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 $t := F_k(m_1) || F_k(m_2 \oplus F_k(m_1))$.

   **Attack**: query for a signature on $m_1, m_2$
   get back $t := t_1 || t_2$ where $t_1 = F_k(m_1)$, $t_2 = F_k(m_2 \oplus F_k(m_1))$
   query for a signature on $m_1', m_2'$
   get back $t': = t_1' || t_2'$ where $t_1' = F_k(m_1')$, $t_2' = F_k(m_2' \oplus F_k(m_1'))$

   Forge a signature on $m_1'', m_2''$
   where $m_1'' := m_1$
   $m_2'' := t_1 \oplus m_1' = F_k(m_1') \oplus m_1'$

   **Tag** $t'' := t_1 || t_1'$

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

   **Attack**: query for a signature on $m = m_1 || \cdots || m_e$
   get back $t := r || t_1 || \cdots || t_e$

   Forge a signature on $m_i \oplus r || \cdots || m_e \oplus r$

   by outputting tag

   $t' := 0 || t_1 || \cdots || t_e$. 