Quiz 5

Student ID Number: Name ____________________________
Math 17A, 3PM
Please justify all your answers July 19, 2019
Please also write your full name on the back

1. Fill in the blank.

   (a) Fix an integer n. We say that an integer a is a ____________________ for the compositeness of n if $a^n \not\equiv a \pmod{n}$.

   (b) A composite number n such that $a^n \equiv a \pmod{n}$ for all integers a is called ____________________.

2. Suppose your RSA modulus is $n = 55$ and your encryption exponent is $e = 3$.

   (a) Find the decryption modulus d.

   (b) Decrypt the ciphertext $c \equiv 42 \pmod{55}$.