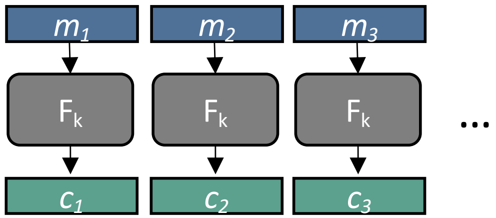
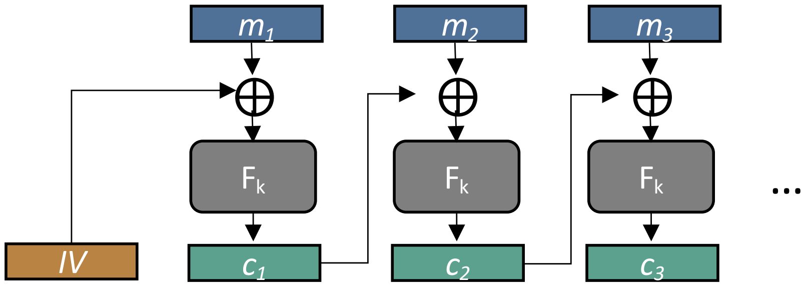
Modes of Operation (Block Ciphers)-

Electronic Code Book (ECB)



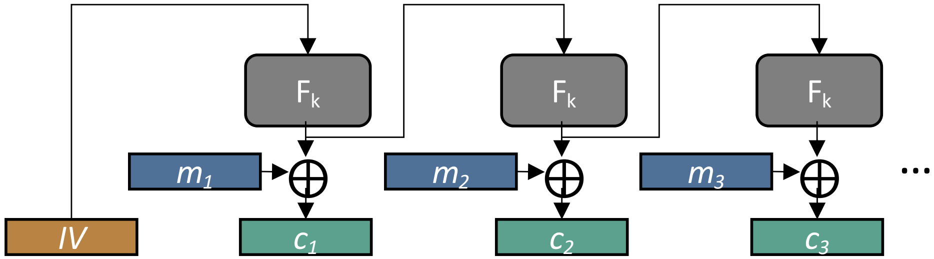
Encryption: $c_i = F(k,m_i)$
Decryption: $m_i = F^{-1}(k,c_i)$

Cipher Block Chaining (CBC)



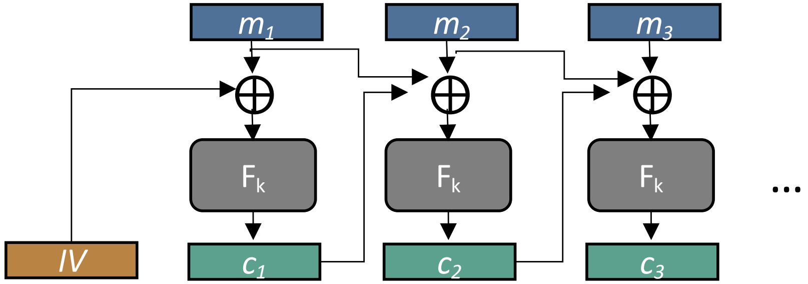
Encryption: $c_0=IV ; c_i = F(k,c_{i-1} \oplus m_i)$
Decryption: $m_i = F^{-1}(k,c_i) \oplus c_{i-1}$

Output Feedback (OFB)



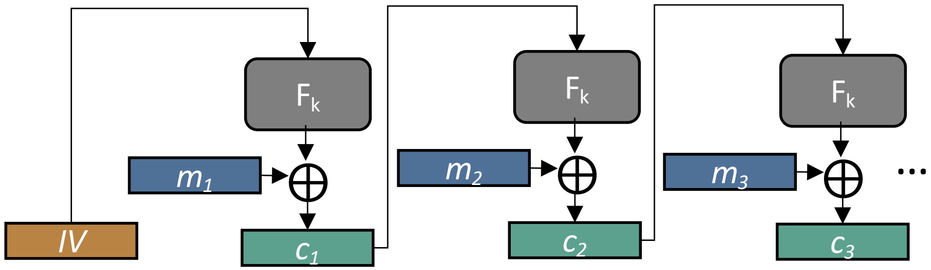
Encryption: $c_0 = IV; c_i = F^{(i)}(k,IV) \oplus m_i$
Decryption: $m_i = F^{(i)}(k,IV) \oplus c_i$

Propagating Cipher Block Chaining (PCBC)



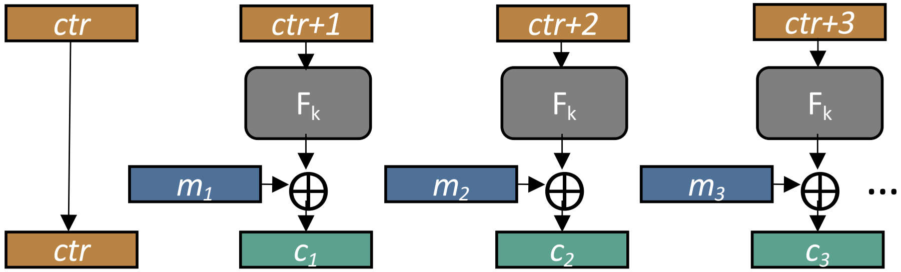
Encryption: $c_0=IV ; c_i = F(k,c_{i-1} \oplus m_{i-1} \oplus m_i)$
Decryption: $m_0=0^n$; $m_i = F^{-1}(k,c_i)\oplus c_{i-1} \oplus m_{i-1}$

Cipher Feedback Mode (CFB)



Encryption: $c_0 = IV; c_i = F(k, c_{i-1}) \oplus m_i$
Decryption: $m_i = F(k, c_{i-1}) \oplus c_i$

Counter Mode (CTR)



Encryption: $c_0 = ctr ; c_i = F(k,ctr+i) \oplus m_i$
Decryption: $m_i = F(k,ctr+i) \oplus c_i$

*For simplicity in drawing, let F_k denote the PRF F with the key k given as input

www.ruxandraolimid.weebly.com/pagesonsecurity

Pages on SecuRity
by Ruxandra F. Olimid