Question 1. Marks: 6.0

The following are two questions on MACs.

1. Show that appending the message length to the end of the message before applying basic CBC-MAC does not result in a secure MAC for arbitrary-length messages.
2. Consider a MAC $\Pi = (Gen, MAC, Verify)$ for $2n - 2$ length inputs, Gen outputs a key $k \in \{0,1\}^n$

For a message $m = m_1||m_2, |m_1| = |m_2| = n - 1$, let $MAC_k(m) = t := F_k(0||m_1)||F_k(1||m_2)$, where F is a PRF. Is this a secure MAC? Prove your answer or give an example of a forgeability attack.

(3+3 marks)

Question 2. Marks: 4.0

Given two collision-resistant hash functions $(Gen_1, H_1), (Gen_2, H_2)$, show that the following hash function is collision resistant.

$$H_c^{(s_1,s_2)}(x) := H_1^{s1}\left(H_2^{s2}(x)||x\right)||H_2^{s2}\left(H_1^{s1}(x)||x\right)$$

Is H_c necessarily collision-resistant if only one of the hash functions, H_1 or H_2 is collision-resi*stant?*

(3+1 marks)