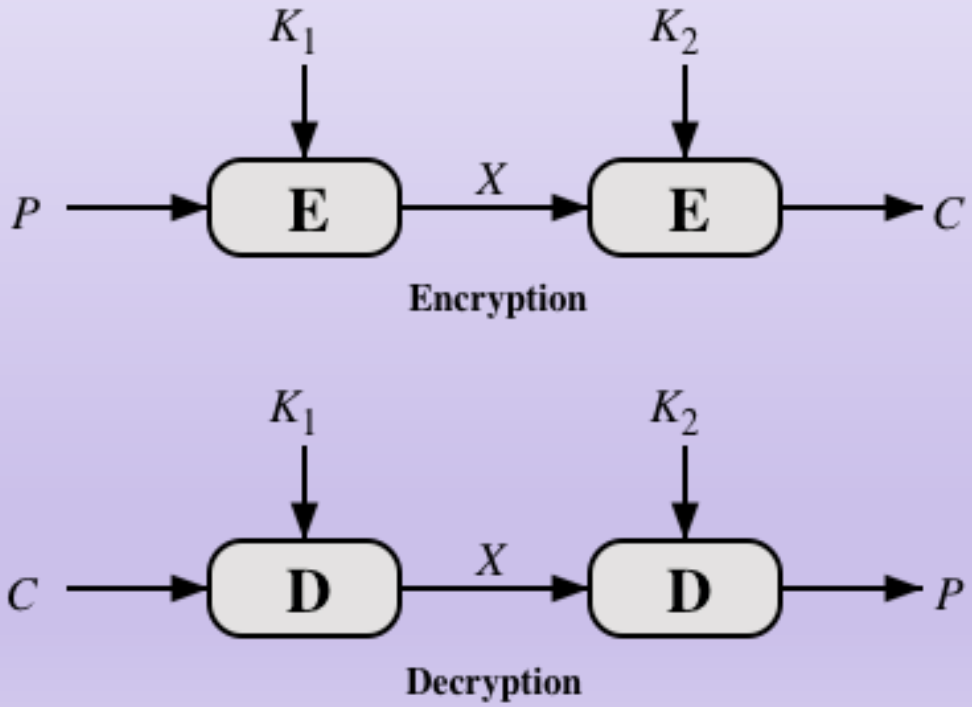
Chapter 7

Block Cipher Operation

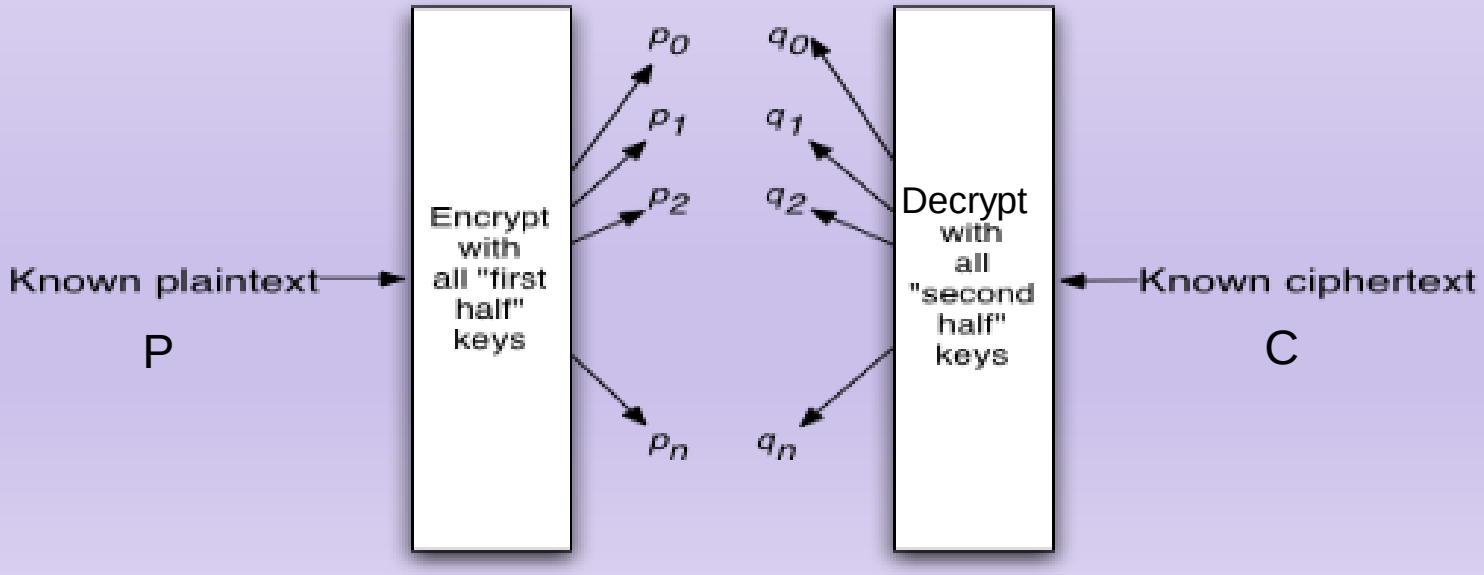
Double encryption

- If the key is too short, such as DES's 56-bit key, we can use multiple encryption

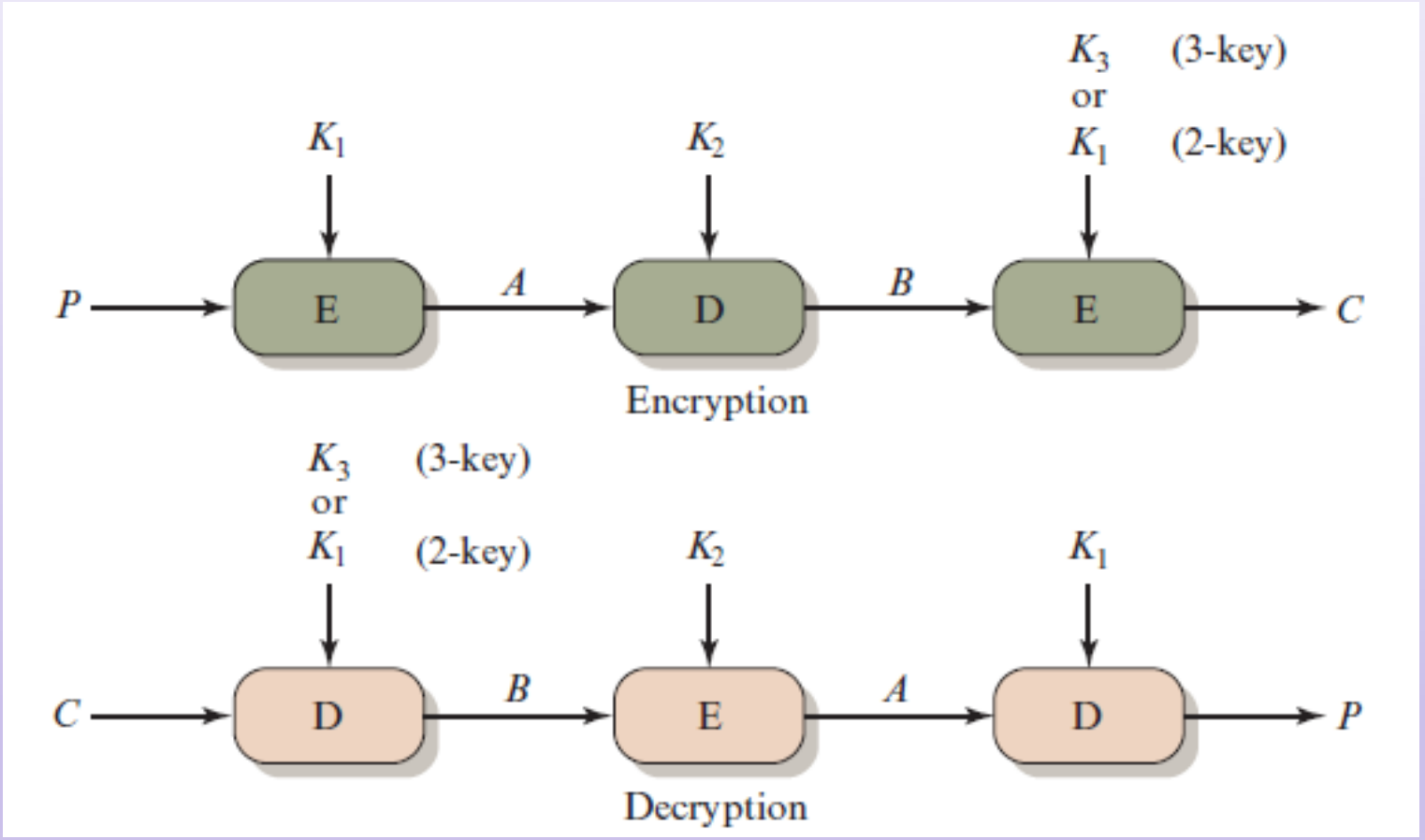


Double encryption: meet-in-the-middle attack

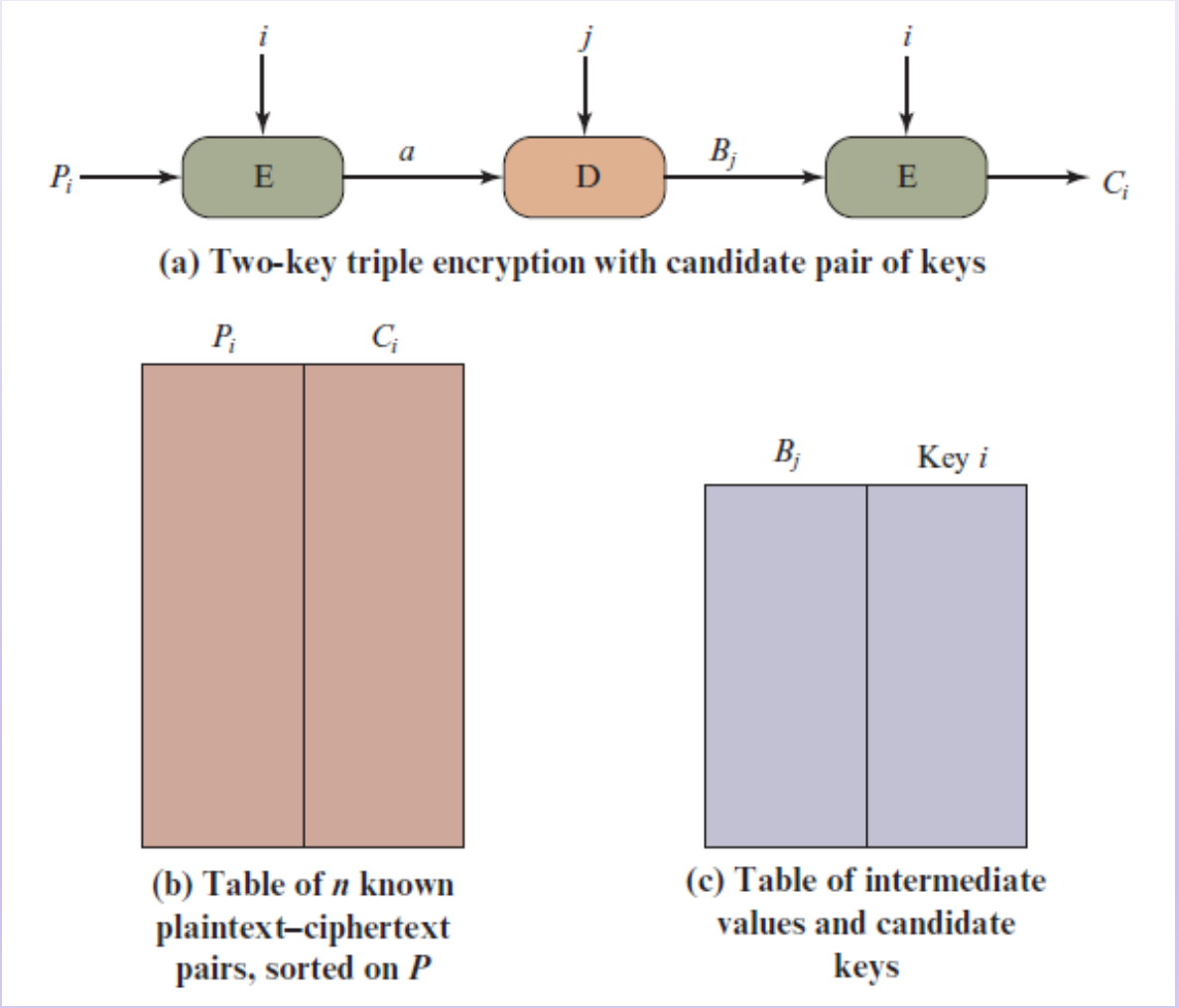
- Known plaintext attack: given (P, C)
  - Naïve attack: try all possible K_1 and K_2 to test $E(E(P, K_1), K_2) = C$.
  - It takes 2^{112} tries
- Meet-in-the-middle-attack: complexity is 2×2^{56}



Triple encryption



Triple encryption: known plaintext attack



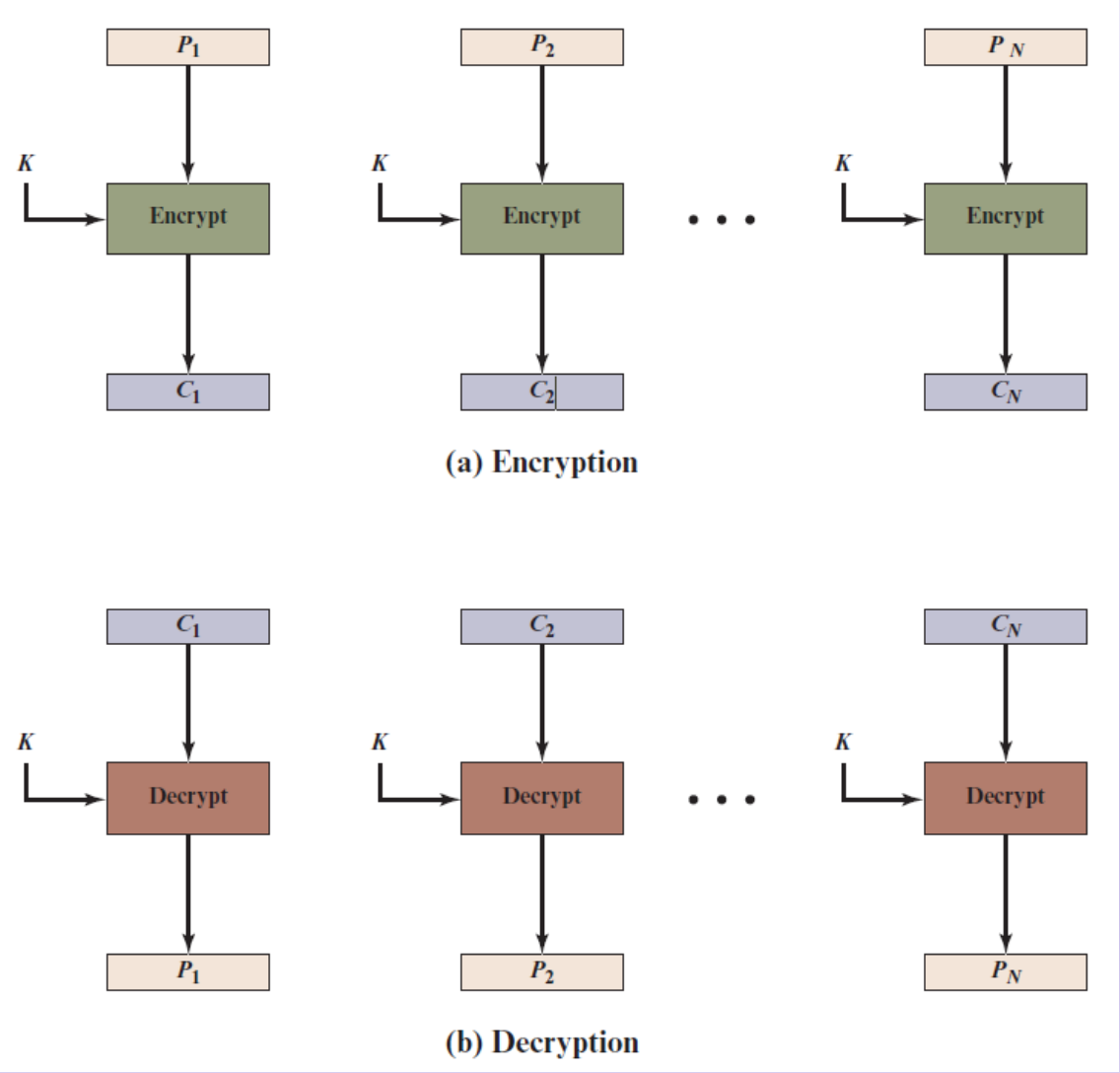
- Pick a random ciphertext 'a'
  - For each possible key i for K_1, compute $P = D(i, a)$
    If (P, C) is in the table A, put $(D(i, C), i)$ into table B
  - This i is a candidate for K_1
- For each possible j for K_2, if $(D(j, a), i)$ is in table B, then (i, j) is a candidate for (K_1, K_2)
- Analysis
  - For n pairs of given (P, C), a correct guess for a is $n/2^{64}$ for a pair (P, C). Thus, the expected number of guesses to get a correct a is $2^{64}/n$
  - For each such guess, it takes 2^{56} to search K_2
  - So, the expected time of attack is $(2^{64}/n) \times (2^{56}) = 2^{120}/n$

Modes of operation

- Purposes
  - Enhance usage and security
  - Adaption for other applications, such as cipher ciphers
- For encryption, a message P is padded into a special form such that the length of padded message is a multiple of block length
  - Zero-padding: $P' = P||100 \cdots 0$
- A padded message P' is partitioned into full blocks $P_1 P_2 \ldots P_n$
- NIST defines 5 modes for block encryption
  - ECB, CBC, CFB, OFB, CTR

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 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 block of plaintext and the preceding block of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* 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 encryption output, and full blocks are used.	• 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

ECB mode

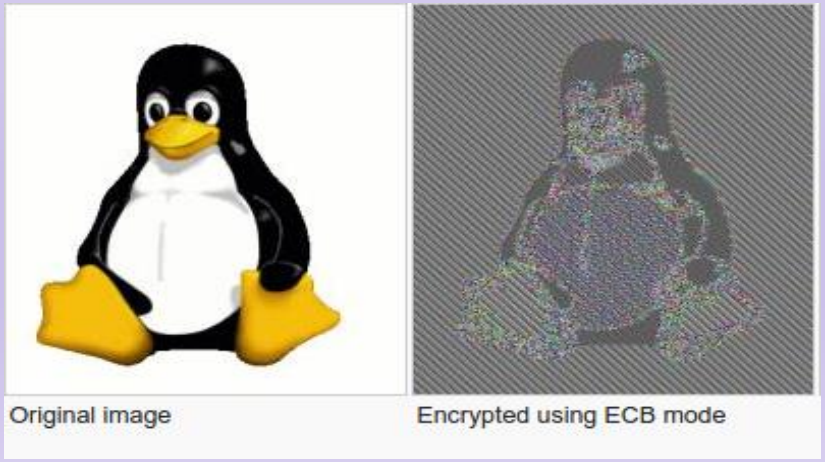

P_1
P_2
P_N
K
Encrypt
C_1
C_2
C_N
(a) Encryption
C_1
C_2
C_N
K
Decrypt
P_1
P_2
P_N
(b) Decryption

ECB mode: properties

- No error propagation for erroneous and missing blocks

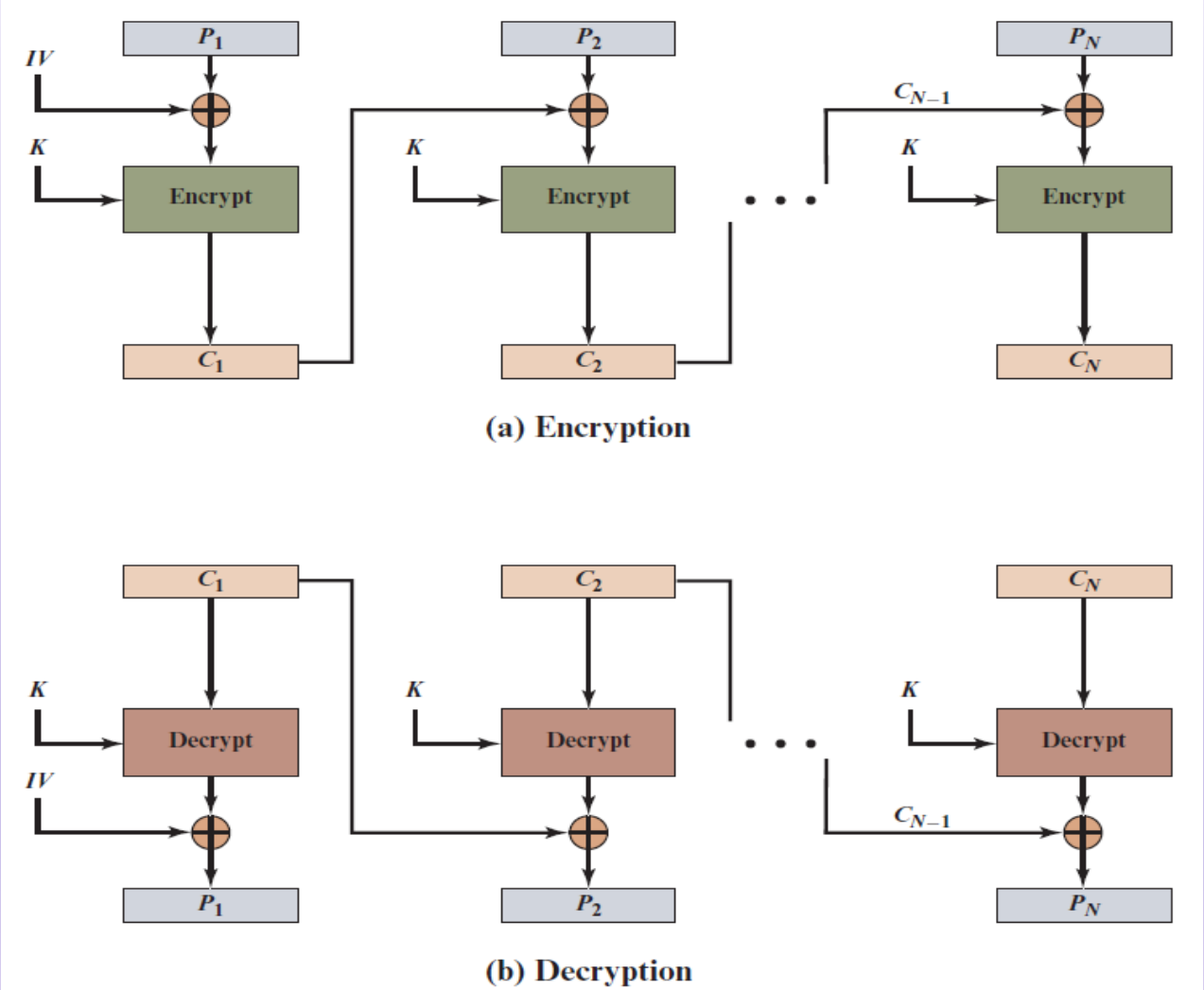
$$C_1\ C_2\ \dots\ C_{i-1}\ C_i'\ C_{i+1}\ C_{i+2}\ \dots\ C_n$$
$$\Rightarrow\ P_1\ P_2\ \dots\ P_{i-1}\ P_i'\ P_{i+1}\ P_{i+2}\ \dots\ P_n$$

- Cannot be parallelized
- Security problem: the same plaintext in different locations are encrypted into the same ciphertext



Original image | Encrypted using ECB mode

CBC mode

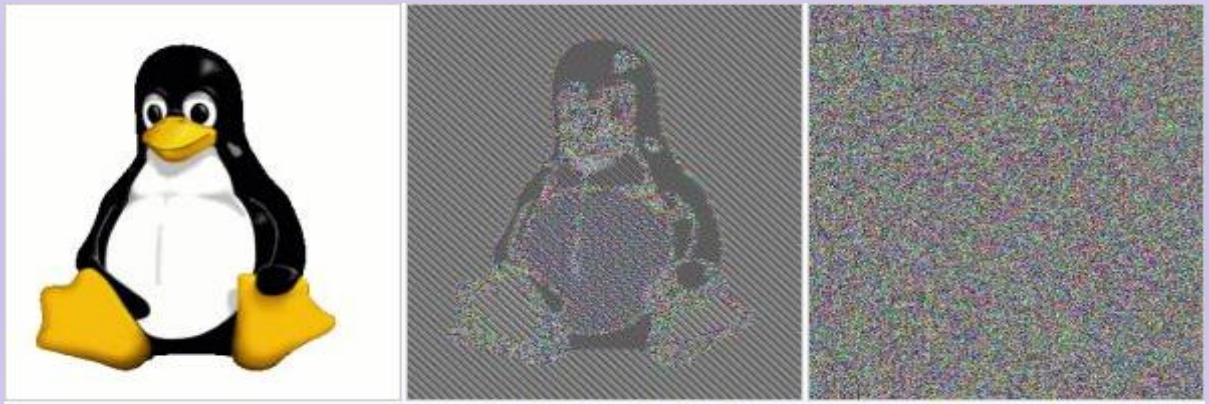

P_1
P_2
P_N
IV
K
Encrypt
C_{N-1}
C_1
C_2
C_N
(a) Encryption
Decrypt
(b) Decryption

CBC mode: properties

- Limited error propagation caused by erroneous and missing block

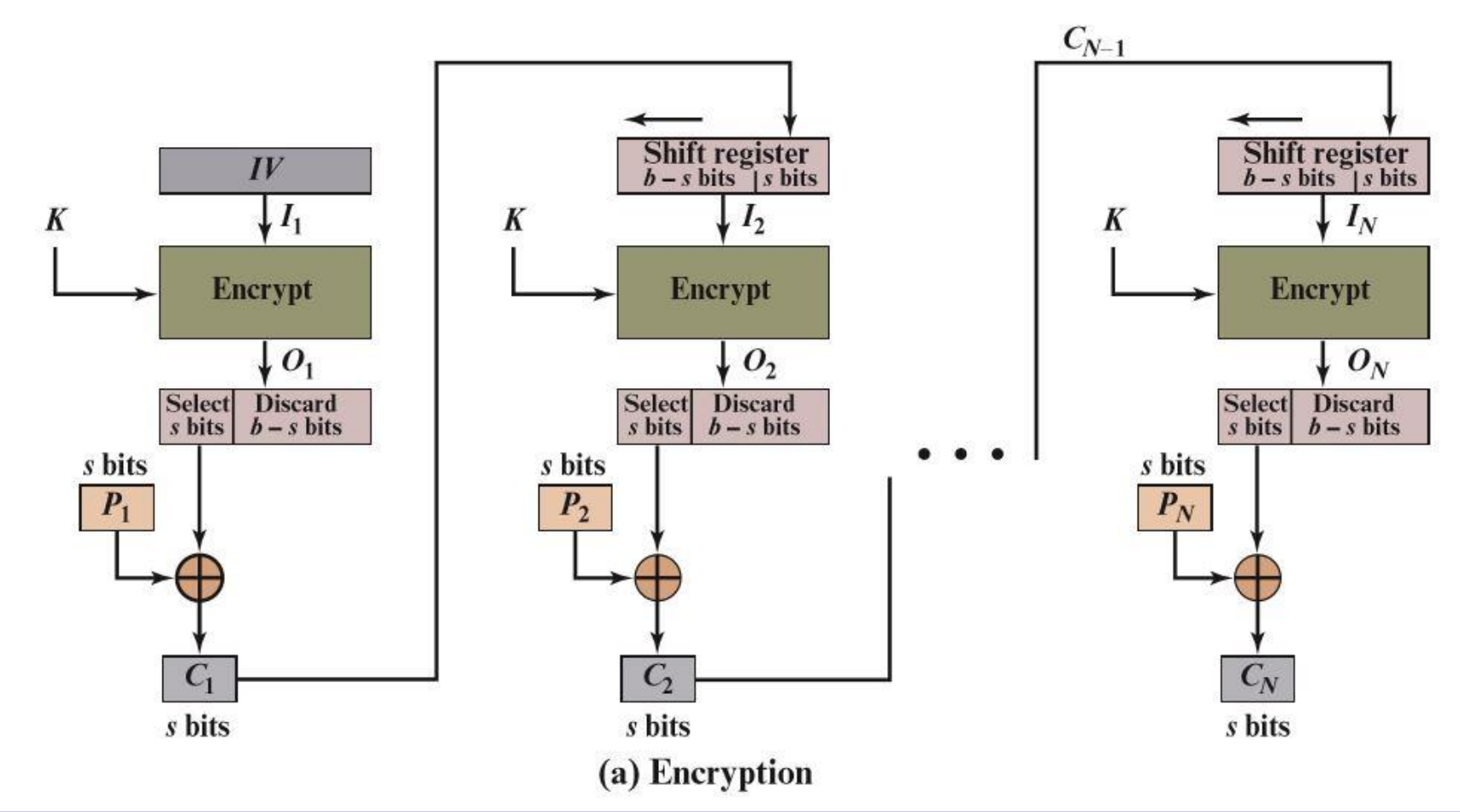
$$C_1 \; C_2 \; \dots \; C_{i-1} \; \cancel{C_i'} \; C_{i+1} \; C_{i+2} \; \dots \; C_n$$
$$\Rightarrow \quad P_1 \; P_2 \; \dots \; P_{i-1} \; \cancel{P_i'} \; P'_{i+1} \; P_{i+2} \; \dots \; P_n$$

- Cannot be parallelized
- The same plaintext in different locations are encrypted into different ciphertexts

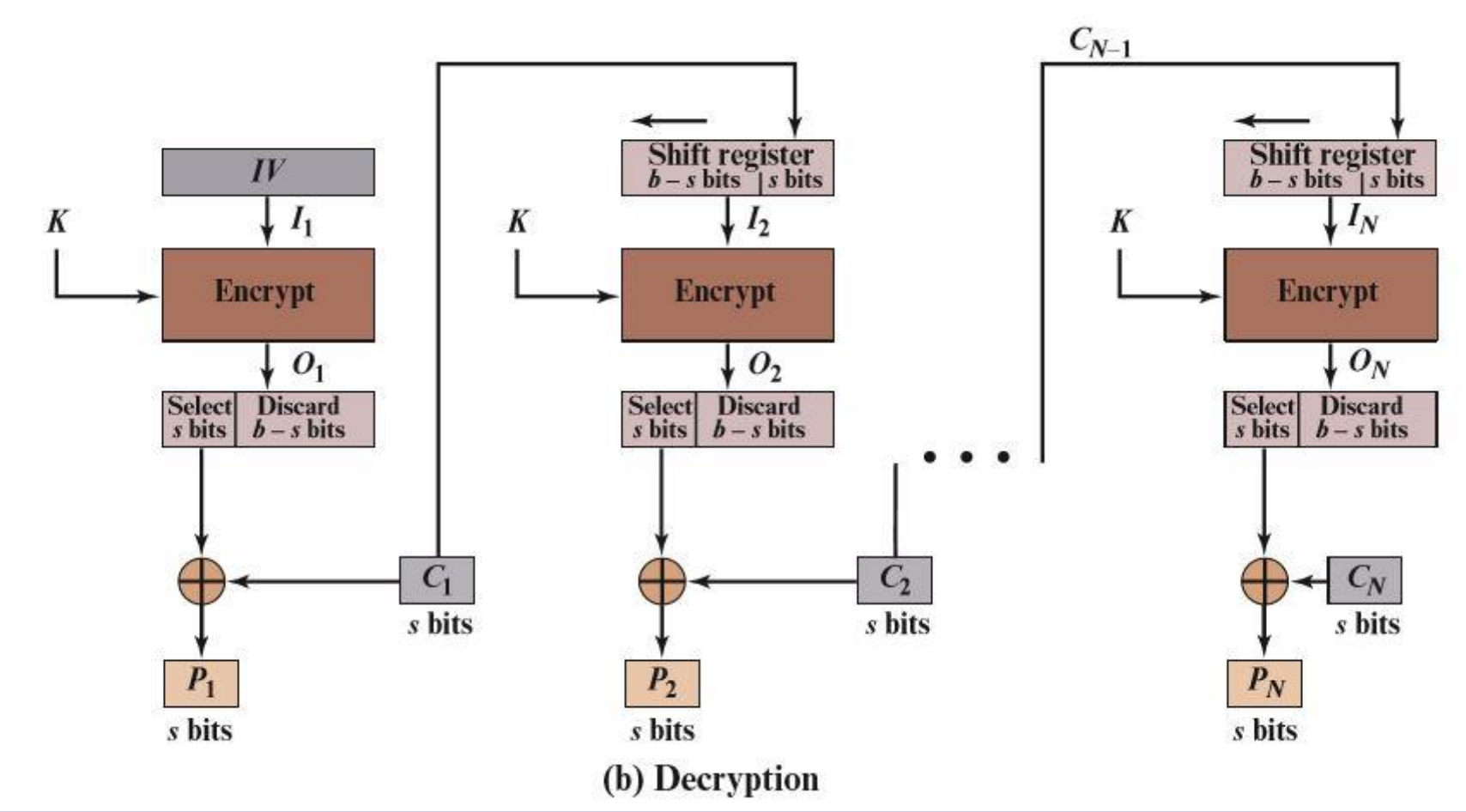


Original image | Encrypted using ECB mode | Modes other than ECB result in pseudo-randomness

CFB mode: encryption



CFB mode: decryption



(b) Decryption

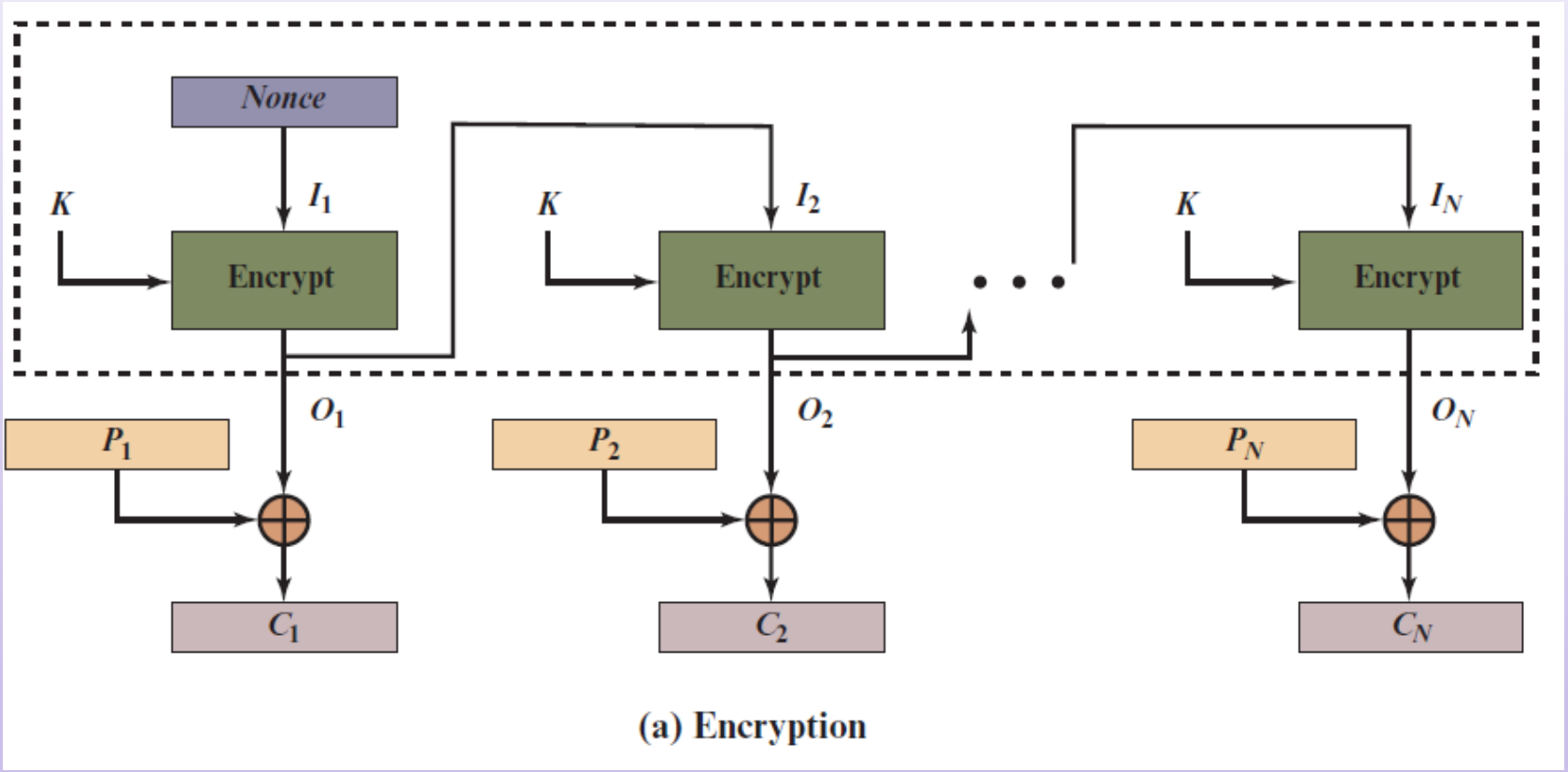
CFB mode: properties

- Limited error propagation caused by erroneous and missing block

$$\begin{array}{rl} & C_1\ C_2\ \ldots\ C_{i-1}\ \cancel{C_i'}\ C_{i+1}\ \ldots\ P_k\ P_{k+1}\ \ldots\ C_n \\ \Rightarrow & P_1\ P_2\ \ldots\ P_{i-1}\ \cancel{P_i'}\ P_{i+1}'\ \ldots\ P_k'\ P_{k+1}\ \ldots\ P_n \end{array}$$

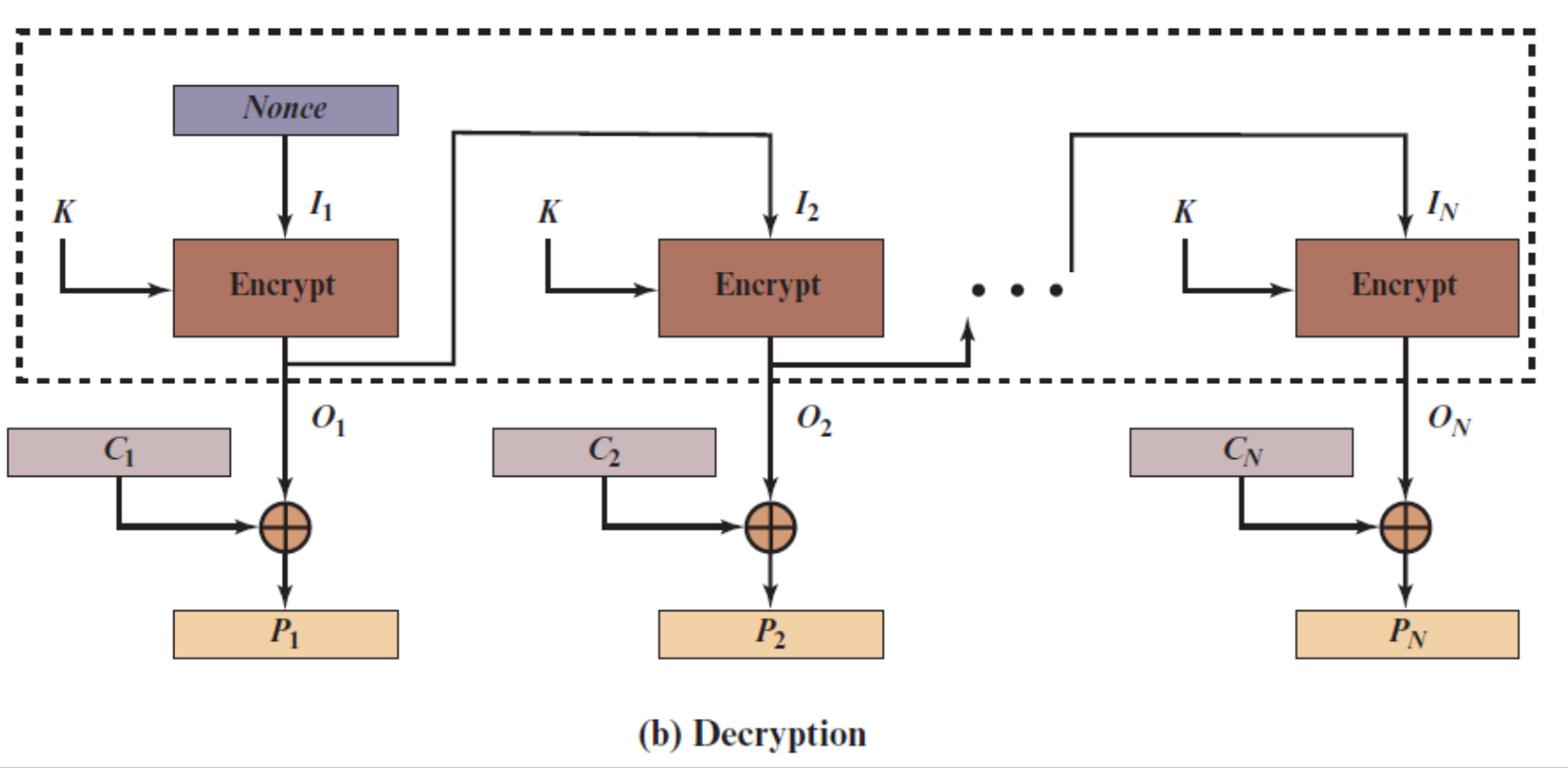
  - Example: AES and s=16, the number of propagated decryption errors is $128/16 + 1 = 9$ blocks
- Cannot be parallelized
- Used as a stream cipher?
  - Not typical since the key stream depends on ciphertexts

OFB mode: encryption



(a) Encryption

OFB mode: decryption

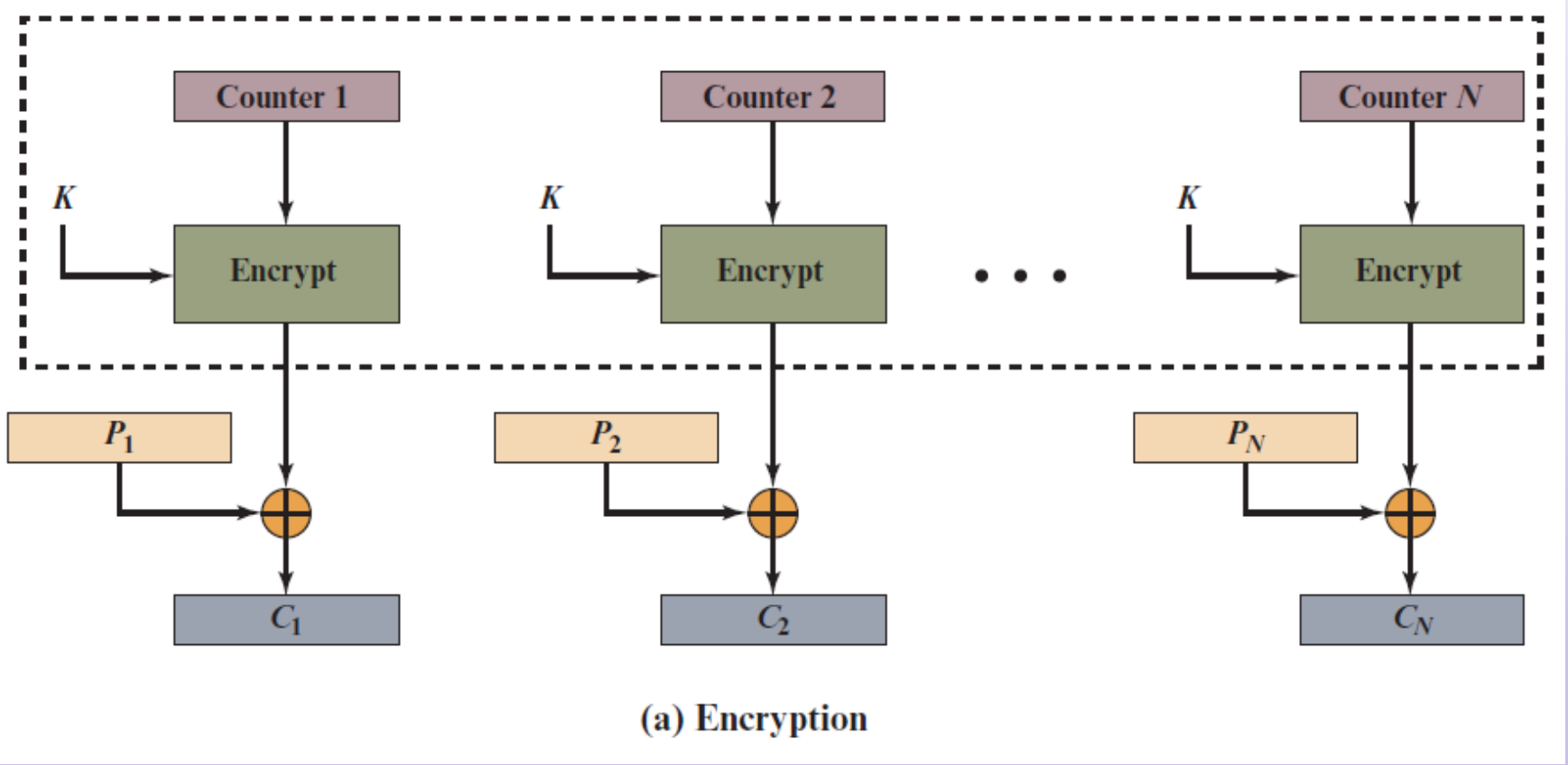


(b) Decryption

OFB mode: properties

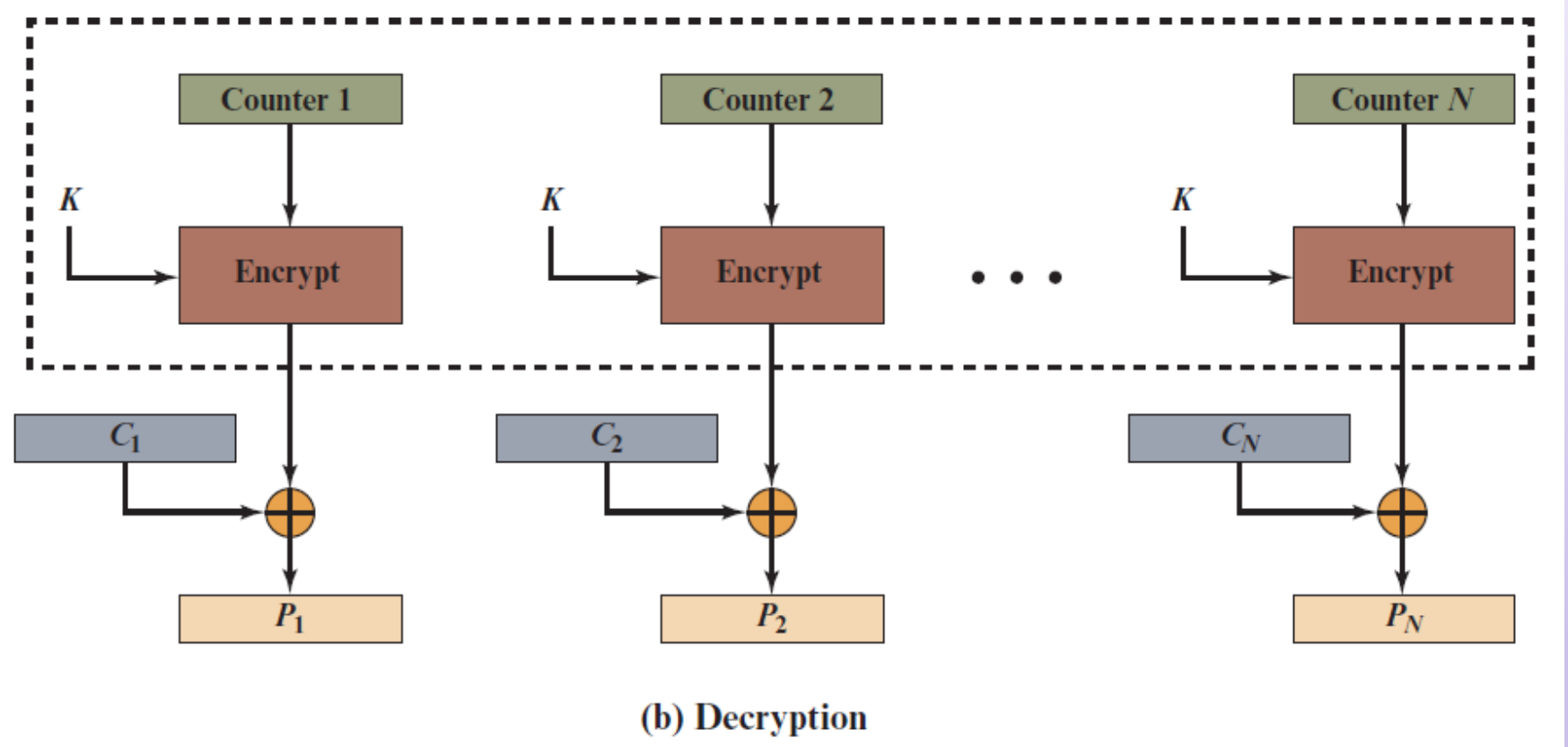
- No error propagation caused by erroneous block
- Serious error propagation caused by missing block
  - If C_i is missed, all decrypted message blocks $P'_i, P'_{i+1}, \ldots, P'_n$ are incorrect
- O_1, O_2, ... can be computed in advance.
- Cannot be parallelized
- Can be used as a stream cipher

CTR mode: encryption



(a) Encryption

CTR mode: decryption



(b) Decryption

CTR mode: properties

- No error propagation caused by erroneous block
- Serious error propagation caused by missing block
- Advantages
  - Hardware efficiency
  - Software efficiency
  - Pre-processing
  - Can be parallelized
  - Random access
  - Provable security
  - Simplicity
- Can be used as a stream cipher

Feedback characteristics