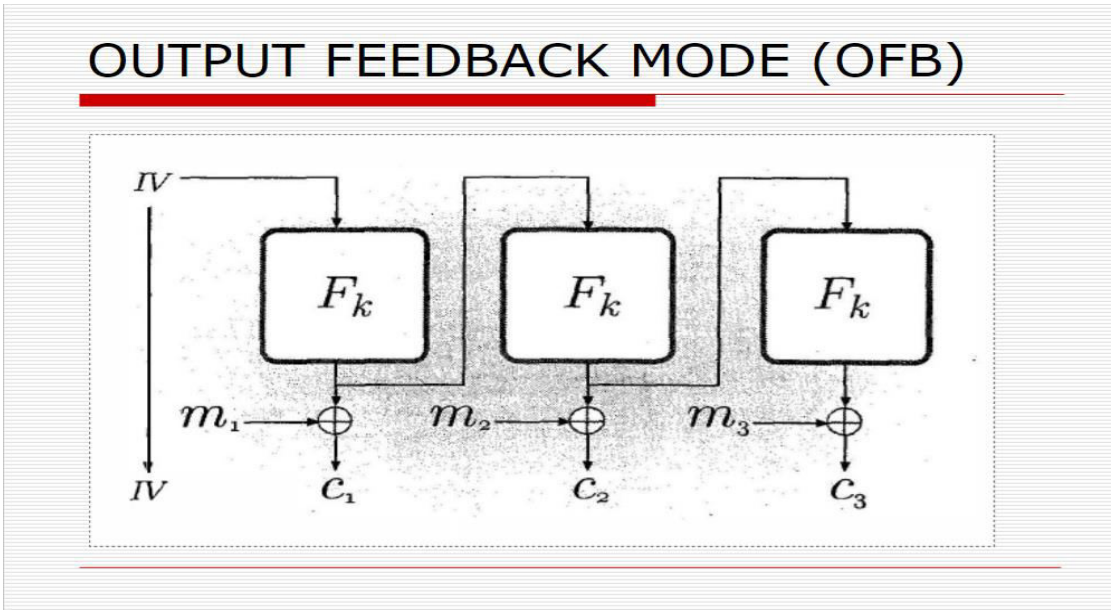
Sudipta Halder (2021202011)

# Use the PRF in some secure mode of operation to obtain a CPA-secure encryption scheme

Here I have used Output Feedback Mode(OFB) to build the CPA secure encryption scheme. Also, I have used the previously built PRF and PRG here.

The below diagram is followed for the construction of CPA by OFB mode.




**Working Flow:**

1. First, we asked for input: prime, generator, data, block-size, key.
2. Then, it will generate a random vector of length = block-size through the prebuilt PRG.
3. It will then divide the data in blocks of given block-size. It will then iterate through the data blocks.
4. For each data block, first pass the initial vector through the PRF and obtain a prf. Then calculate xor between data block and the obtained prf. The result will the corresponding ciphertext-block for that corresponding data block. For the next iterations the obtained prf from the previous iteration will be used as initial vector. For better understanding refer to the above pic of OFB mode. Now, concatenating the ciphertext-blocks(c1, c2, c3, …), we'll get the actual ciphertext c.
5. In the decryption stage the initial vector taken in encryption stage is passed along with the ciphertext and block-size. There the ciphertext is decrypted in the same way as OFB. We then check whether the initial data and the decrypted data same or not.
6. We then run the encryption and decryption once again with a different initial vector to show that the encryption data is different this time which is the main agenda of CPA that the encrypted data should be different every time for the same data.