Modes Of Operations

Modes Of Operation

OUTLINE

- Introduction
- Electronic Code Book
- Cipher Block Chaining
- Cipher Feedback Mode
- Output Feedback Mode
- Counter Mode

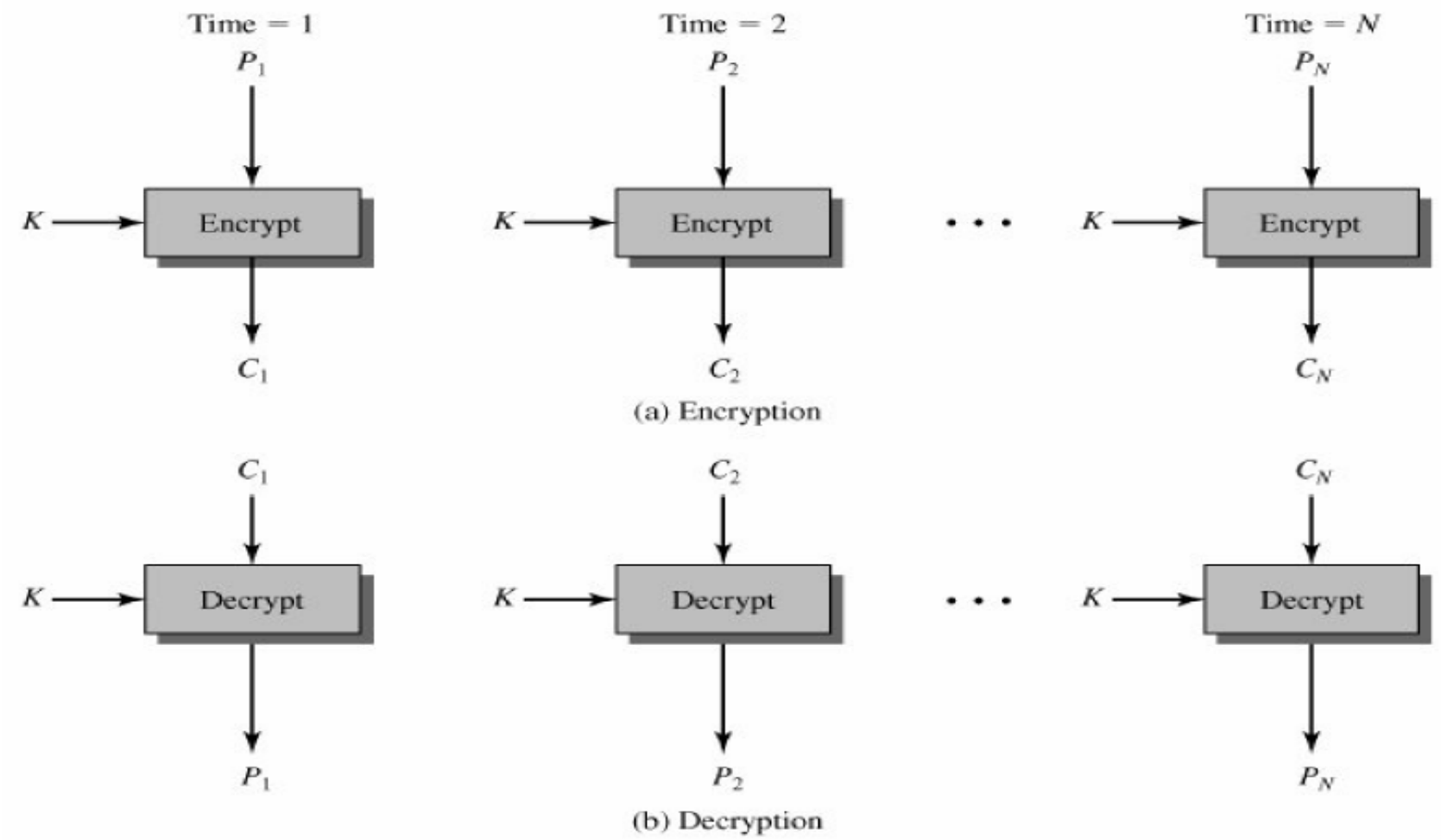
Introduction

- Block ciphers encrypt fixed-size blocks
  - e.g. DES encrypts 64-bit blocks, AES encrypts 128-bity blocks.
- We need some way to encrypt a message of arbitrary length .
- The plaintext message is broken into blocks, P_1, P_2, P_3, ...
- NIST defines several ways to do it
  - called **modes of operation**
- The last block may be short of a whole block
  - padding.

Introduction

- Modes of Operation:
  - Electronic codebook mode (ECB)
  - Cipher block chaining mode (CBC) – Most used
  - Output feedback mode (OFB)
  - Cipher feedback mode (CFB)
  - Counter mode (CTR)

Electronic Code Book



ECB

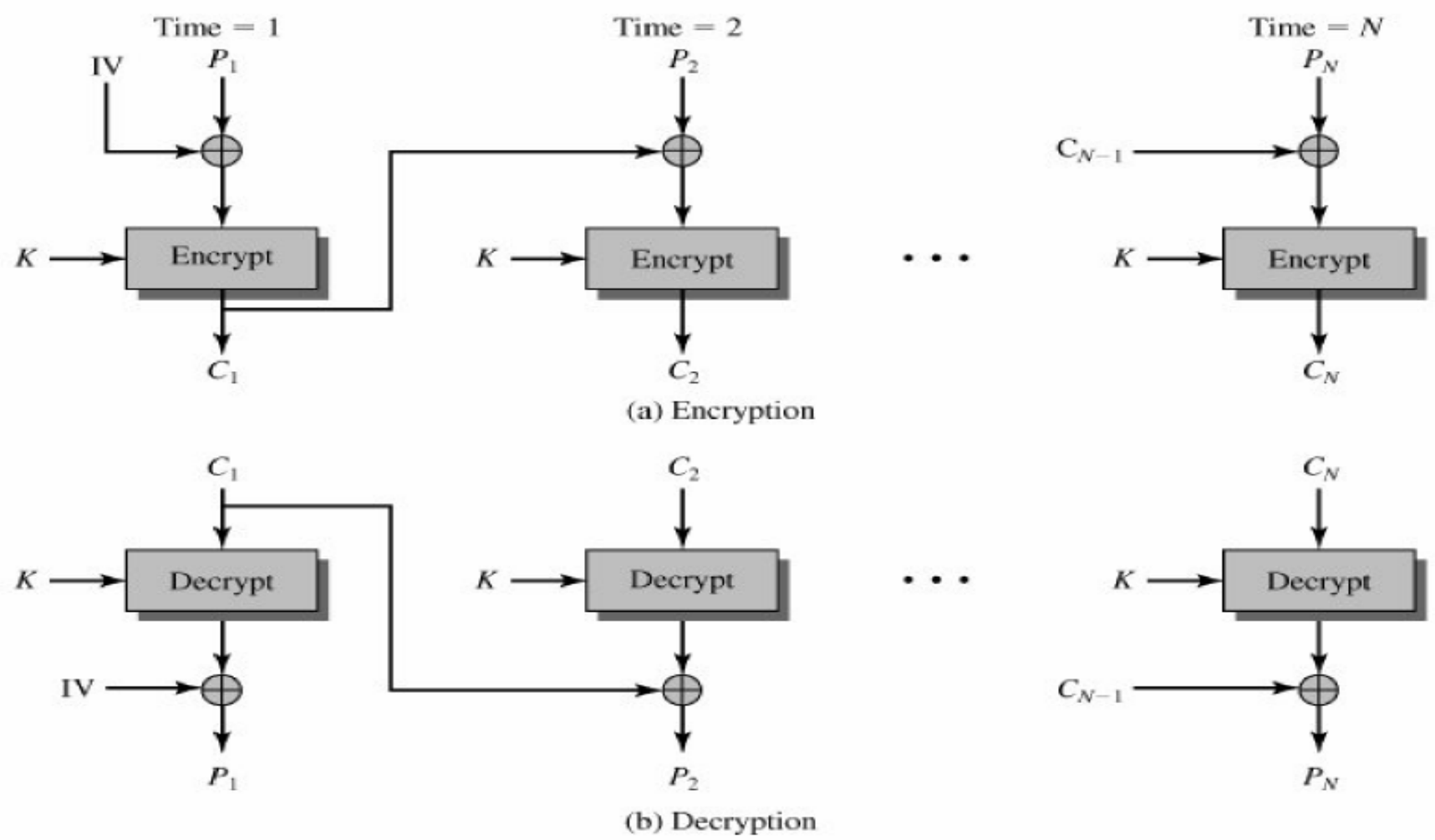
Strength

- it's simple

Weakness

- In the ECB mode, under a given key, any given plaintext block always gets encrypted to the same ciphertext block.
- Repetitive information contained in the plaintext may show in the ciphertext

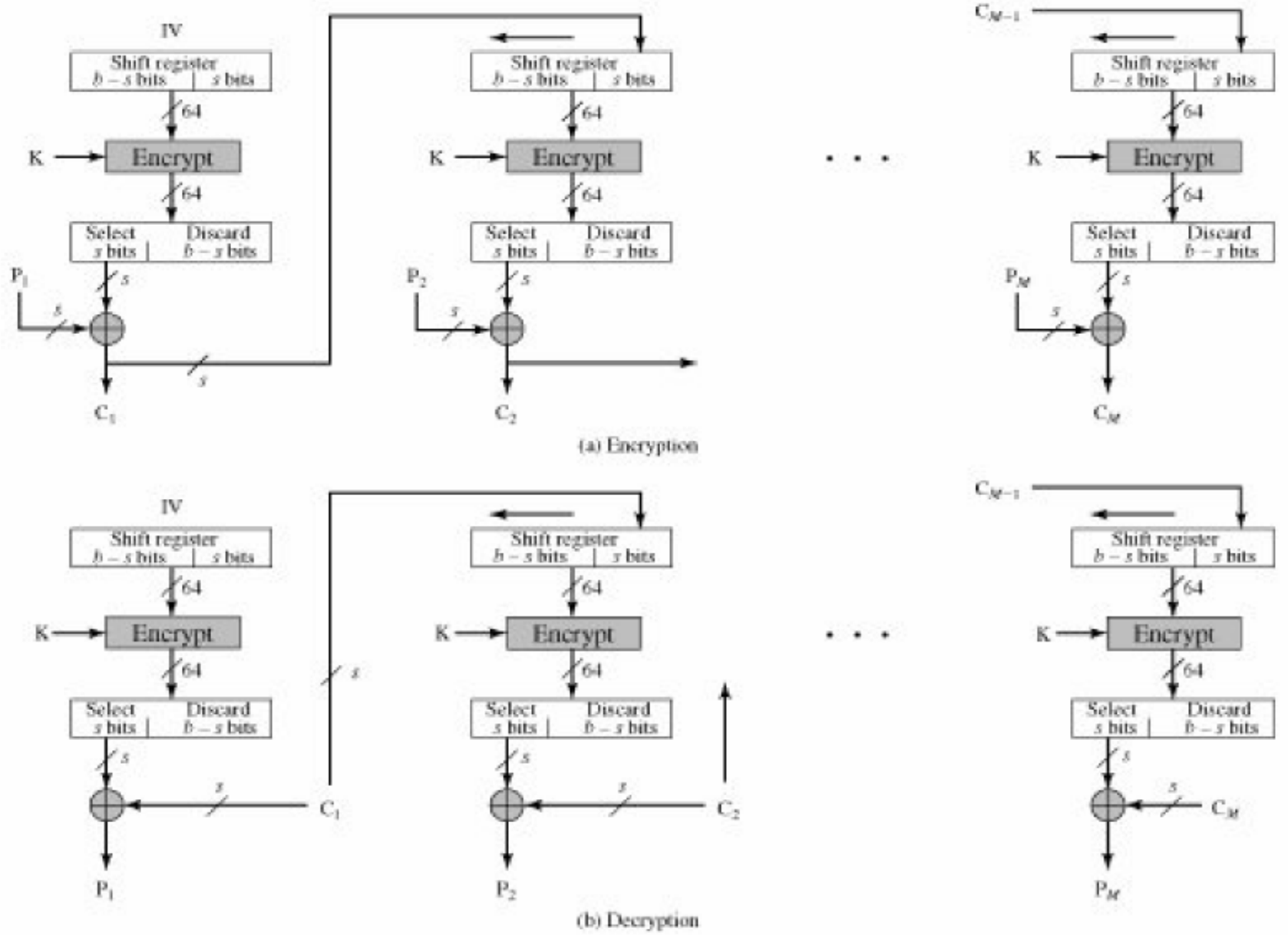
Cipher Block Chaining



CBC

- Each plaintext blocks is Xored (chained) with the previous ciphertext block before encryption
- Use an initial Vetor (IV) to start the process
  - Must be known to both the sender & receiver
  - Typically, IV is either a fixed value or is sent encrypted in ECB mode before the rest of ciphertext.
- The encryption of a block depends on the current and **all** blocks before it.

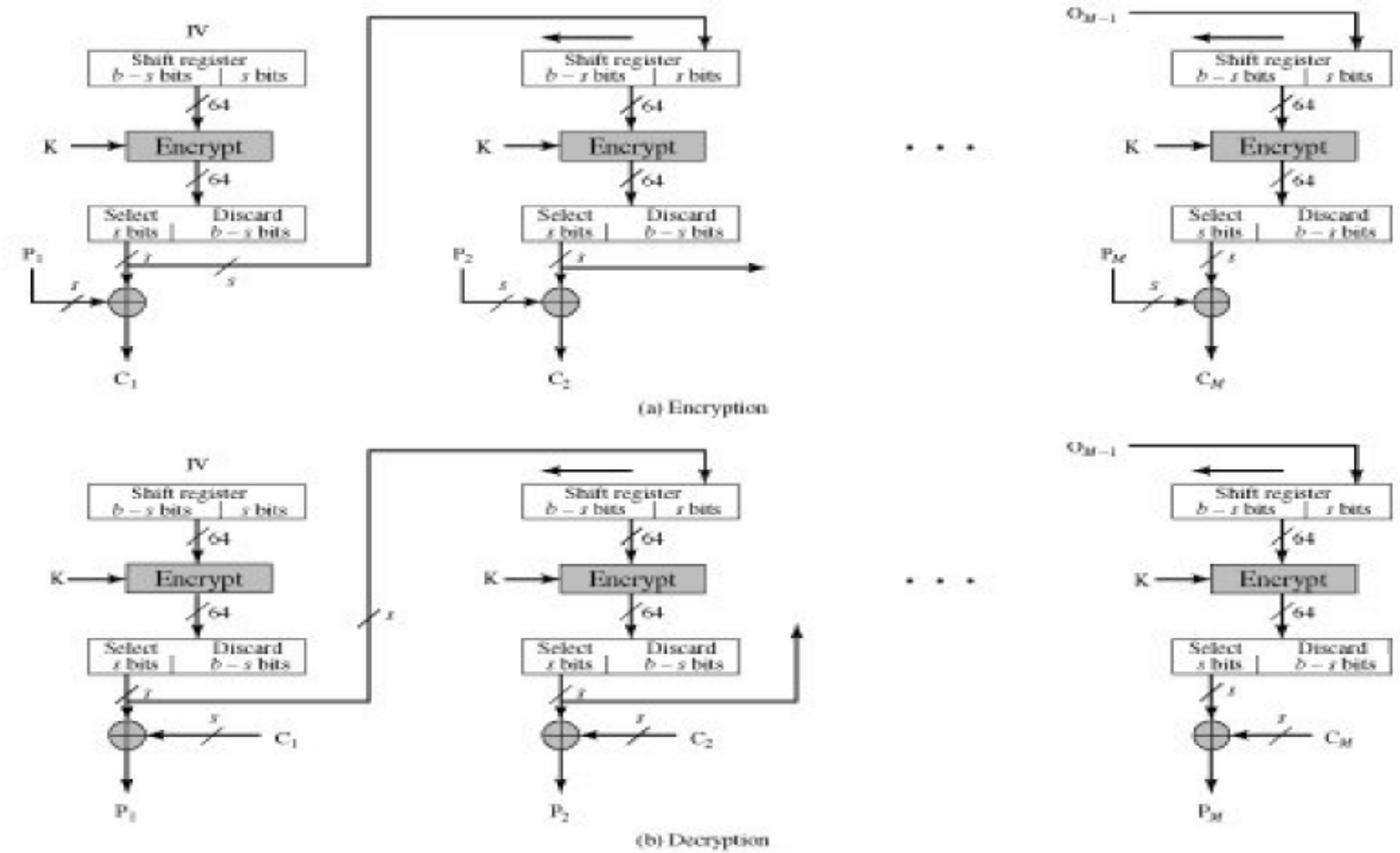
Cipher Feedback Mode



CFB

- In CFB encryption, like CBC encryption, the input block to each forward cipher function (except the first) depends on the result of the previous forward cipher function.
- Multiple forward cipher operations cannot be performed in parallel.
- Appropriate when data arrives in bits/bytes.
- s can be any value; a common value is s = 8.
- A ciphertext segment depends on the current and all preceding plaintext segments.

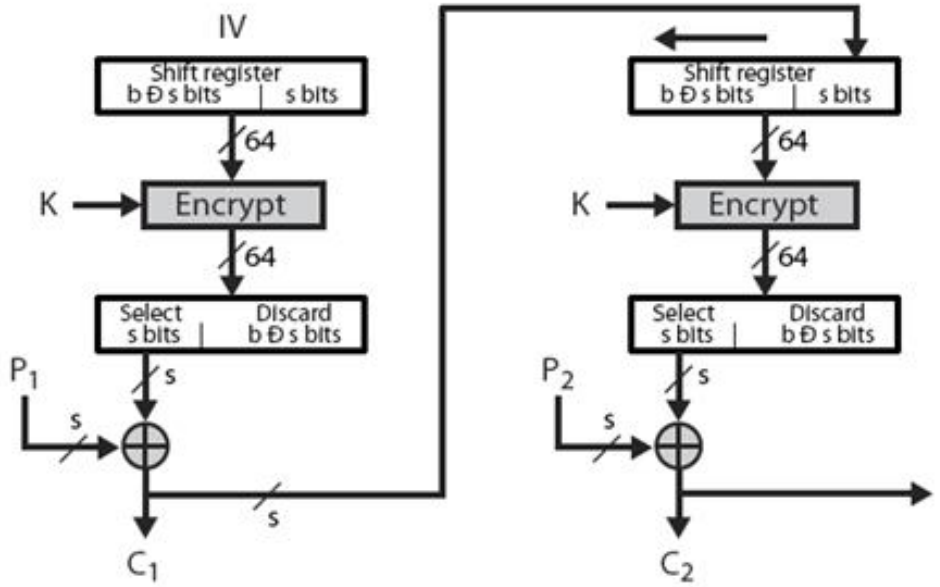
Output Feedback Mode



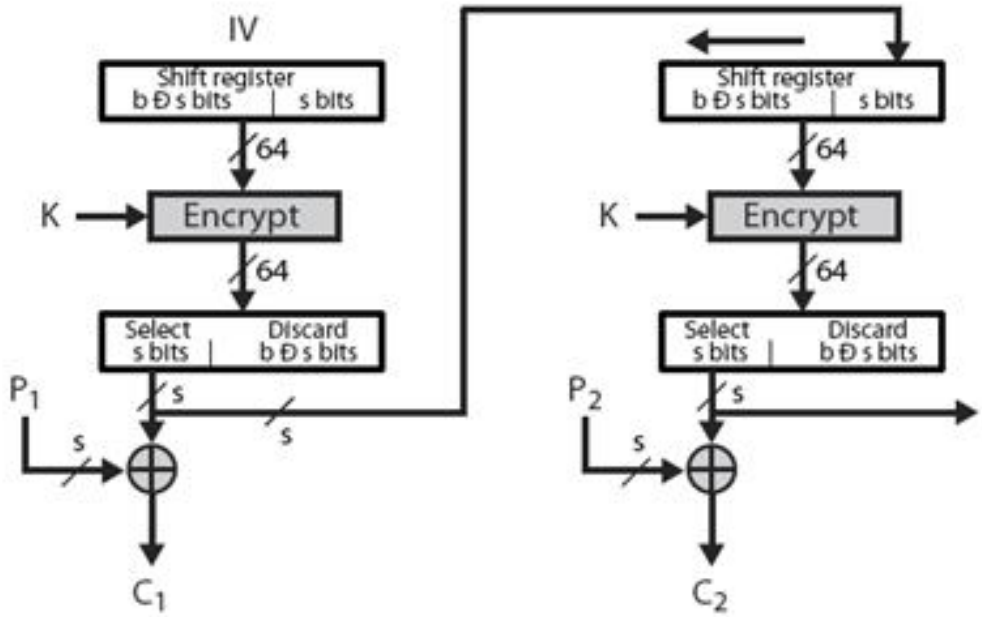
OFB

- The output feedback (OFB) mode is similar in structure to that of CFB it is the output of the encryption function that is fed back to the shift register in OFB, whereas in CFB the ciphertext unit is fed back to the shift register.

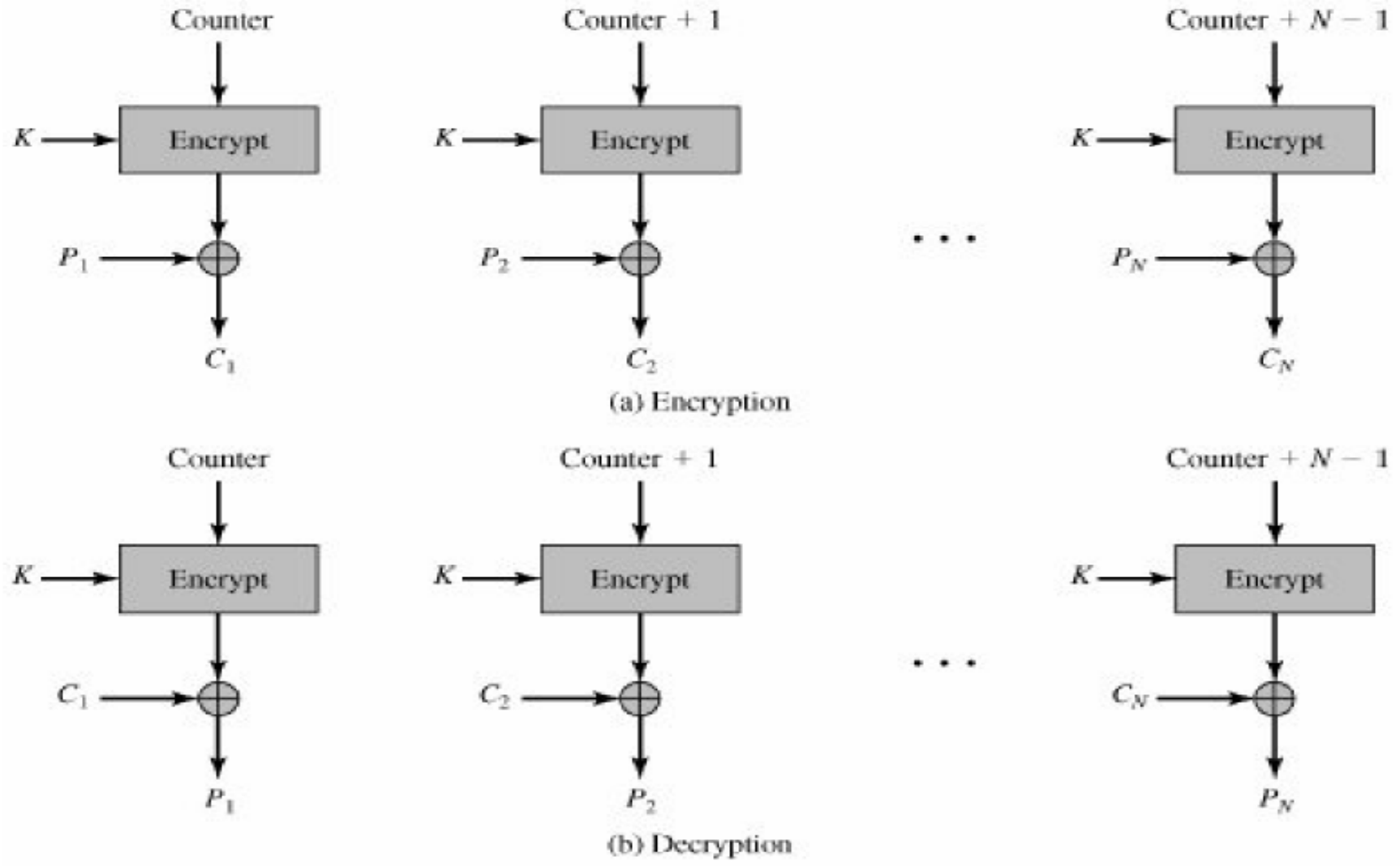
Cipher Feedback



Output Feedback



Counter Mode



Ctr Mode

- Needs only the encryption algorithm
- Fast encryption/decryption; blocks can be processed (encrypted or decrypted) in parallel; good for high speed links
- Random access to encrypted data blocks

Bits Error

Mode	Effect of Bit Errors in C_j	Effect of Bit Errors in the IV
ECB	RBE in the decryption of C_j	Not applicable
CBC	RBE in the decryption of C_j SBE in the decryption of C_{j-1}	SBE in the decryption of C_1
CFB	SBE in the decryption of C_j RBE in the decryption of $C_{j+1},\ldots,C_{j+b/s}$	RBE in the decryption of $C_1, C_2, \ldots, C_j$ for some j between 1 and b/s
OFB	SBE in the decryption of C_j	RBE in the decryption of $C_1, C_2, \ldots, C_n$
CTR	SBE in the decryption of C_j	Not applicable *

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *j* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Example

- With the ECB mode of DES, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates.
- Show the propagation error If an error occurs in the transmitted *C*1
  - It corrupts *P*1 and *P*2.
- Are any blocks beyond *P*2 affected?
  - No. For example, suppose C1 is corrupted. The output block P3 depends only on the input blocks C2 and C3.
- Suppose that there is a bit error in the source version of *P*1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?
  - An error in P1 affects C1. But since C1 is input to the calculation of C2, C2 is affected. This effect carries through indefinitely, so that all ciphertext blocks are affected. However, at the receiving end, the decryption algorithm restores the correct plaintext for blocks except the one in error