Quiz 5

Student ID Number: Name _____

Math 173A, 3PM

Please justify all your answers November 7, 2019

Please also write your full name on the back

1. Fill in the blank.

   (a) True or false? For all integers $N > 1$, the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$ has a primitive root.

   (b) True or false? The security of the RSA cryptosystem relies on the supposed hardness of the discrete logarithm problem.

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

   (a) Find the decryption exponent d.

   (b) Describe how you would decrypt the ciphertext $c \equiv 42 \pmod{55}$. *Don't actually compute the plaintext.*