

**CSCI971 Advance Computer Security:
Homework #7**

**Mei Wangzhihui
2019124044**

Problem 1

AE-secure \Leftrightarrow semantically secure under CPA and CI.

For the first cipher, assume an attacker who can perform CPA. He intercept the ciphertext $c = E_1(k, m) = (E(k, m), H_1(m))$. He can perform as many as CPA. We assume in CPA attack game. Adversary \mathcal{A} first send m_0, m_0 to challenger \mathcal{C} , he get the ciphertext $c = (E(k_0, m_0), H_1(m_0))$. Then \mathcal{A} send m_0, m_1 to \mathcal{C} , as E is CPA secure, so key has to be changed. \mathcal{A} get the ciphertext $c = (E(k_1, m_0), H_1(m_0))$ or $c = (E(k_1, m_1), H_1(m_1))$ based on b . Then if $b = 1$, \mathcal{A} can easily differ the plaintext from the tag $H_1(m_b)$. So $Adv_{CPA}(\mathcal{A}, \mathcal{E}) = 1/2$ is not negligible. Cipher1 is not CPA-secure, so it's not AE-secure.

For the second cipher, attacker can intercept the ciphertext $(c, H_2(c))$, so he can learn the mapping model of H_2 function. So in CI attack game, Adversary \mathcal{A} can easily generate a valid ciphertext-tag pair $(c_{atk}, H_2(c_{atk}))$. Then Decryptor $D_2(k, (c_{ack}, H_2(c_{ack}))) \neq \perp$. So $Adv_{CI}(\mathcal{A}, \mathcal{E})$ is not negligible. Cipher1 does not satisfy CI, so it's not AE-secure.

Problem 2

Problem 3