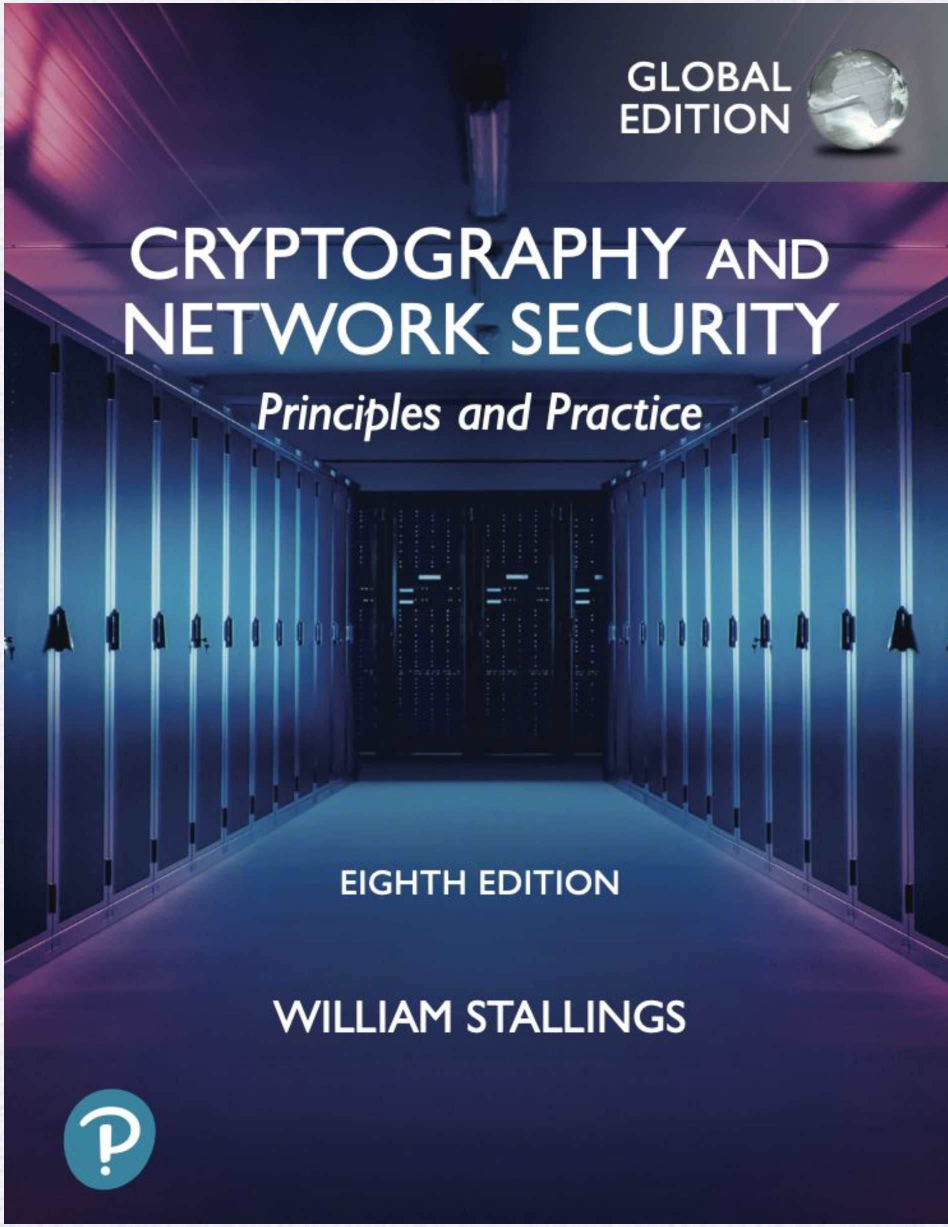
University of Nevada – Reno
Computer Science & Engineering
Department

CS454/654 Reliability and Security of Computing Systems - Fall 2024

Lecture 13

Dr. Batyr Charyyev
bcharyyev.com



CHAPTER 7

Block Cipher Operation

7.1 MULTIPLE ENCRYPTION AND TRIPLE DES

DES (Data Encryption Standards) is vulnerable to brute force attacks.

Table 4.5 Average Time Required for Exhaustive Key Search

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns $= 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns $= 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns $= 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns $= 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns $= 1.8 \times 10^{60}$ years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns $= 6.3 \times 10^{9}$ years	6.3×10^{6} years

Completely new algorithm that is resistant to both cryptanalytic and brute-force attacks, of which AES is a prime example.

Continue investment in existing approach, such as using multiple encryption with DES and multiple keys.

7.1 MULTIPLE ENCRYPTION AND TRIPLE DES

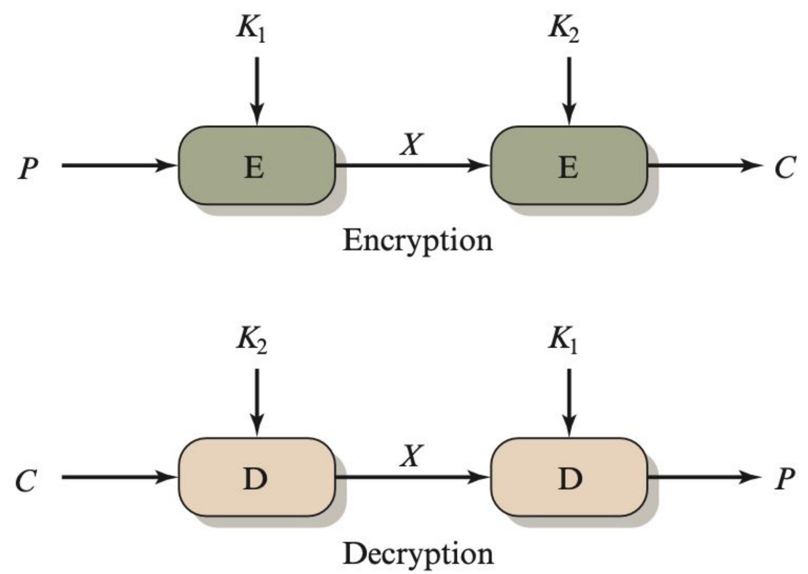
Double DES

Given a plaintext P and two encryption keys K_1 and K_2, ciphertext C is generated as

$$C = \mathrm{E}(K_2, \mathrm{E}(K_1, P))$$

Decryption requires that the keys be applied in reverse order:

$$P = \mathrm{D}(K_1, \mathrm{D}(K_2, C))$$



(a) Double encryption

7.1 MULTIPLE ENCRYPTION AND TRIPLE DES

Suppose it were true for DES, for all 56-bit key values, that given any two
With 2^{64} possible inputs, the number of different mapping is

$$(2^{64})! = 10^{347380000000000000000} > (10^{10^{20}})$$

DES defines one mapping for each different key, and a total number of mappings is

$$2^{56} < 10^{17}$$

Therefore, it is reasonable to assume that if DES is used twice with different keys, it will produce one of the many mappings that are not defined by a single application of DES.

7.1 MULTIPLE ENCRYPTION AND TRIPLE DES

Meet in the Middle Attack

$$C = \mathrm{E}(K_2, \mathrm{E}(K_1, P))$$

$$X = \mathrm{E}(K_1, P) = \mathrm{D}(K_2, C)$$

First, encrypt P for all 2^{56} possible values of K1. Store these results in a table and then sort the table by the values of X. Next, decrypt C using all 2^{56} possible values of K2. As each decryption is produced, check the result against the table for a match.

The result is that a known plaintext attack will succeed against double DES, with an effort on the order of 2^{56}, which is not much more than the 2^{55} required for single DES.

7.1 MULTIPLE ENCRYPTION AND TRIPLE DES

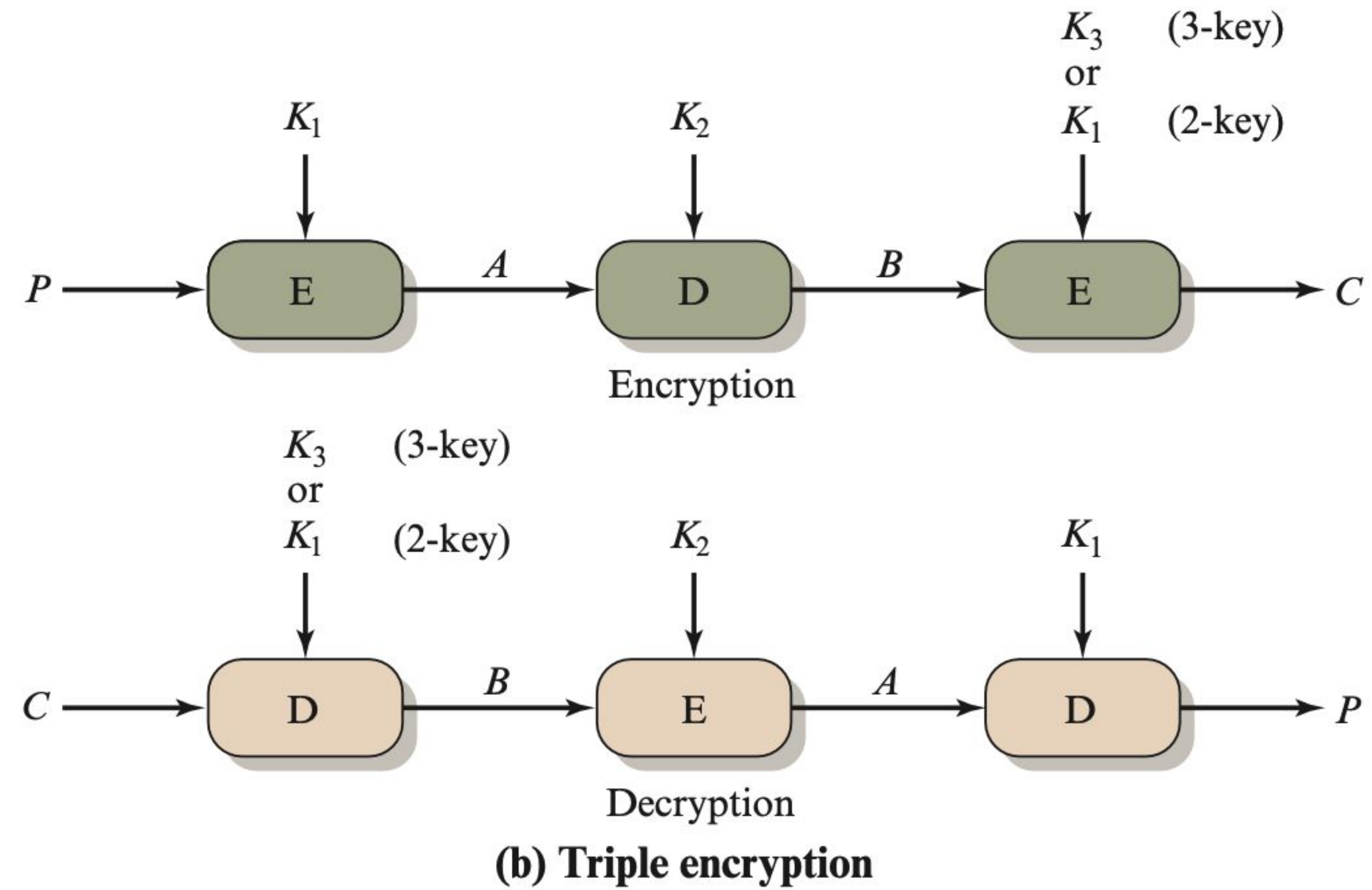


Figure 7.1 Multiple Encryption

two versions of 3DES; one using two keys and one using three keys.

7.1 MULTIPLE ENCRYPTION AND TRIPLE DES

- Currently, there are no practical cryptanalytic attacks on 3DES.
- Couple attacks techniques mentioned in book but they are not practical.
  - In general proposed approaches try to reduce the 3DES to 2DES.

Table 4.5 Average Time Required for Exhaustive Key Search

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns $= 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns $= 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns $= 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns $= 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns $= 1.8 \times 10^{60}$ years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns $= 6.3 \times 10^{9}$ years	6.3×10^{6} years

Modes of Operation

- To apply a block cipher in a variety of applications, there are five modes of operation.

- In essence, a mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream.

- These modes are intended for use with any symmetric block cipher, including triple DES and AES.

1. Electronic Codebook (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)
5. Counter (CTR)

ELECTRONIC CODEBOOK

- The simplest mode, in which plaintext is handled one block at a time and each block of plaintext is encrypted using the same key.
- The term codebook is used because, for a given key, there is a unique ciphertext for every b-bit block of plaintext. Thus, resembles a gigantic codebook in which there is an entry for every possible b-bit plaintext pattern showing its corresponding ciphertext.
- For a message longer than b bits, split into b-bit blocks and pad the last if necessary.
- The ECB mode should be used only to secure messages shorter than a single block such as to encrypt a secret key.
- For lengthy messages, it may not be secure. If the message is highly structured, it may be possible for a cryptanalyst to exploit these regularities.

CIPHER BLOCK CHAINING MODE

- Technique in which the same plaintext block, if repeated, produces different ciphertext blocks.

- In this scheme, the input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block; the same key is used for each block.

- CBC mode requires that the last block be padded to a full b bits if it is a partial block.

CIPHER BLOCK CHAINING MODE

IV is **nonce**: counter, a timestamp, or a message number.

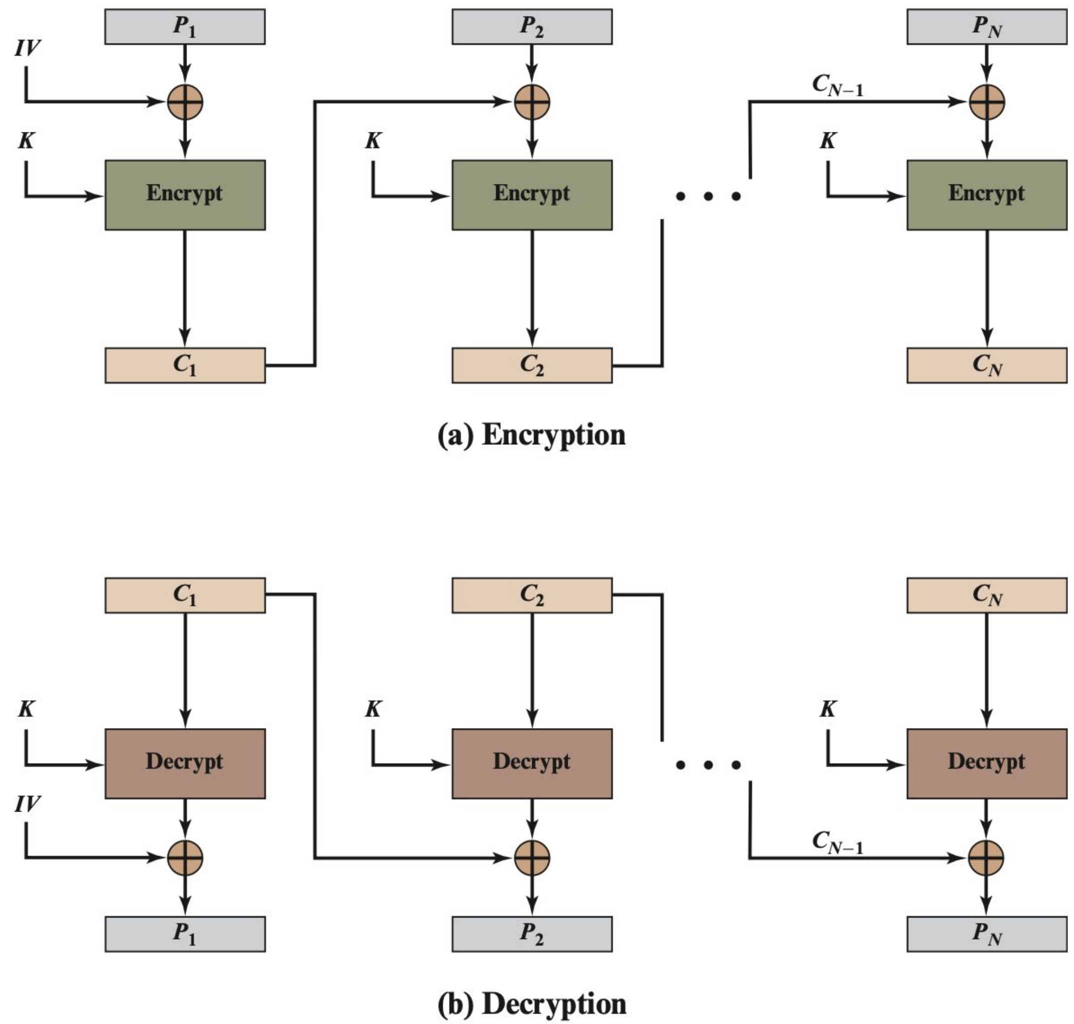


Figure 7.4 Cipher Block Chaining (CBC) Mode

CIPHER FEEDBACK MODE

Unit of transmission is s bits; a common value is s = 8.

Rather than blocks of b bits, the plaintext is divided into segments of s bits.

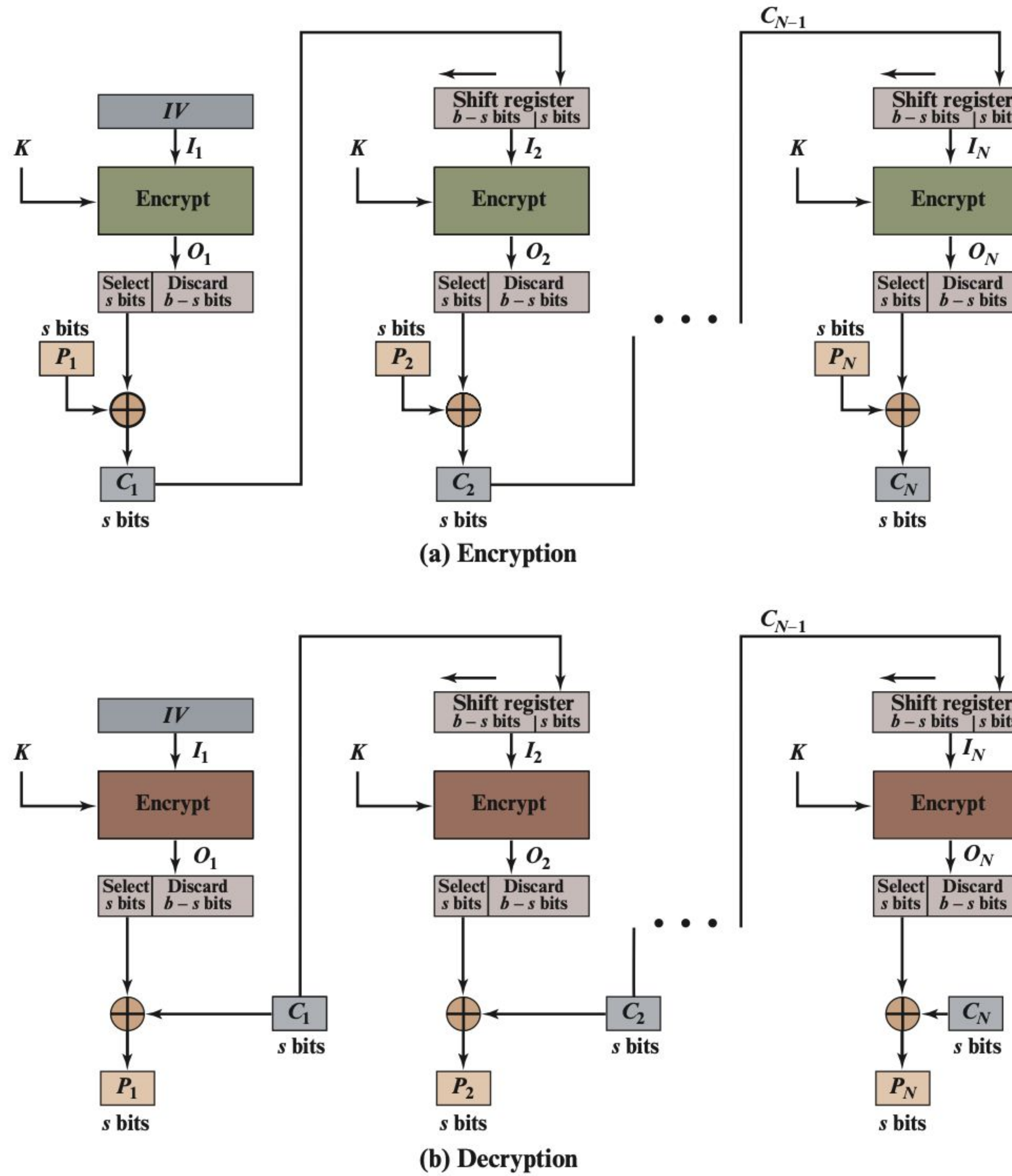


Figure 7.5 *s*-bit Cipher Feedback (CFB) Mode

OUTPUT FEEDBACK MODE (OFB)

One advantage of the OFB method is that bit errors in transmission do not propagate. For example, if a bit error occurs in C1, only the recovered value of P1 is affected; subsequent plaintext units are not corrupted.

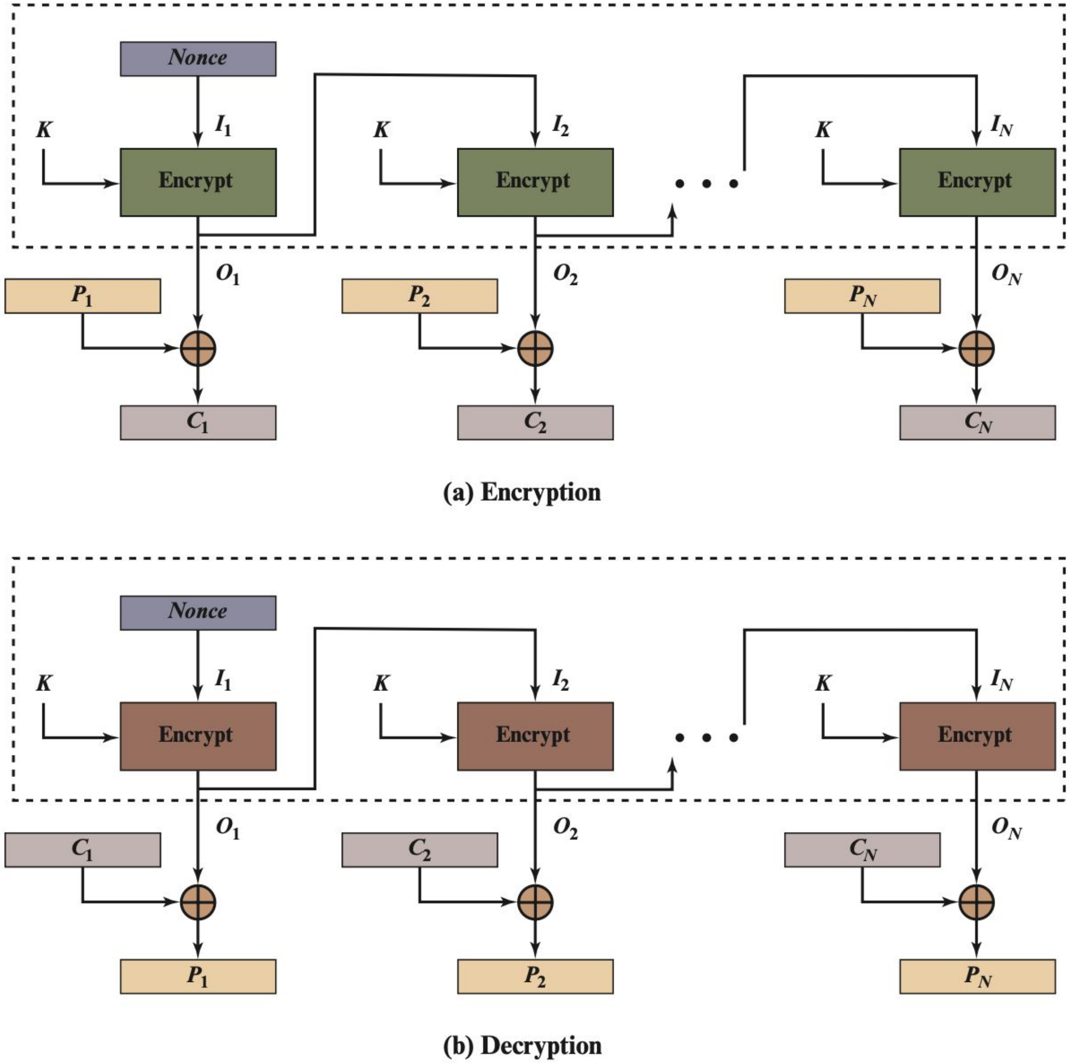


Figure 7.6 Output Feedback (OFB) Mode

COUNTER MODE (CTR)

Although interest in the counter (CTR) mode has increased recently with applications to ATM (asynchronous transfer mode) network security and IPsec, this mode was proposed in 1979.

A counter equal to the plaintext block size is used, it must be different for each plaintext block that is encrypted.

Typically, the counter is initialized to some value and then incremented by 1 for each subsequent block.

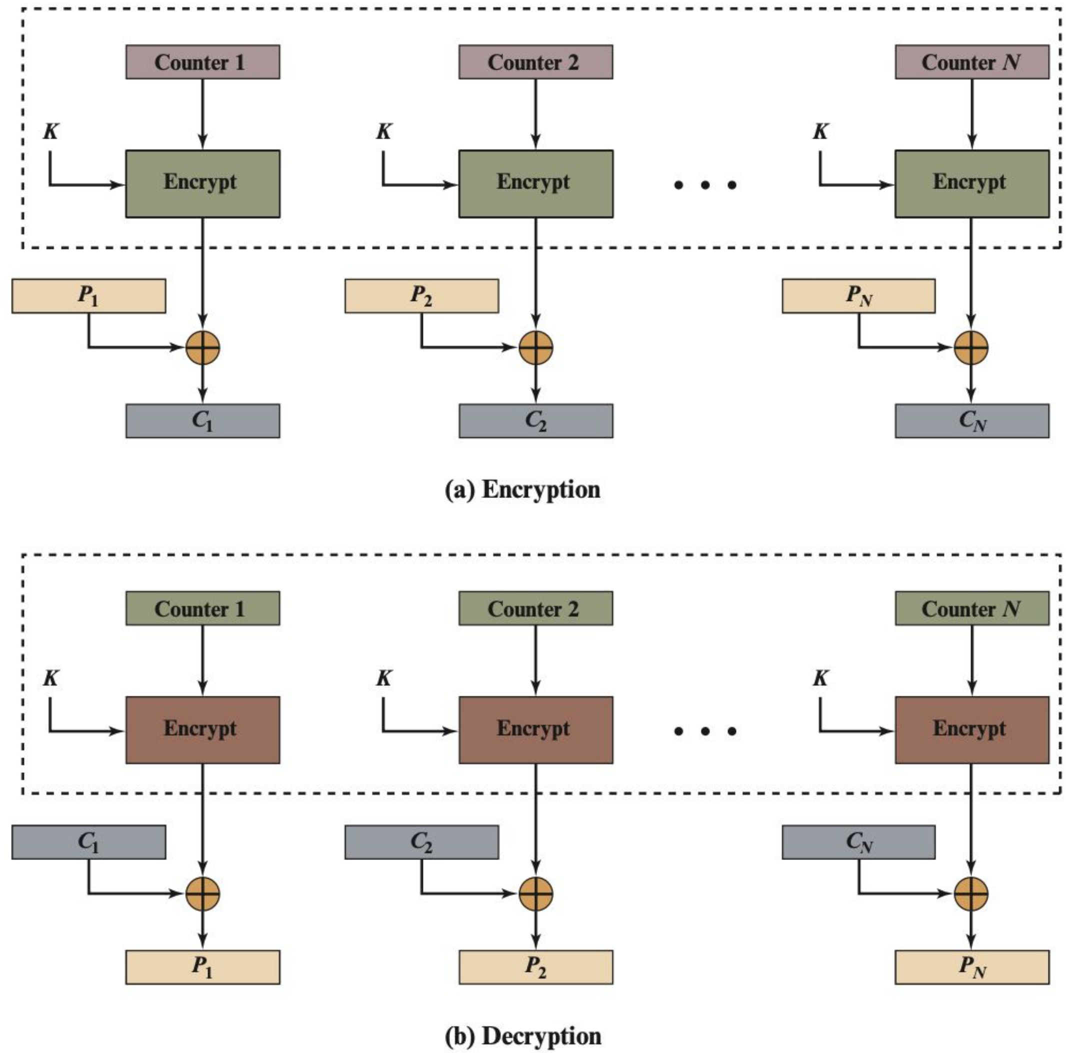


Figure 7.7 Counter (CTR) Mode

COUNTER MODE (CTR)

Hardware efficiency: Unlike the three chaining modes, encryption in CTR mode can be done in parallel on multiple blocks of plaintext.

Preprocessing: The execution of the underlying encryption algorithm does not depend on input of the plaintext or ciphertext.

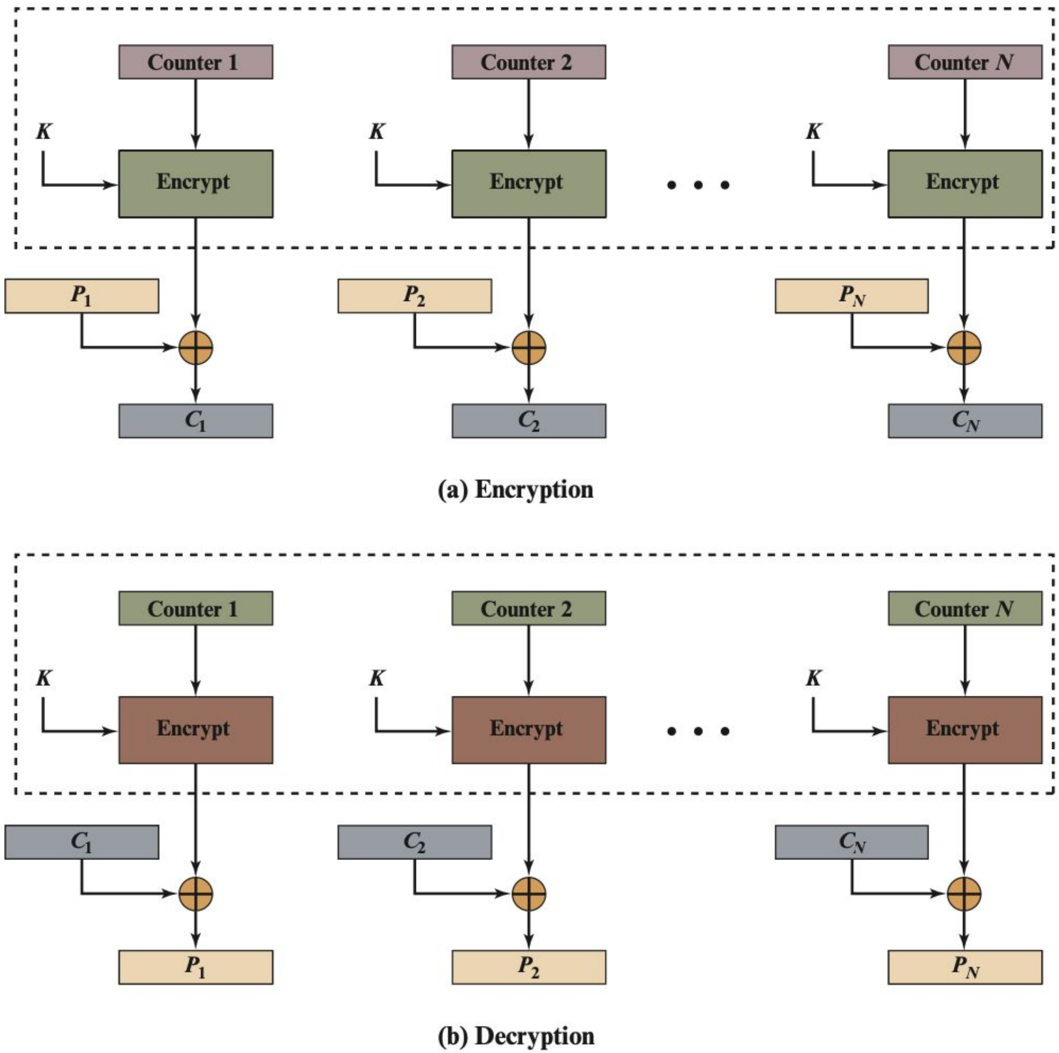


Figure 7.7 Counter (CTR) Mode

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

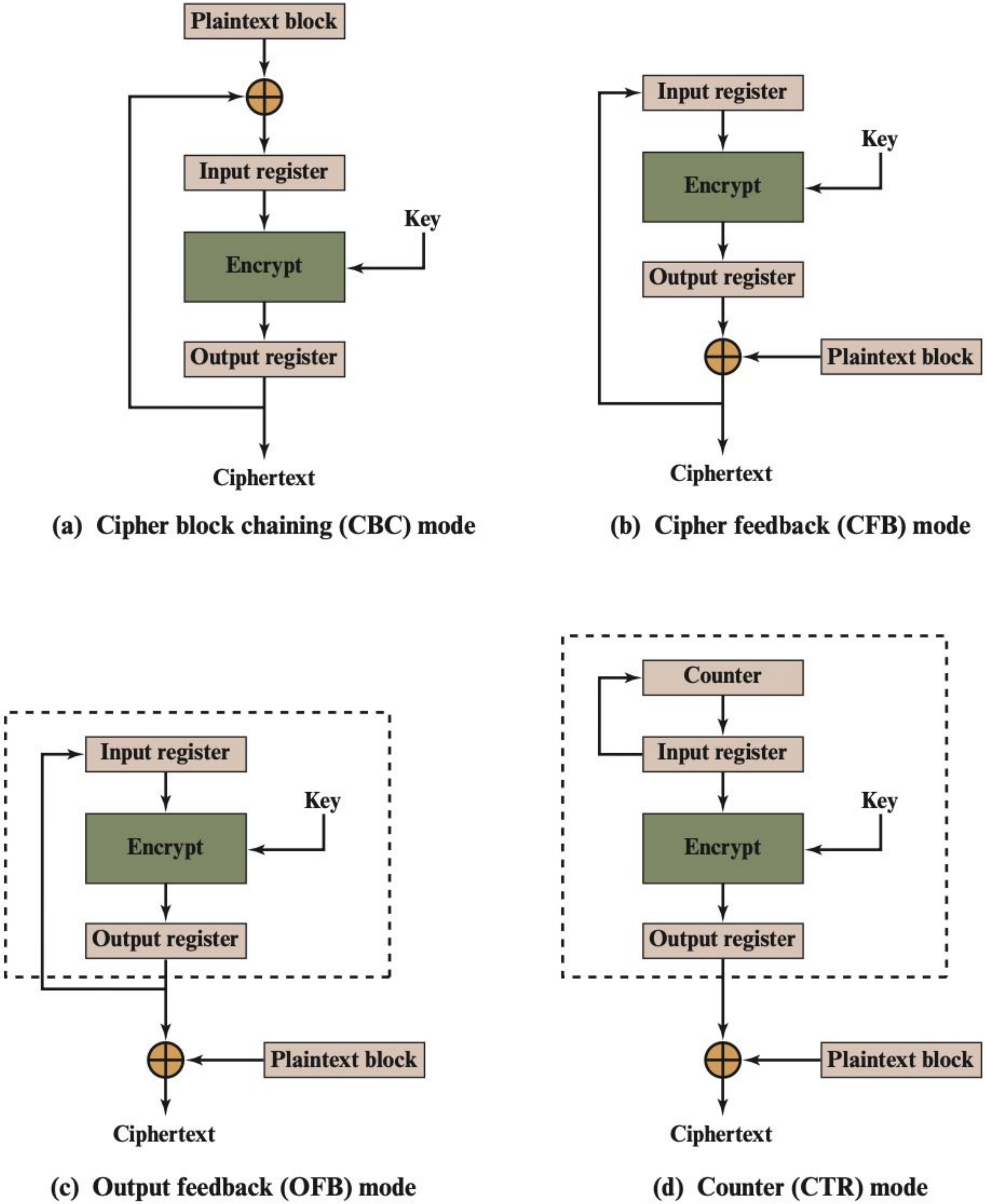


Figure 7.8 Feedback Characteristic of Modes of Operation