Question 1. Before HMAC was invented, it was quite common to define MAC by \( \text{MAC}_k(m) = H^s(k||m) \) where \( H \) is a collision resistant hash function. Show that this is not a secure MAC when \( H \) is constructed via the Merkle-Damgard transform (note that \( s \) is public and \( k \) is private).

Question 2. Let \( F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \) be a pseudorandom function. Given \( m = m_1, \ldots, m_\ell \) where each \( m_i \in \{0,1\}^n \) (consider only messages whose length is a multiple of the block size). Define that hash function \( h^s(m) \) as follows:

- \( c_0 = s \), where \( s \) is some public random string.
- \( c_i = F_{m_i}(c_{i-1}) \) for every \( i \in \{1, \ldots, \ell\} \).
- Output: \( c_\ell \).

Prove or refute: \( h \) is a collision resistant hash function.

Question 3. For each of the following modifications to the Merkle-Damgard transformation, determine whether the result is collision resistant or not. If yes, provide a proof; if not, demonstrate an attack.

1. Instead of using a fixed \( IV \), choose a random \( IV \in_R \{0,1\}^n \) and define \( z_0 := IV \). Then, set the output to be \( IV || h^s(z_B || L) \).
2. Modify the construction so that the input length is not included at all (i.e., output \( z_B \) and not \( z_B+1 = h^s(z_B || L) \)).
3. Modify the construction so that instead of outputting \( z = h^s(z_B || L) \), the algorithm outputs \( z_B || L \).

Question 4. In the actual construction of DES, the two halves of the output of the final round of the Feistel network are swapped. That is, if the output of the final round is \((L_{16}, R_{16})\) then the output of the cipher is in fact \((R_{16}, L_{16})\). Show that the only difference between the computation of \( DES_k \) and \( DES_k^{-1} \) (given the swapping of halves) is the order of sub-keys.

Question 5. (This exercise assume the results of the previous exercise.)

1. Show that for \( k = 0^{56} \) it holds that \( DES_k(DES_k(x)) = x \).
2. Find three other DES keys with the same property. These keys are known as “weak keys for DES”.
3. Does the existence of these 4 weak keys represent a serious vulnerability in DES? Explain your answer.
Question 6. Two changes were suggested for the implementation of the DES function. First, it was suggested to remove the permutation inside the implementation of the $f$ function. Second, it was suggested to remove the permutation $IP$ in the beginning and in the end of the Feistel structure. Does DES still a pseudorandom permutation? Consider each change separately, and justify your answers.