

GLOBAL
EDITION



Cryptography and Network Security

Principles and Practice

SEVENTH EDITION

William Stallings

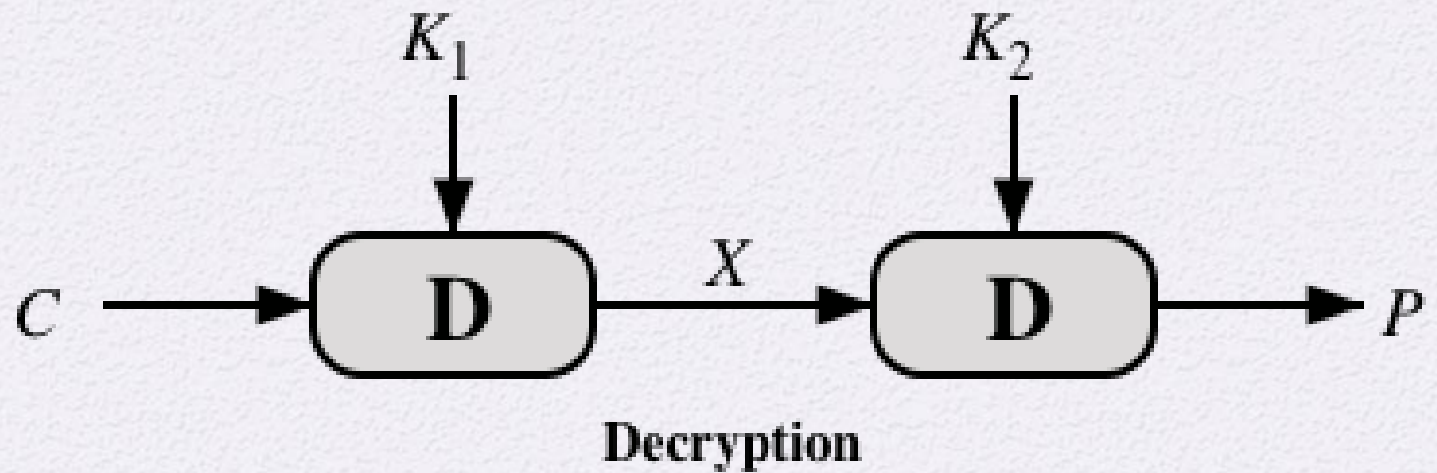
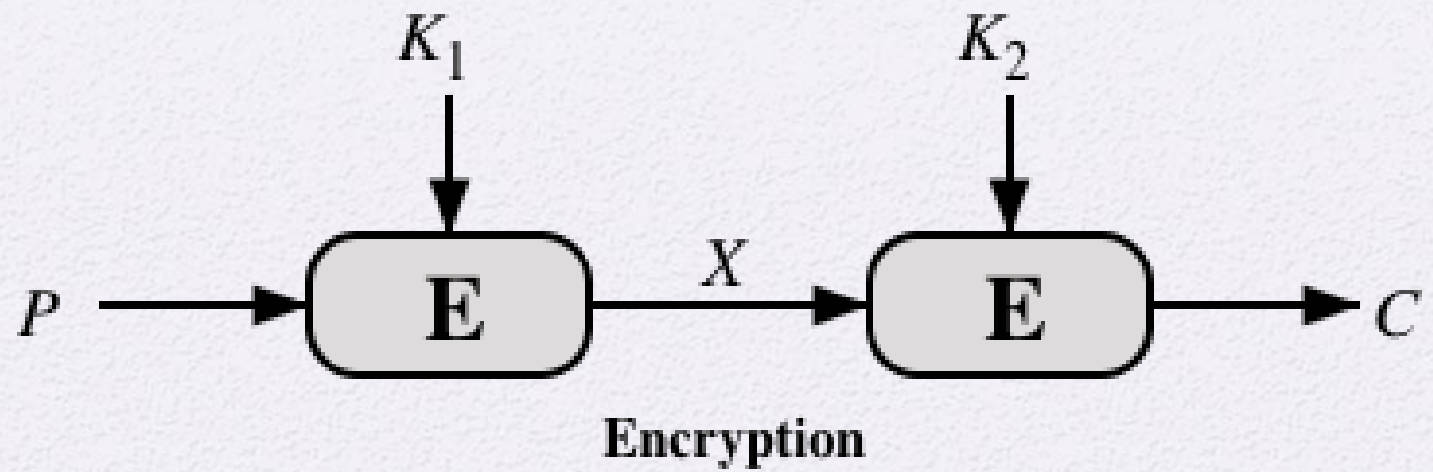


Pearson



Chapter 7

Block Cipher Operation



(a) Double Encryption

Figure 7.1 Multiple Encryption

Meet-in-the-Middle Attack

The use of double DES results in a mapping that is not equivalent to a single DES encryption

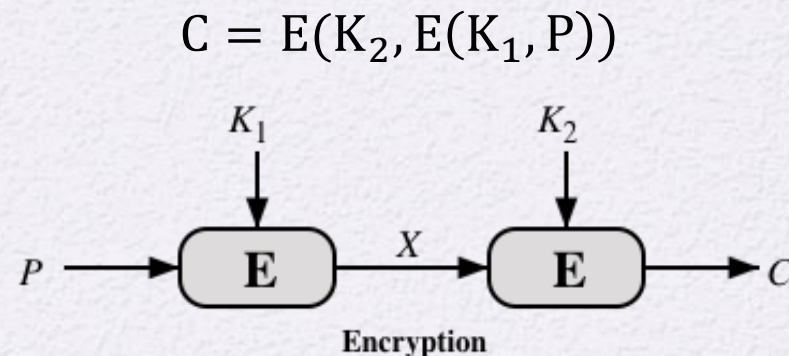
The meet-in-the-middle attack algorithm will attack this scheme and does not depend on any particular property of DES but will work against any block encryption cipher



Meet-in-the-Middle Attack

Given a known pair (P, C):

1. Encrypt P for all 2^{56} values of K_1 .
2. Store results in a table and sort them.
3. Decrypt C using all 2^{56} possible values of K_2 . After each decryption check values in table.
4. If match found then test this K_1, K_2 pair on another plaintext-ciphertext pair to check if it works.

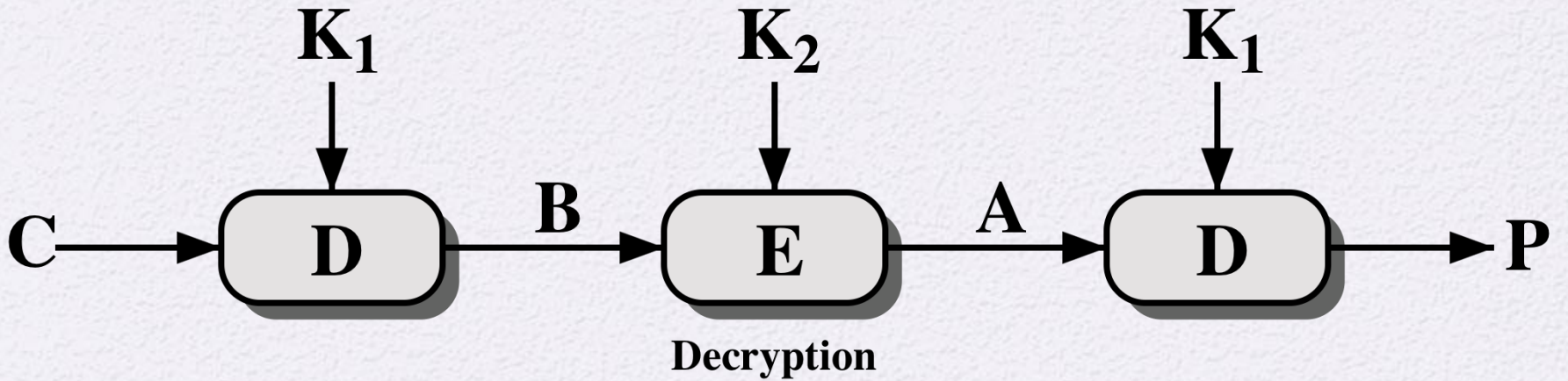
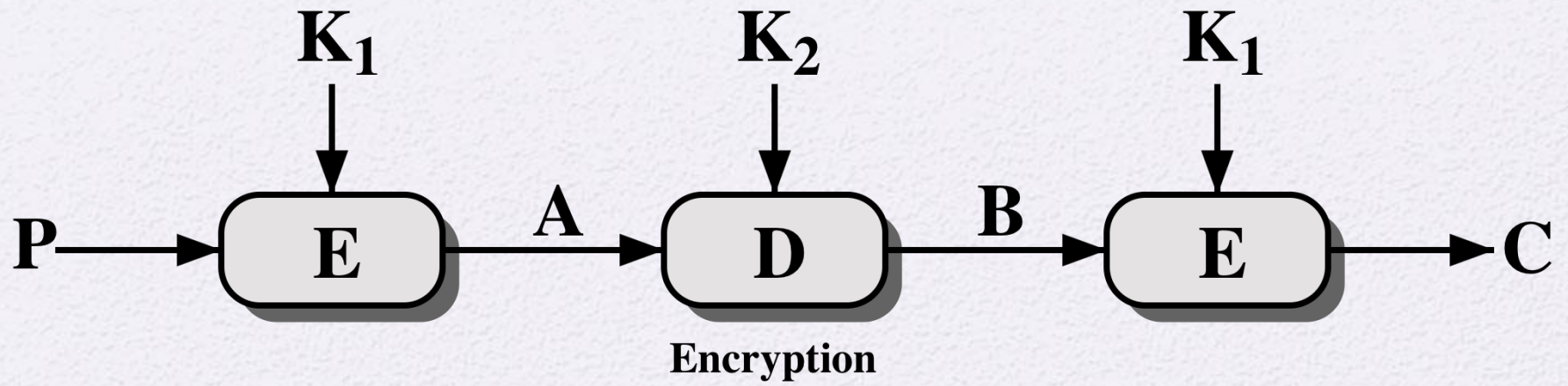


We know

$$X = E(K_1, P) = D(K_2, C)$$

Triple-DES with Two-Keys

- Obvious counter to the meet-in-the-middle attack is to use three stages of encryption with three different keys
 - This raises the cost of the meet-in-the-middle attack to 2^{112} , which is beyond what is practical
 - Has the drawback of requiring a key length of $56 \times 3 = 168$ bits, which may be somewhat unwieldy
 - As an alternative Tuchman proposed a triple encryption method that uses only two keys
- 3DES with two keys is a relatively popular alternative to DES and has been adopted for use in the key management standards ANSI X9.17 and ISO 8732



(b) Triple Encryption

Figure 7.1 Multiple Encryption

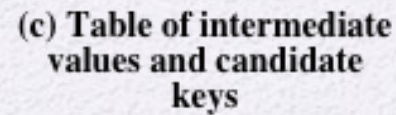
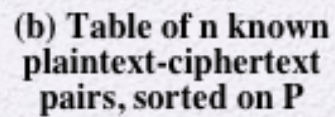
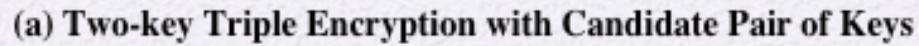


Figure 7.2 Known-Plaintext Attack on Triple DES

Triple DES with Three Keys

- Many researchers now feel that three-key 3DES is the preferred alternative

Three-key 3DES has an effective key length of 168 bits and is defined as:

$$\bullet C = E(K_3, D(K_2, E(K_1, P)))$$

Backward compatibility with DES is provided by putting:

$$\bullet K_3 = K_2 \text{ or } K_1 = K_2$$

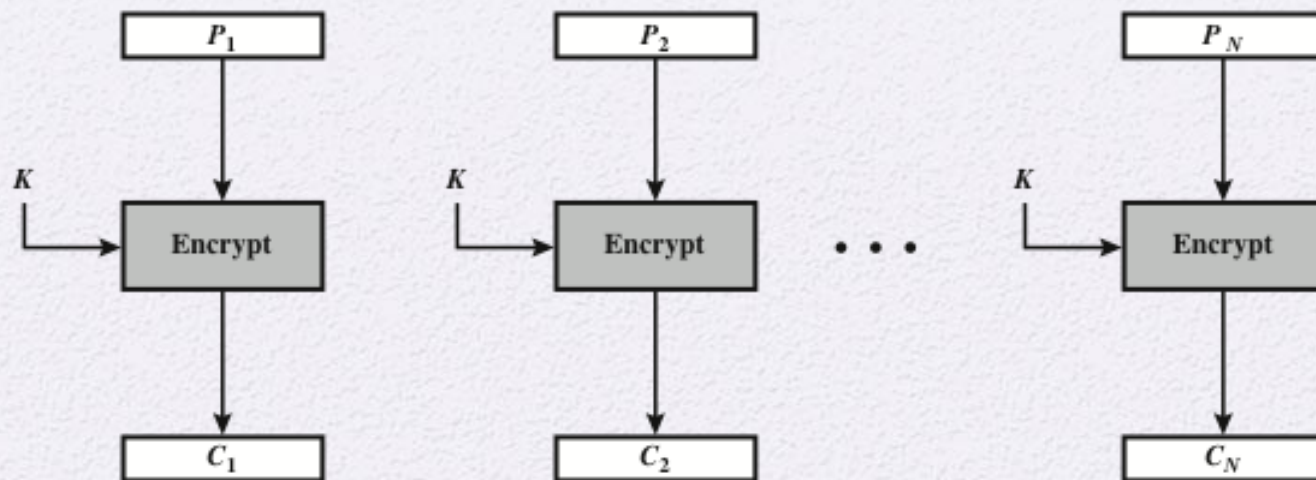
- A number of Internet-based applications have adopted three-key 3DES including PGP and S/MIME

Modes of Operation

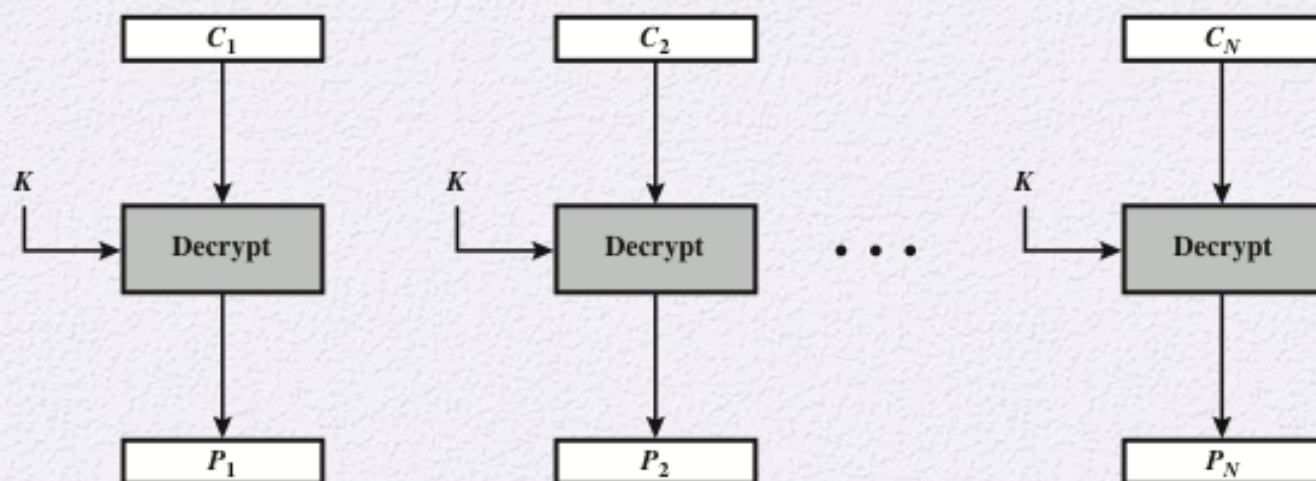
- A technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application
- To apply a block cipher in a variety of applications, five *modes of operation* have been defined by NIST
 - The five modes are intended to cover a wide variety of applications of encryption for which a block cipher could be used
 - These modes are intended for use with any symmetric block cipher, including triple DES and AES

Table 7.1 Block Cipher Modes of Operation

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



(a) Encryption



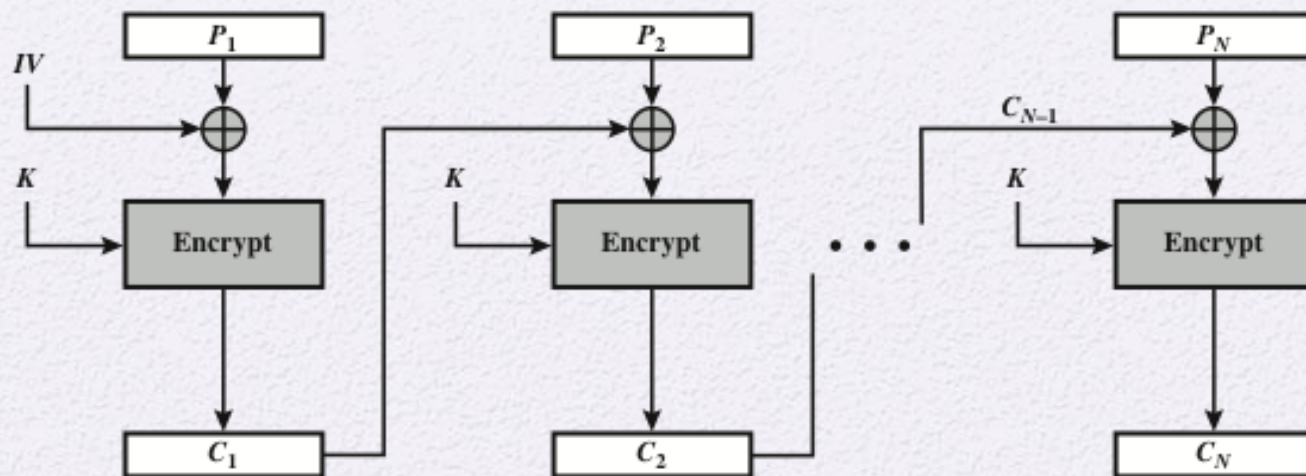
(b) Decryption

Figure 7.3 Electronic Codebook (ECB) Mode

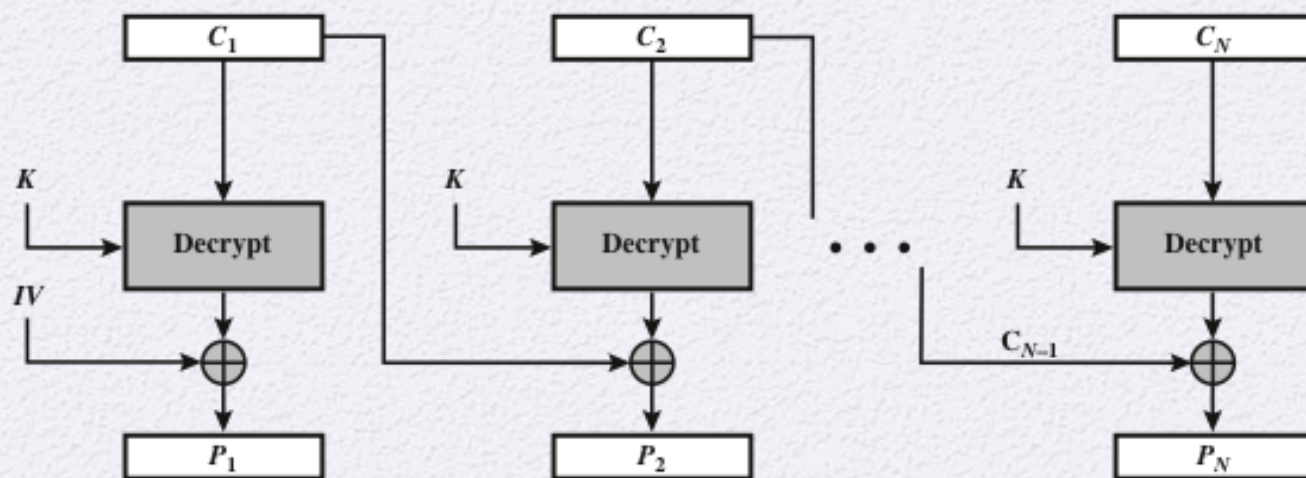
Criteria and properties
for evaluating and
constructing block
cipher modes of
operation that are
superior to ECB:



- Overhead
- Error recovery
- Error propagation
- Diffusion
- Security



(a) Encryption



(b) Decryption

Figure 7.4 Cipher Block Chaining (CBC) Mode

Cipher Feedback Mode

- For AES, DES, or any block cipher, encryption is performed on a block of b bits
 - In the case of DES $b = 64$
 - In the case of AES $b = 128$

There are three modes that make it possible to convert a block cipher into a stream cipher:

Cipher feedback (CFB) mode

Output feedback (OFB) mode

Counter (CTR) mode

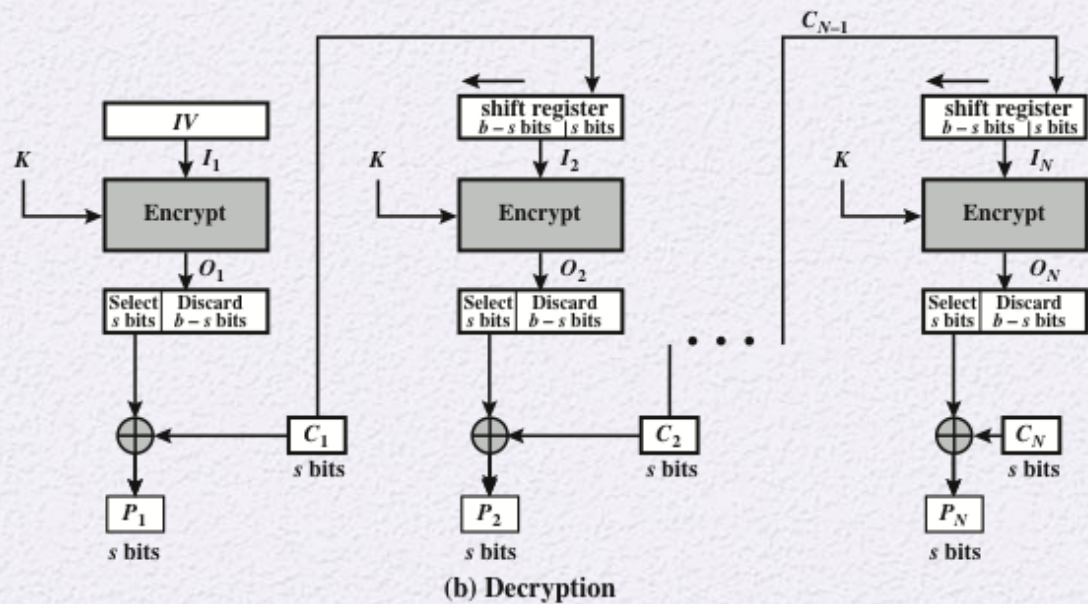
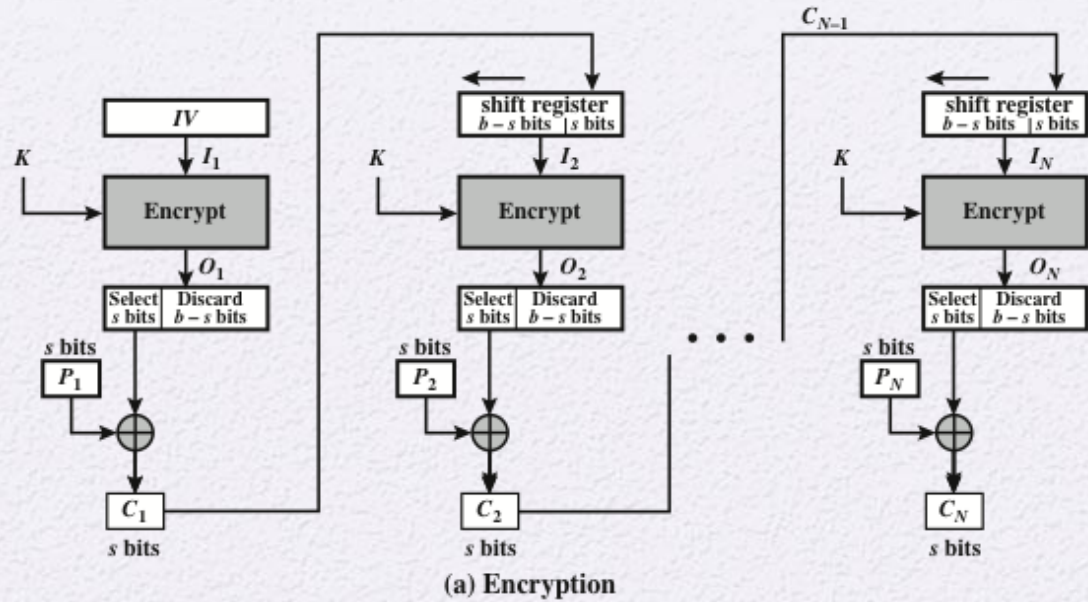
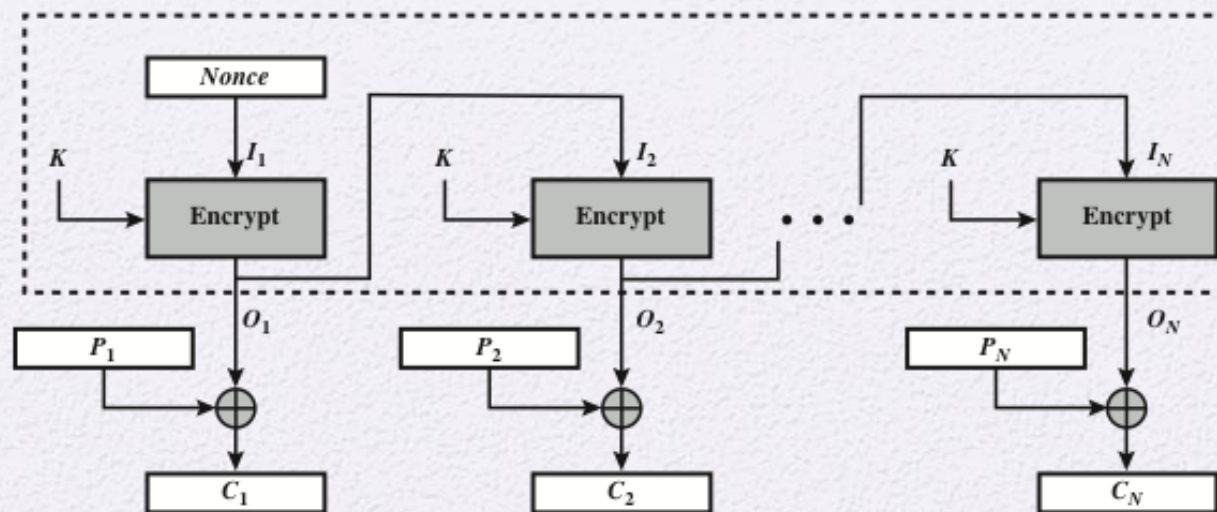
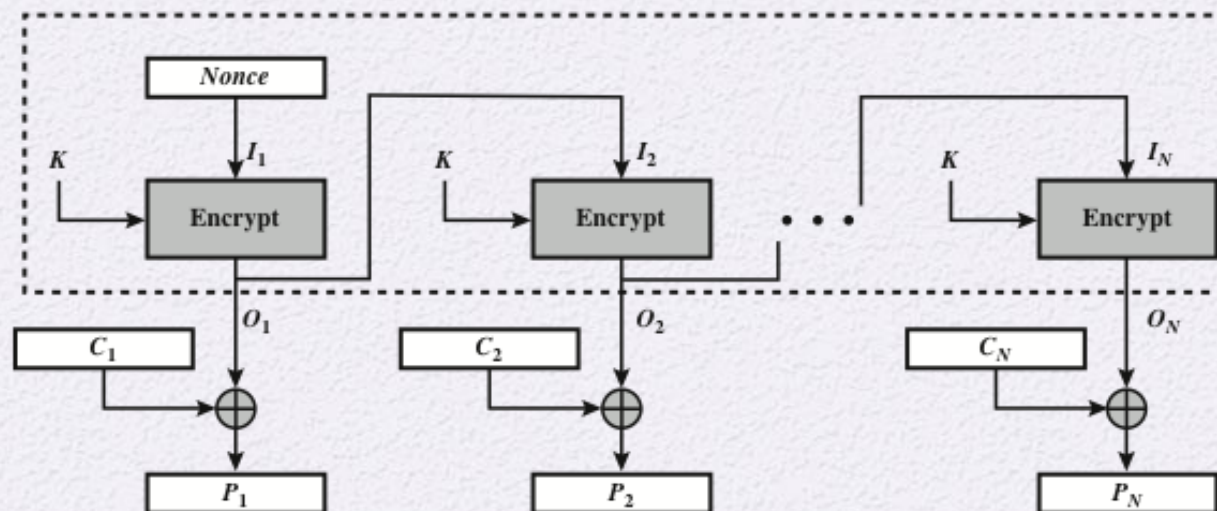


Figure 7.5 s -bit Cipher Feedback (CFB) Mode

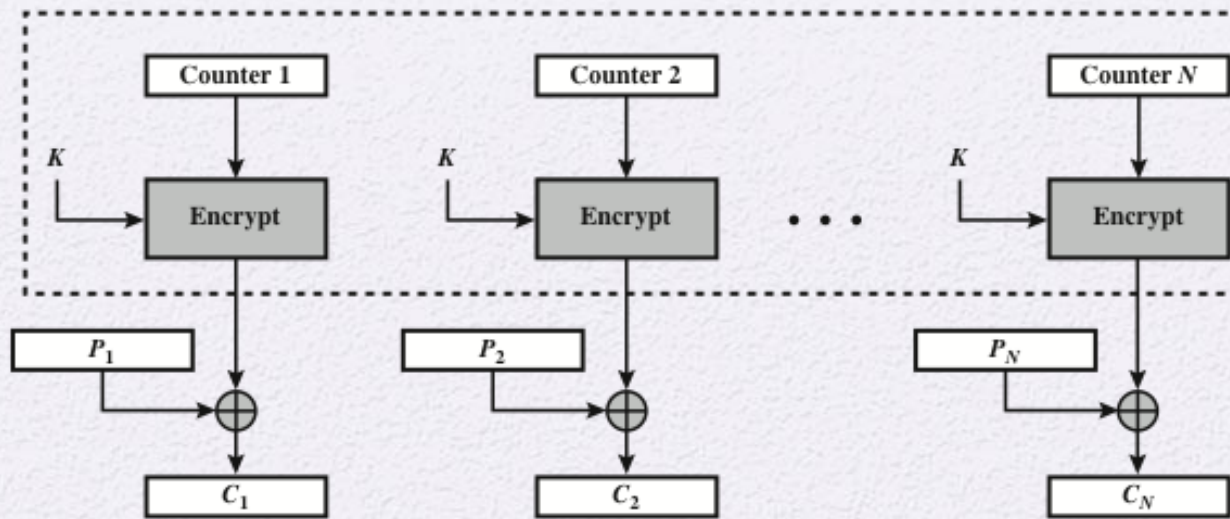


(a) Encryption

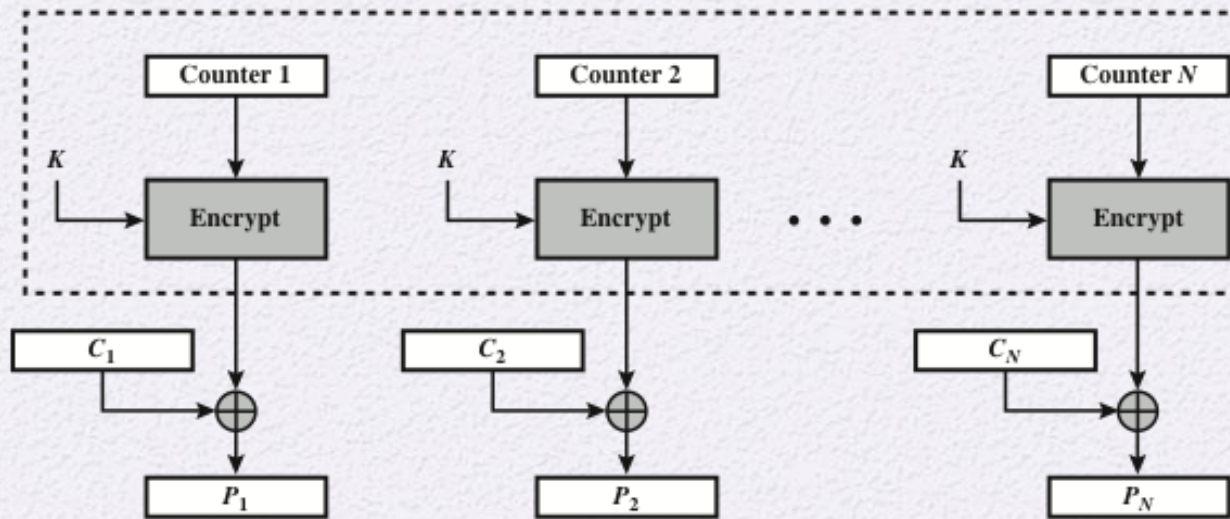


(b) Decryption

Figure 7.6 Output Feedback (OFB) Mode



(a) Encryption



(b) Decryption

Figure 7.7 Counter (CTR) Mode

Advantages of CTR



- Hardware efficiency
- Software efficiency
- Preprocessing
- Random access
- Provable security
- Simplicity