

ENEE/CMSC/MATH 456: Cryptography
MAC Class Exercise 3/1/23

Let F be a length-preserving pseudorandom function. Show that each of the following message authentication codes is insecure. (In each case the shared key is a random $k \in \{0,1\}^n$.)

1. To authenticate a message $m = m_1 || m_2$, where $m_1, m_2 \in \{0,1\}^n$, compute $t := F_k(m_1) || F_k(m_2 \oplus F_k(m_1))$.
2. To authenticate a message $m = m_1 || \dots || m_\ell$, where $m_i \in \{0,1\}^n$, choose $r \in \{0,1\}^n$ at random and compute $t := r || F_k(m_1 \oplus r) || \dots || F_k(m_\ell \oplus r)$.