Modes of Operation

Mode 1 - Electronic Code Book(ECB) Mode

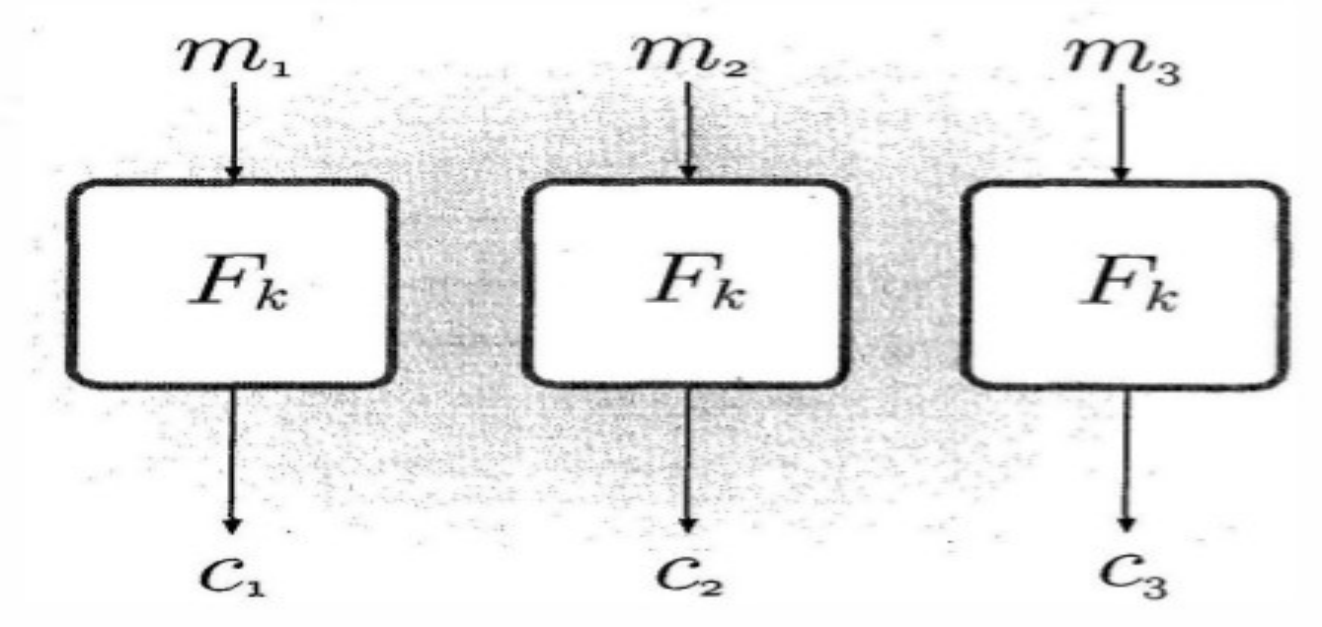
Mode 2 – Cipher Block Chaining(CBC) Mode

Mode 3 – Output Feedback(OFB) Mode

Mode 4 – Counter(CTR) Mode

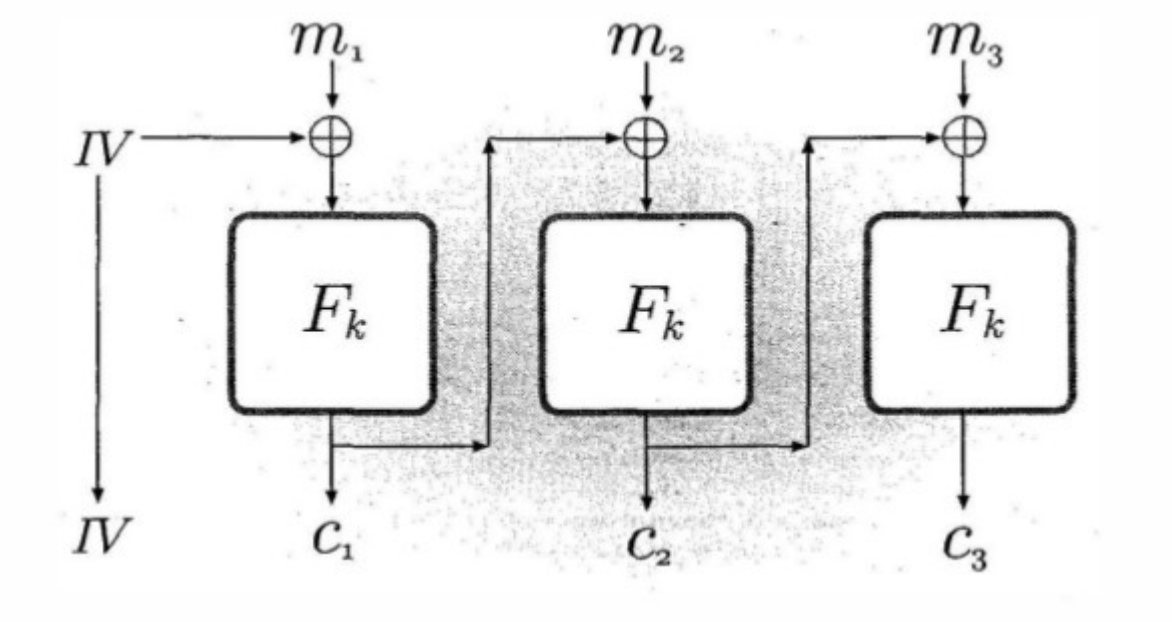
Electronic Code Book(ECB) Mode

- Plaintext 'm' is divided into 'l' blocks.
- Each block is encrypted separately using Pseudorandom Permutation **Fk** to generate 'l' cipher's.
- This 'l' ciphers are combined into single cipher 'c'.



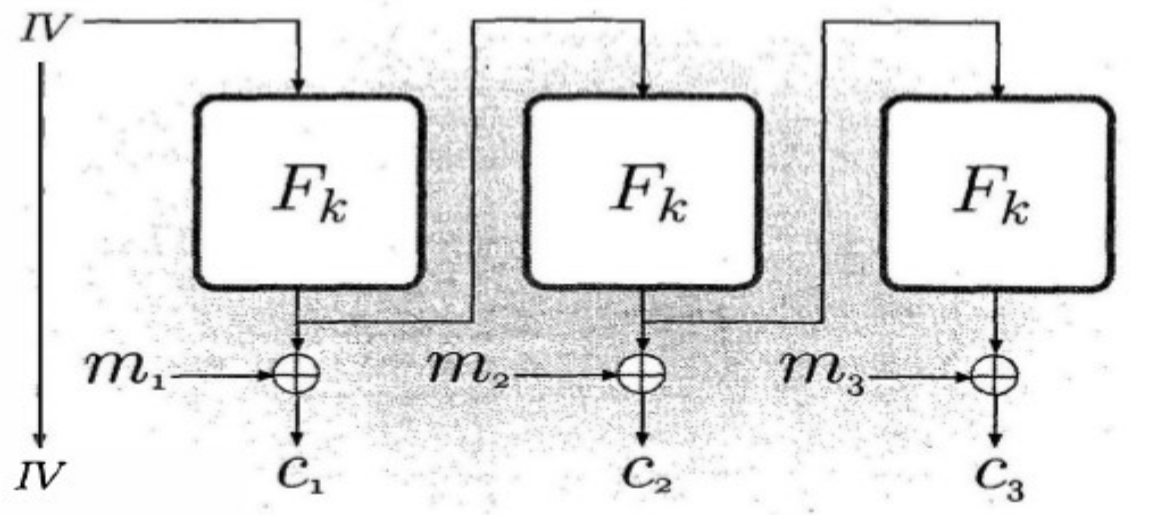
Cipher Block Chaining(CBC) Mode

- **Plaintext 'm' is divided into 'l' blocks into m1,m2...ml.**
- **'m1' XOR IV(random Initialization Vector) is passed to Fk to get 'c1' and cycle is repeated for all ml.**



Output Feedback(OFB) Mode

- **Plaintext 'm' is divided into 'l' blocks into m1,m2...ml.**
- **Random Intialization vector(IV) is passed to Fk.**
- **'m1' XOR with output of Fk to get 'c1' and cycle is repeated for all ml 's.**



Counter(CTR) Mode

- **Plaintext 'm' is divided into 'l' blocks into m1,m2...ml.**
- **Random Intialization vector(ctr+1) is passed to Fk and ctr is incremented.**
- **'m1' XOR with output of Fk to get 'c1' and cycle is repeated for all ml 's.**