CSCI971 Advance Computer Security: Homework #7

Mei Wangzhihui
2019124044

Problem 1

Because AE-secure $\Leftrightarrow$ CPA-secure and CI. Assume a attacker who can perform CPA. He intercept the ciphertext $c = E_1(k, m) = (E(k, m), H(m))$, He can perform as many as CPA, so he can learn the mapping relation of H.

Problem 2

Problem 3