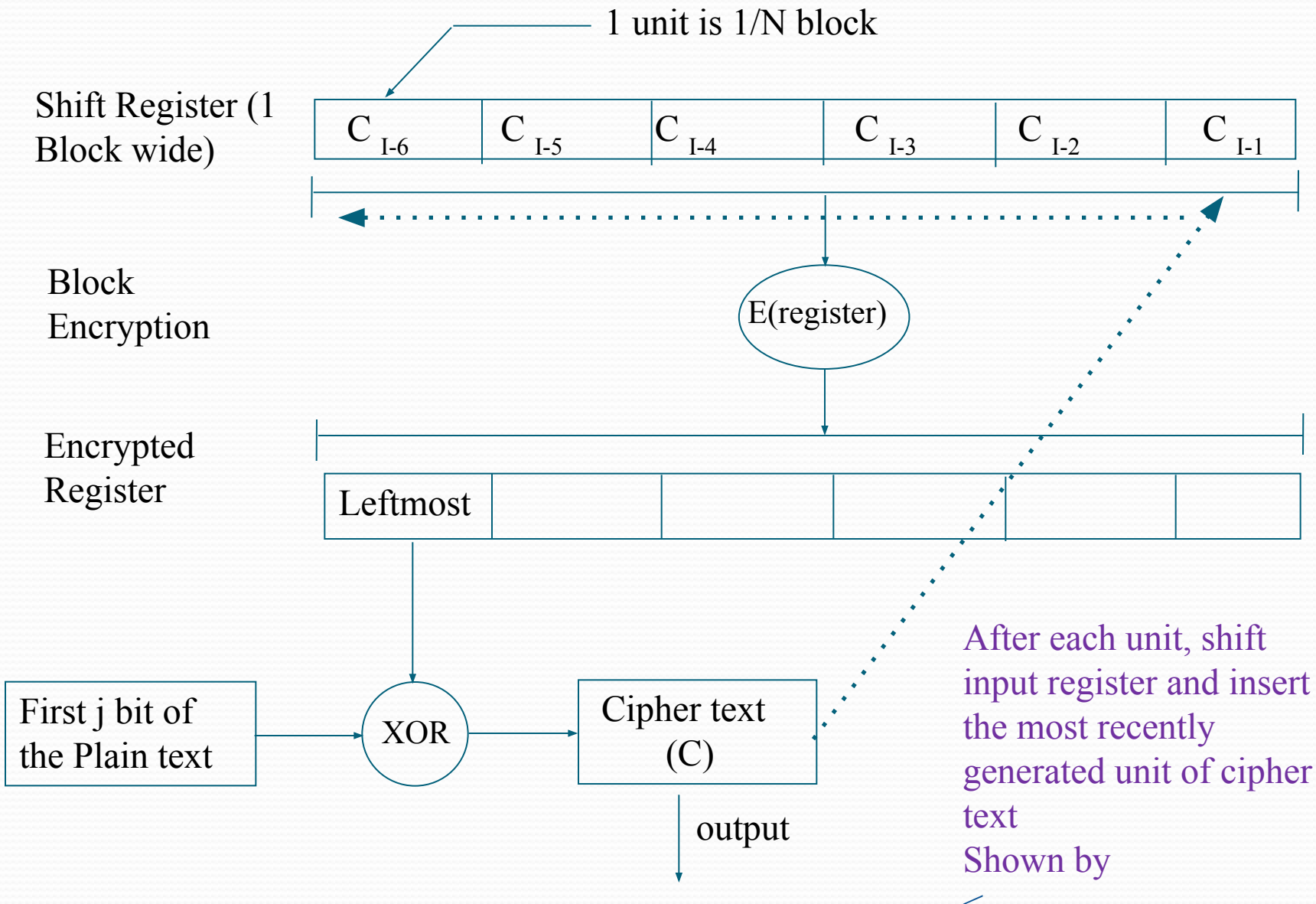
- Leftmost bit (i.e MSB)

Step 3

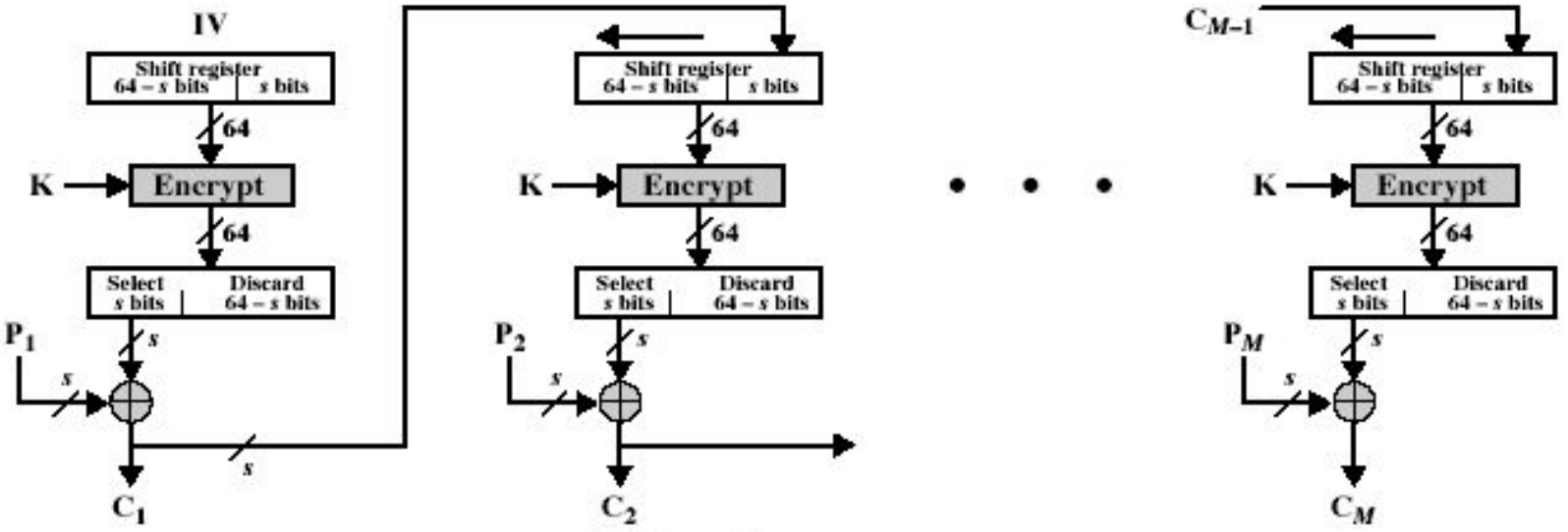
- Left Shift IV by j positions.
- Move j bits of C into the rightmost side of blank IV .
- Step 1 through 3 continue until all the PT units are encrypted.
- *C=Cipher Text from step 2.



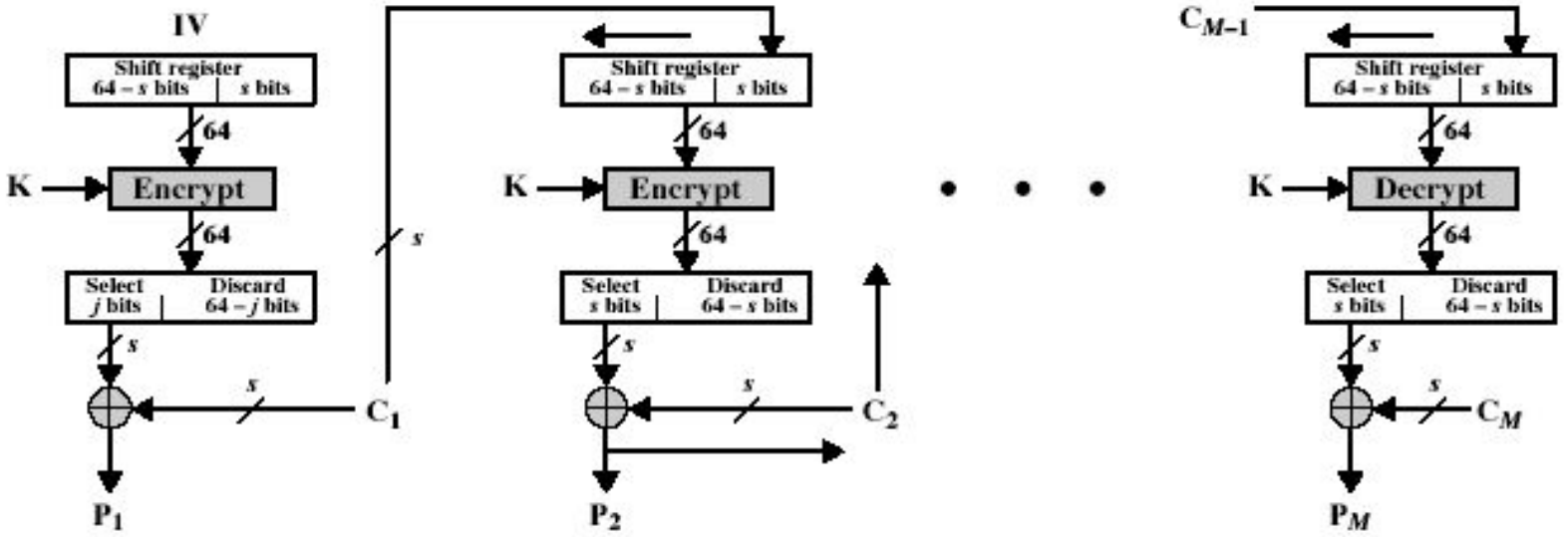
Cipher Feedback Mode (CFB)



Cipher FeedBack (CFB)



(a) Encryption



(b) Decryption

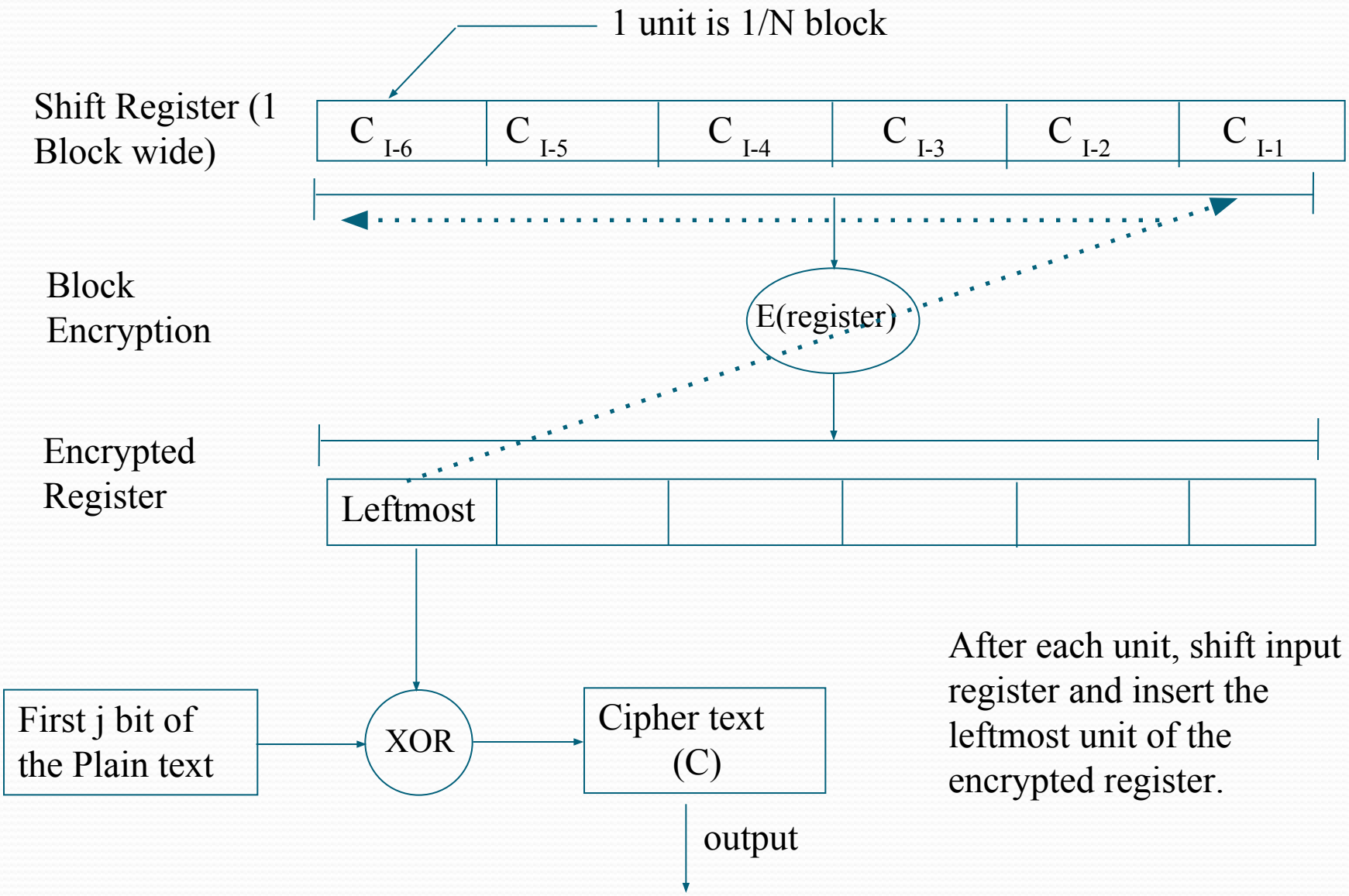
Limitations of CFB

- Errors propagation if Ci bit contain error.
- Ci is feed back as input to the shift register & would corrupt the other bits in the message.

4.OFB

- The output of the IV encryption process is feed into the next of the encryption process.
- Advantage Of This Scheme:-
- Bit error do not get propagated(i.e;-Other bits are not affected)
- If there are error in individual bits will not corrupt the whole message.
- disadvantage Of This Scheme:-
- Attacker ***changes*** both the cipher text and the checksum at the same time hence there is no way to detect this change.

Output Feedback Mode (OFB)



5.CTR(Counter)

- It uses sequence numbers called as counters as the inputs to the algorithm.
- After each block is encrypted, the next counter value is used to fill the register.
- *Usually, a constant is used as a initial counter value and is incremented by 1 for every iteration , hence name*
- The size of counter block is same as PT.
- Encryption:- Decryption:-
- Counter is encrypted ->Same Sequence is used
- XOR'ed with PT -> XOR'ed with CT
- CT ->PT

Advantages & Limitations Of CRT

- Encryption & Decryption process can be done in *parallel* on multiple text blocks.
- No chaining process is involved.
- Faster execution Speed.
- Used in Multiprocessing to reduce overall processing time.
- Pre processing can be achieved to prepare the O/P of the encryption boxes that I/P to the XOR operation.