Quiz 7

Student ID Number: Name _____

Math 173A, 3PM

Please justify all your answers November 14, 2019

Please also write your full name on the back

1. Fill in the blank.
   (a) True or False? If $a^n \equiv a \pmod{n}$ for all a, then n is prime.
   (b) The security of RSA relies on the supposed difficulty of factoring large integers.
2. The exponents $e = 1$ and $e = 2$ should not be used in RSA. Why?

3. Suppose that there are two users on a network. Let their RSA moduli be N_1 and N_2. with $N_1 \neq N_2$. If you are told that N_1 and N_2 are not relatively prime, how would you compromise their communications?