CSCI971 Advance Computer Security: Homework #5

Mei Wangzhihui
2019124044

Problem 1

Solution:
Suppose Adversary $\mathcal{A}$ query once get (m_0, t_0) and the second time he give (m_1, t_0). Because for 1/2 of all the keys, $S(k, m_0) = S(k, m_1)$, that is $t_0 = t_1$. So Adversary win the game for the Probability 1/2 with 1-query.
That is:

$$Adv_{MAC}[\mathcal{A}, \mathcal{I}] = 1/2$$

is not negligible. So MAC is not secure MAC.

Problem 2

Solution:
As the $t = S(k, m)$ is 5 bit long, so $|\mathcal{T}| = 2^5$, that is to say, for any given key k, there are at most 32 message m with different tag t.
So if adversary $\mathcal{A}$ query 33 times, he surely have that $S(k, m_x) = S(k, m_y), 0 < x, y < 33$ In the worst situation(all message has the same tag), he has the Probability 1/32 to output $m_3 3$ with the same tag.
So

$$Adv_{MAC}[\mathcal{A}, \mathcal{I}] \geq 1/32$$

is not negligible. So MAC is not secure MAC.