*Function* cbc\_mac

*Input Arguments*

M – plain text message -binary string

Block\_length – This is the size of each block, an integer

K- key used for PRF

*Output*

CMAC - A binary string

*Logic*

This is the clear implementation of the CBC mode of operation with a slight modification

As the result, only the last block output is taken

*Usage*

This is used to generate CMAC of the input plain text