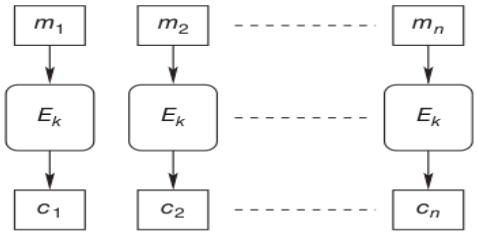
ECB Electronic Code Book NEVER USED

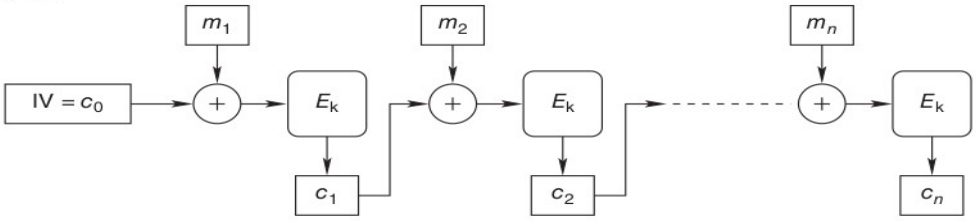
$$c_i = E_k(m_i)$$



CBC Cipher Block Chaining WIDELY USED

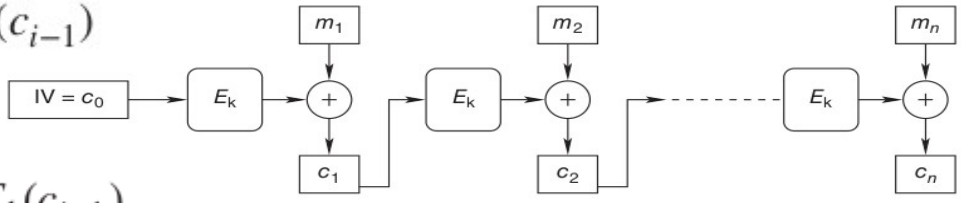
$$c_i = E_k(m_i \oplus c_{i-1})$$

$$D_k = E_k^{-1}: m_i = c_{i-1} \oplus D_k(c_i).$$



CFB Cipher FeedBack NETWORK USED

$$c_i = m_i \oplus E_k(c_{i-1})$$

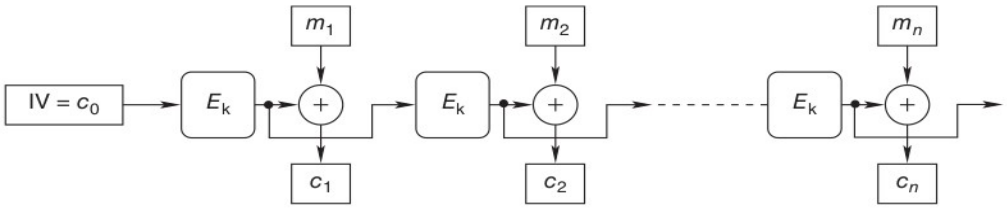


$$m_i = c_i \oplus E_k(c_{i-1})$$

OFB Output FeedBack MINIMAL CIRCUITS

$$z_0 = c_0 \; ; \; z_i = E_k(z_{i-1}) \; ; \; c_i = m_i \oplus z_i$$

$$z_i = E_k(z_{i-1}) \; ; \; m_i = c_i \oplus z_i$$



CTR Counter Mode Encryption PARALLEL IMPLEMENTATION

$$c_i = m_i \oplus E_k(T + i)$$

$$m_i = c_i \oplus E_k(T + i).$$