Ceng 471 Cryptography

Symmetrical Cryptosystems

Block Cipher

MODES OF OPERATION

Asst. Prof. Dr. Serap ŞAHİN

Izmir Institute of Technology

- The encryption modes prevent an eavesdropper from reading the traffic.
- They do not provide any authentication, so an attacker can still change the messages.
- Therefore; **all encryption processes should be combined with authentication**.
- In general, the length of the plaintext can not be an exact multiple of block size. This requires some padding.

$$\underline{\quad l(P)\quad}\ \underline{\qquad\qquad\qquad P \qquad\qquad\qquad}\ \underline{\quad Padding\quad}$$

- After padding, we cut padded plaintext into blocks.
- The number of blocks : $k = \lceil (l(P)+1)/b \rceil$

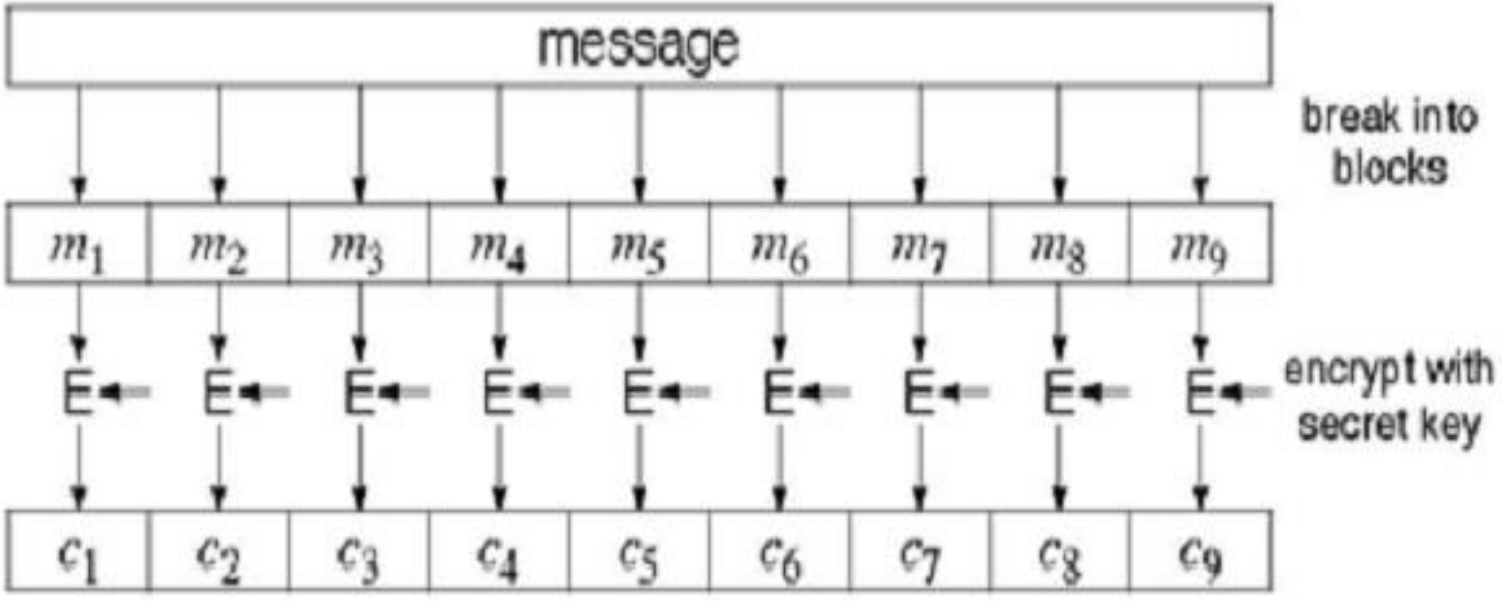
- Modes of operation
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

ELECTRONIC CODE 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

$C_i = E_{K1}(P_i)$

ELECTRONIC CODE BOOK (ECB)



Limitations of ECB

- Repetitions in message can be reflected 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 is because enciphered message blocks are independent of each other
- It has serious weaknesses.

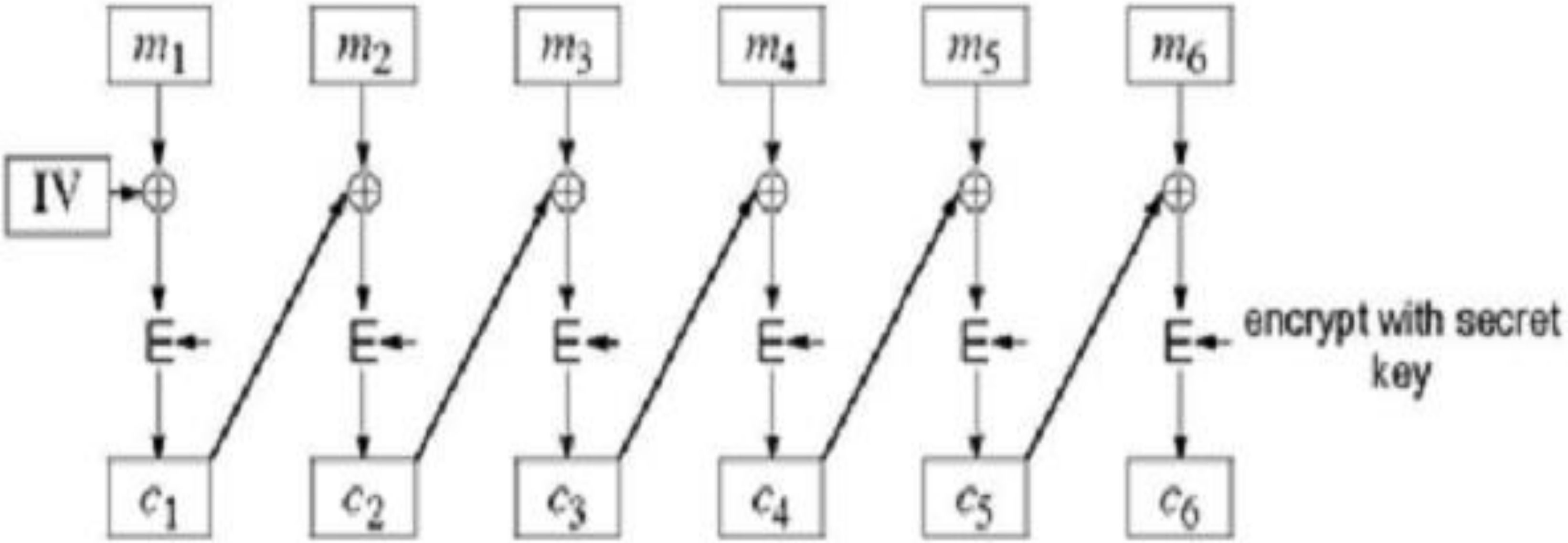
CIPHER BLOCK CHAINING (CBC)

- Is an enhanced mode of ECB
- Message is broken into blocks
- Linked together in encryption operation
- Each previous cipher blocks is chained with current plaintext block, hence name
- Use Initial Vector (IV) to start process

$$C_{-1} = IV$$

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

CIPHER BLOCK CHAINING (CBC)



Advantages and Limitations of CBC

- A cipher text block depends on all blocks before it
- Any change to a block affects all following cipher text blocks

– To start need an **Initial Value** (IV) which must be known by both sender and 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 (as in EFTPOS) or it must be sent encrypted in ECB mode before rest of message

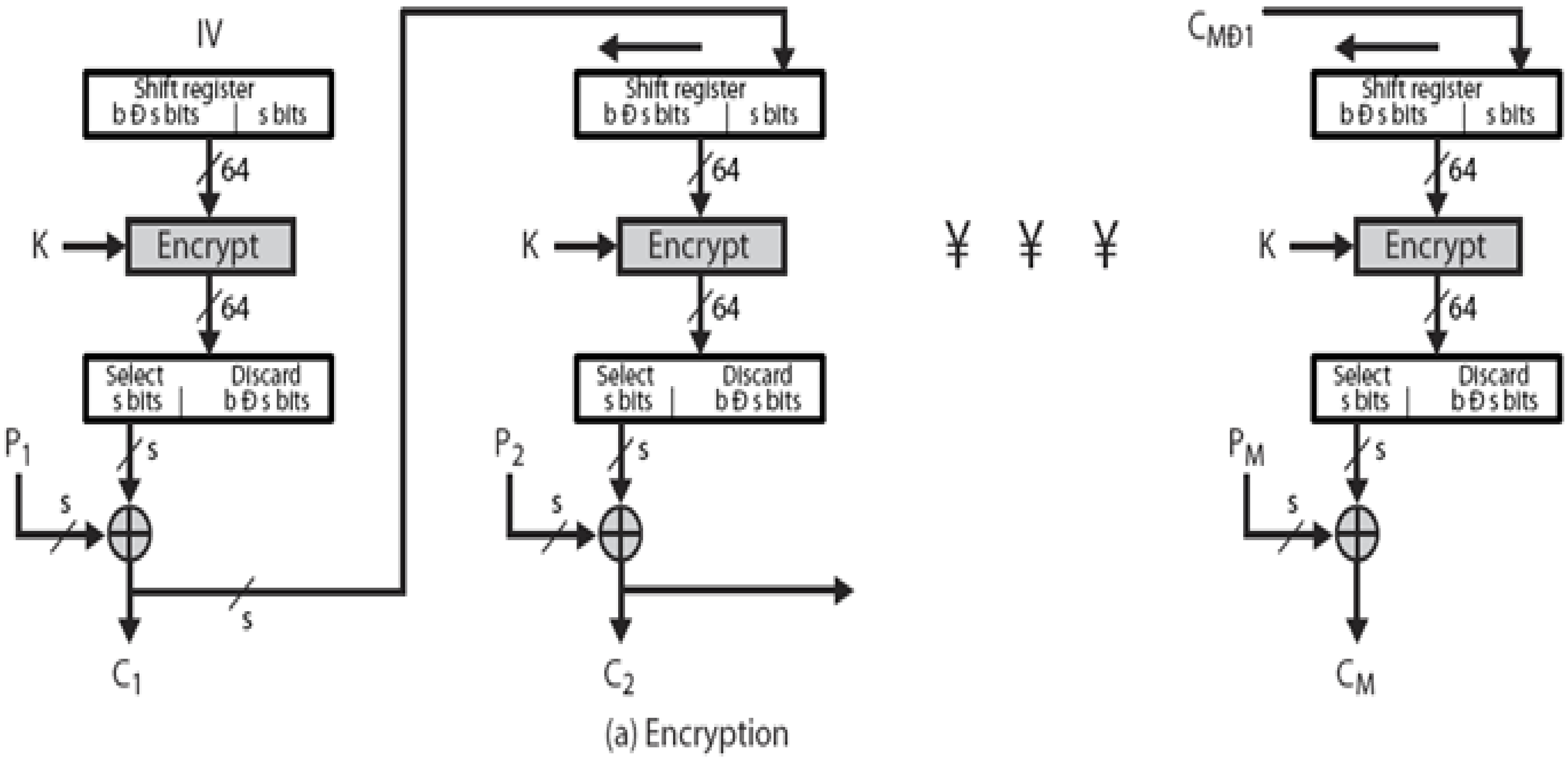
CIPHER FEEDBACK (CFB)

- Message is treated as a stream of bits or bytes
- Result is feed back for next stage (hence name)
- Standard allows any number of bit (1,8, 64 or 128 etc) to be feed back
  - denoted CFB-1, CFB-8, CFB-64, CFB-128 etc
- Most efficient to use all bits in block (64 or 128)

  $C_{-1} = IV$

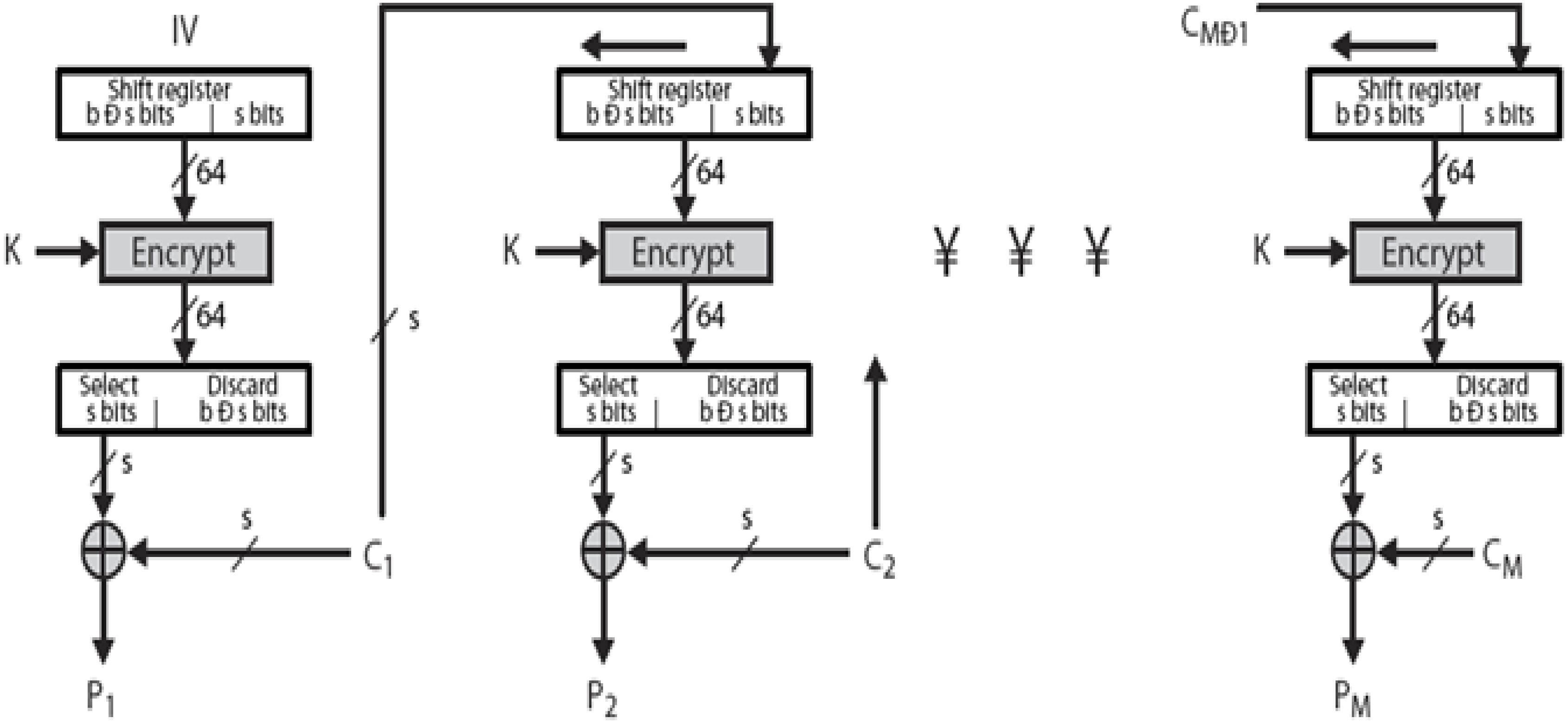
  $C_i = P_i \text{ XOR } E_K(C_{i-1})$
- Used for stream data encryption

CIPHER FEEDBACK (CFB)



(a) Encryption

CIPHER FEEDBACK (CFB)



(b) Decryption

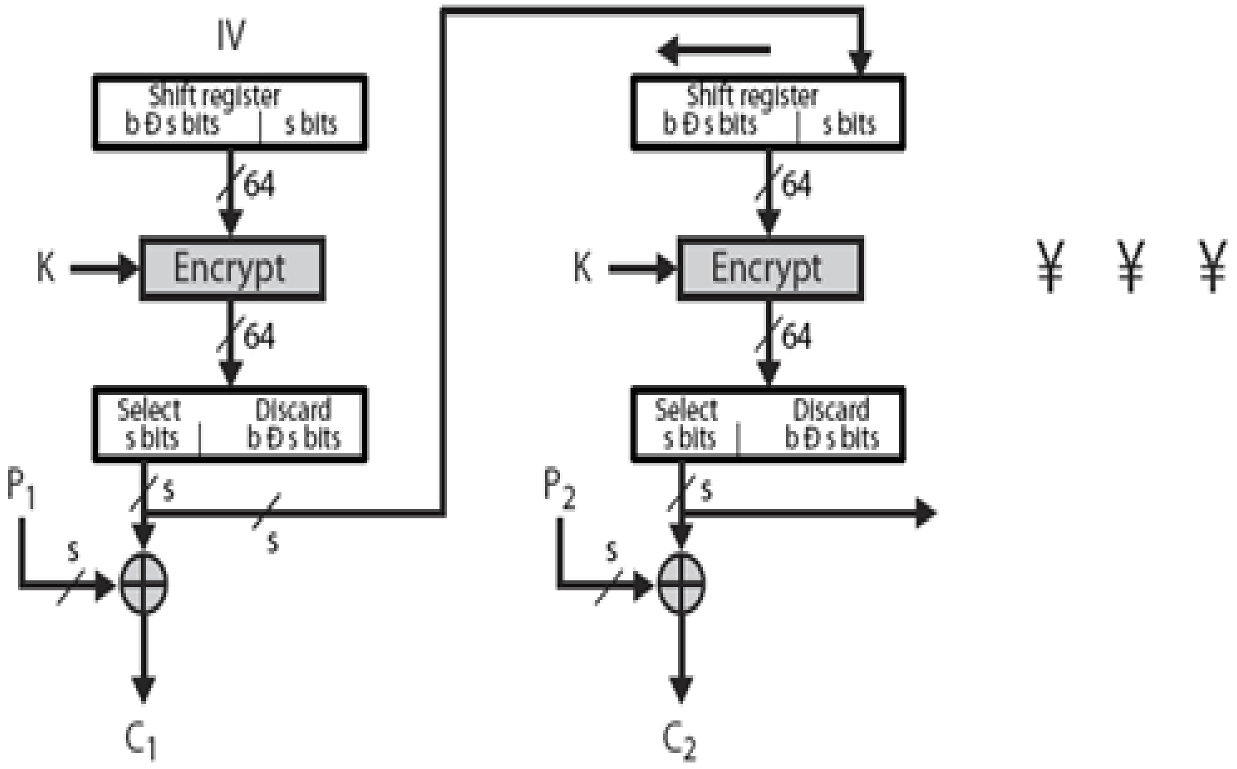
Advantages and Limitations of CFB

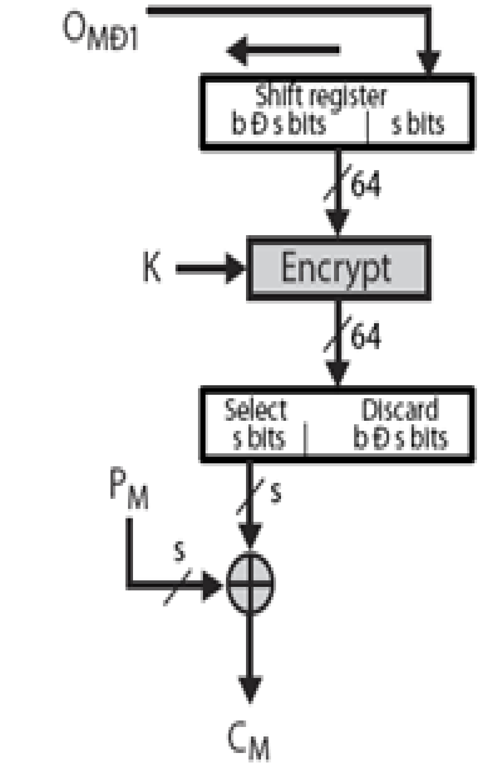
- Appropriate when data arrives in bits/bytes
- Most common stream mode
- Note that the block cipher is used in encryption mode at both ends
- Errors during transmission propagate for several blocks only (till the “dirty” part is eliminated from the shift register).

OUTPUT FEEDBACK (OFB)

- Message is treated as a stream of bits
- Output of cipher is added to message
- Output is then feed back (hence name)
- Feedback is independent of message
  - $C_i = P_i \oplus E_k(O_{i-1})$, with $O_{-1} = IV$
- So feedback can be computed in advance

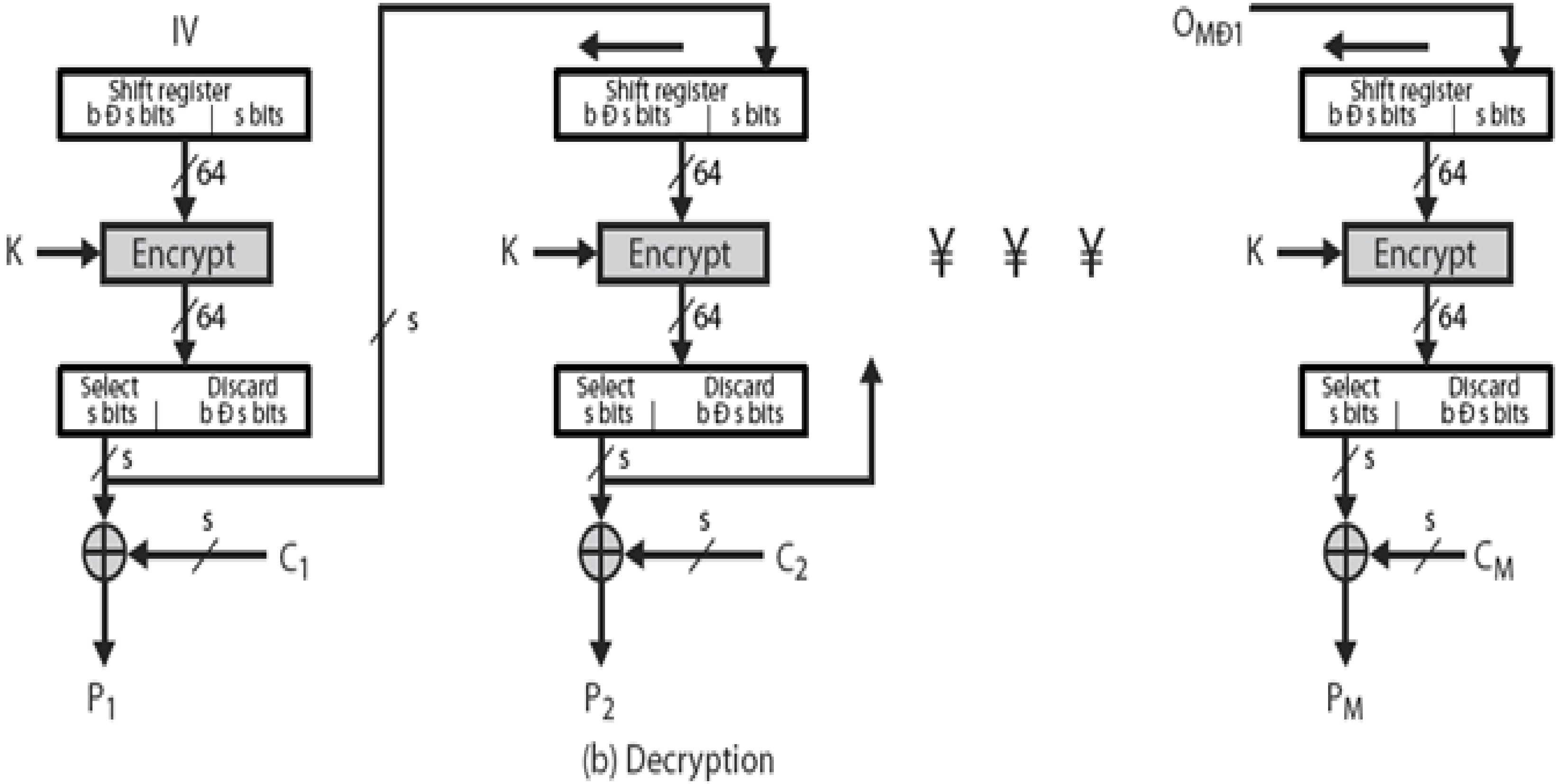
OUTPUT FEEDBACK (OFB)





(a) Encryption

OUTPUT FEEDBACK (OFB)



(b) Decryption

Advantages and Limitations of OFB

- Bit errors do not propagate
  - Is superficially similar to CFB, but the feedback is from the output of the block cipher and is independent of the message
  - Encryption and decryption of blocks can be done in parallel

COUNTER (CTR)

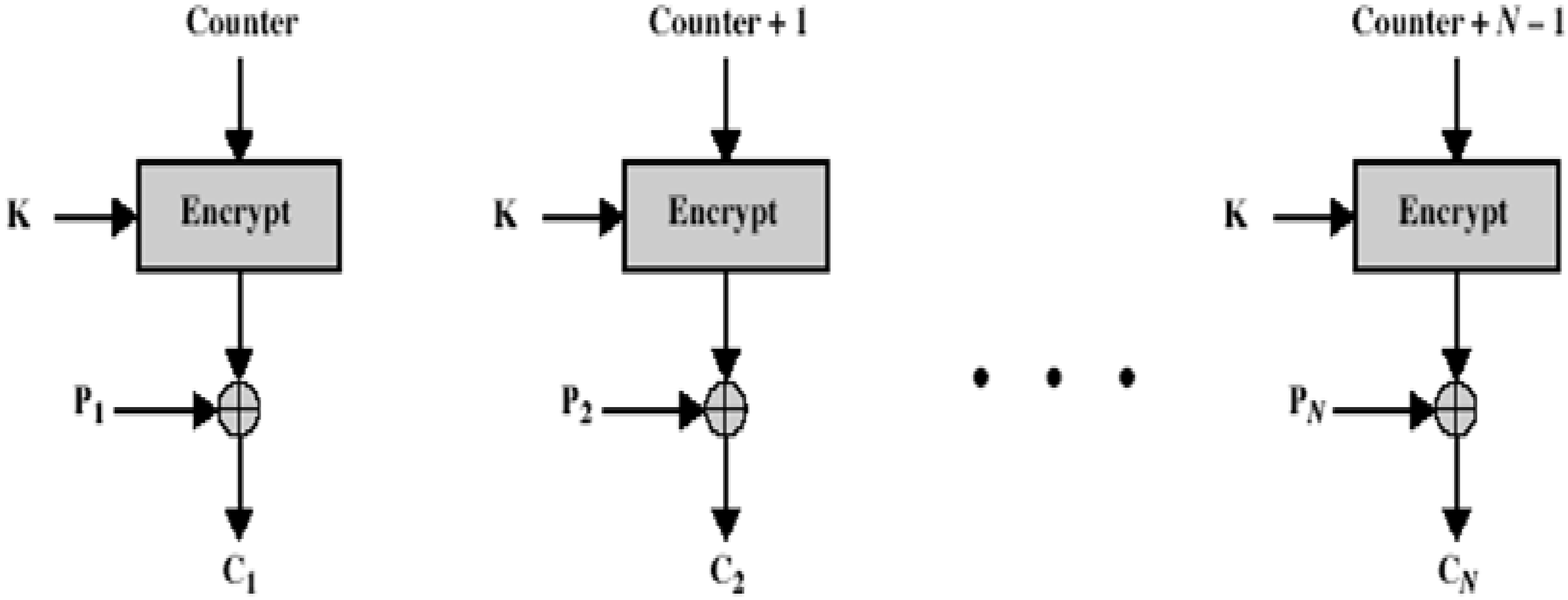
- Similar to OFB but encrypts counter value rather than any feedback value
- Must have a different counter value for every plaintext block (never reused)

  $C_i = P_i \text{ XOR } O_i$

  $O_i = E_{K1}(i)$

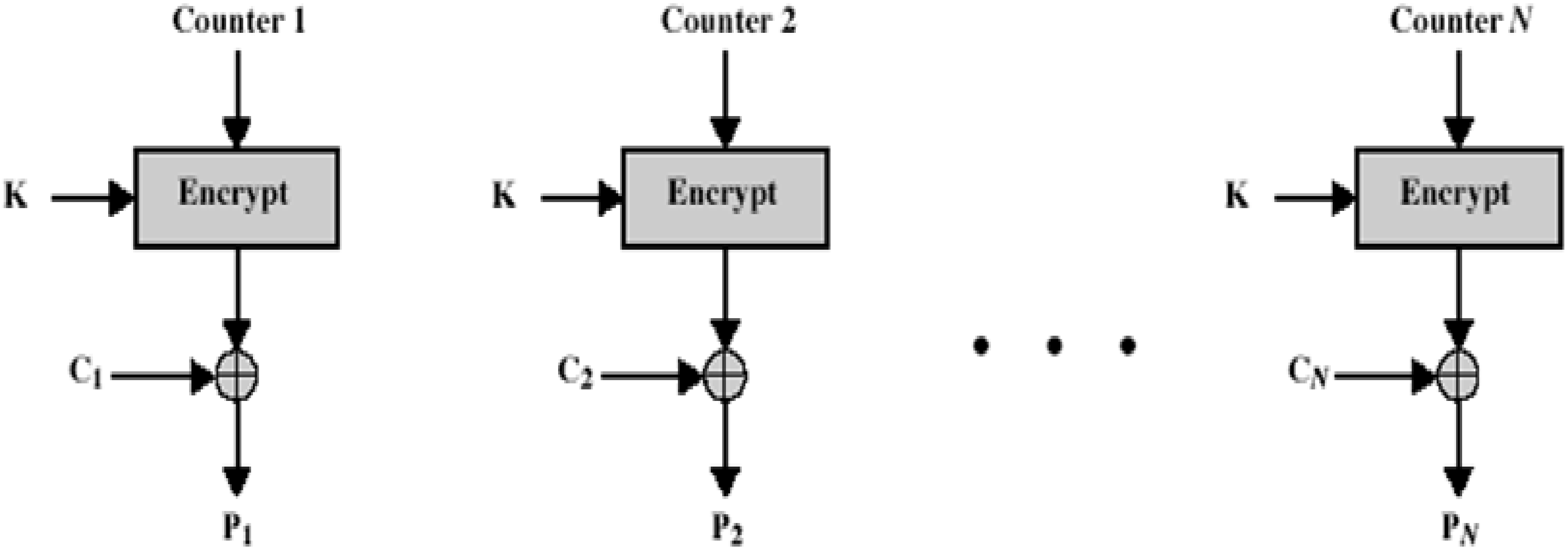
- Uses: high-speed network encryptions

COUNTER (CTR)



(a) Encryption

COUNTER (CTR)



(b) Decryption

Advantages and Limitations of CTR

- Efficiency
  - can do parallel encryptions in h/w or s/w
  - can preprocess in advance of need
- Random access to encrypted data blocks
- Provable security (good as other modes)
- But must ensure never reuse key/counter values, otherwise could break.