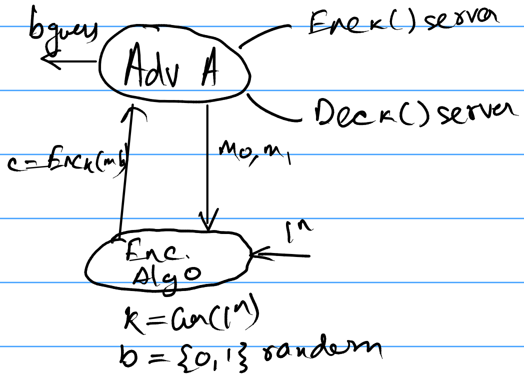
CCA-Secure Encryption

CCA is an attack when the adversary has access to both the encryption and decryption server. They can also alter the ciphertext which is sent to the receiver leading to mis communication.



CCA secure
if for all PPT adv. A
$P[b_{guess} = b] <= \frac{1}{2} + negl(n)$

The construction of a CCA secure server can be done by-

1. Gen - Choose keys $k_1, k_2 \in \{0,1\}^n$
2. $Enc_k(m)$ - $c = Enc_{k_1}(m)$ ciphertext
   $t = Mac_{k_2}(m)$ tag.
3. $Dec_k(c,t)$ - keys k_1, k_2 & ciphertext, c, t
   Verify (c, t) = 1 using MAC (Vrfy)
   if verify == 1,
       output $Dec_k(c)$
   else
       discard.

This construction is CCA-secure as the MAC tag will verify if the ciphertext has been tampered with.