Question 1. Marks: 5.0

Consider the DES construction we discussed in class with one additional constraint: the output of the final round of the Feistel network is swapped, (i.e. if the output of the Feistel network is (L_{16}, R_{16}) then the output of DES is (R_{16}, L_{16}). Show that when $k = 0^{56}$ then $DES_k(DES_k(x)) = x$ for all x. Find one more DES key with the same property. These keys are called weak keys for DES. Do these keys represent a serious vulnerability in the use of triple-DES as a pseudorandom permutation? Explain.

Question 2. Marks: 5.0

Show that if $G : \{\{0,1\}^n \to \{0,1\}^{2n}\}$ is a length-doubling PRG, then G is a one-way function (OWF).