Assignment 5 - 2019.10.22

Submission deadline: 2019.10.31

1. Let I=(S,V) be a MAC. Suppose an attacker is able to find $m_0 \neq m_1$ such that $S(k, m_0) = S(k, m_1)$ for ½ of the keys k in K. Please provide your argument using the challenger and adversary game that whether this MAC is a secure MAC or not.

2. Let I=(S, V) be a MAC. Suppose S(k, m) is always 5 bits long. Please provide your argument using the challenger and adversary game that whether this MAC is a secure MAC or not.