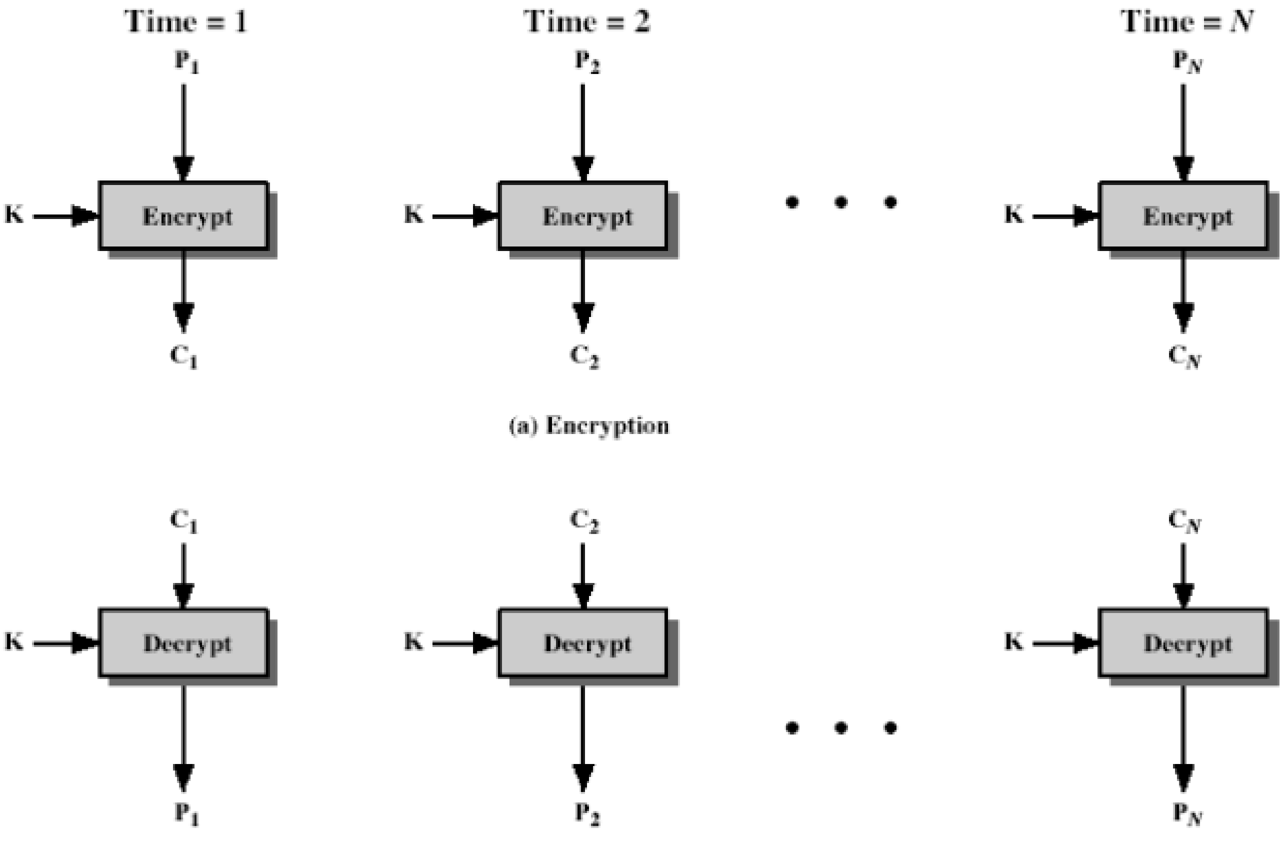
Block Cipher Modes of operations

- To apply a block cipher in a variety of applications, four "modes of operation" have been defined by NIST.

- 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.

Electronic code book (ECB)

The simplest mode is the electronic codebook (ECB) 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.



(a) Encryption

(b) Decryption

For a message longer than b bits, the procedure is simply to break the message into b-bit blocks, padding the last block if necessary. Decryption is performed one block at a time, always using the same key.

Advantages :

- The ECB method is ideal for a short amount of data, such as an encryption key.
- For the same b-bit block of plaintext, if it appears more than once in the message, ECB always produces the same cipher text.

For lengthy messages, the ECB mode may not be secure.

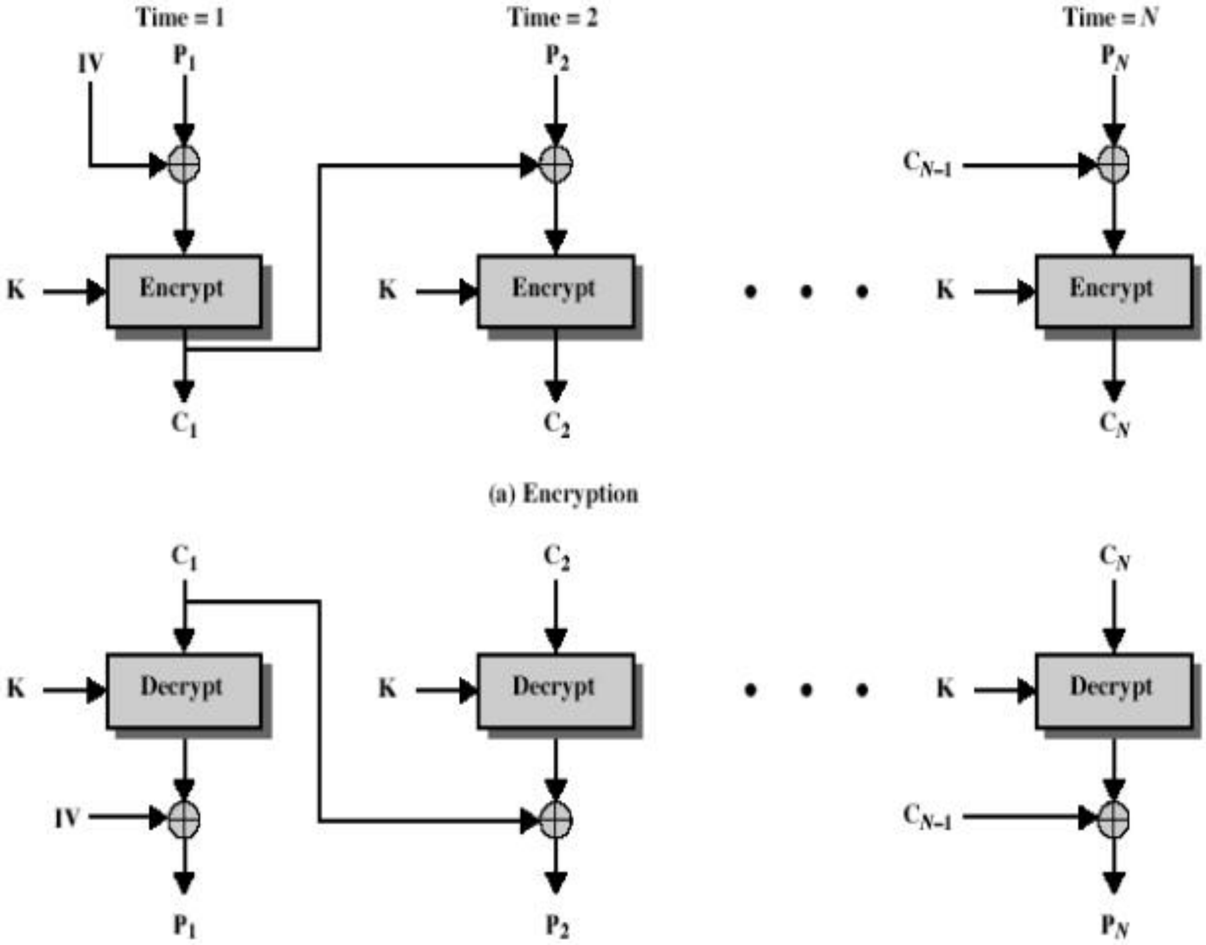
If the message is highly structured, it may be possible for a cryptanalyst to exploit these regularities.

Cipher Block Chaining Mode (CBC) –

I/P= current plaintext block XOR preceding cipher text block

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

There is no relationship between plaintext block.



(a) Encryption

(b) Decryption

Advantages :

An appropriate mode for encrypting messages of length greater than b bits. In addition to its use to achieve confidentiality, the CBC mode can be used for authentication.

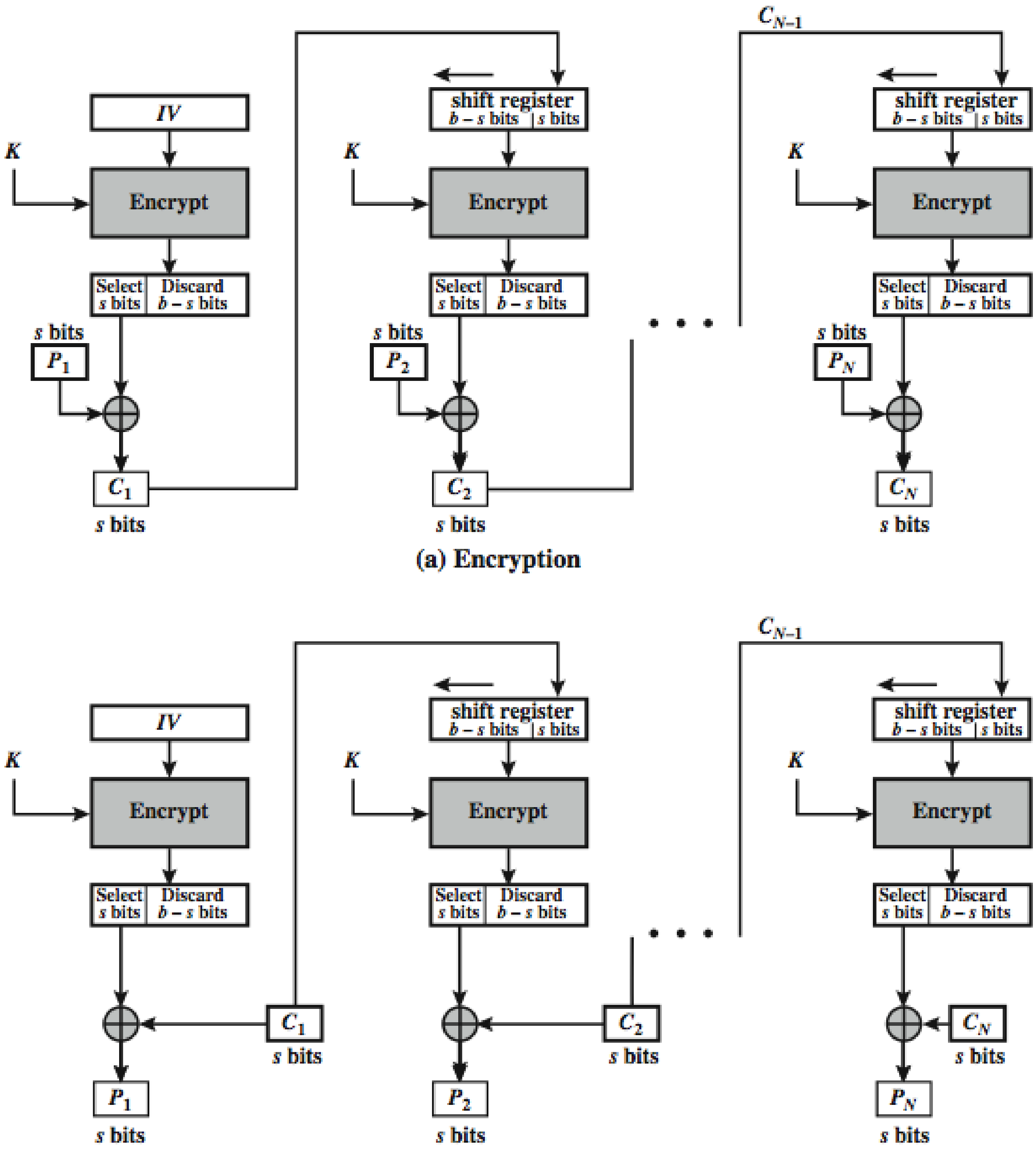
Cipher feedback mode

A stream cipher eliminates the need to pad a message to be an integral number of blocks. It also can operate in real time.

Thus, if a character stream is being transmitted, each character can be encrypted and transmitted immediately using a character-oriented stream cipher. The input to the encryption function is a *b*-bit shift register that is initially set to some initialization vector (IV).

The leftmost (most significant) *s* bits of the output of the encryption function are XORed with the first segment of plaintext *P1* to produce the first unit of ciphertext *C1*. The contents of the shift register are shifted left by s bits and C1 is placed in the rightmost.This process continues until all plaintext units have been encrypted.

For **decryption**, the same scheme is used, except that the received ciphertext unit is XORed with the output of the encryption function to produce the plaintext unit. Note that it is the **encryption function** that is used, not the decryption function. This is easily explained. Let Ss(X) be defined as the most significant s bits of X.



(a) Encryption

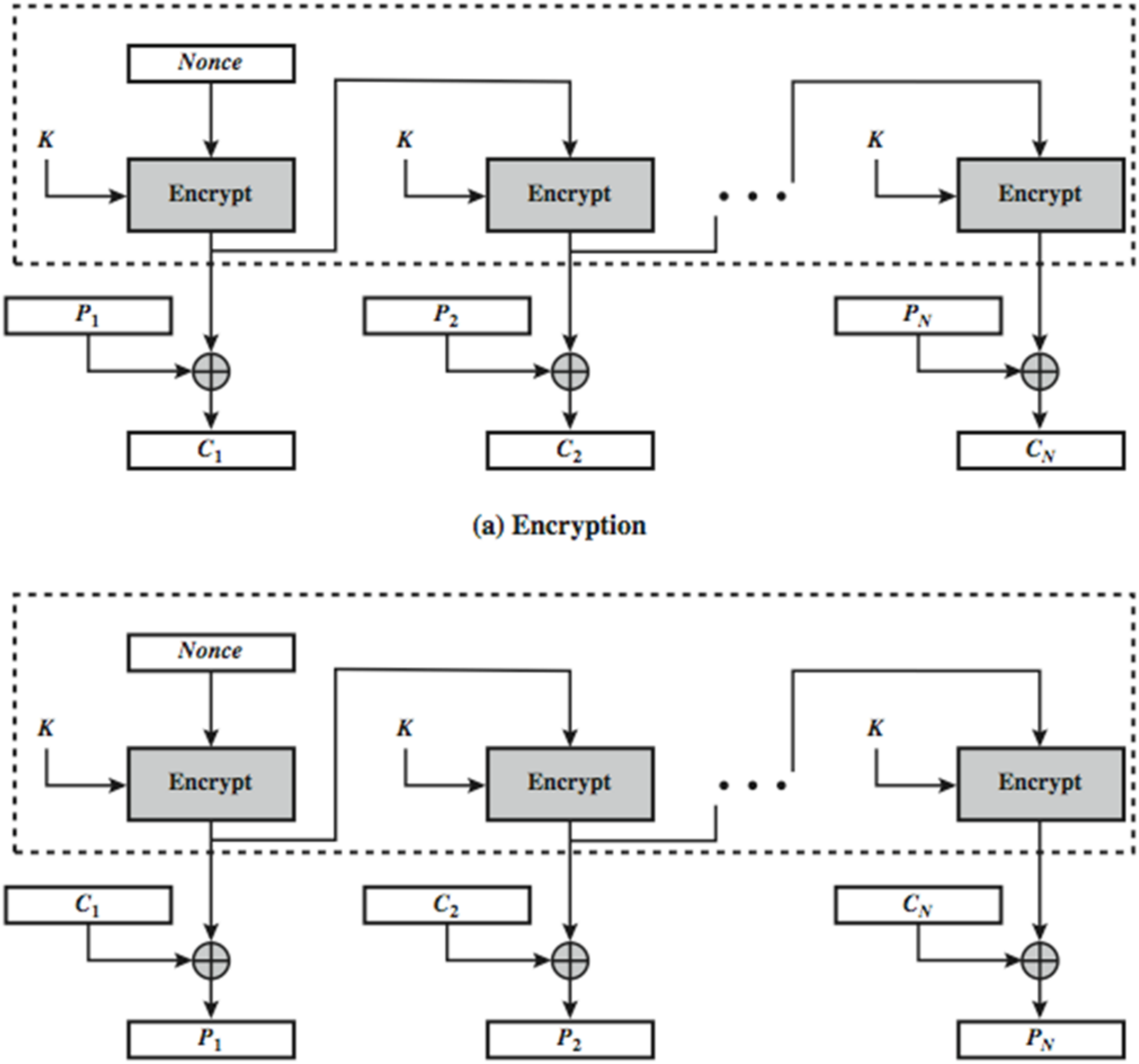
(b) Decryption

Output feedback mode

The output feedback (OFB) mode is similar in structure to that of CFB.

The output of the encryption function that is fed back to the shift

register in OFB, whereas in CFB the cipher text unit is fed back to the shift register.



(a) Encryption

(b) Decryption

Advantage :

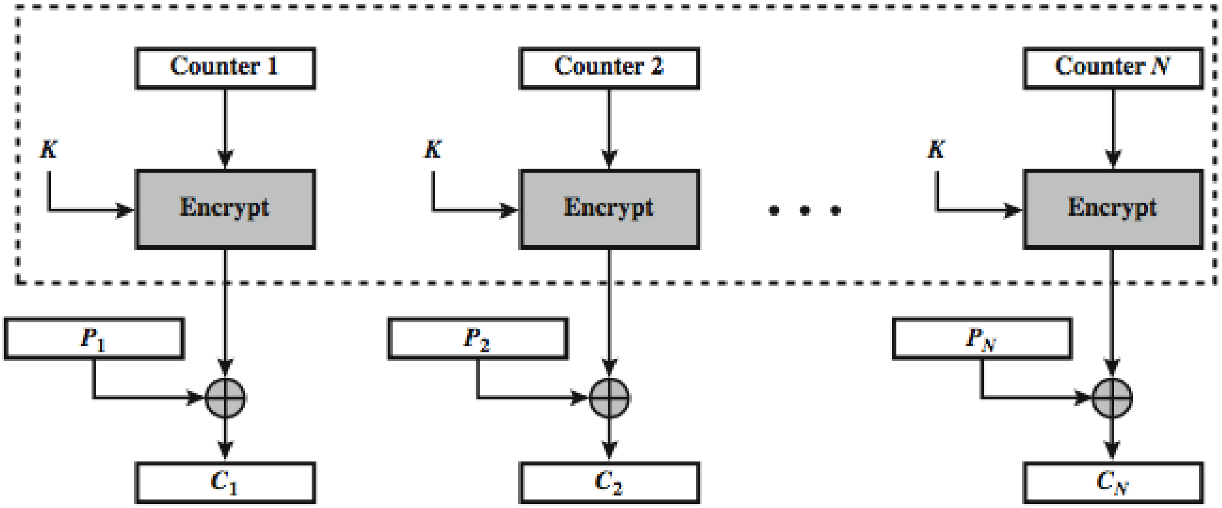
One advantage of the OFB method is that bit errors in transmission do not propagate.

Disadvantage :

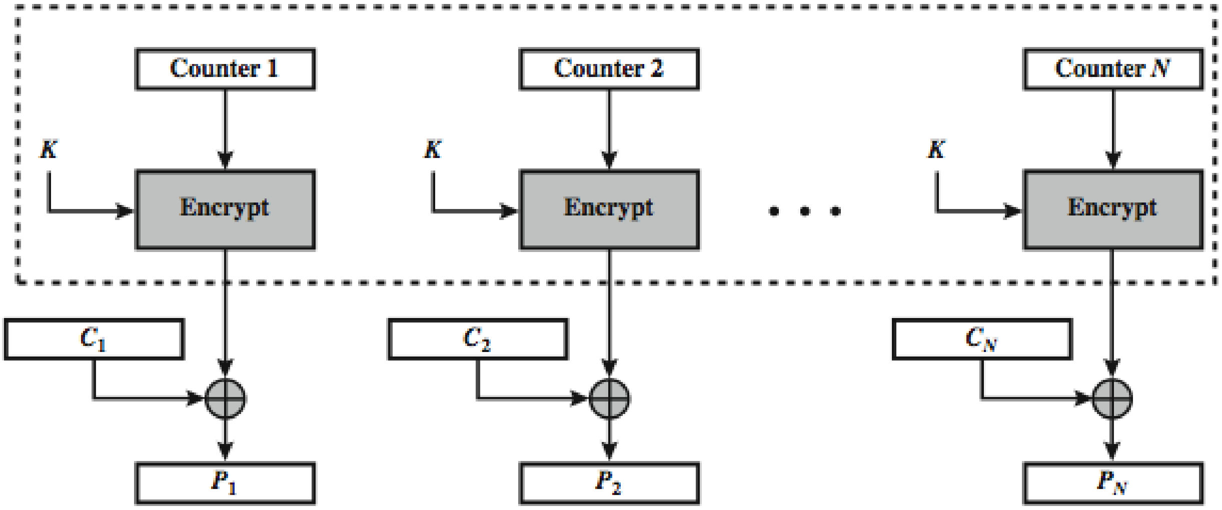
The disadvantage of OFB is that it is more vulnerable to a message stream modification attack than is CFB.

Counter Mode – (CTR)

A counter, equal to the plaintext block size is used. The counter is initialized to some value and then incremented by 1 for each subsequent block. For encryption, the counter is encrypted and then XORed with the plaintext block to produce the cipher text block; there is no chaining. For decryption, the same sequence of counter values is used, with each encrypted counter XORed with a cipher text block to recover the corresponding plaintext block.



(a) Encryption



(b) Decryption

Advantages :

Hardware efficiency: Unlike the three chaining modes, encryption (or decryption) in CTR mode can be done in parallel on multiple blocks of plaintext or cipher text.

Software efficiency: Similarly, because of the opportunities for parallel execution processors that support parallel features can be utilized

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

Random access: The ith block of plaintext or ciphertext can be processed in random-access fashion.