*Function* output\_feedback\_encrypt

*Input Arguments*

* iv- initialization vector, a binary string
* m- plain text
* k – k is the key for PRF, a binary string

*Output*

cipher text as binary string

*Logic*

1. It is the clear implementation of output feedback mode operation.
2. The inputs iv, k are given to PRF.
3. The output of PRF is XORed with the message\_block and then appended to cipher text string.
4. The same output is used as iv for PRF in the next iteration.

*Usage*

This is used to create CPA secure cipher text

*Function* cpa\_secure

*Input Arguments*

* iv- initialization vector, a binary string
* m- plain text
* k – k is the key for PRF, a binary string

*Output*

A binary string

*Logic*

* Here the function output\_feedback\_encrypt is called with the respective parameters.
* The output of the above function is concatenated with the IV and then returned as this function’s output

*Usage*

The output generated here is send to the receiver