ENEE 457
RSA Signatures Class Exercise

Consider the "Plain" RSA Signature scheme covered in the lecture.

1. Show how an adversary can create a forgery with a "no-message attack." I.e. the adversary makes no queries to the signing oracle.

   Choose any \sigma \in Z_N. Set m = \sigma^e \mod N. Output (m, \sigma) as the forgery.

2. Assume the adversary wants to forge a signature on a target message m^***.** Show how the adversary can make 2 queries to the signing oracle to create a forgery on m^*. Can this be done with less than 2 signing queries?

   Pick m_1, m_2 \neq 1 such that m_1 * m_2 = m^* mod N.
   Query oracle on m_1, get back \sigma_1
   Query oracle on m_2, get back \sigma_2
   Output forgery (m^*, \sigma^*), where \sigma^* = \sigma_1*\sigma_2.

   Note that the forger is correct since
   \sigma_1 * \sigma_2 = (m_1)^d * (m_2)^d = (m_1*m_2)^d,
   which is exactly a signature on m_1*m_2 = m^*.