# CCA code explanation:

- User will enter message m initially
- Two keys k1,k2,r1 are generated randomly.k1 is used for cpa encryption , k2 is used for MAC and r1 is for PRF
- We will pass msg,k1,k2,r1,N=16 (block size) to Encr_cca() function
- In this function we will get ciphertext using cpa encryption
- This ciphertext will be given to MAC to generate tag for that ciphertext.
- At the end we will return cipher_text and tag

```
def Encr_cca(msg,key1,r1,key2,N):
   cipher_msg=Encr_cpa(msg,key1,r1)
   len_cipher=len(cipher_msg)
   mac_tag=CBC_MAC(cipher_msg,key2,N)
   return [cipher_msg,mac_tag]
```

- To decrypt cipher text , we will pass cipher_text,tags,key1,key2,r1 and N to Decr_cca() function
- In this function we will check tag of ciphertext using k2 and if tag are matched with given tag then we will decrypt the cipher_text and will return plain message

```
def Decr_cca(msg,key1,key2,r1,tag,N):
   plain_msg=Decr_cpa(msg,key1,r1)

   isTagMatched=verification_CBC_MAC(msg,key2,N,tag)
   if isTagMatched:
       print("decrypted successfully and tag is matching")
       return plain_msg
   else:
       print("Error in MAC")
       return ""
```