1. Let $F$ be a pseudorandom function, and let $k \in \{0, 1\}^n$ be a key. Show that the following MAC for messages of length $2n$ is insecure.

To authenticate the message $m_1||m_2$ with $|m_1| = |m_2| = n$ compute the tag

$$\langle F_k(m_1), F_k(m_1 \oplus m_2') \rangle,$$

where $m_2'$ is $m_2$ with its last bit flipped (so $110' = 111$). What is the minimum number of queries that the adversary has to make to the MAC-oracle to forge this MAC?

**Proof that the MAC is insecure:**

The adversary $A$ asks the MAC-oracle for the tag of: $m_1||0^n$ to get $(t_1, t_2)$, where $t_1 = F_k(m_1)$ and $t_2 = F_k(m_1')$.

Now $A$ can forge the tag of $m_1'||0^n$, which is: $\langle F_k(m_1'), F_k(m_1) \rangle = \langle t_2, t_1 \rangle$.

**Minimum number of queries needed to be made to forge a message:** One.

Mike Burmester