Modes of Operation

Mode 1 - Electronic Code Book(ECB) Mode

Mode 2 – Cipher Block Chaining(CBC) Mode

Mode 3 – Output Feedback(OFB) Mode

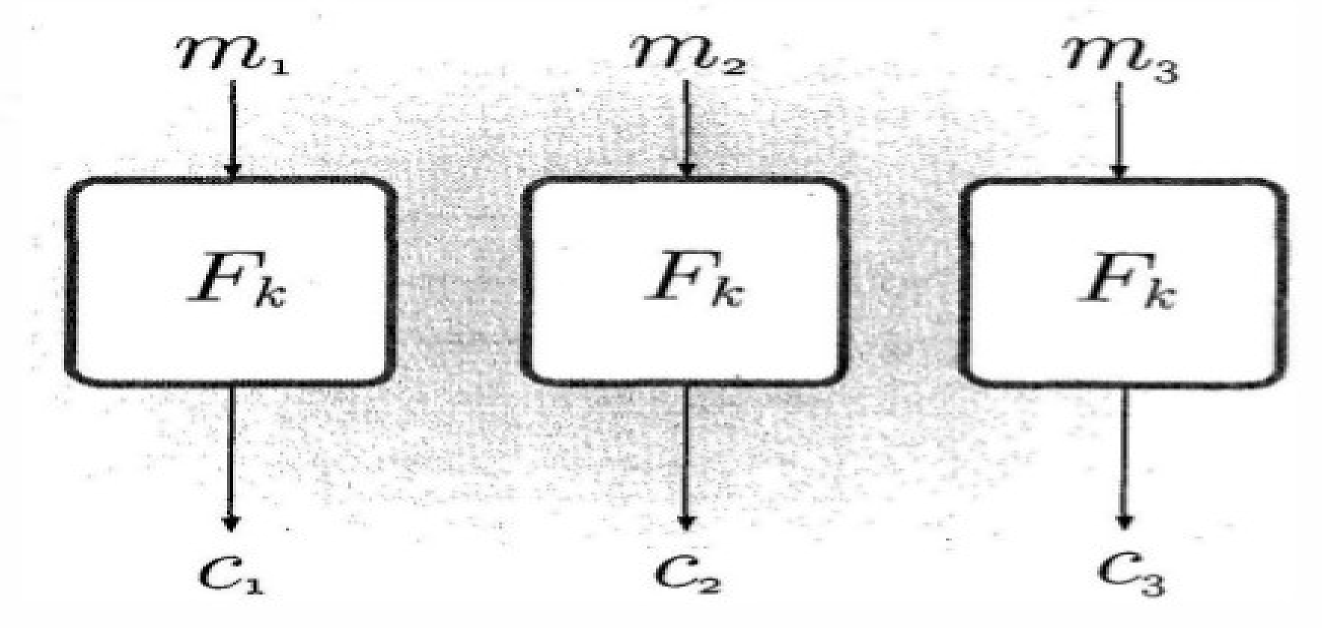
Mode 4 – Counter(CTR) Mode

Electronic Code Book(ECB) Mode

a) Plaintext 'm' is divided into 'n' blocks.

b) Each block is encrypted separately using Pseudorandom Permutation **F_k** to generate 'n cipher's.

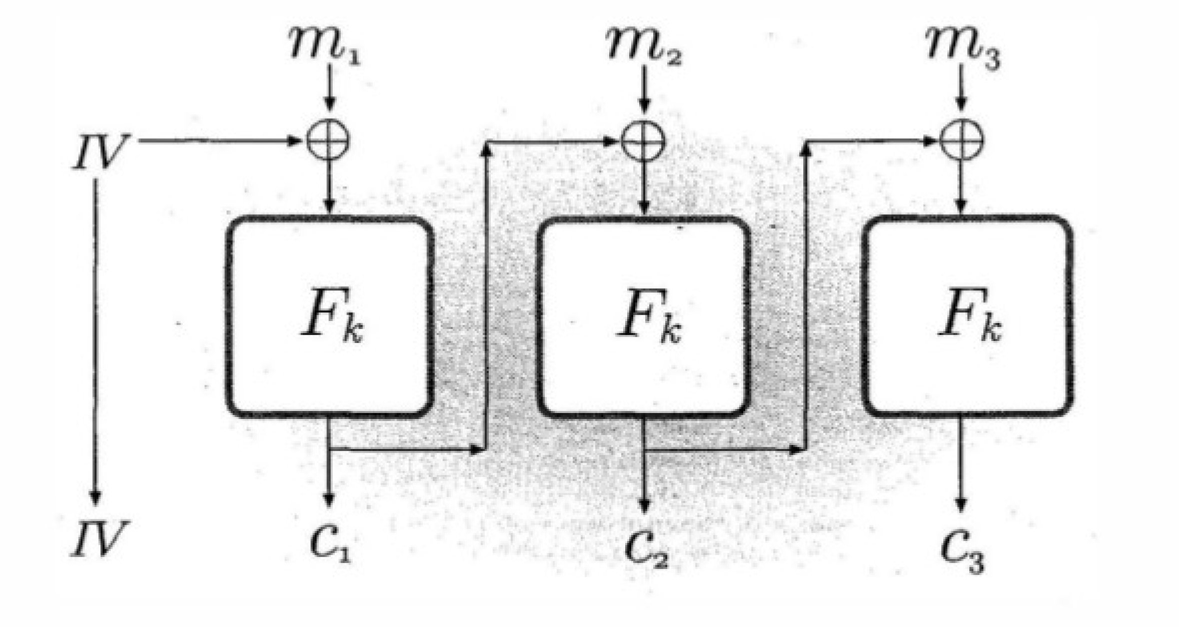
c) This 'n' ciphers are combined into single cipher 'c'.



Cipher Block Chaining(CBC) Mode

a) Plaintext 'm' is divided into 'n' blocks into m_1,m_2...m_n.

b) 'm_1' XOR IV(random Initialization Vector) is passed to $\mathbf{F_k}$ to get 'c_1' and cycle is repeated for all m_i .

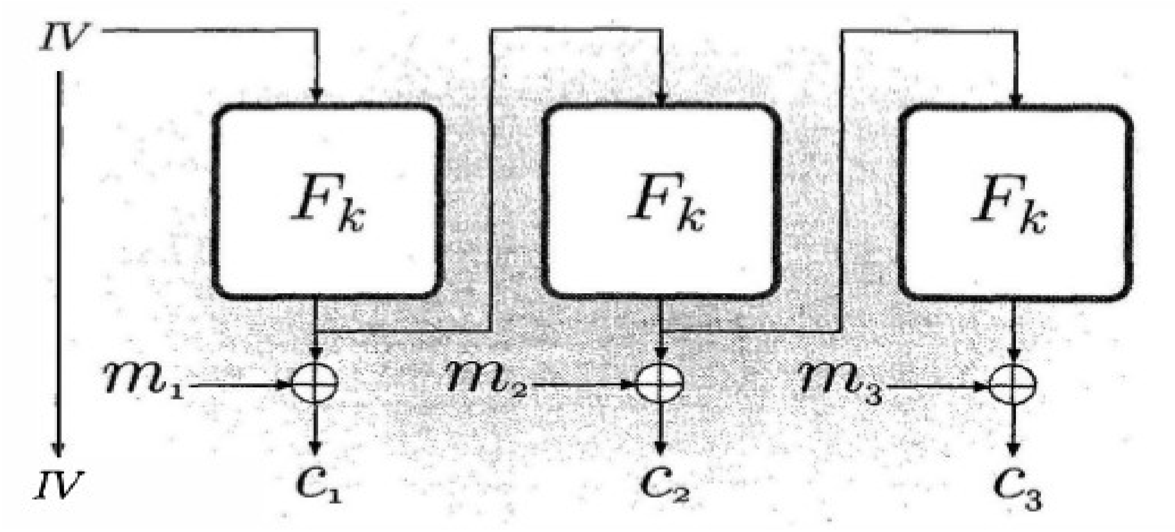


Output Feedback(OFB) Mode

a) Plaintext 'm' is divided into 'n' blocks into m_1,m_2...m_n.

b) Random Intialization vector(IV) is passed to F_k.

c) 'm_1' XOR with output of F_k to get 'c_1' and cycle is repeated for all m_i .

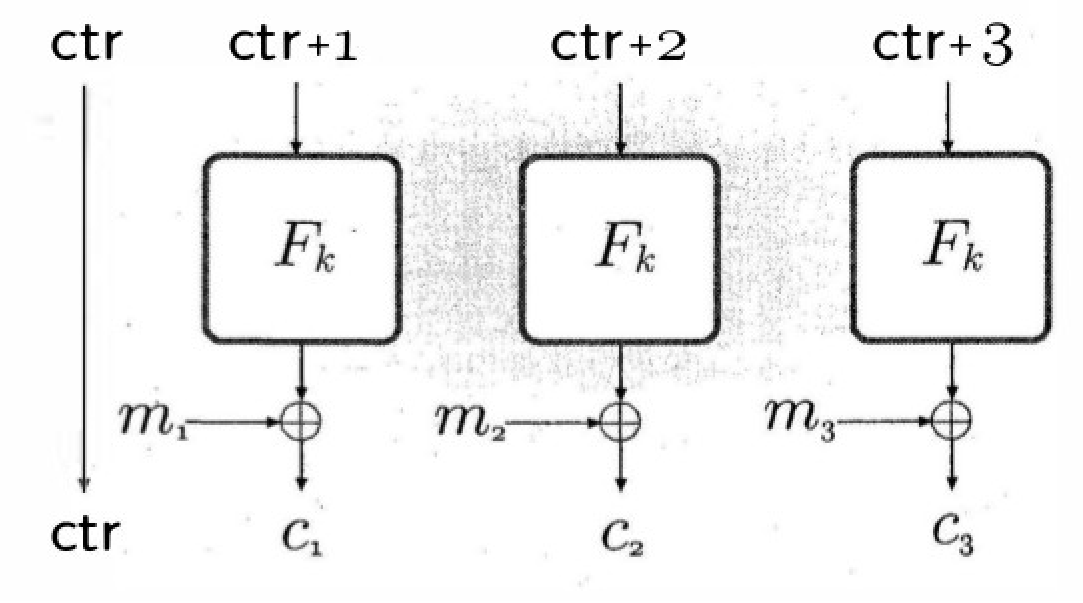


Counter(CTR) Mode

a) Plaintext 'm' is divided into 'n' blocks into m_1,m_2...m_n.

b) Random Intialization vector(ctr+1) is passed to F_k and ctr is incremented.

c) 'm_1' XOR with output of F_k to get 'c_1' and cycle is repeated for all m_i.



ctr
ctr+1
ctr+2
ctr+3
F_k
F_k
F_k
m_1
m_2
m_3
ctr
c_1
c_2
c_3