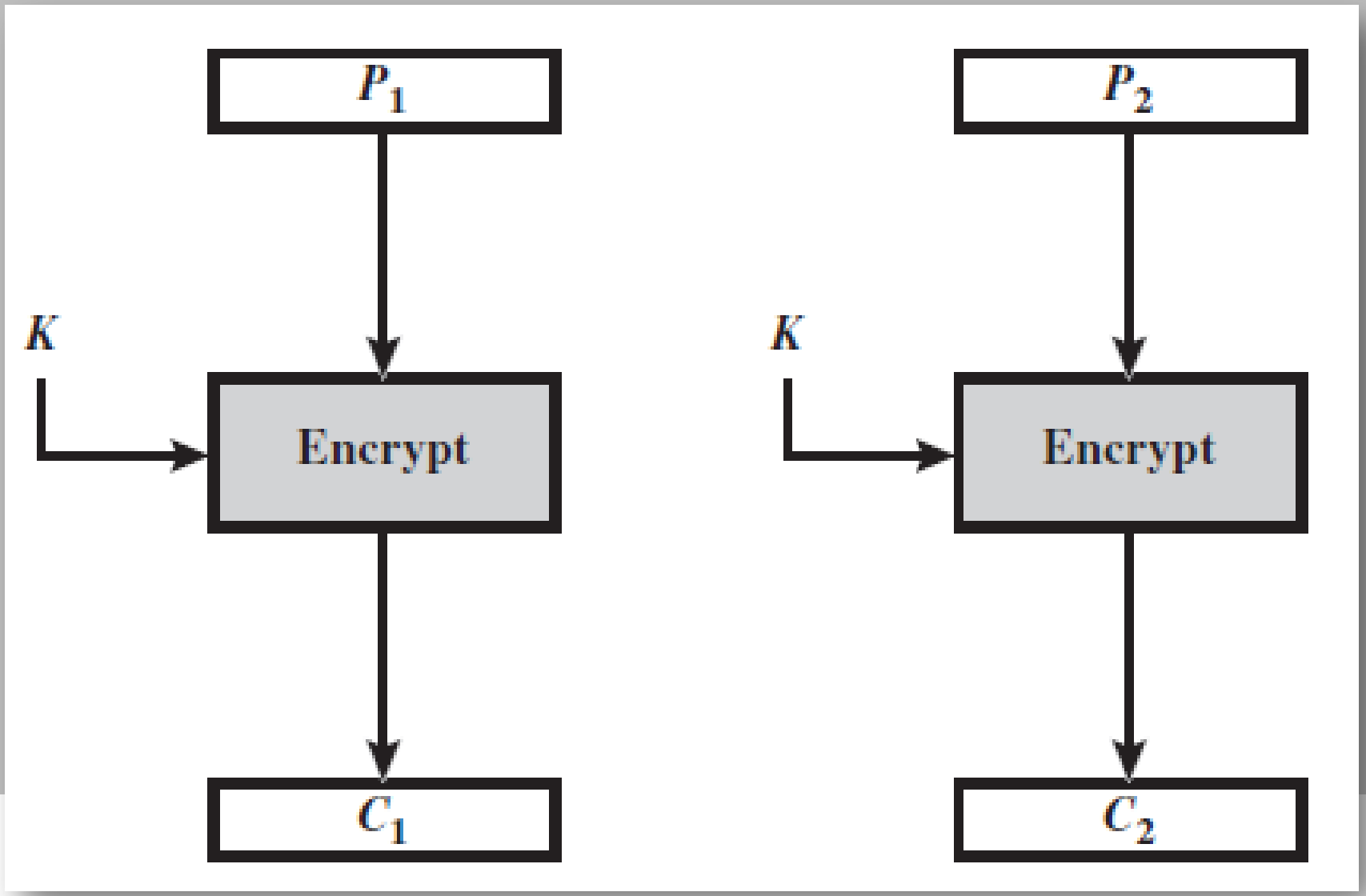
Modes of Operation for Block Ciphers

There are **five** different modes in which a block cipher, such as DES or AES, can be used:

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

Electronic Code Book (ECB)

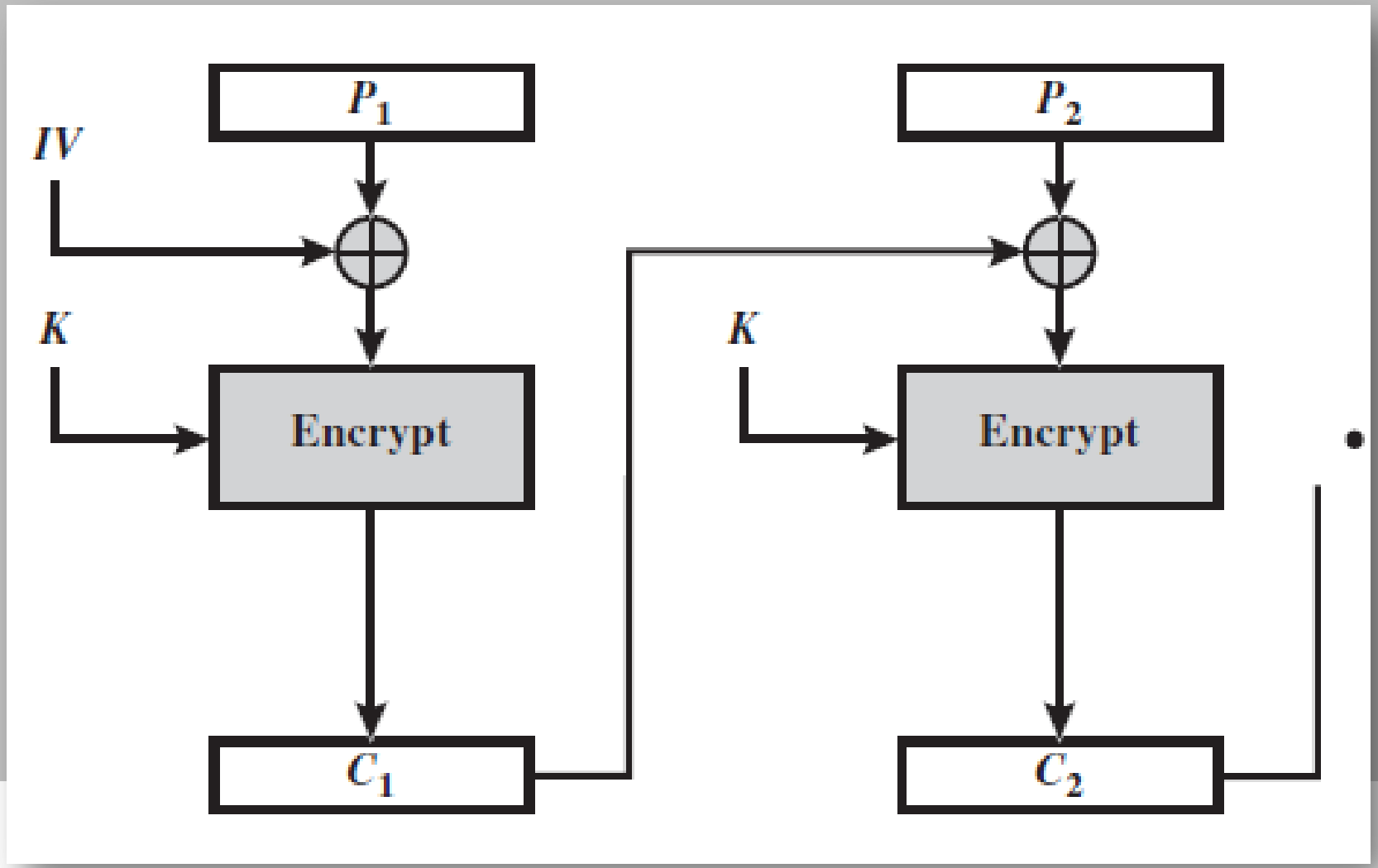
- Each block of plaintext is coded independently. Not very secure for long segments of plaintext, especially plaintext containing repetitive information.
- Used primarily for secure transmission of short pieces of information, such as an encryption key.
- Another shortcoming of ECB is that the length of the plaintext message must be integral multiple of the block size. When that condition is not met, the plaintext message must be padded appropriately.
- The rest of the modes discussed below provide enhanced security by making the ciphertext for any block a function of all the blocks seen previously.



ECB Encryption

CIPHER BLOCK CHAINING MODE (CBC)

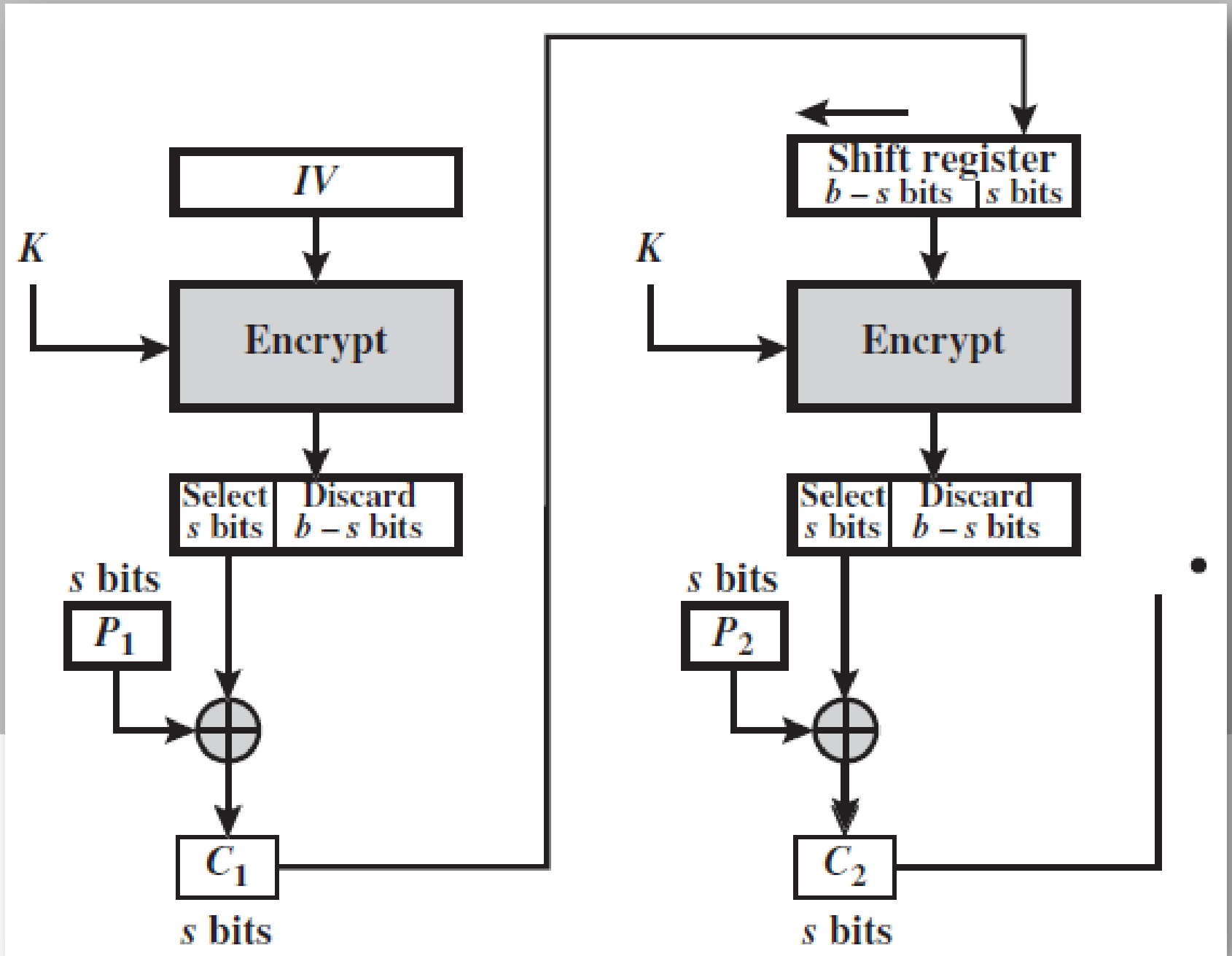
- The input to the encryption algorithm is the XOR of the next block of plaintext and the previous block of ciphertext. This is obviously ***more secure for long segments*** of plaintext.
- This mode also requires that length of the plaintext message be an integral multiple of the block size. When that condition is not satisfied, the message must be suitably padded.
- To get started, the chaining scheme obviously needs what is known as the initialization vector for the first invocation of the encryption algorithm.
- With this chaining scheme, the ciphertext block for any given plaintext block becomes a function of all the previous ciphertext blocks.



CBC Encryption

Cipher Feedback Mode (CFB)

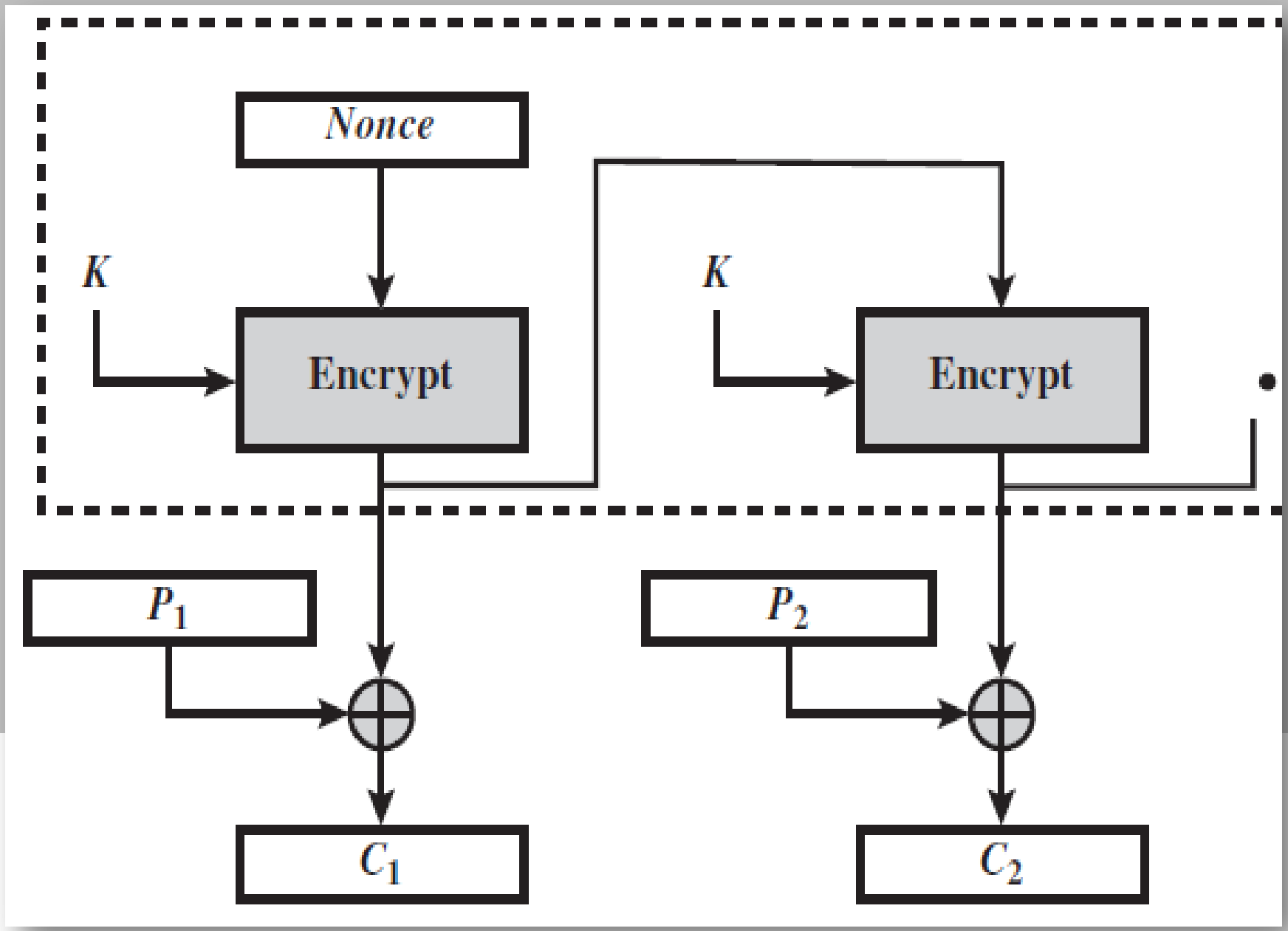
- Whereas the CBC mode uses all of the previous ciphertext block to compute the next ciphertext block, the CFB mode uses only a fraction thereof.
- Also, whereas in the CBC mode the encryption system digests b bits of plaintext at a time (where b is the block size used by the block cipher), now the encryption system digests only $s < b$ number of plaintext bits at a time even though the encryption algorithm itself carries out a b-bits to b-bits transformation. Since s can be any number, including one byte, that makes CFB suitable as a ***stream cipher***.
- CFB uses only the encryption algorithm in both encryption and decryption.



CFB Encryption

Output Feedback Mode (OFB)

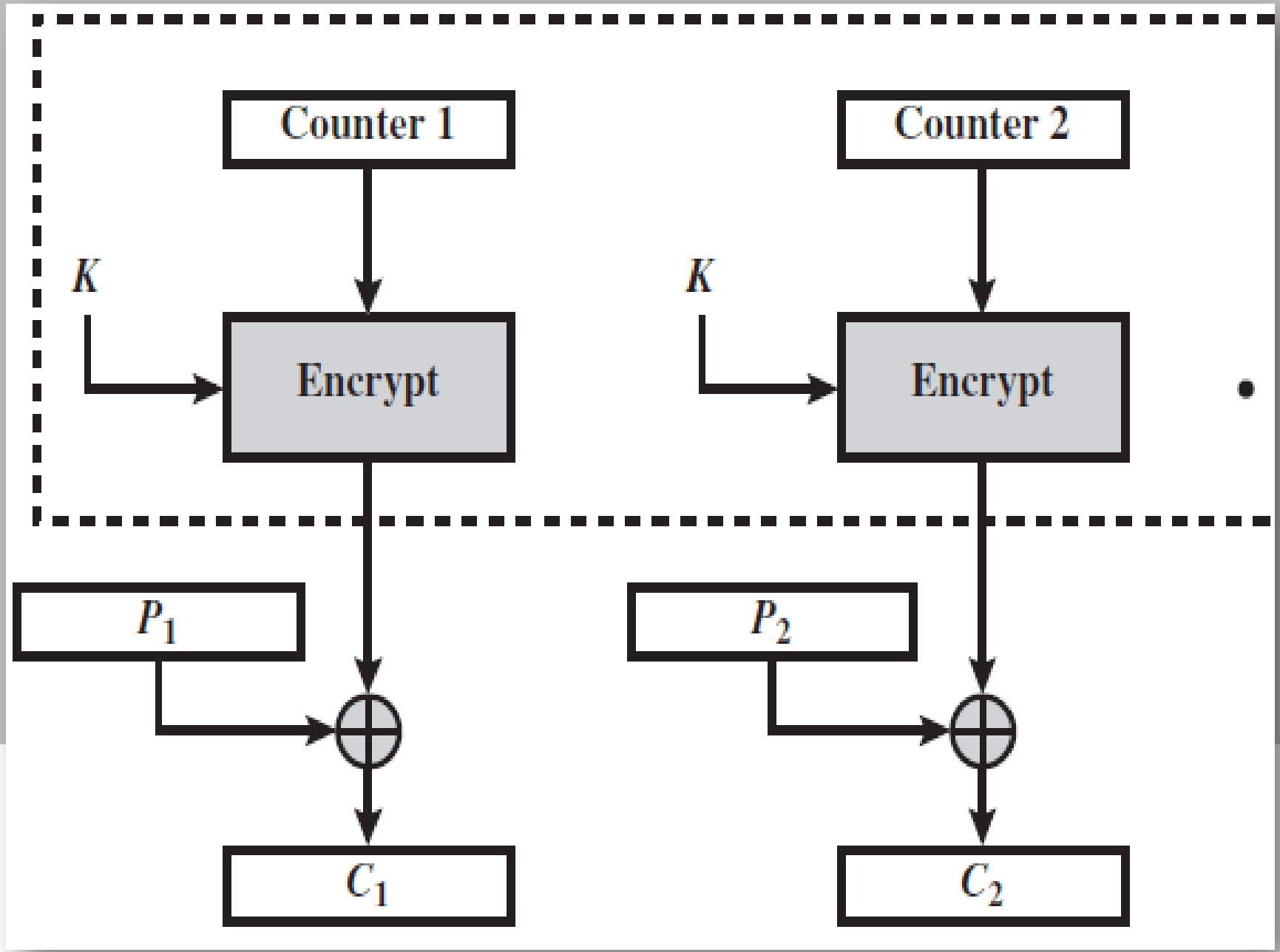
- The basic logic here is the same as in CFB, only the nature of what gets fed from stage to stage is different. In CFB, you feed $s < b$ number of ciphertext bits from the current stage into the b-bits to b-bits transformation carried out by the next-stage encryption. But in OFB, you feed s bits from the output of the transformation itself.
- This mode of operation is also suitable if you want to use a block cipher as a ***stream cipher***.
- Similarly to CFB, OFB uses only the encryption algorithm in both encryption and decryption.
- OFB is more resistant to transmission bit errors.



OFB Encryption

COUNTER MODE (CTR)

- Whereas the previous four modes for using a block cipher are intuitively plausible, this new mode at first seems strange and seemingly not secure. But it has been theoretically established that this mode is at least as secure as the other modes.
- As for CFB and OFB, an interesting property of this mode is that only the encryption algorithm is used at both the encryption end and at the decryption end.
- The basic idea consists of applying the encryption algorithm not to the plaintext directly, but to a b-bit number (and its increments modulo 2^b for successive blocks) that is chosen beforehand. The ciphertext consists of what is obtained by XORing the encryption of the number with a b-bit block of plaintext.



CTR Encryption

Advantages of CTR

1. Fast encryption and decryption. If memory is not a constraint, we can pre-compute the encryptions for as many counter values as needed. Then, at the transmit time, we only have to XOR the plaintext blocks with the pre-computed *b*-bit blocks. The same applies to fast decryption.
2. It has been shown that the CTR is at least as secure as the other four modes for using block ciphers.
3. Because there is no block-to-block feedback, the algorithm is highly amenable to implementation on parallel machines.
4. For the same reason, any block can be decrypted with random access.

Finally . . .

- **Acknowledgment:** These lecture notes are based on the textbook by William Stallings and notes prepared by Avinash Kak, Purdue University. My sincere thanks are devoted to them and to all other people who offered the material on the web.

- Students are advised to study and solve the problems and answer the questions in **Assignment-7**.