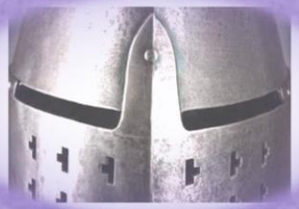


Chapter 7

Block Cipher Operation

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

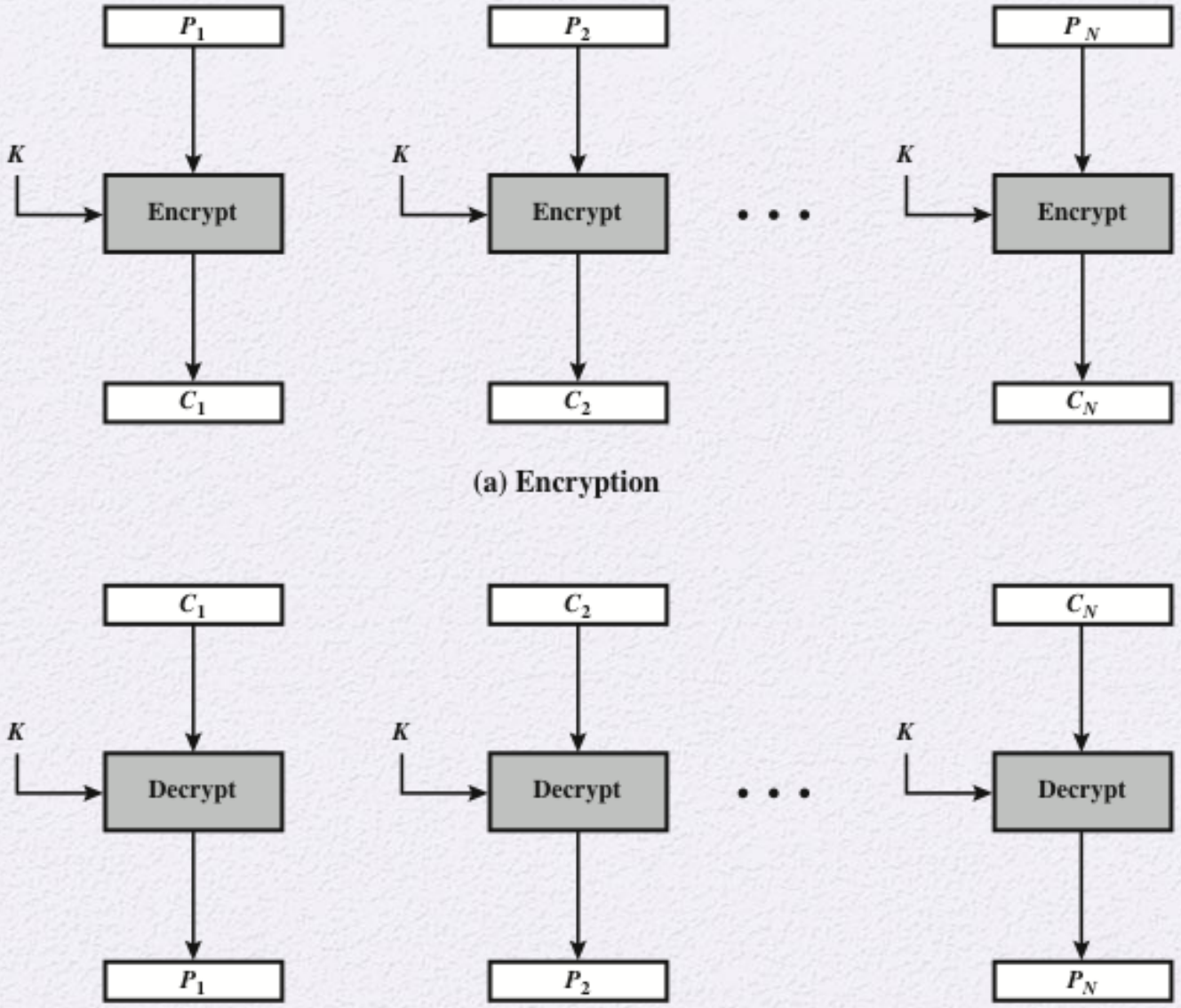


Figure 7.3 Electronic Codebook (ECB) Mode

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

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

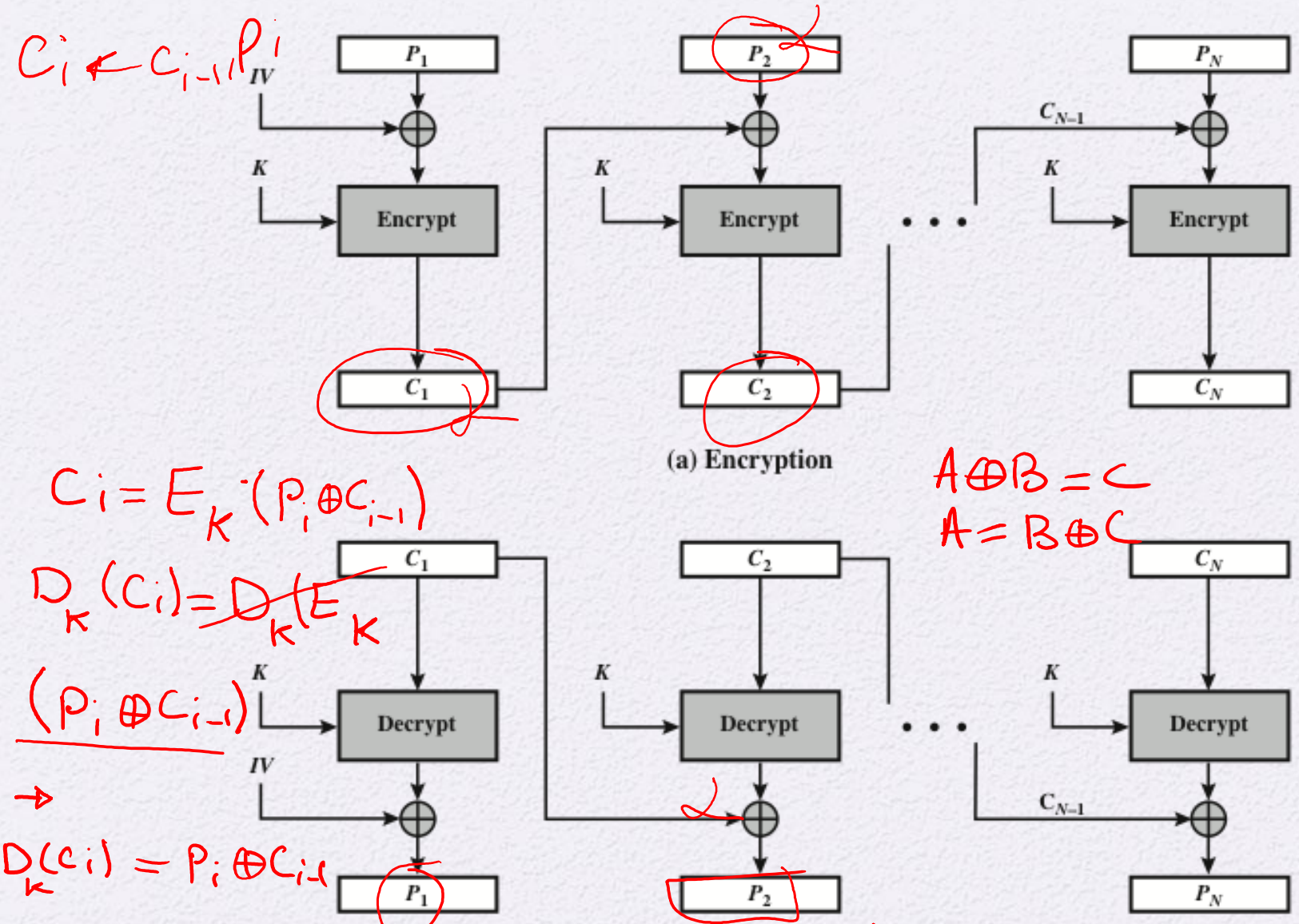
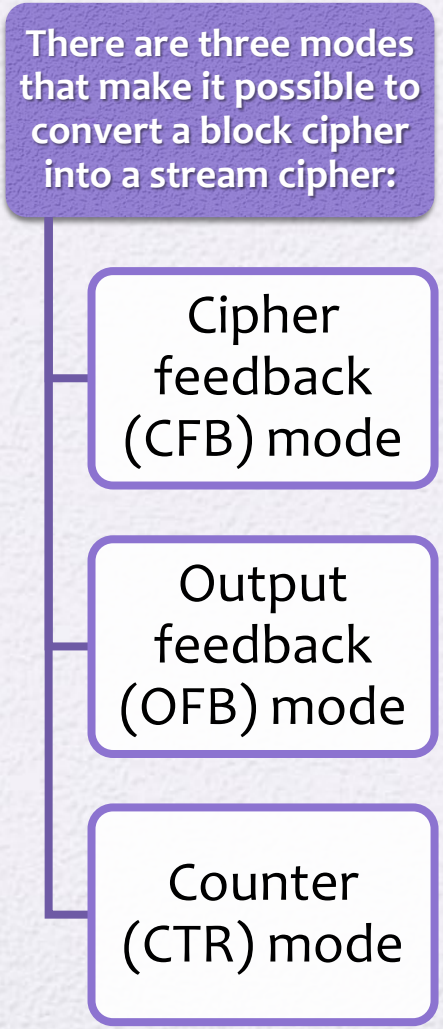


Figure 7.4 Cipher Block Chaining (CBC) Mode

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



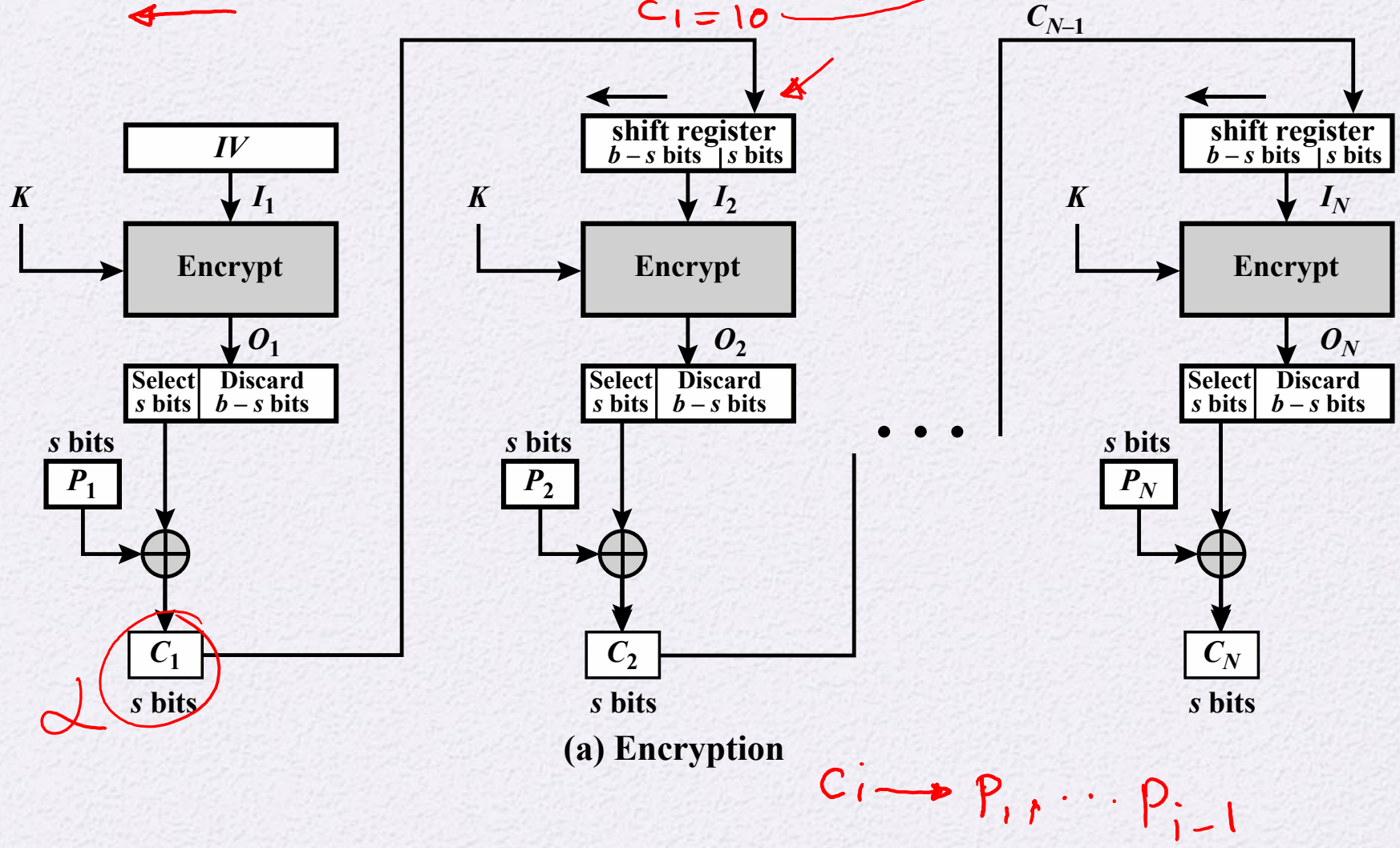
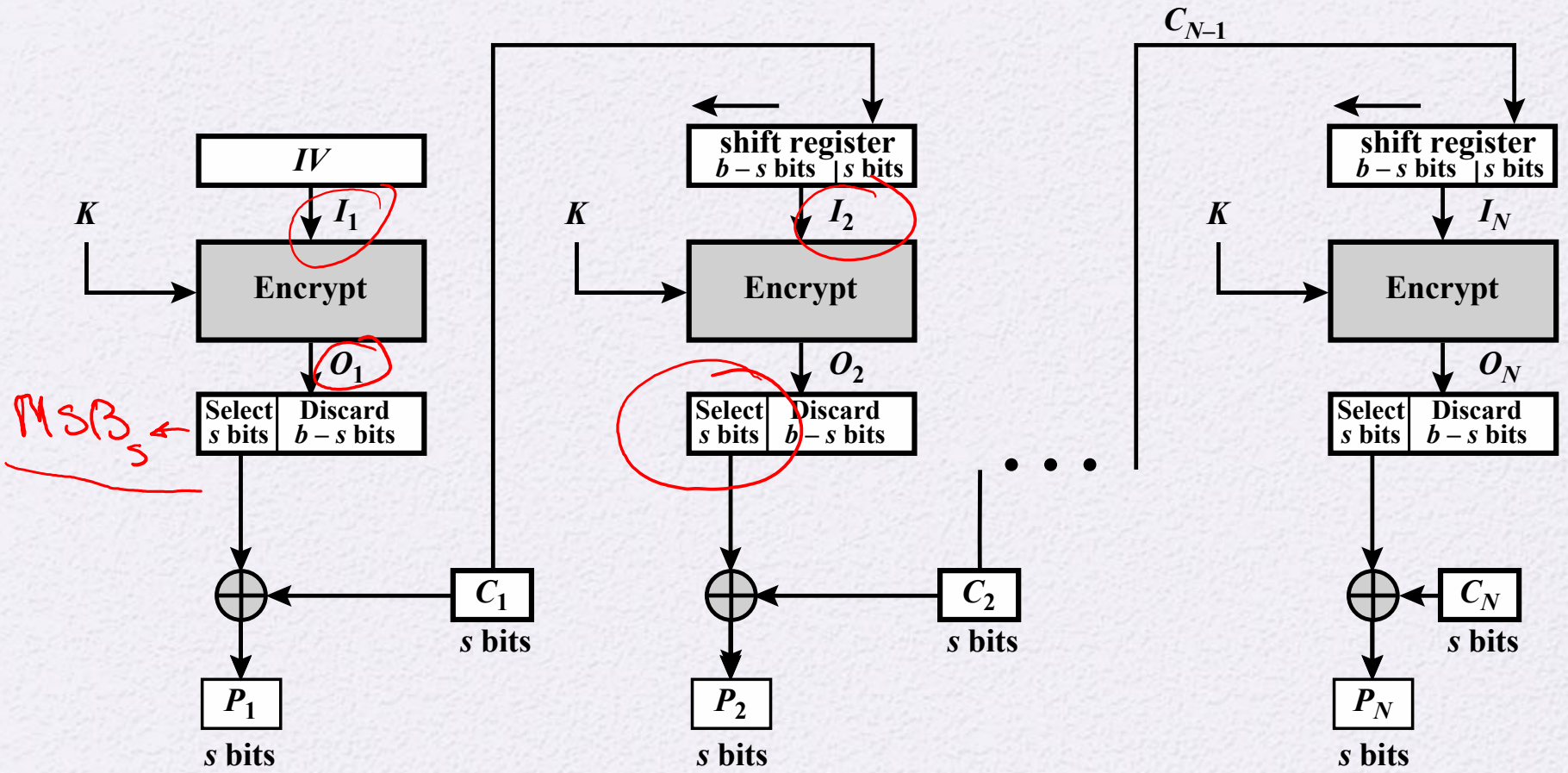


Figure 7.5 *s*-bit Cipher Feedback (CFB) Mode

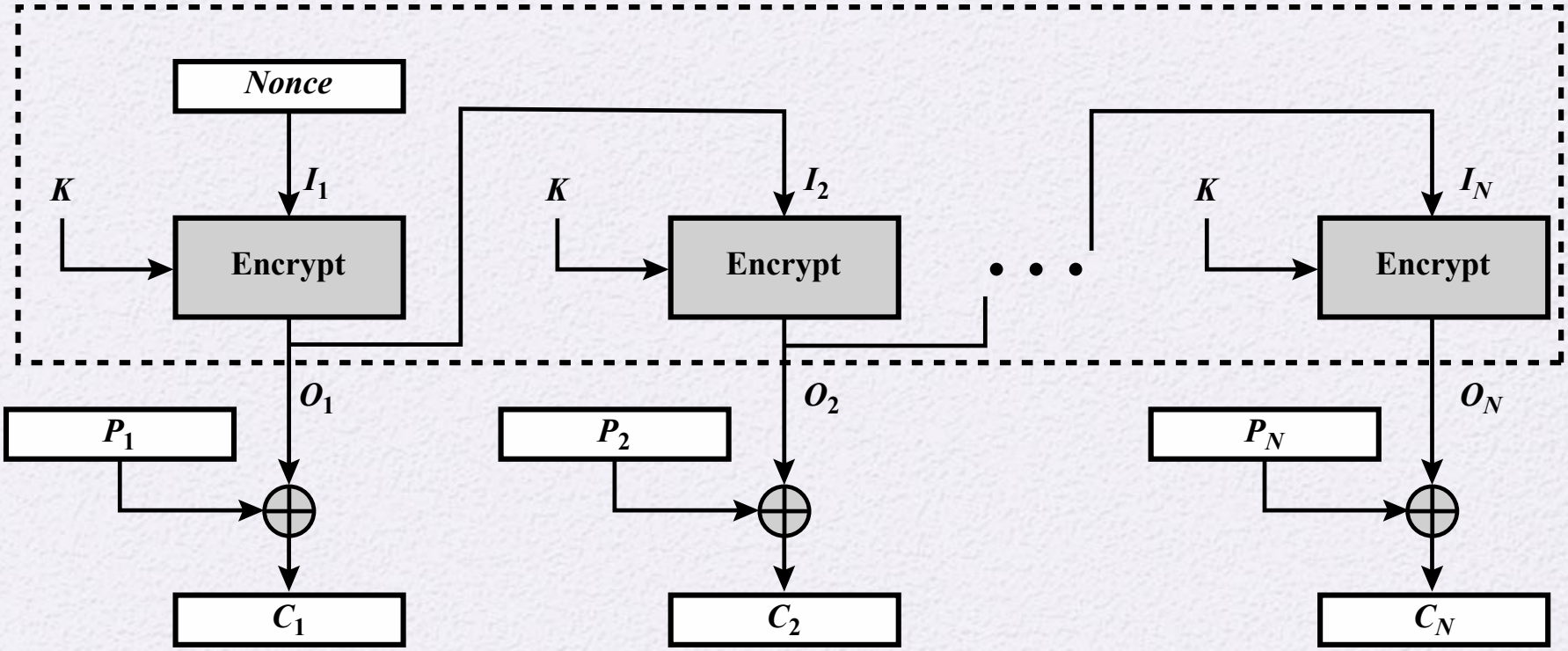


(b) Decryption

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

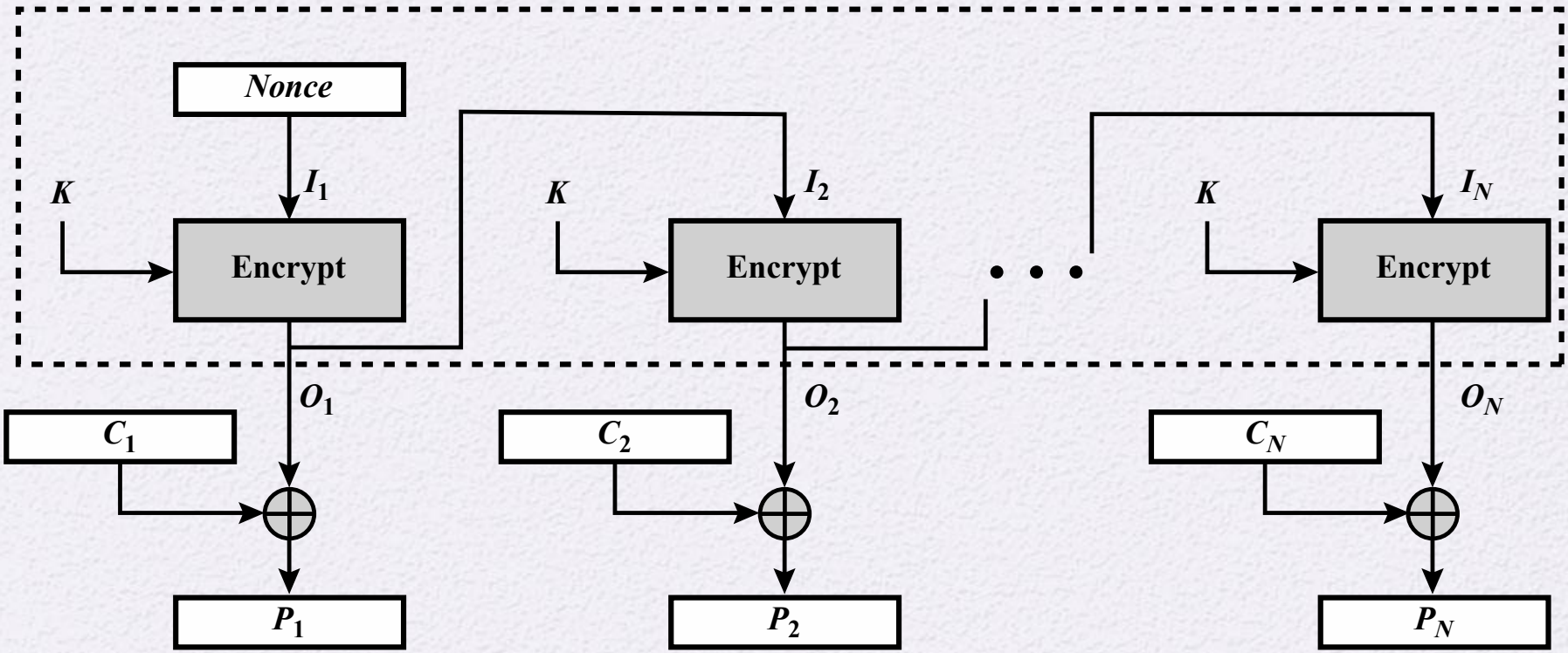
$O_j \oplus P_j = C_j$

CFB	$I_1 = IV$		$I_1 = IV$	
	$I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1}$	$j = 2, \ldots, N$	$I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1}$	$j = 2, \ldots, N$
	$O_j = \text{E}(K, I_j)$	$j = 1, \ldots, N$	$O_j = \text{E}(K, I_j)$	$j = 1, \ldots, N$
	$C_j = P_j \oplus \text{MSB}_s(O_j)$	$j = 1, \ldots, N$	$P_j = C_j \oplus \text{MSB}_s(O_j)$	$j = 1, \ldots, N$



(a) Encryption

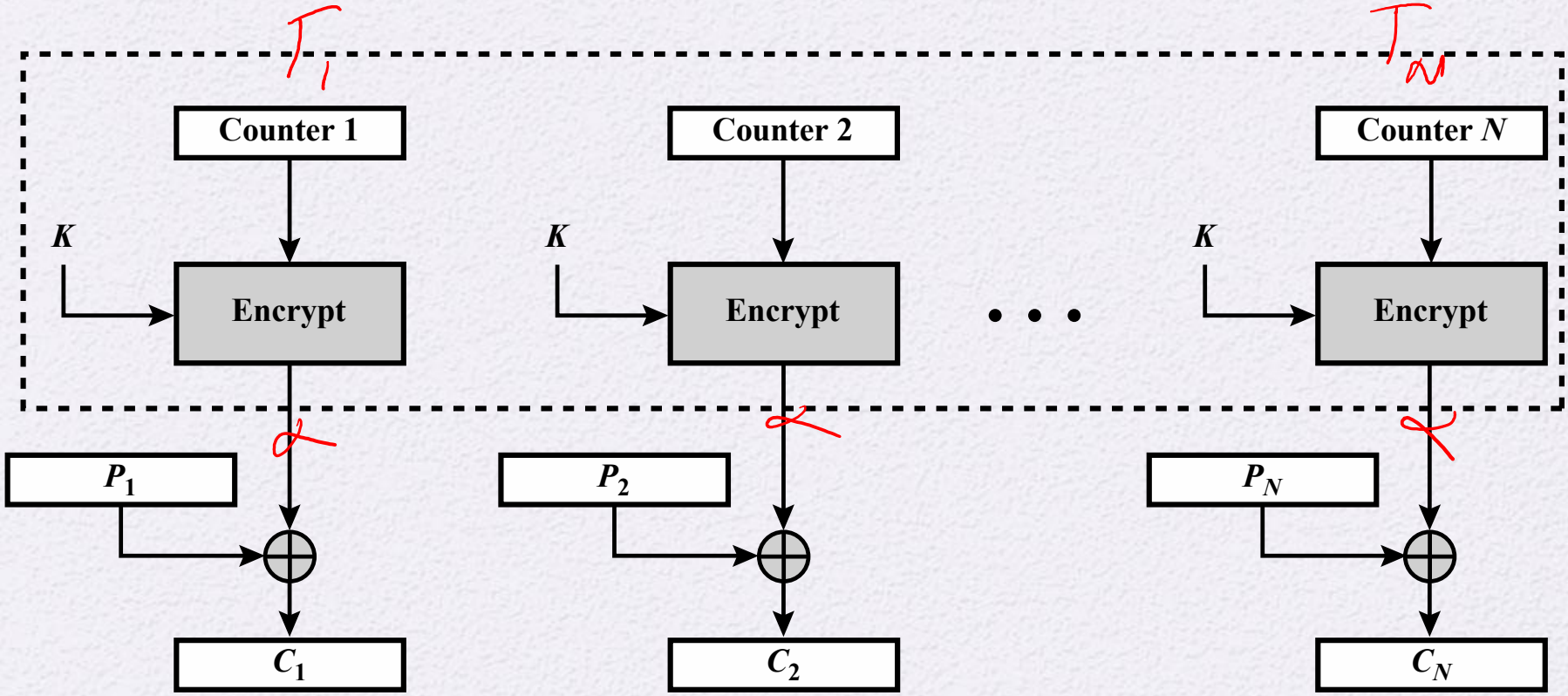
Figure 7.6 Output Feedback (OFB) Mode



(b) Decryption

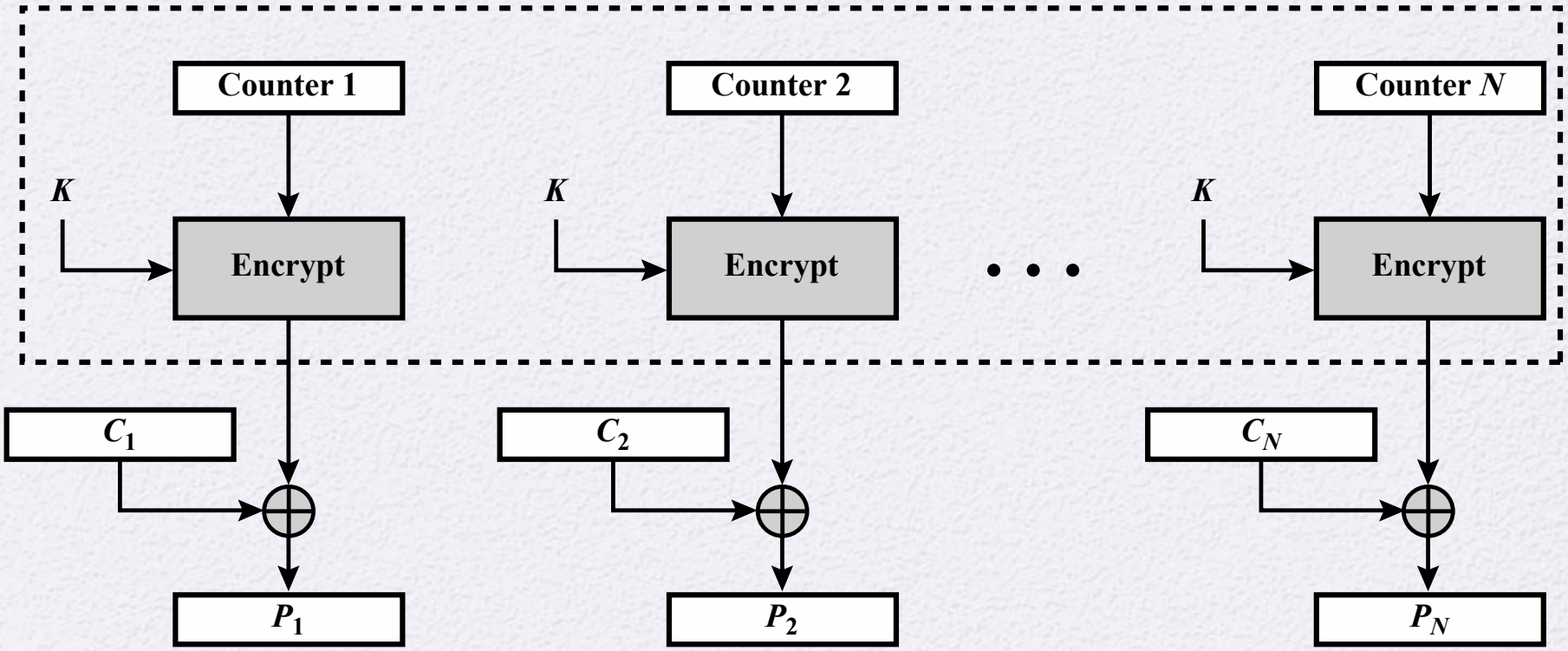
Figure 7.6 Output Feedback (OFB) Mode

OFB	$I_1 = Nonce$ $I_j = O_{j-1} \quad j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j) \quad j = 1, \ldots, N$ $C_j = P_j \oplus O_j \quad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u(O_N)$	$I_1 = Nonce$ $I_j = O_{j-1} \quad j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j) \quad j = 1, \ldots, N$ $P_j = C_j \oplus O_j \quad j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus \mathrm{MSB}_u(O_N)$



(a) Encryption

Figure 7.7 Counter (CTR) Mode

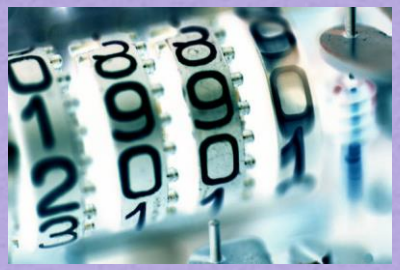


(b) Decryption

Figure 7.7 Counter (CTR) Mode

CTR	$C_j = P_j \oplus \mathrm{E}(K, T_j) \qquad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$	$P_j = C_j \oplus \mathrm{E}(K, T_j) \qquad j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$

Advantages of CTR



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

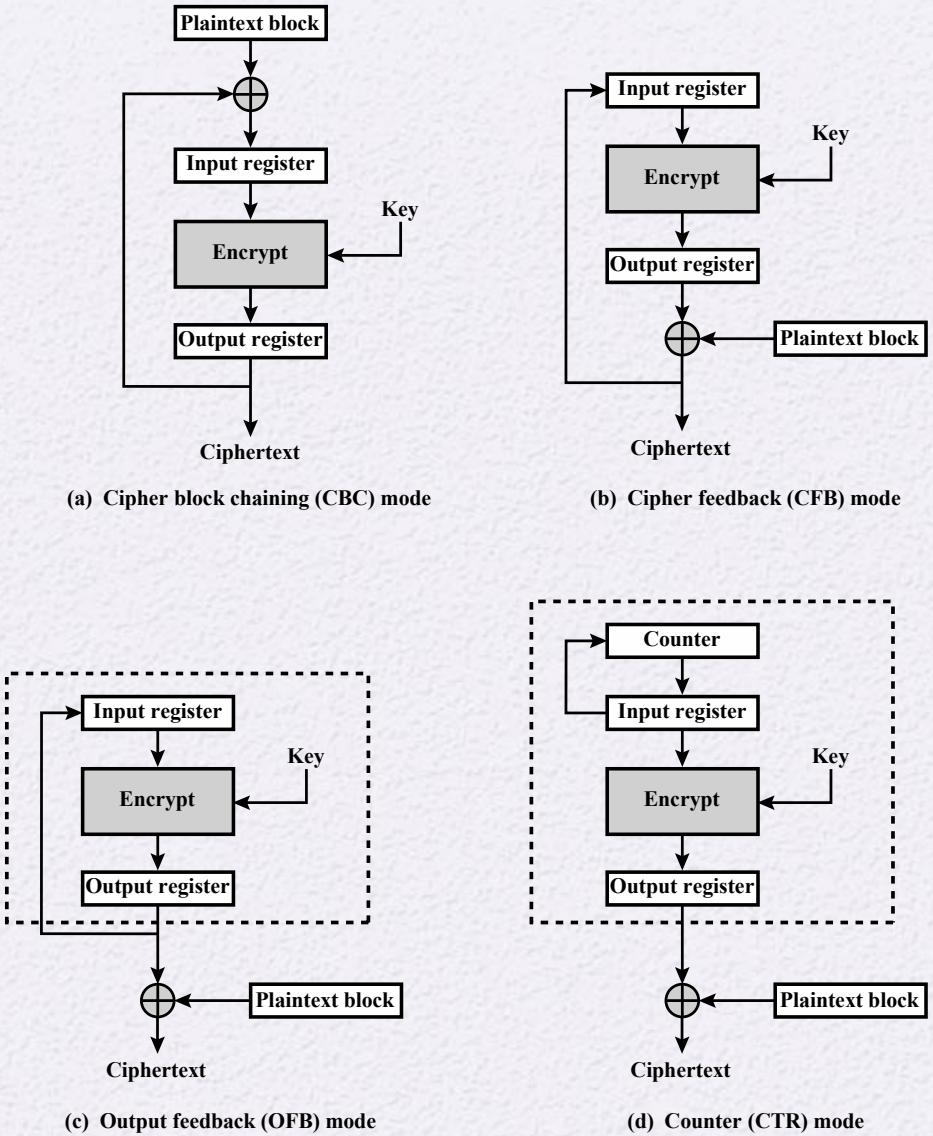
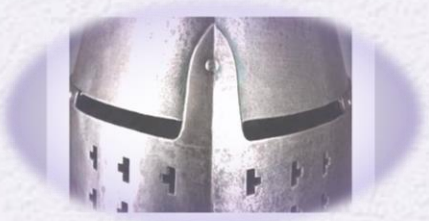


Figure 7.8 Feedback Characteristic of Modes of Operation

Summary

- Analyze the security of multiple encryption schemes



- Compare and contrast ECB, CBC, CFB, OFB, and counter modes of operation