CCA Secure Encryption scheme

Function CCA_gen

Input: Length of keys that has to be generated.

Output: 2 keys of size equal to the length given in the input.

Algorithm :

Generate seed_size random bit sequence and return the keys as key1 and key2.

Function CCA_Encrypt:

Input: 2 keys of the length equal to block_size and a message of arbitrary length.

Output: Return the cipher text along with Message Authentication Code tag.

Algorithm:

Encrypt the message m with key1 using CPA secure encryption. Let c be the cipher text.

Find the tag of the cipher text c using CBC_MAC.

Return cipher along with tag.

Function CCA_Decrypt:

Input: 2 keys of length equal to the block_size and a cipher text of arbitrary length.

Output: Return the original message or None.

Logic:

Verify the tag given and the Tag generated using CBC_Mac with key2 and cioher c.

If the generated matches with the given tag, decrypt the message using CPA secure decryption with the help of key2. Return the decrypted message.

Else return None.