1. Recall our construction of CPA-secure encryption from PRF (Construction 3.30 in the textbook). Show that while providing secrecy, this encryption scheme does not provide message integrity. Specifically, show that an attacker who sees a ciphertext \( c := \langle r, s \rangle \), but does not know the secret key \( k \) or the message \( m \) that is encrypted, can still create a ciphertext \( c' \) that encrypts \( m \oplus 1^n \).

2. 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.
   \textbf{Hint:} Consider the probability of randomly guessing a valid tag.

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 \( t := F_k(\langle 1 \rangle || m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle || m_\ell) \).