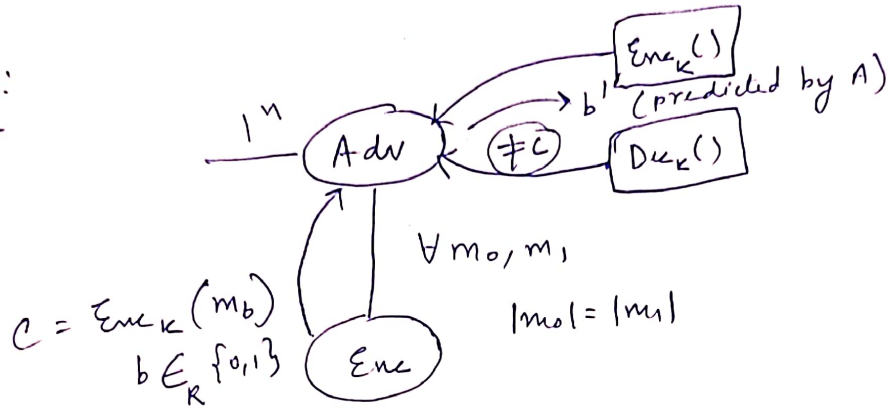
Message Authentication Codes (MAC)

In case of Chosen Ciphertext attack, attacker has access to both the encryption and decryption server. We donot want the attacker to ~~get~~ be able to know which message (plaintext) given ciphertext corresponds to.

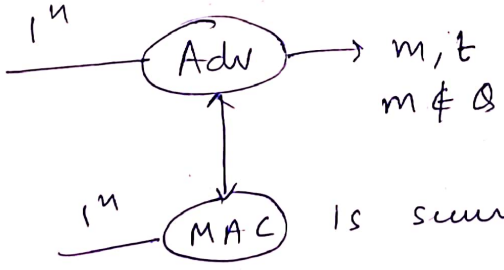
CCA:



$Enc_K()$ is CCA-secure iff $\forall$ PPTM A,

$$P[b = b'] \leq 1/2 + negl(n)$$

CCA-security is handled by using message authentication code or a tag that allows decryption only if the tag on the ciphertext (or plaintext depending on scheme) matches the tag sent in the query. Formally,



is secure if $\forall$ PPTM A,

$$P[Vrfy_K(m, t) = Y \mid m \notin Q] \leq negl(n)$$

meaning the attacker shouldn't be (almost) able to get the tag of any message that hasn't been queried by them.

MAC Construction used :—

Key $k \in \{0,1\}^n$

message $m \in \{0,1\}^*$ of length atmost $2^{n/4 - 1}$

— Parse m into d blocks $m_1, m_2 \ldots m_d$ each of length $n/4$ (padded by 10^* in the end)

— choose $r \leftarrow \{0,1\}^{n/4}$

— For $i = 1, 2, \ldots, d$

$$t_i = F_k(r \| d \| i \| m_i)$$

— Final tag $t = (r, t_1, t_2, \ldots, t_d)$

— $Vrfy_k(m, t) \longrightarrow 1$ if tag calculated by running mac using k, m is same as tag t received.

Proof of security :—

Let us assume attacker ~~wants to~~ sends $m' \neq m$, $m' \notin Q$

Case #1 : r is reused.

Case#1.1 : $|m| = |m'|$

$m \neq m' \Rightarrow \exists\, i$ s.t. $m_i \neq m_i'$

$\therefore t_i = F_k(r \| d \| i \| m_i)$

t_i' cannot be obtained as there is no way to obtain tag t_i' of message $(r \| d \| i \| m_i')$ given F_k is a pseudo random function.

Hence, PPTM A cannot obtain tag t' of m' given tags of $m \neq m'$.

Case#1.2 : $|m| \neq |m'| = l' \longrightarrow$ Not possible to get tag of $(r \| l' \| i \| m_i')$