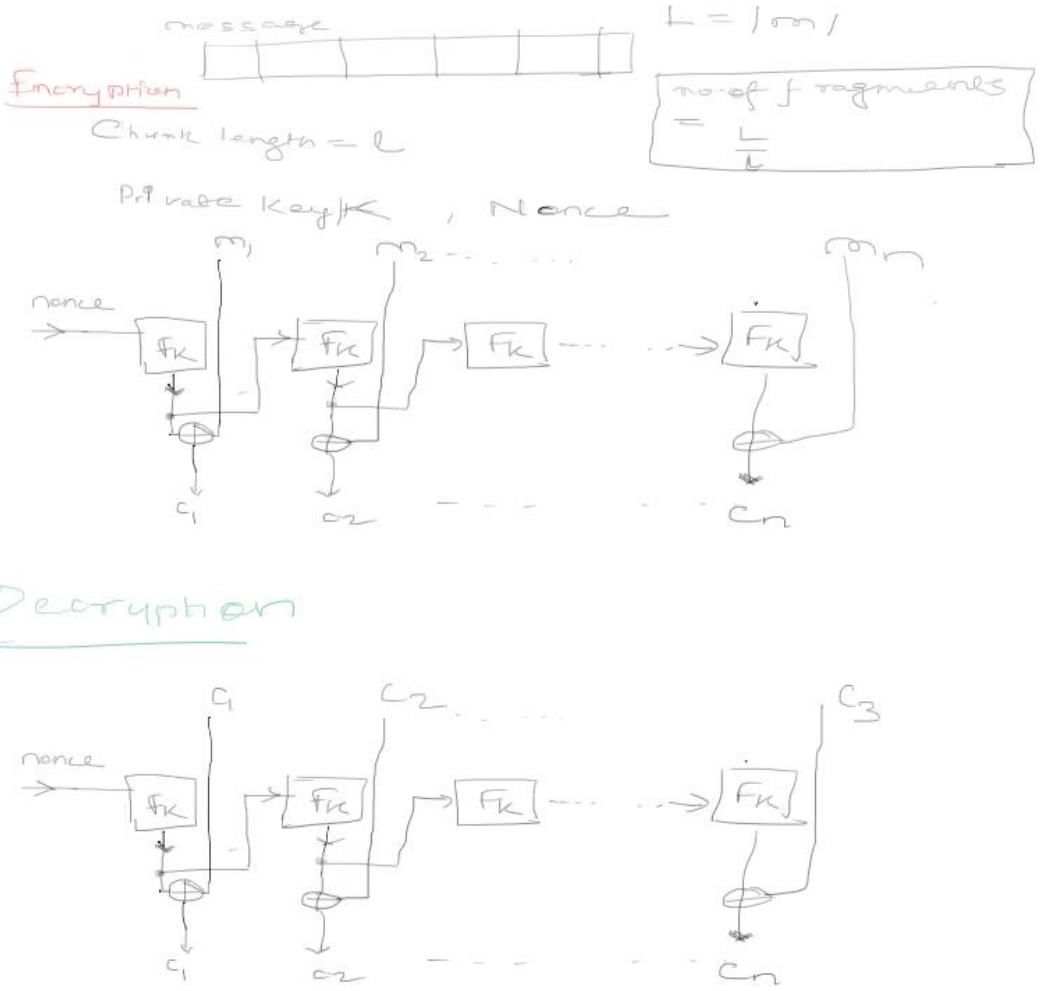
Soumodipta Bose| 2021201086

Use the PRF in some secure mode of operation to obtain CPA Secure encryption scheme (Theory)

We have already seen the construction of a PRF using DLP, now we can use this to create our very own CPA Secure Encryption.

Sketches/Ideas:

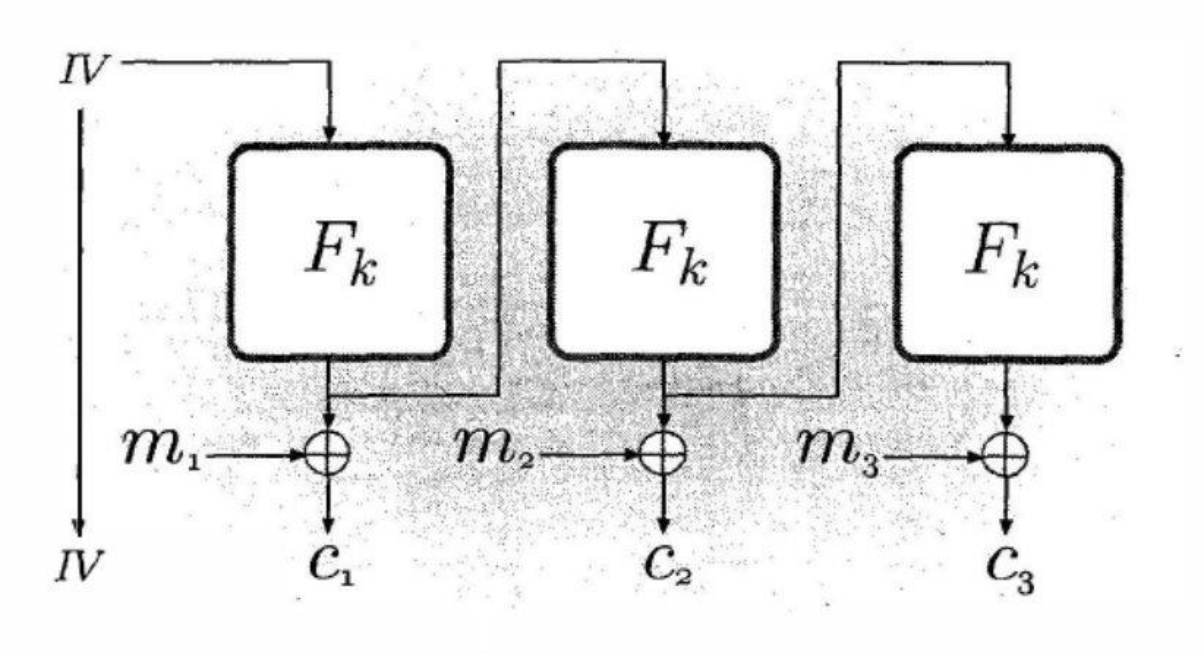


Construction:

To implement this we will make quick use of our pseudo random function F(k,x) in our crypto library. We will first discuss the encryption scheme.

So for this we simply start with an initial random binary string nonce(initialization vector or iv) which is generated again by our very own random bit generator of any length called get_random_bits(n) from our crypto library. We are then using a pseudo random function on it to further scramble it and gain r, which we will send to the

reciver. We also take a private key which is used in our pseudo random function F(k,x).



In our implementation I have chosen Output Feedback mode operation mode. In this mode we create a propagation of Pseudo Random Functions such that the result of the previous stage is feeded into the next stage and this keeps on happening and in each stage we get a sequence of random bits. These bits are then xored with the message to create our cipher text fragments. These cipher text fragments are sent to the receiver side for decryption. So what is so cool about it. Well the size of the private key and initialization vector is very small compared to size of message, hence we are saving our selves a lot of bandwidth.

At the receiver we regenerate all the random bit sequences using r and the same pseudo random function whose private key we have already stored. So after the same sequences have been generated, we will simply xor to obtain our original message fragments and then join them together to create the full message.