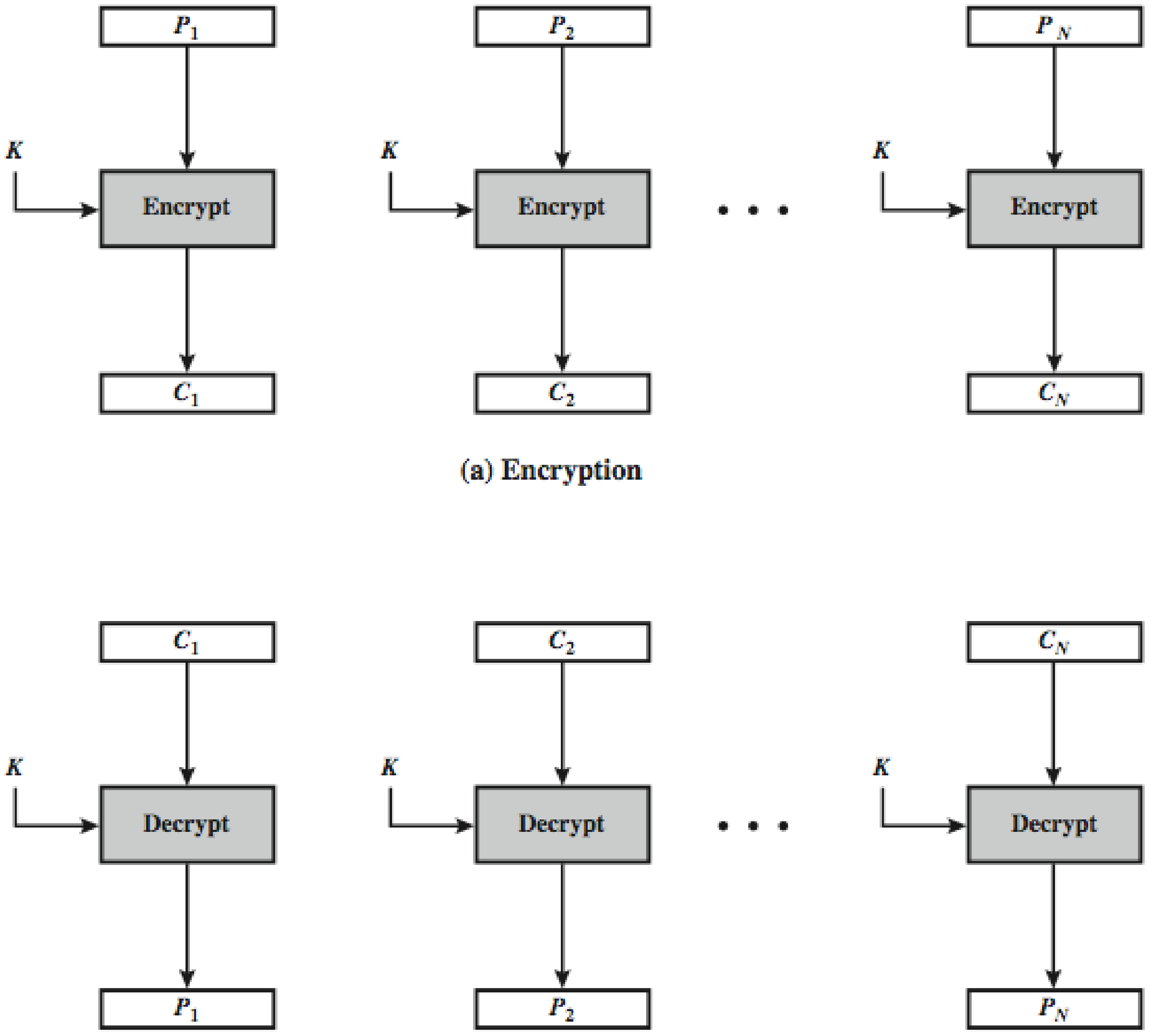
Modes of DES

DES has several **block** and **stream** modes to cover a wide variety of applications. Some of the modes are discussed below.

Electronic Code Book (ECB) Mode

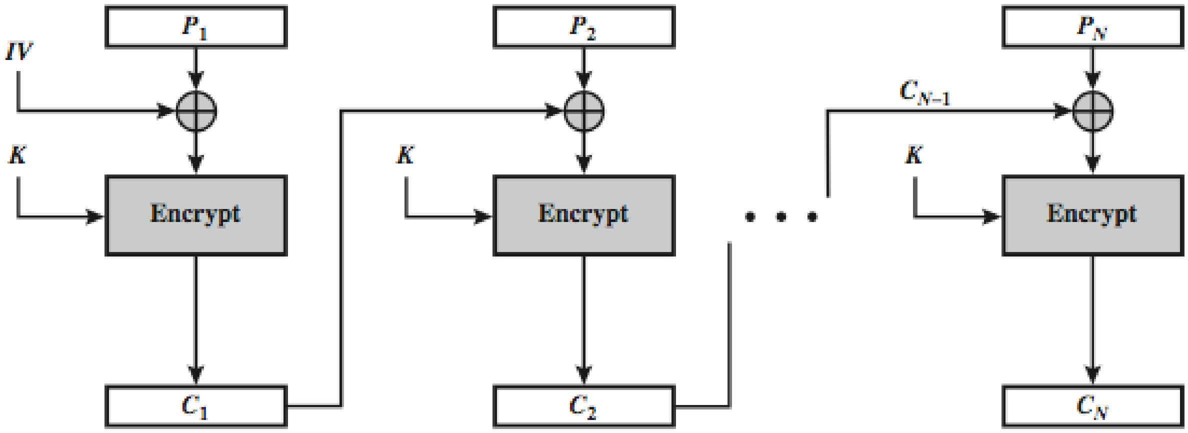


(a) Encryption

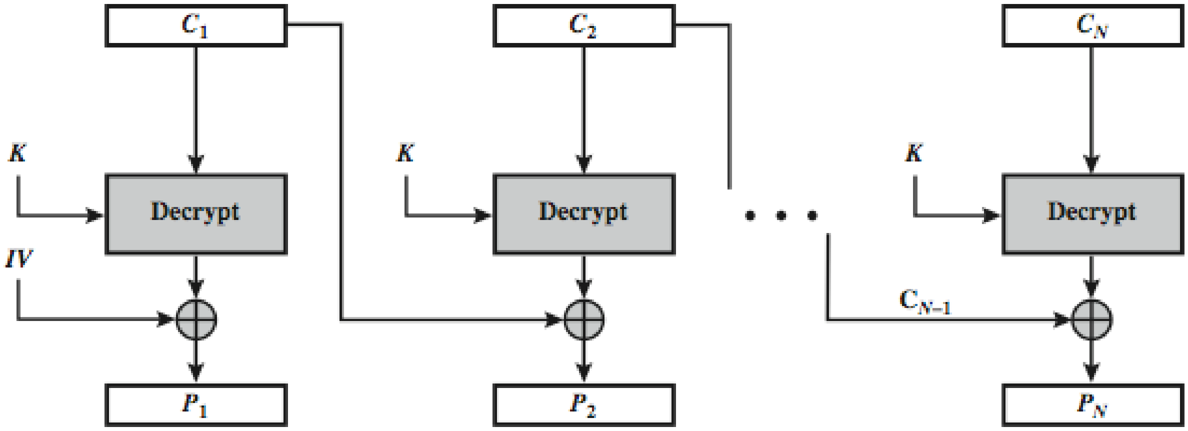
(b) Decryption

In EBC mode, message is broken into independent blocks which are encrypted. Here, each block is a value which is substituted, like a codebook, hence the name. In this mode, each block is encoded independently of the other blocks. It can be said $C_i = E_K(P_i)$

Cipher Block Chaining (CBC) Mode



(a) Encryption

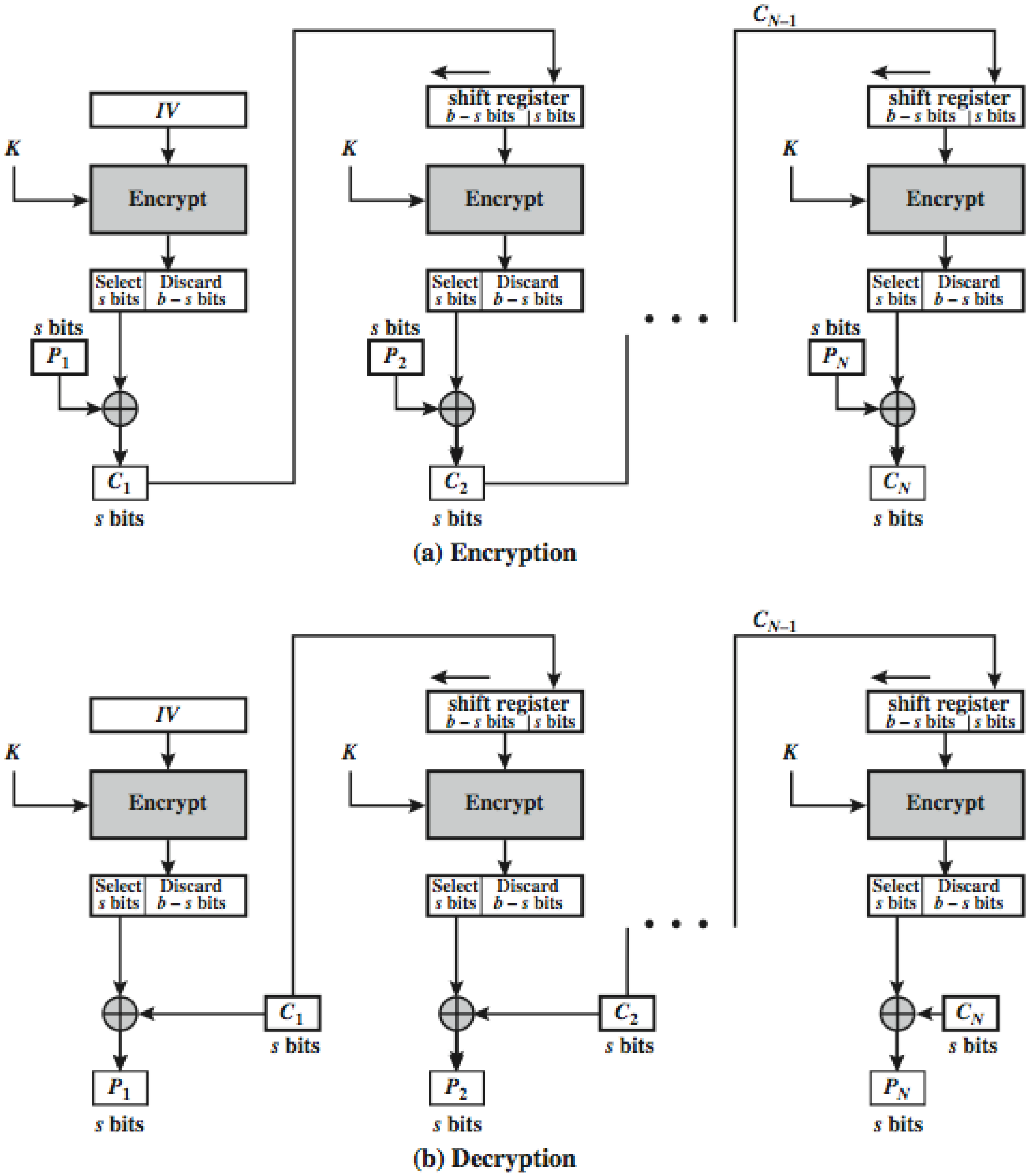


(b) Decryption

In CBC mode, message is broken into blocks and linked together in encryption operation. Each previous cipher block is chained with current plaintext block, hence name. The process uses Initial Vector (IV) to start process. IV must be known to the sender and the receiver.

- $C_i = E_K(P_i \text{ XOR } C_{i-1})$
- $C_{-1} = IV$

Cipher Feed Back (CFB) Mode



(a) Encryption

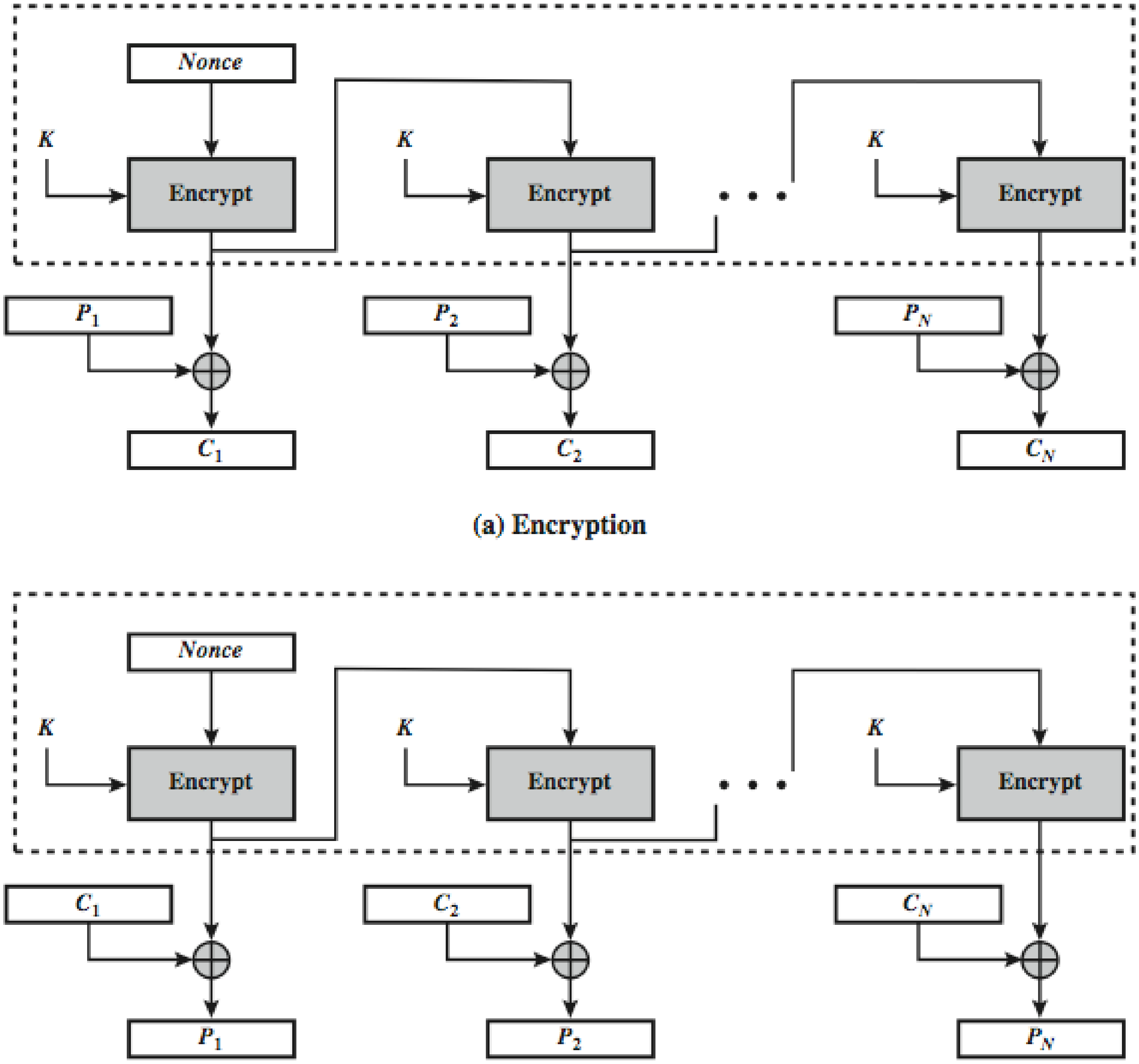
(b) Decryption

s-bit Cipher Feed Back (CFB-s)

Here, message is treated as a stream of bits and added to the output of the block cipher. The result is feedback for the next stage, hence the name. Standard allows any number of bit (1,8, 64 or 128 etc.) to be feedback, denoted CFB-1, CFB-8, CFB-64, CFB-128 etc.

- $C_i = P_i$ XOR $E_K(C_{i-1})$
- C_{-1} = IV

Output Feed Back (OFB) Mode



(a) Encryption

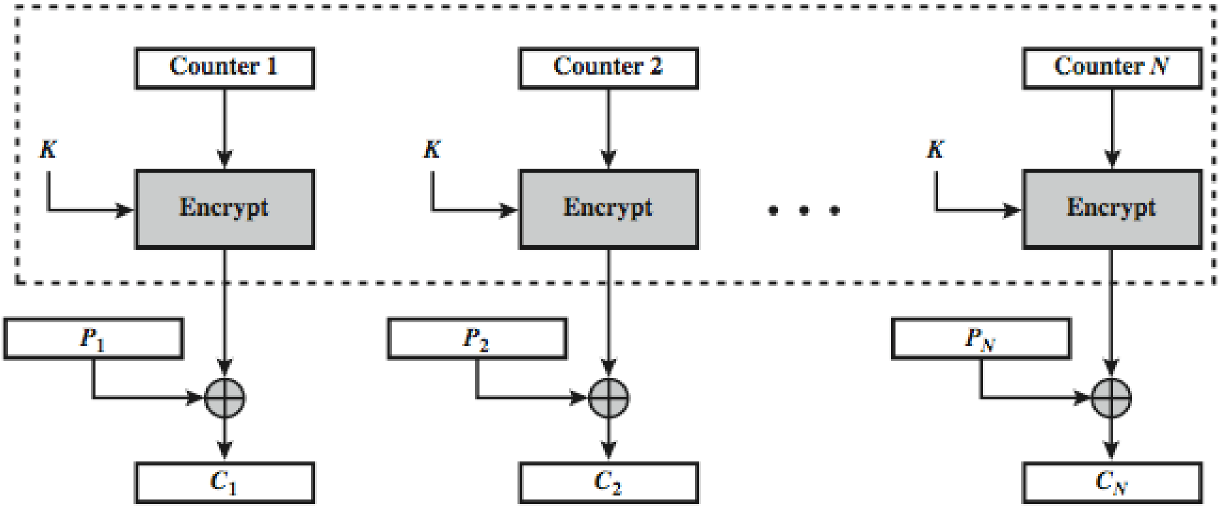
(b) Decryption

Here, Output of cipher is added to message. Output is then feedback (hence name). Feedback is independent of message and can be computed in advance.

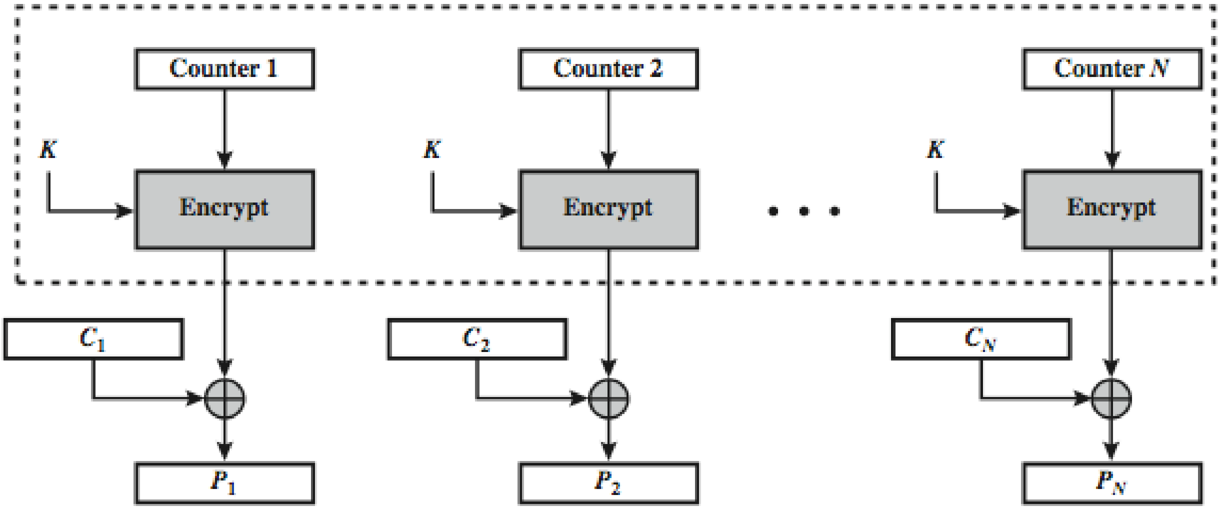
- $O_i = E_K(O_{i-1})$
- $C_i = P_i$ XOR O_i
- O_{-1} = IV

IV and nonce are often used interchangeably. However, a careful definition does differentiate between these two concepts. For our purposes, an IV is a nonce with an additional requirement: it must be selected in a nonpredictable way. That is, the IV can't be sequential; it must be random.

Counter (CTR) Mode



(a) Encryption



(b) Decryption

CTR is similar to OFB but encrypts counter value rather than any feedback value. It must have a different key & counter value for every plaintext block.

- $O_i = E_K(i)$
- $C_i = P_i$ XOR O_i