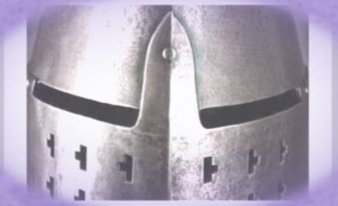


Chapter 7

Block Cipher Operation

Padding

- Plaintext is not a multiple of block length
- P → P’: P is padded to P’ that is a multiple of block length
- P’→P: automatic de-padding without ambiguity
- Padding standards: even though P has multiple block length, it still needs to be padded.

Zeros bit padding

Example

- | DD DD DD DD DD DD DD DD | DD DD DD DD D0010 00_H 00_H 00_H|
- | DD DD DD DD DD DD DD DD | 10000000 00_H 00_H 00_H 00_H 00_H 00_H 00_H |

Zeros byte padding

Example

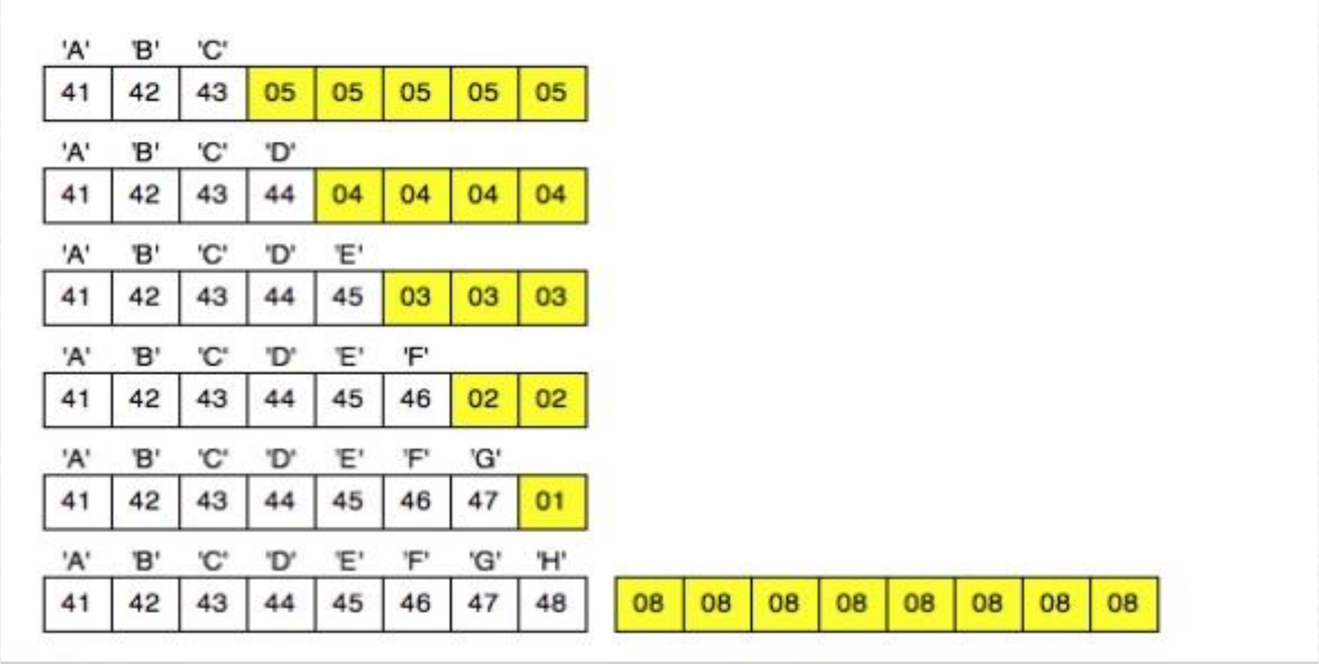
- | DD DD DD DD DD DD DD DD | DD DD DD 00_H 00_H 00_H 00_H 00_H |
- | DD DD DD DD DD DD DD DD | 00_H 00_H 00_H 00_H 00_H 00_H 00_H 00_H |

Problem

- The original plaintext may not be recovered exactly

PKCS#5, PKCS#7

- PKCS#5 is only used for block size = 8 bytes.
- PKCS#7 is used for block size = 1 byte to 255 bytes



'A'	'B'	'C'					
41	42	43	05	05	05	05	05

'A'	'B'	'C'	'D'				
41	42	43	44	04	04	04	04

'A'	'B'	'C'	'D'	'E'			
41	42	43	44	45	03	03	03

'A'	'B'	'C'	'D'	'E'	'F'		
41	42	43	44	45	46	02	02

'A'	'B'	'C'	'D'	'E'	'F'	'G'	
41	42	43	44	45	46	47	01

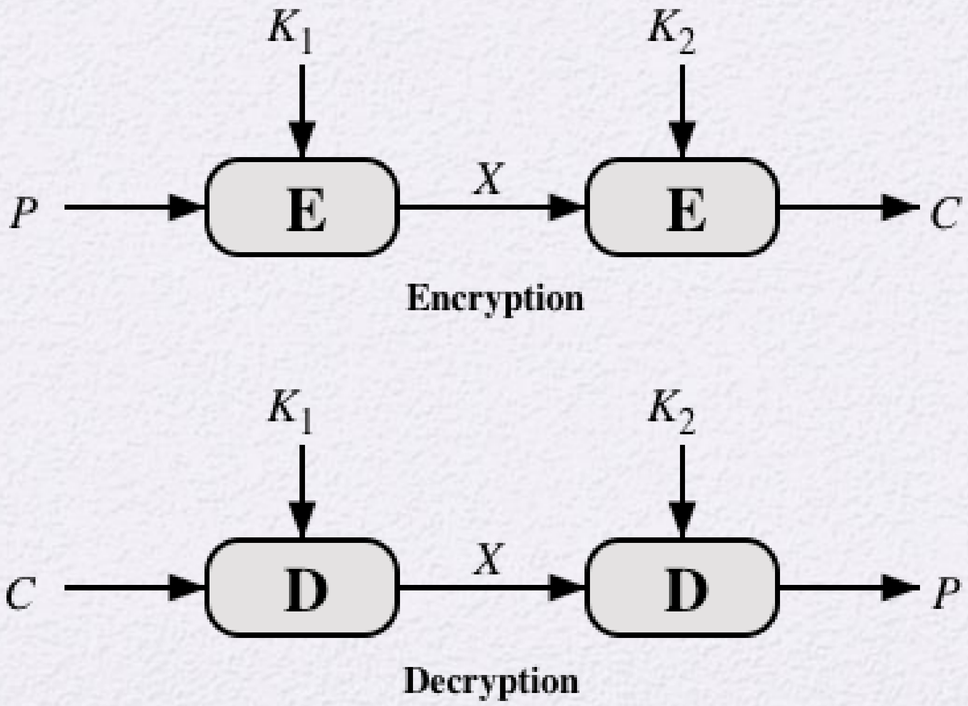
'A'	'B'	'C'	'D'	'E'	'F'	'G'	'H'								
41	42	43	44	45	46	47	48	08	08	08	08	08	08	08	08

ANSI X9.23, ISO 10126

- ANSI X9.23
  - |DD DD DD DD DD DD DD DD | DD 00 00 00 00 00 00 **07**|
  - The last byte is the number of padded bytes and the rest are 00
- ISO 10126
  - |DD DD DD DD DD DD DD DD | DD 7D 2A 75 EF F8 EF **07**|
  - The last byte is the number of padded bytes and the rest are random

Double Encryption

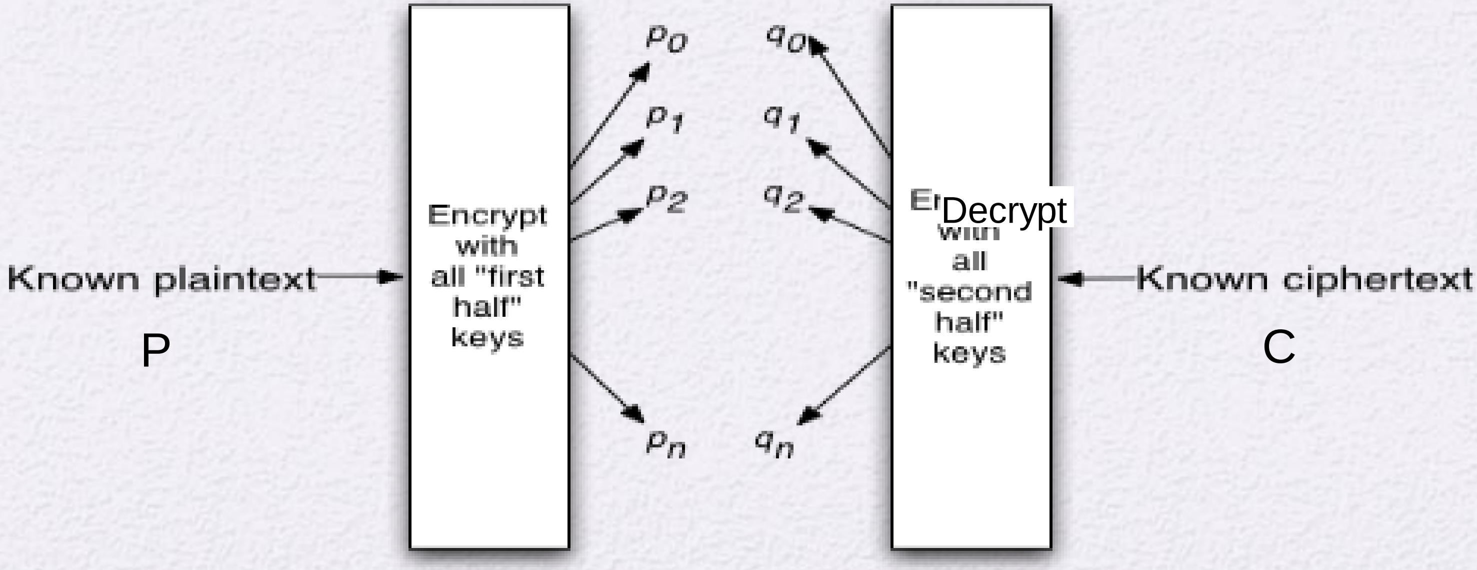
- If the key is too short, such as DES's 56-bit key, we can use multiple encryption



Meet-in-the-Middle Attack

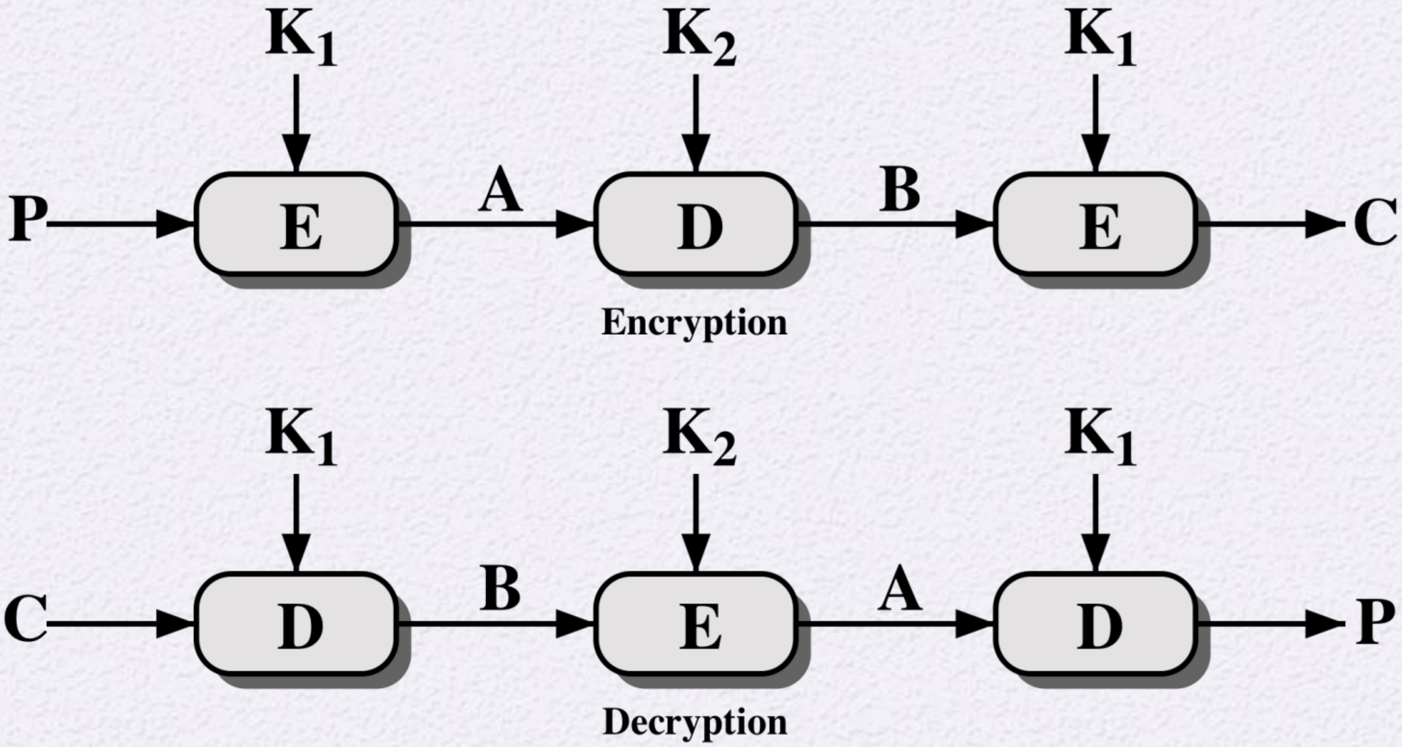
Known plaintext attack: given (P, C)

- Naïve attack: try all possible K_1 and K_2 to test $E(E(P, K_1), K_2)=C$.
- Better attack: attack complexity is $2x2^{56}$, not 2^{112}



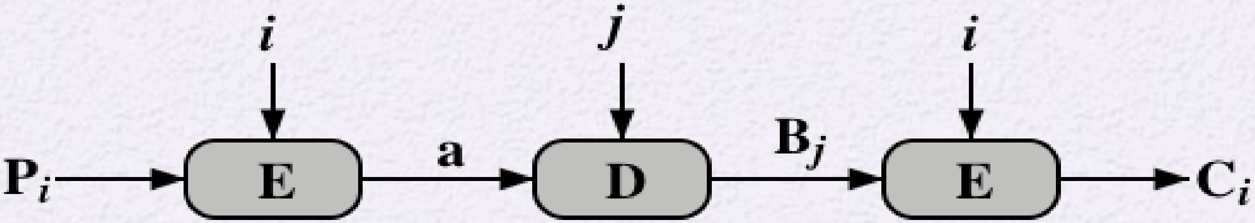
Triple-DES with Two-Keys

- To counter the meet-in-the-middle attack, we can use three stages of encryption with three different keys
  - The cost of the meet-in-the-middle attack is 2^{112}
  - Drawback : key length is 56 x 3 = 168 bits
- 3DES with two keys has been adopted for use in the key management standards ANSI X9.17 and ISO 8732

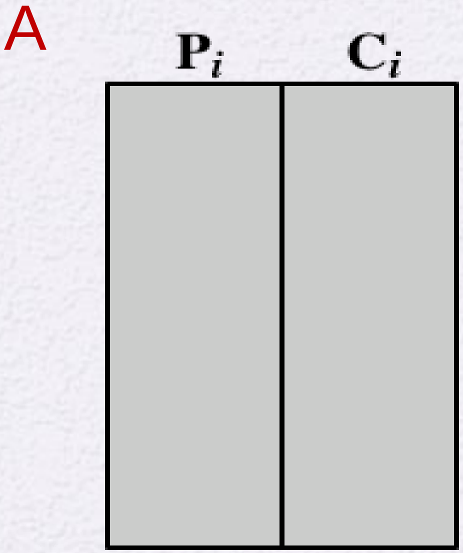


(b) Triple Encryption

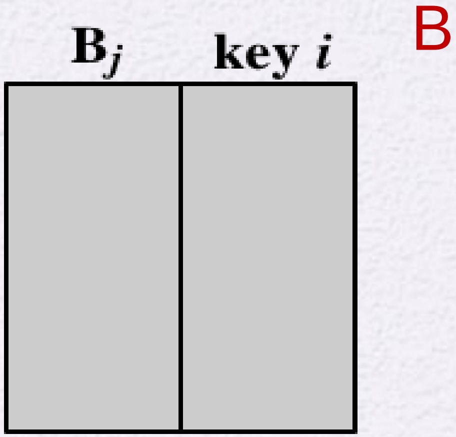
Known plaintext attack on 3DES



(a) Two-key Triple Encryption with Candidate Pair of Keys



(b) Table of n known plaintext-ciphertext pairs, sorted on P



(c) Table of intermediate values and candidate keys

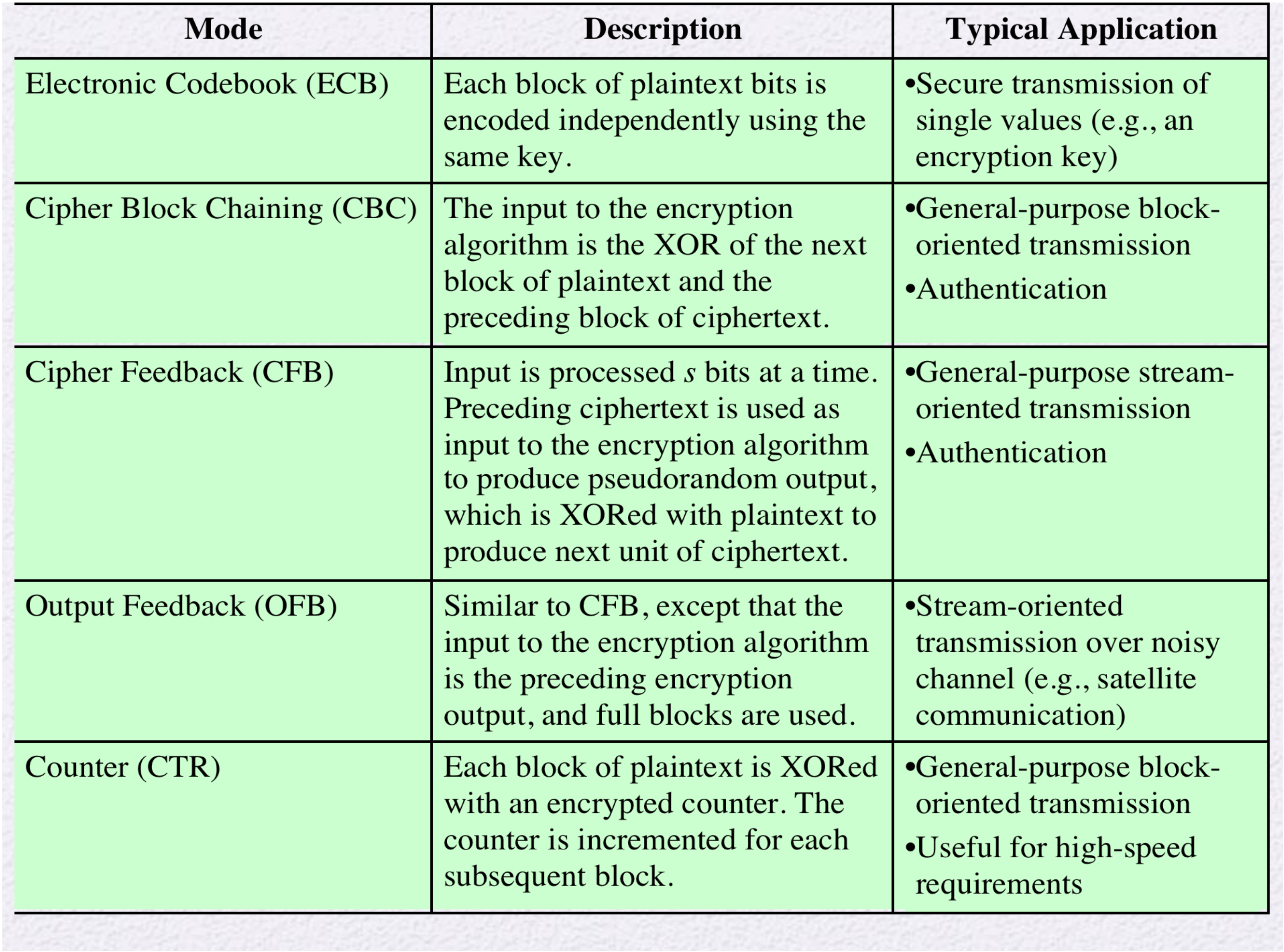
- Pick a random ciphertext ‘a’
  - For each possible key i for K_1, compute P=D(i, a). If (P, C) is in the table A, put (D(i, C), i) into table B
  - This “i” is a candidate for K_1
- For each possible j for K_2,
  - If (D(j, a), i) is in table B, then (i, j) is a candidate for (K_1, K_2)

Analysis

1. For n pairs of given (P, C), a correct guess for a is $n/2^{64}$. Thus, the expected number of guesses to get a correct a is $2^{64}/n$
2. For each such correct guess, it takes 2^{56} to search K_2.
3. So, the expected time of attack is $(2^{64}/n)x(2^{56}) = 2^{120}/n$.

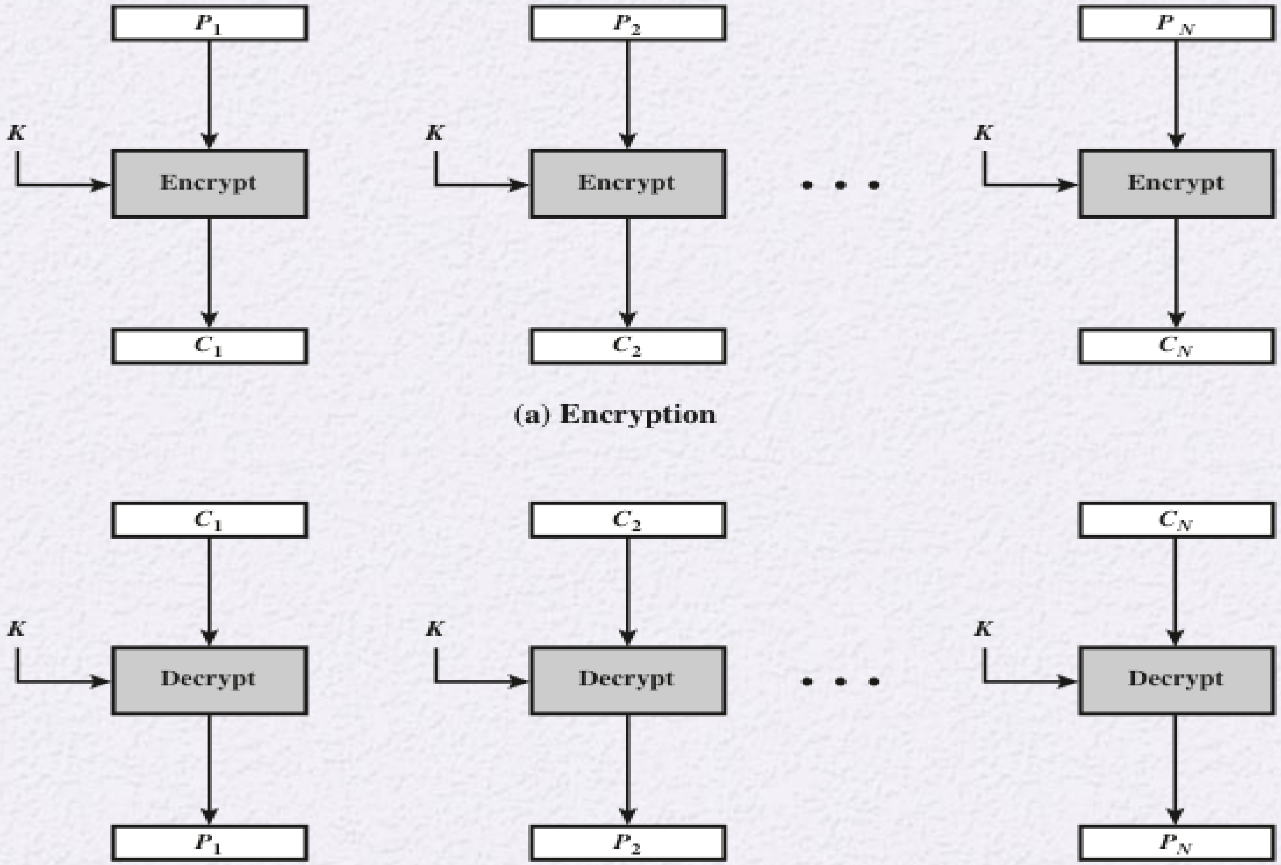
Modes of Operation

- For a block cipher to encrypt multiple blocks of a message.
- A technique for enhancing security and adapting for applications
- Five *modes of operations* have been defined by NIST



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

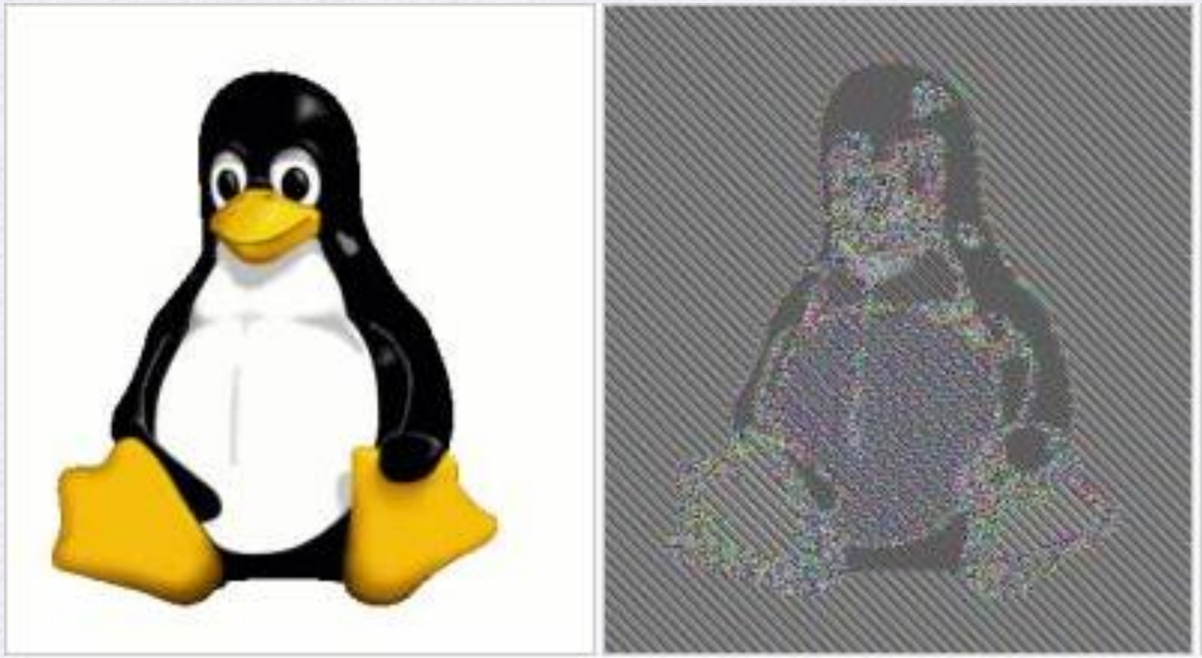
ECB mode



(a) Encryption

(b) Decryption

ECB mode problem



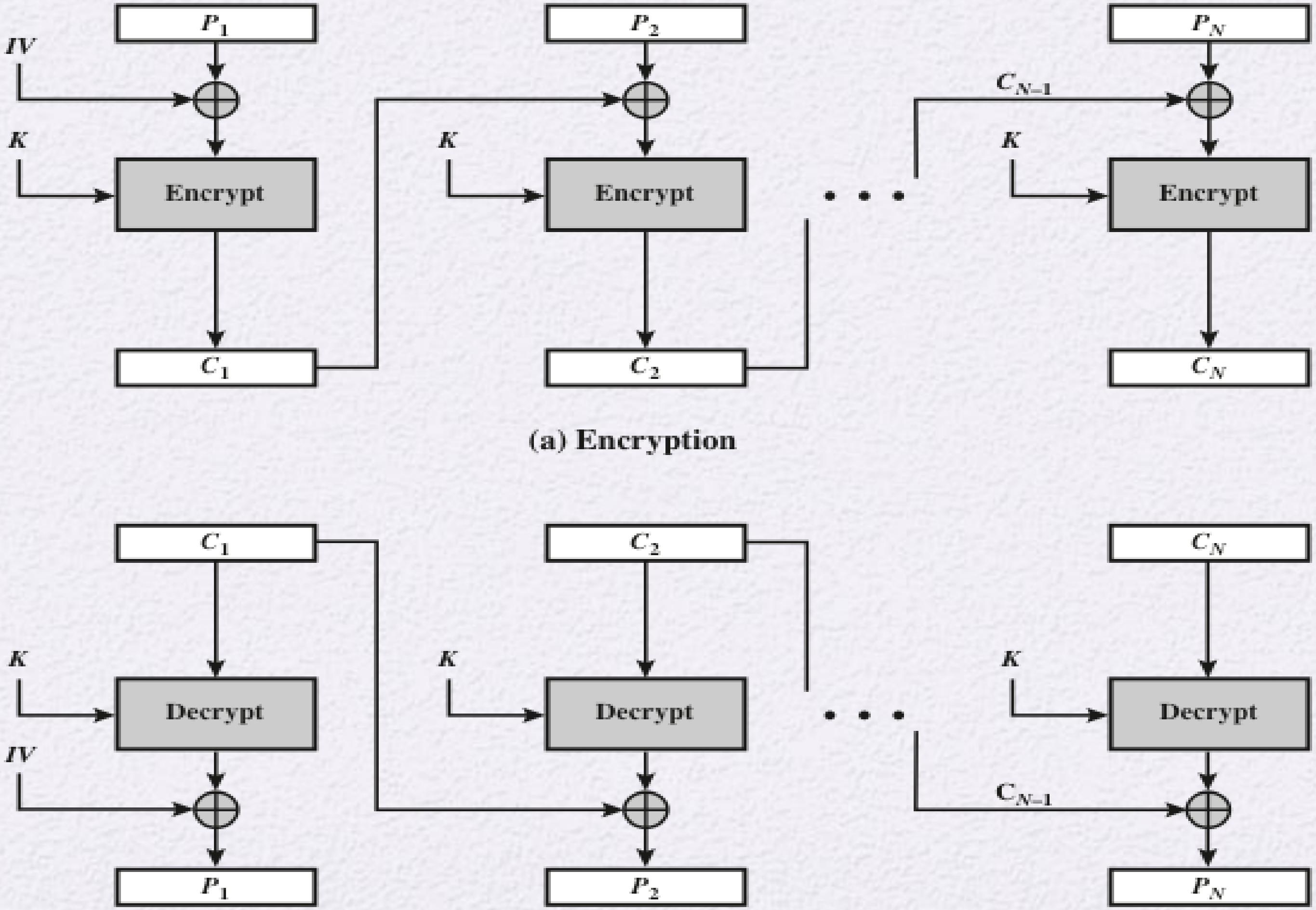
Original image

Encrypted using ECB mode

Design Factors

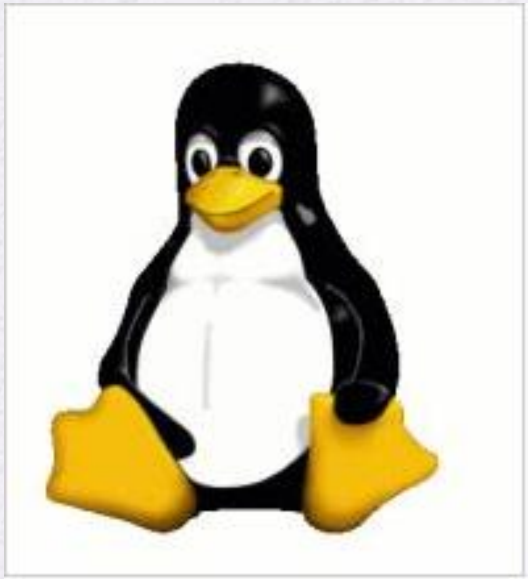
- Performance
  - Overhead
  - Parallelizable
- Error recovery
- Error propagation
- Diffusion
- Security

CBC mode

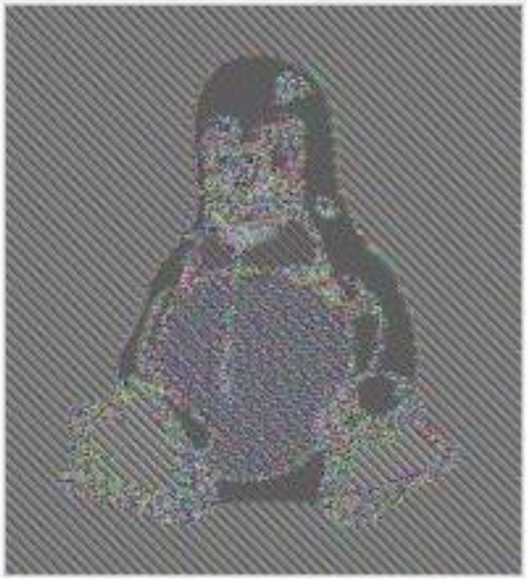


(a) Encryption

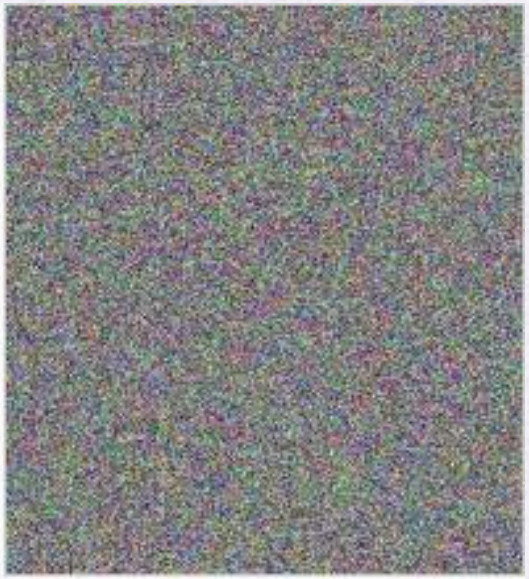
(b) Decryption



Original image



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness

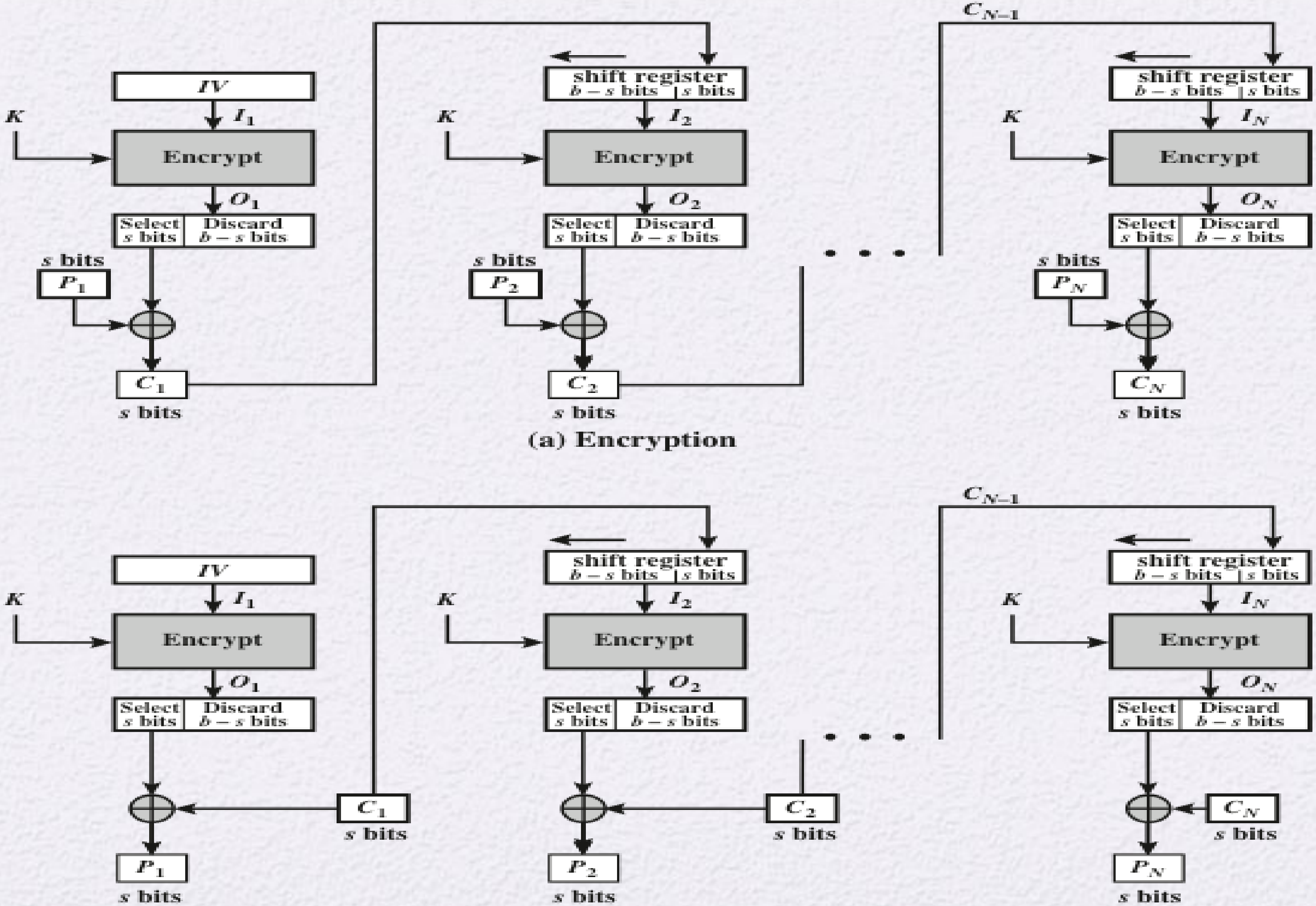
CBC mode properties

- The same plaintext in different locations are encrypted into different ciphertexts
- Encryption cannot be parallelized
- Error propagation: an error in a ciphertext block causes the next decryption error
  - $C_1 \;\; C_2 \ldots \; C_{i-1} \;\; C_i' \;\; C_{i+1} \; C_{i+2} \ldots \; C_n$
    → $P_1 \;\; P_2 \ldots \; P_{i-1} \; P_i' \;\; P_{i+1}' P_{i+2} \ldots P_n$
- Two types of errors: erasing (missing) and erroneous

Block cipher → stream cipher

- A block is not 64 -bit (for DES) or 128-bit (for AES)
- We need stream ciphers, in particular, for online communication

CFB mode



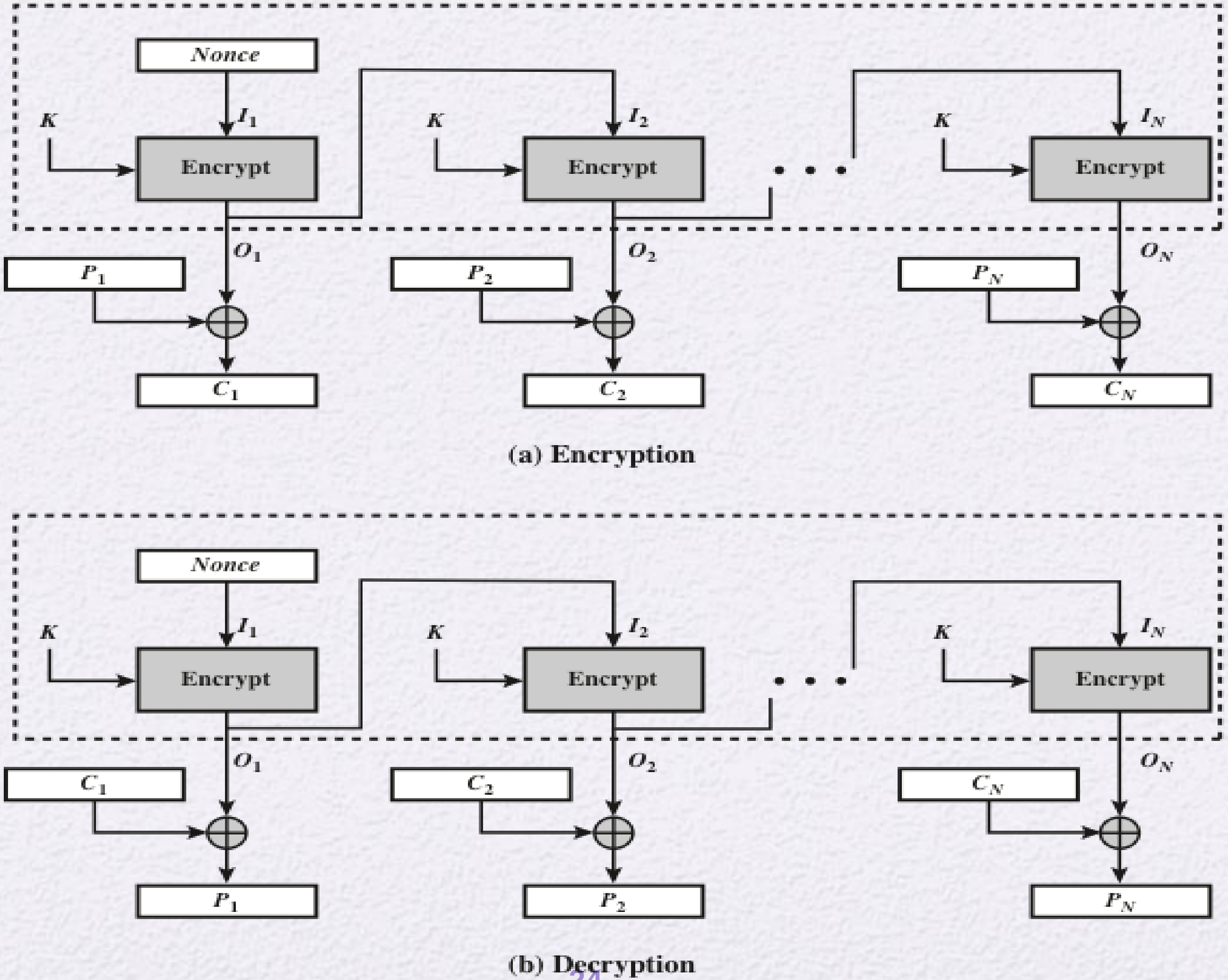
(a) Encryption

(b) Decryption

CFB : Self-Synchronization

- Limited error propagation: an error in a ciphertext block causes some subsequent decryption errors
  - C_1 C_2 … C_{i-1} C_i' C_{i+1} … C_k C_{k+1} … C_n
    → P_1 P_2 … P_{i-1} P_i' P_{i+1}' … P_k' P_{k+1} … P_n
  - Example
    - for AES, s=16, the number of propagated decryption errors is 128/16+1=9 blocks
- Cannot be parallelized.

OFB mode



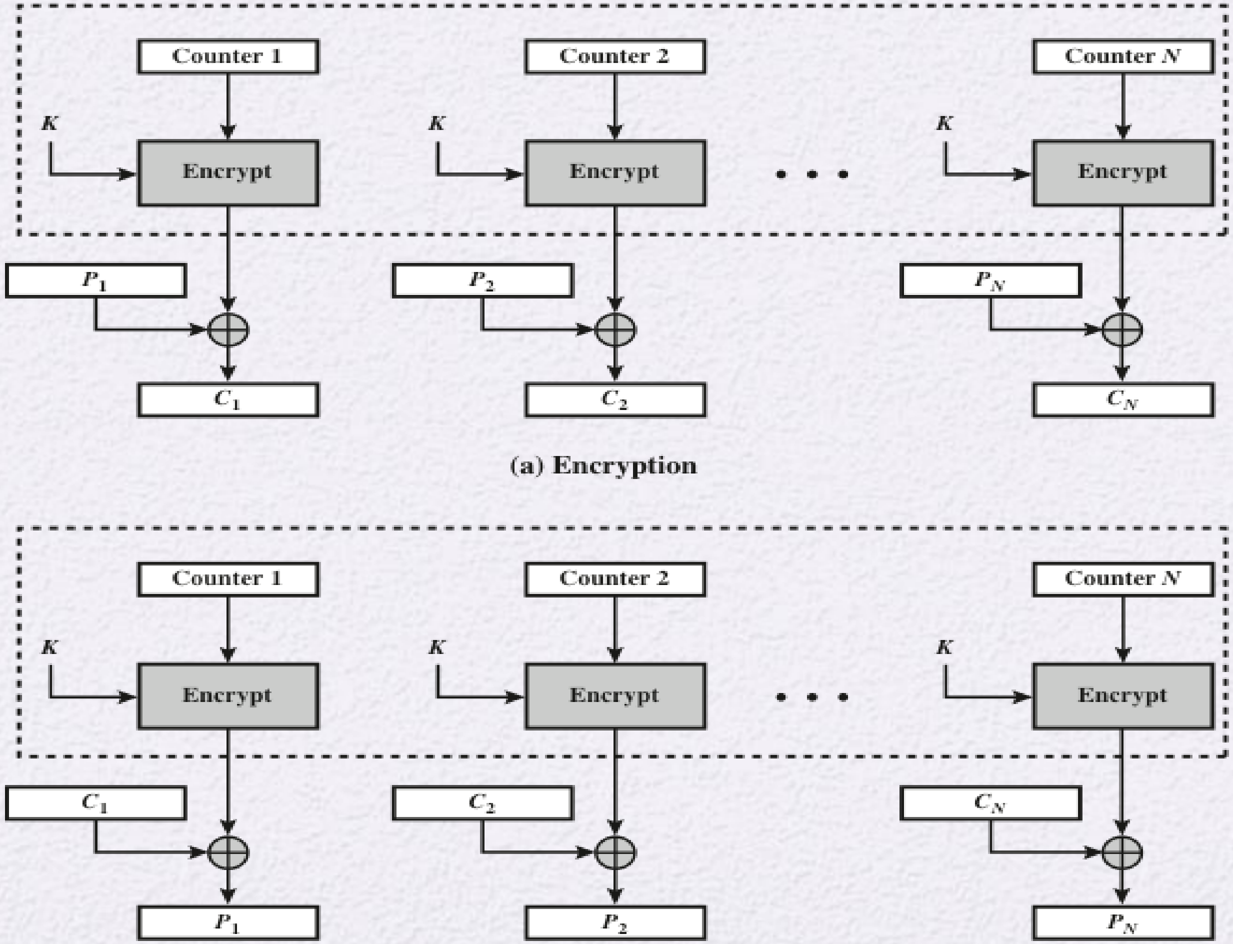
(a) Encryption

(b) Decryption

OFB mode

- Can be used as a stream cipher
- No error propagation
- O1, O2, … can be computed in advance.
  - Not parallelized

CTR mode



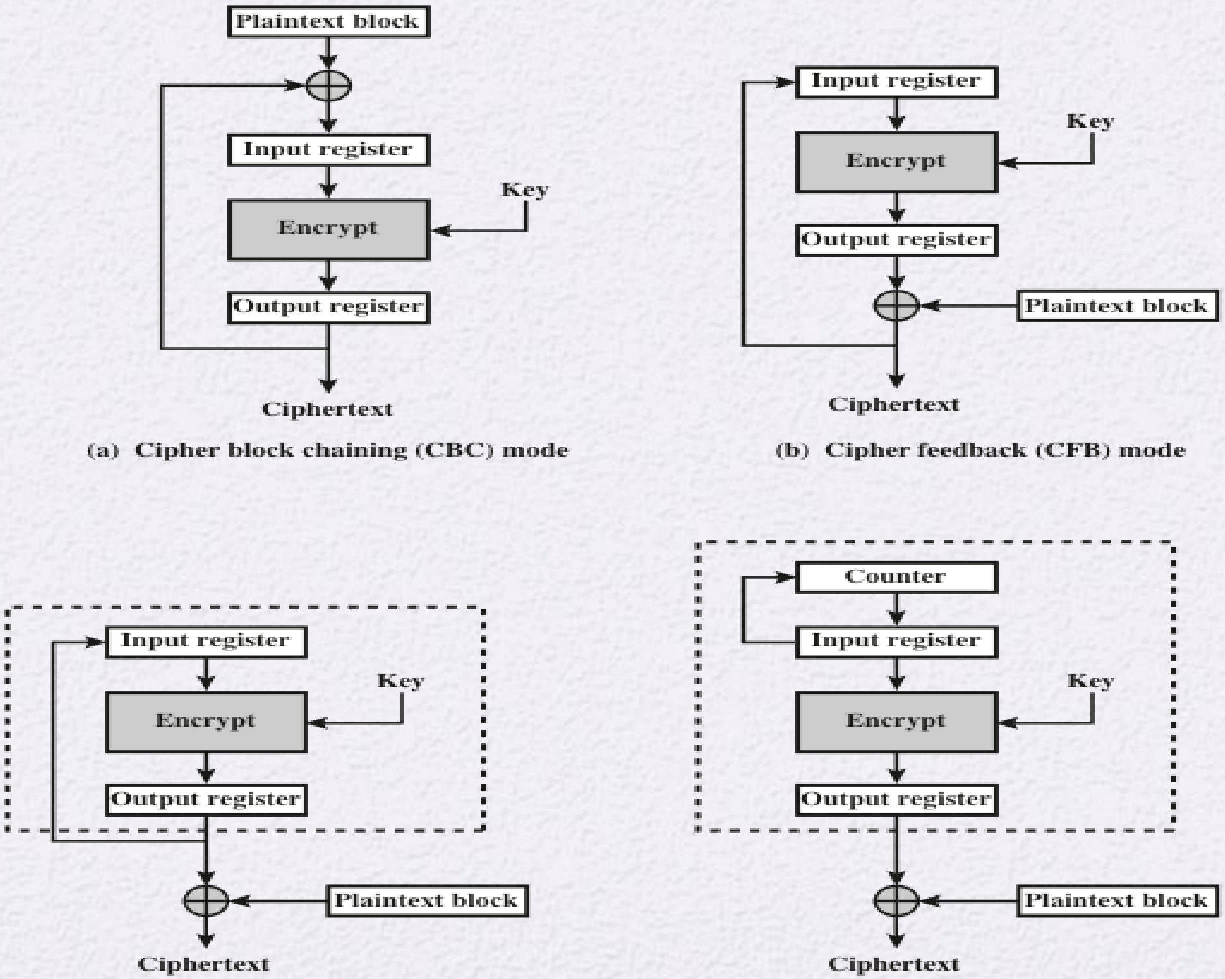
(a) Encryption

(b) Decryption

CTR mode

- Can be used as a stream cipher
- No error propagation
- Can be parallelized

Feedback Characteristics



(a) Cipher block chaining (CBC) mode

(b) Cipher feedback (CFB) mode

(c) Output feedback (OFB) mode

(d) Counter (CTR) mode

Advantages of CTR

- Hardware efficiency
- Software efficiency
- Pre-processing
- Random access
- Provable security
- Simplicity

Summary

- Padding
- Multiple encryption and triple DES
  - Double DES
  - Triple DES with two keys
  - Triple DES with three keys
- Operation modes
  - Electronic codebook
  - Cipher block chaining mode
  - Cipher feedback mode
  - Output feedback mode
  - Counter mode