Function cca_secure

Input Arguments

- m- plain text, binary string
- iv-initialization vector, binary string
- block_length- integer
- k- key, binary string

Output

Cipher text – binary string

Logic

1. This function calls the cpa_secure with the respective inputs.
2. The output obtained above is the CPA secure cipher text. It given as input for the function call cbc_mac and generates CMAC
3. The final output is CMAC concatenated to cipher text.

Usage

This function is used to generate CCA secure cipher text that is sent to the receiver.