*Function*

*Input Arguments*

*Output*

*Logic*

*Usage*

*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*

It is the clear implementation of output feedback mode operation

*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

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