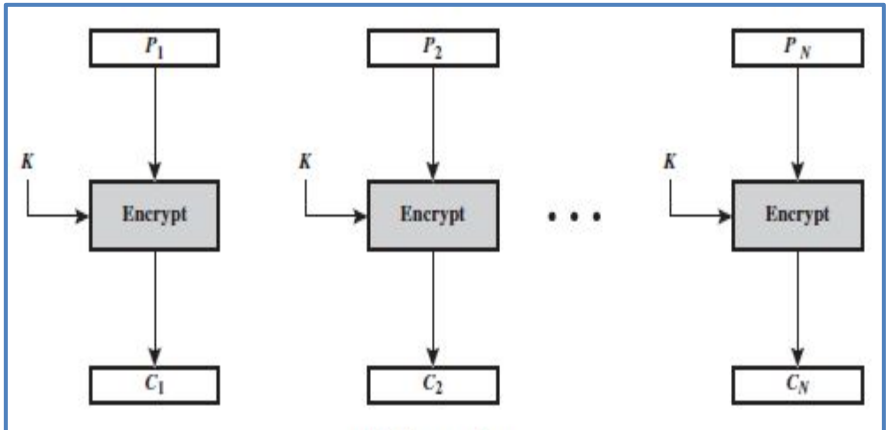
Block Cipher Modes of Operation

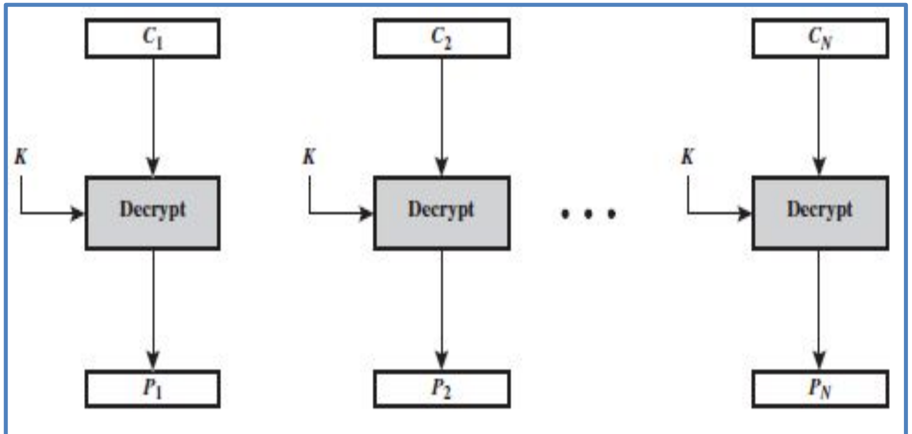
A block cipher takes a fixed-length block of text of length *b* bits and a key as input and produces a *b*-bit block of ciphertext. If the amount of plaintext to be encrypted is greater than ***b*** bits, then the block cipher can still be used by breaking the plaintext up into *b*-bit blocks. When multiple blocks of plaintext are encrypted using the same key, a number of security issues arise. To apply a block cipher in a variety of applications, five *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.

(1) Electronic code book (ECB): 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. The ECB method is ideal for a short amount of data, such as an encryption key.



(a) Encryption



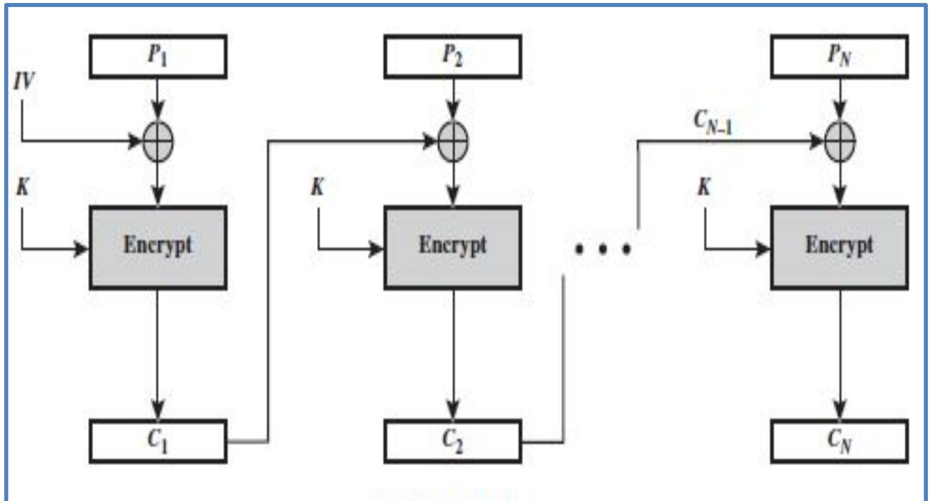
(b) Decryption

Block Cipher Modes of Operation

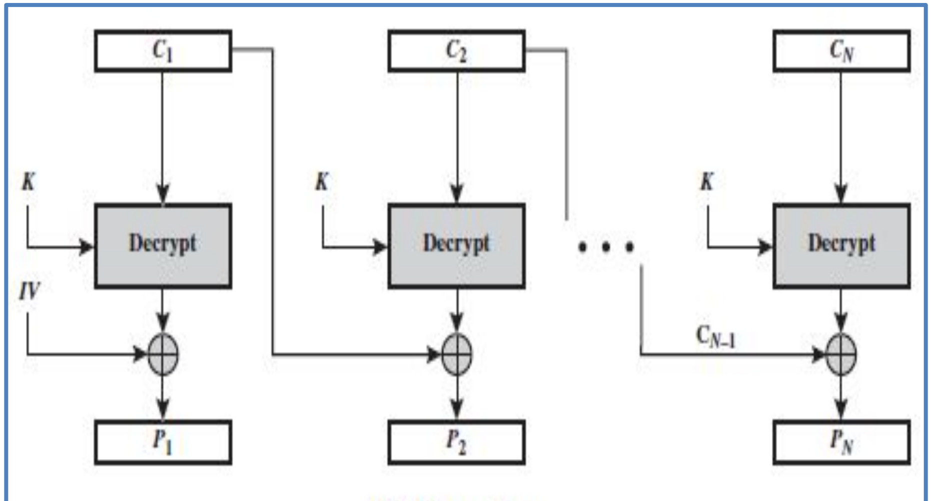
(2) Cipher Block Chaining Mode (CBC): In this scheme, the input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block; the same key is used for each block. Therefore, if the same plaintext block is repeated, different ciphertext blocks are produced. For decryption, each cipher block is passed through the decryption algorithm. The result is XORed with the preceding ciphertext block to produce the plaintext block. We can define CBC mode as

CBC	$C_1 = \mathrm{E}(K, [P_1 \oplus \mathrm{IV}])$	$P_1 = \mathrm{D}(K, C_1) \oplus \mathrm{IV}$
	$C_j = \mathrm{E}(K, [P_j \oplus C_{j-1}])\ j = 2, \ldots, N$	$P_j = \mathrm{D}(K, C_j) \oplus C_{j-1}\ j = 2, \ldots, N$

The **IV** is an initialization block, which is produced using random number generator and it should be the same size as the cipher block. This must be known to both the sender and receiver but it should be unpredictable by a third party.



(a) Encryption



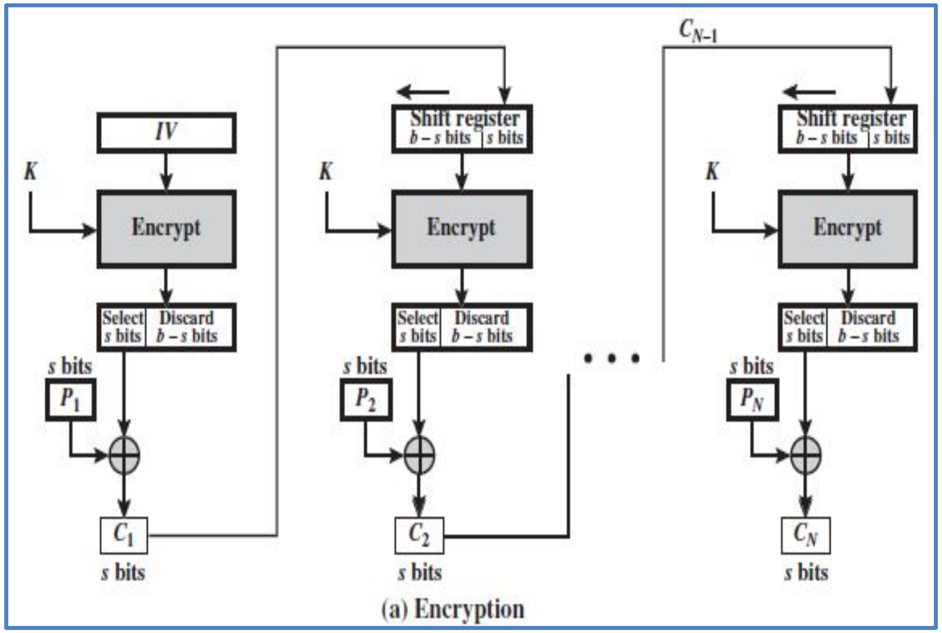
(b) Decryption

Block Cipher Modes of Operation

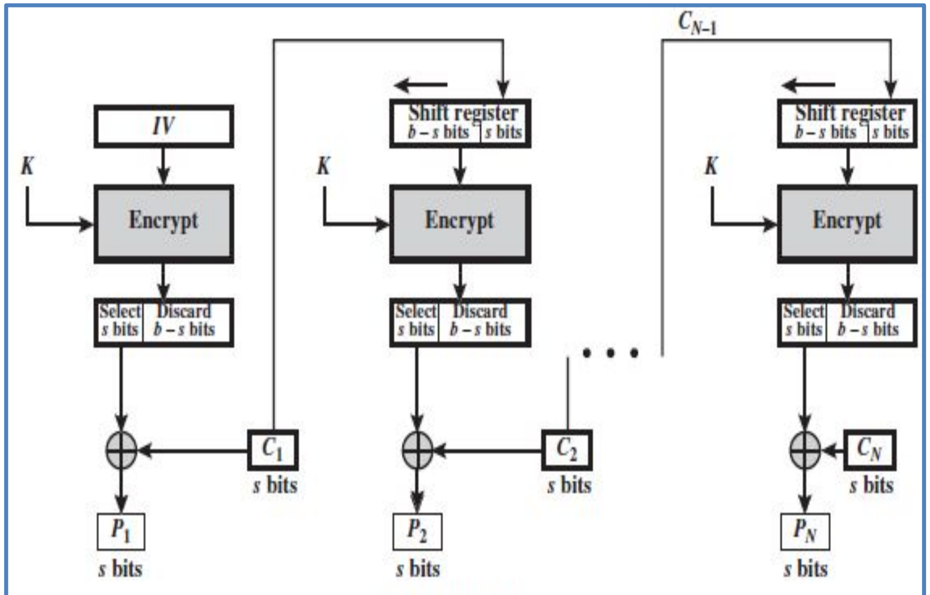
(3) Cipher Feedback Mode (CFB): In this scheme, the input is processed ***s*** bits at a time. The preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with the plaintext to produce the next unit of ciphertext. We can define CFB mode as follows:

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

Where **LSB** is defined as the most significant ***s*** bits of *X*.



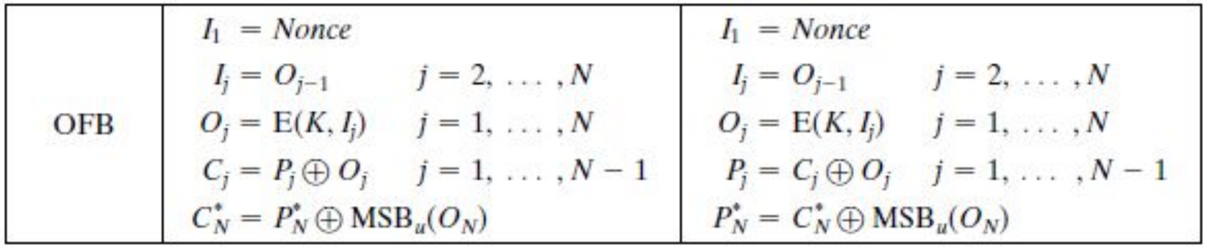
(a) Encryption



(b) Decryption

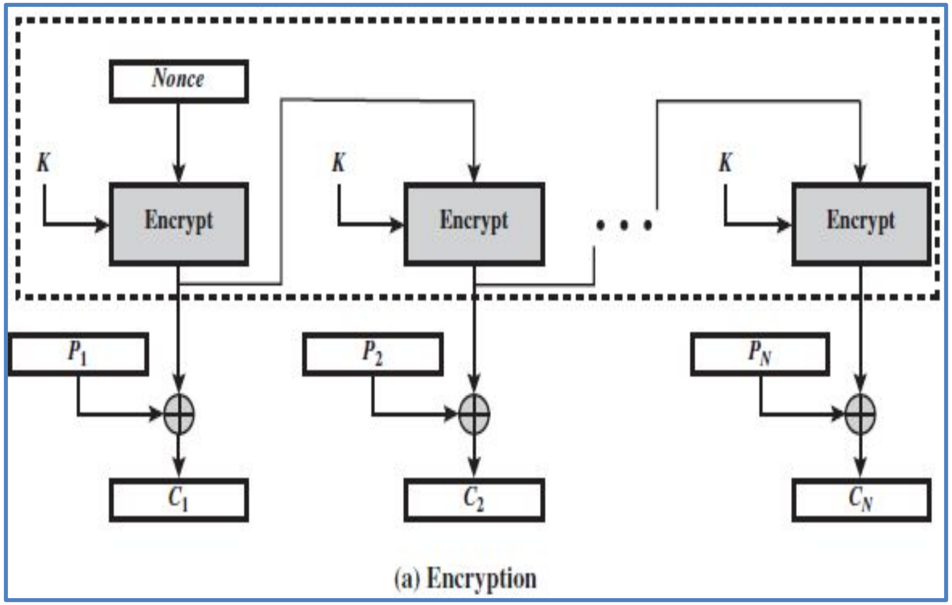
Block Cipher Modes of Operation

(4) Output Feedback Mode (OFB): This scheme operates on full blocks of plaintext and ciphertext where the output of the encryption function is fed back to become the input for encrypting the next block of plaintext. We can define OFB mode as follows:

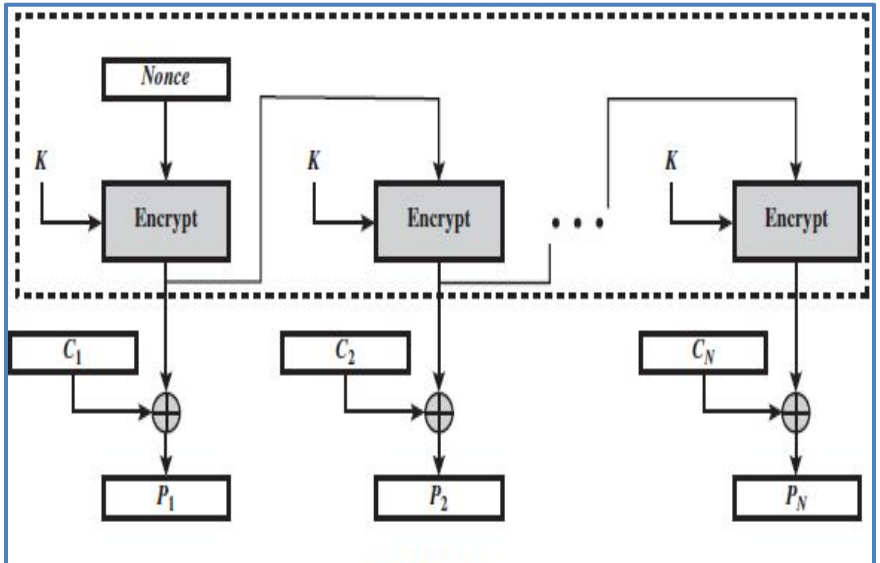


OFB	$I_1 = \mathit{Nonce}$ $I_j = O_{j-1} \qquad j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j) \qquad j = 1, \ldots, N$ $C_j = P_j \oplus O_j \qquad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u(O_N)$	$I_1 = \mathit{Nonce}$ $I_j = O_{j-1} \qquad j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j) \qquad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

Let the size of a block be ***b***. If the last block of plaintext contains ***u*** bits, with ***u* < *b***, the most significant ***u*** bits of the last output block $\boldsymbol{O_N}$ are used for the XOR operation. In the case of OFB, the IV must be a nonce; that is, the IV must be unique to each execution of the encryption operation.



(a) Encryption



(b) Decryption

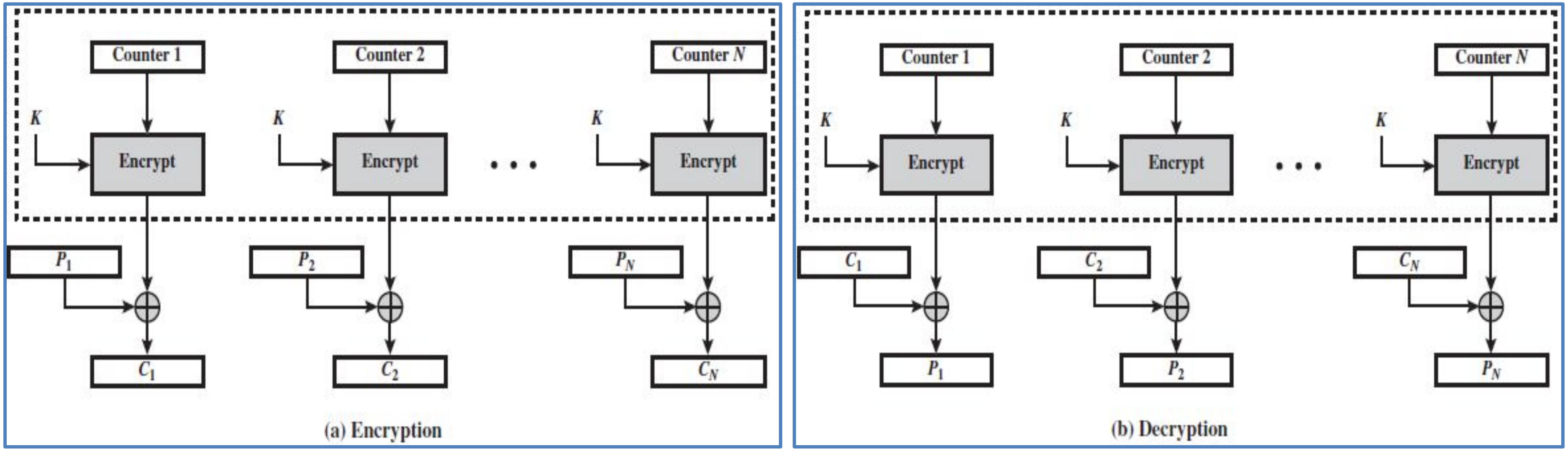
Block Cipher Modes of Operation

* One advantage of the OFB method is that bit errors in transmission do not propagate. The disadvantage of OFB is that it is more vulnerable to a message stream modification attack than in CFB.

(5) Counter Mode (CTR): In this mode, each block of plaintext is XORed with an encrypted counter. Typically, the counter is initialized to some value and then incremented by 1 for each subsequent block being encrypted using the same key. Given a sequence of counters $\boldsymbol{T_1}$, $\boldsymbol{T_2}$, …, $\boldsymbol{T_N}$, we can define CTR mode as follows:

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

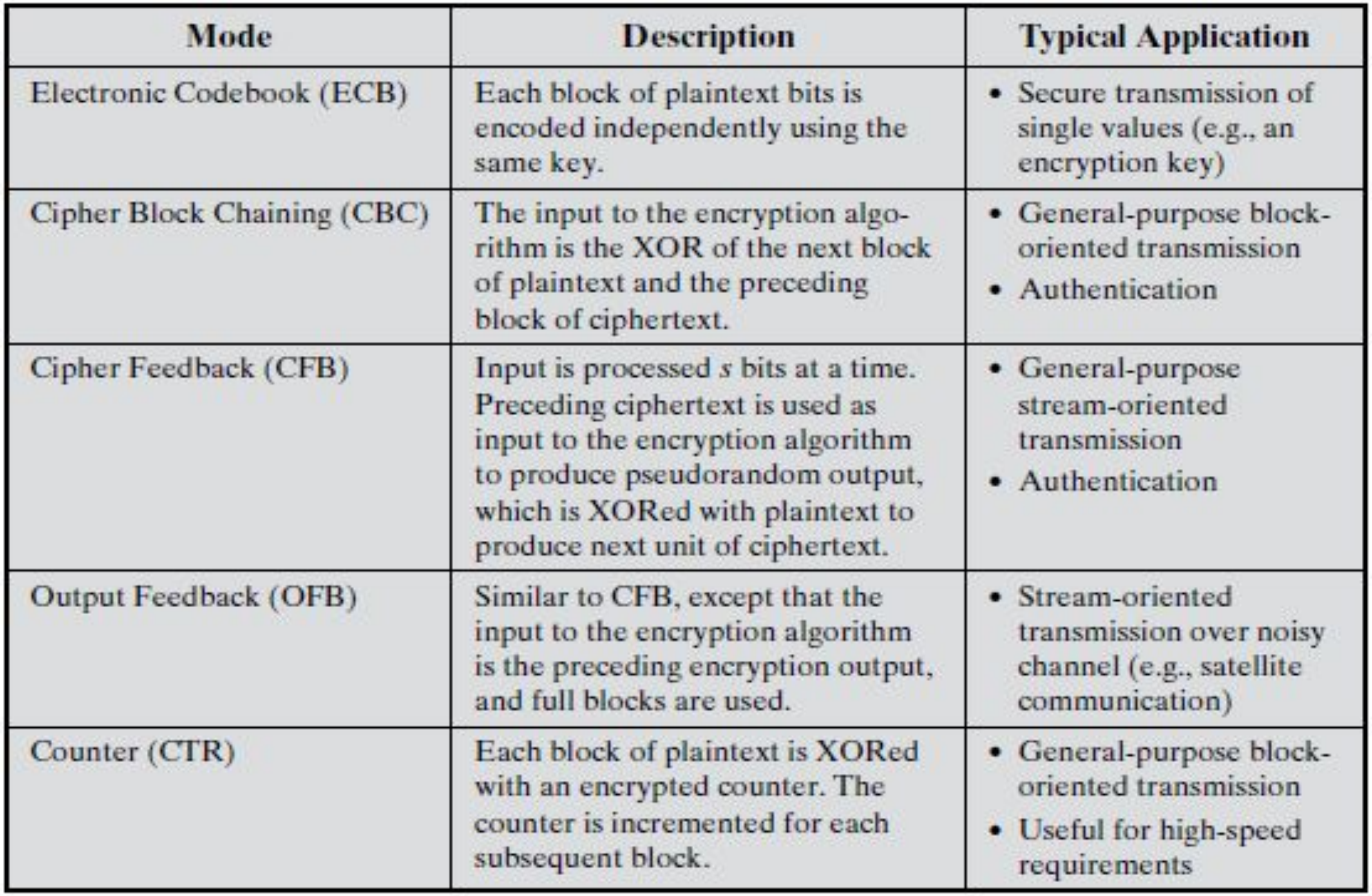
The advantages of the CTR are (1) hardware and software efficiency, (2) preprocessing, (3) random access, (4) provable security and (5) simplicity.



(a) Encryption

(b) Decryption

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