1. Say \( \Pi = (\text{Gen}, \text{Mac}, \text{Vrfy}) \) is a secure MAC, and for \( k \in \{0, 1\}^n \), the tag-generation algorithm \( \text{Mac}_k \) always outputs tags of length \( t(n) \). Prove that \( t \) must be super-logarithmic or, equivalently, that if \( t(n) = O(\log n) \) then \( \Pi \) cannot be a secure MAC.

**Hint:** Consider the probability of randomly guessing a valid tag.

2. Assume secure MACs exist. Prove that there exists a MAC that is secure (by Definition 4.2) but is not strongly secure (by Definition 4.3).

3. Consider the following MAC for messages of length \( \ell(n) = 2n - 2 \) using a pseudorandom function \( F \):

   On input a message \( m_0||m_1 \) (with \( |m_0| = |m_1| = n - 1 \)) and key \( k \in \{0, 1\}^n \), algorithm \( \text{Mac} \) outputs \( t = F_k(0||m_0)||F_k(1||m_1) \). Algorithm \( \text{Vrfy} \) is defined in the natural way. Is \( (\text{Gen}, \text{Mac}, \text{Vrfy}) \) secure? Prove your answer.

4. Let \( F \) be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticated fixed-length messages. (In each case \( \text{Gen} \) outputs a uniform \( k \in \{0, 1\}^n \). Let \( \langle i \rangle \) denote an \( n/2 \)-bit encoding of the integer \( i \).

   (a) To authenticate a message \( m = m_1, \ldots, m_\ell \), where \( m_i \in \{0, 1\}^n \), compute \( t := F_k(m_1) \oplus \cdots \oplus F_k(m_\ell) \).

   (b) To authenticate a message \( m = m_1, \ldots, m_\ell \), where \( m_i \in \{0, 1\}^{n/2} \), compute \( t := F_k(\langle 1 \rangle||m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle||m_\ell) \).

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

   (a) To authenticate a message \( m = m_1||m_2, \ldots||m_\ell \), where \( m_i \in \{0, 1\}^n \), compute \( t := F_k(m_1 \oplus \cdots \oplus m_\ell) \).

   (b) To authenticate a message \( m = m_1||m_2 \), where \( m_1, m_2 \in \{0, 1\}^n \), compute \( t := F_k(m_1)||F_k(m_2 \oplus F_k(m_1)) \).

   (c) To authenticate a message \( m = m_1||m_2 \), where \( m_1, m_2 \in \{0, 1\}^n \), compute \( t := F_k(m_1 \oplus m_2)||F_k(m_2 \oplus F_k(m_1)) \).

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