Question 1. Marks: 7.0

Recall that $f : \mathbb{N} \to \mathbb{R}^+$ is a negligible function if for every positive polynomial $p(\cdot)$ there exists an N s.t. for all $n > N$ we have $f(n) < 1/p(n)$.

1. Prove that $n^{-\log n}$ is a negligible function.
2. Define $f : \mathbb{N} \to \mathbb{R}^+$ as $f(n) = n \mod 2$. Is f a negligible function? Explain.

(4+3 marks)

Question 2. Marks: 3.0

You are doing a meet-in-the-middle attack against 2DES (double DES with two 56 bit keys and a 64 bit message block) with only one plaintext-ciphertext pair (x, y). What is the expected number of candidate keys that remains to be checked (one of which will be the actual key) assuming that DES gives a uniformly random 64 bit block if we use a wrong key.