Assignment-1

2020111013

(7) Construction of CCA Encryption scheme

For ~~CPA encrypt~~ 2 keys $k_1, k_2 \in \{0,1\}^n$, we use CPA for Encryption & CBC-MAC for tag.

$\therefore \quad c = Enc_{k_1}(m)$

$t = Mac_{k_2}(c)$

$c_f = c \| t$

Proof of Security

In order to prove given encryption scheme, we need to show

$$Pr[PrivK^{cca}_{A,\Pi}(n) = 1] \leq negl(n)$$

Assuming that the CPA scheme & CBCMAC that's being used is secure, we can ensure that the message will only be decrypted if the tag is valid.

$$Pr[Mac\text{-}forge_{A,\Pi}(n) = 1] \leq negl(n)$$

Let ValidQuery be the event that A submits a new, valid ciphertext to the decryption oracle in $PrivK^{cca}_{A,\Pi}(n)$

$$\therefore Pr(ValidQuery) \leq negl(n)$$ ($\because$ CPA & CBCMAC are secure)

$\because$ There is no possibility of decryption, A cannot use the decryption oracle anymore & since CPA secure, A cant use encryption oracle either.

$\therefore Pr[PrivK^{cca}_{A,\Pi}(n) = 1] \leq negl(n)$

$\therefore$ The constructed encryption scheme is CCA secure