Quiz 2

Student ID Number: Name _____

Math 173B, 1PM

Please justify all your answers January 23, 2020

Please also write your full name on the back

1. Fill in the blank.

   (a) Suppose P is a point on the elliptic curve E and $Q = nP$ for some n. The task of finding n given Q is called _____.

   (b) True or false? An elliptic curve E over $\mathbb{F}_p$, p a prime, can have any number of points on it between 0 and $p^2 + 1$.

2. Let P be a point on the elliptic curve E. How many point operations (additions or doublings) does it take to compute $37P$?

3. Suppose Alice and Bob decide to set up a shared secret using the elliptic curve Diffie-Hellman protocol. They publicly agree on some curve E over $\mathbb{F}_p$ for some prime p and a point $G \in E$ of large prime order. Alice sends the point P_A to Bob and Bob sends the point P_B to Alice. Suppose Eve can solve the elliptic curve discrete logarithm problem. Explain how she can compromise Alice and Bob's shared secret.