Exercise 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.

Exercise 2: Let $F$ be a pseudorandom function. Is the following MAC for messages of length $2n$ secure? The shared key is a random $k \in \{0, 1\}^n$. To authenticate a message $m_1 \parallel m_2$ with $|m_1| = |m_2| = n$, compute the tag $\langle F_k(m_1), F_k(F_k(m_2)) \rangle$. Prove your answer.

Exercise 3: Show that the basic CBC-MAC construction is not secure when used to authenticate messages of different lengths (but are of lengths that are a multiple of the block length)

Exercise 4: Provide formal definitions for second (or target) pre-image resistance and pre-image resistance. Formally prove that any hash function that is collision resistant is second pre-image resistant. (For preimage resistance consider random inputs of length $2n$. For second (target) preimage resistance, consider a game where first a message $x$ is output by the adversary, then $s$ is chosen.)

Exercise 5: For each of the following modifications to the Merkle-Damgård transform, determine whether the result is collision resistant or not. If yes, explain where the proof differs from the proof we saw in class; if not, show an attack.

1. Modify the construction so that the input length is not included at all (i.e., output $z_B$ and not $z_{B+1} = h^s(z_B \parallel L)$).
2. Modify the construction so that instead of outputting $z = h^s(z_B \parallel L)$, the algorithm outputs $z_B \parallel L$.
3. Instead of using an IV, just start the computation from $x_1$. That is, define $z_1 := x_1$ and then compute $z_i := h^s(z_{i-1} \parallel x_i)$ for $i = 2, \ldots, B + 1$ and output $z_{B+1}$ as before.
4. Instead of using a fixed IV, set $z_0 := L$ and then compute $z_i := h^s(z_{i-1} \parallel x_i)$ for $i = 1, \ldots, B$ and output $z_B$. 
