Quiz 4

Student ID Number: Name ____________________

Math 173A, 3PM

Please justify all your answers October 24, 2019

Please also write your full name on the back

1. Fill in the blank.

   (a) Given a prime p and numbers $g, g^a \pmod{p}$, and $g^b \pmod{p}$ for some $g \in \mathbb{F}_p^\times$ and integers a and b, the task of finding $g^{ab} \pmod{p}$ is called the ________________ problem.

   (b) In the ElGamal cryptosystem, Alice chooses a prime p and an element $g \in \mathbb{F}_p^\times$. She then secretly chooses an element $a \in \{0, 1, \ldots, p-2\}$ and publishes $g^a \pmod{p}$, called her ________________.

   (c) True or false? If Eve can break the Elgamal cryptosystem then she can solve the Diffie-Hellman problem.

2. (a) Solve $7d \equiv 1 \pmod{30}$.

   (b) Suppose you write a message as a number $m \pmod{31}$. Encrypt m as $m^7 \pmod{31}$. How would you decrypt?