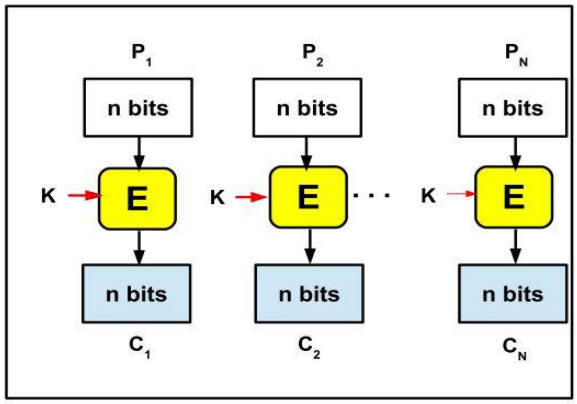
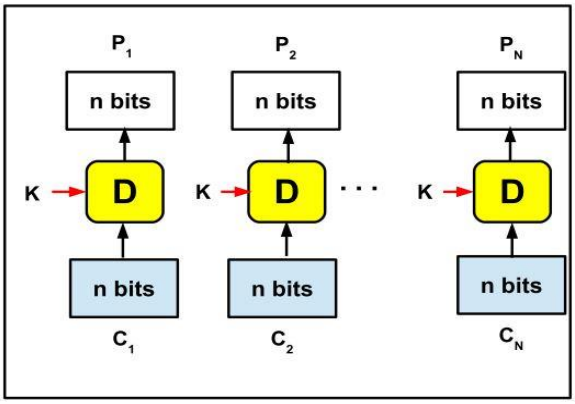
Block Cipher's Mode of Operation

Electronic Code Book (ECB) :

- Encryption : $C_i=E_k(P_i)$
- Decryption : $P_i=D_k(C_i)$



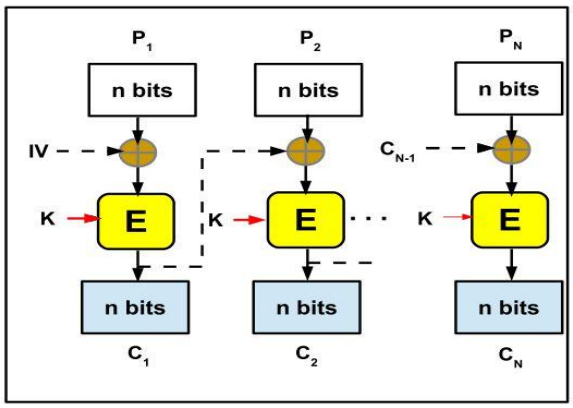
Encryption



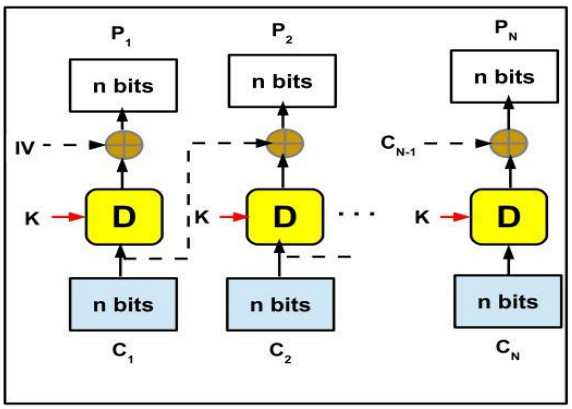
Decryption

Cipher Block Chaining (CBC) :

- Encryption : $C_i=E_k(P_i \oplus C_{i-1})$, with $C_0=IV$
- Decryption : $P_i=D_k(C_i) \oplus C_{i-1}$, with $C_0=IV$



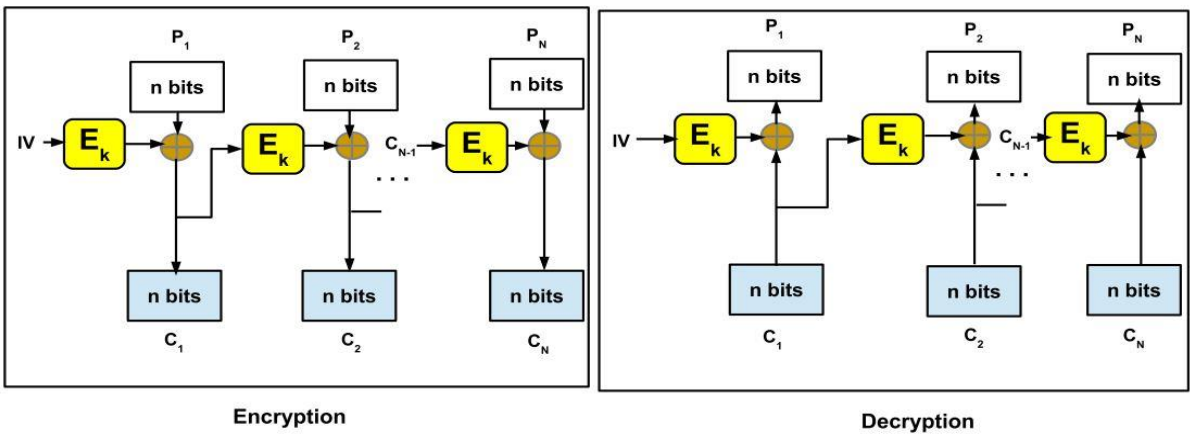
Encryption



Decryption

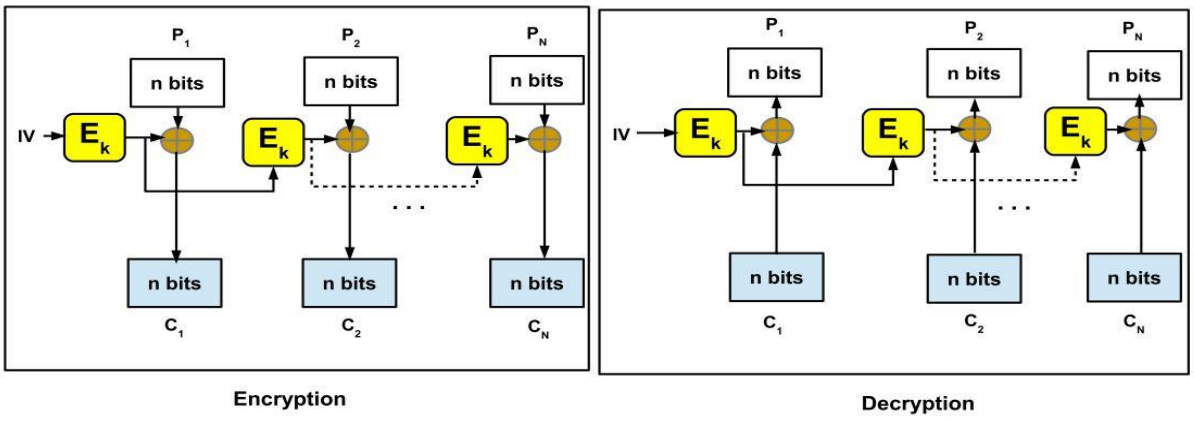
Cipher FeedBack (CFB) :

- Encryption : $Ci=Pi \oplus E_k\ (Ci-1)$, with $C0=IV$
- Decryption : $P_i=C_i \oplus E_k(C_{i-1})$, with $C_0=IV$ (the same encryption function E_K is used for decryption)



Output FeedBack (OFB) :

- Encryption : $Z_i = E_k(Z_{i-1})$; $C_i = P_i \oplus Z_i$, with $Z_0 = C_0 = IV$
- Decryption : $Z_i = E_k(Z_{i-1})$; $P_i = C_i \oplus Z_i$, with $Z_0 = C_0 = IV$



Counter (CTR) mode :

- Encryption : $C_i = P_i \oplus E_k$ [nonce + i] (i: a counter ; nonce used only once equivalent to an IV)
- Decryption : $P_i = C_i \oplus E_k$ [nonce + i]