Problem 3:

2. Different messages that result in the same signature and are grammatically correct English sentences:
   m = "How many stars do you think there are in the universe?"
   m' = "221442317185 at least!"

3. Since signing messages use a hash function, in this case, SHA256, to get the same signature for two different messages, we need a hash collision. We can use the birthday paradox problem to figure out how large d would have to be to ensure that the probability we have a hash collision is less than 50%. From the birthday paradox problem:
   $E[X] = C(k,2)/N \approx k^2 / 2 * N < ½$
   Going back to the birthday paradox problem, k in this equation would be 200 or the number of "balls", in this case, messages signed, we throw in N bins. N is approximately 2^d which is the number of leaves in a binary tree with depth d. So now we have:
   $200^2 / 2 * 2^d < ½$
   $40000 / 2 * 2^d < ½$
   $20000 / 2^d < ½$
   $2^d > 40000$
   $d > \log_2(40000)$
   $d > 15.2877$
   This means we would need d to be at least 16 to ensure that the probability we have a hash collision is less than 50%.