CPA Secure Encryption Scheme

CPA Attack:

Let us assume the adversary has access to the encryption scheme. The adversary knows the messages m_0 and m_1. The adversary also knows that the encrypted message m_b is one of m_0 and m_1. Using this knowledge, the adversary tries to predict which text was chosen for encryption. Such attac is known as Chosen Plain text Attack.

CPA Secure Encryption:

Let F be a Pseudo Random Function which takes the bit of length n and outputs the bit of length n.

Key Generation: Generate a bit sequence of length n{0,1} uniformly at random and output it as ke.

Message Encryption: On input a message of length n{0,1}, and a key of length n{0,1}, choose r of length n{0,1} uniformly at random and output the cipher text.

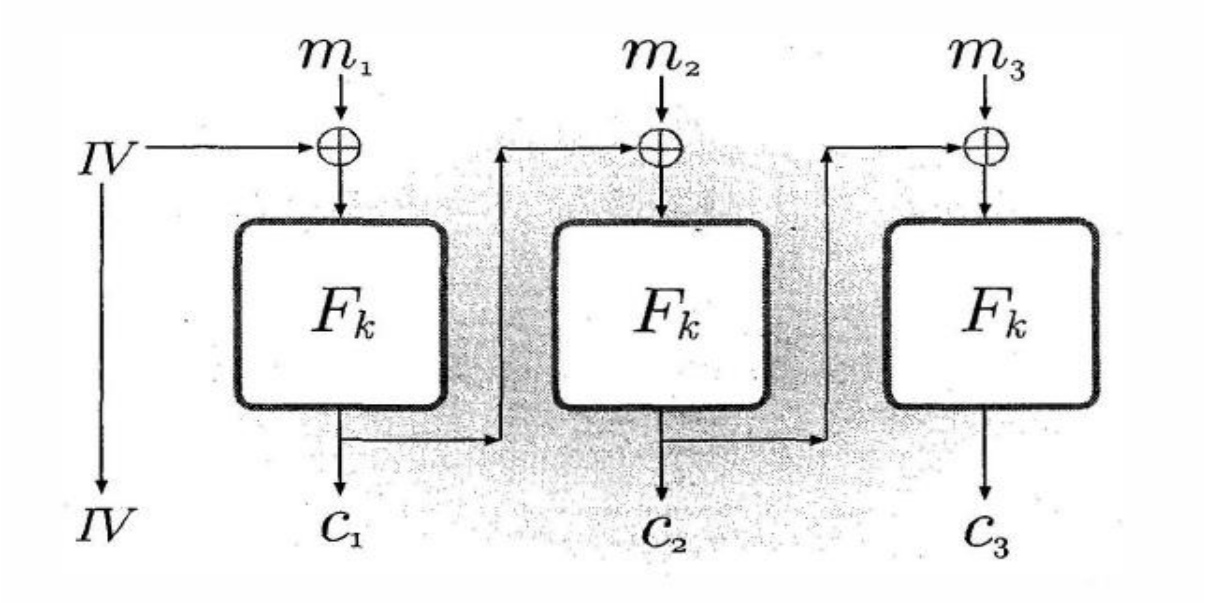
$$c := \langle r, F_k(r) \oplus m \rangle.$$

Message Decryption: On input a key of length n and a cipher text c=<r,s> ,output the plain text message.

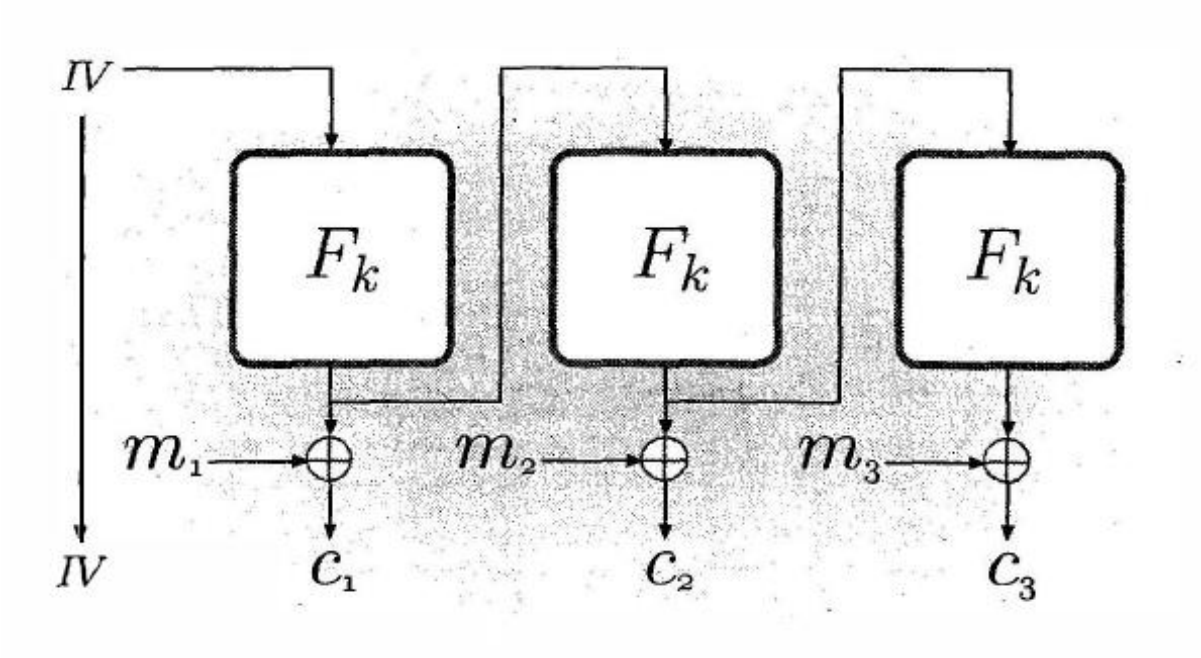
$$m := F_k(r) \oplus s.$$

For a message of variable length, the message is divided into blocks of size n and cipher text is calculated for each block. The final cipher will be the combination of block ciphers. There are several modes of operation for this purpose.

1. **Cipher Block Chaining**



2. **Output Feedback Mode**



3. **Randomized Counter Mode**