Quiz 7

Student ID Number: Name ____________________

Math 173B, 1 PM

Please justify all your answers February 28, 2019

Please also write your full name on the back

Here we describe (with an example) a cryptosystem that requires Alice and Bob to exchange several messages.

Bob and Alice fix a publicly known prime $p = 32611$ and all other numbers used are private. Alice takes her message $m = 11111$, chooses a random exponent $a = 3589$, and sends the number $u = m^a \pmod{p} = 15950$ to Bob. Bob chooses a random exponent $b = 4037$ and sends $v = u^b \pmod{p} = 15422$ back to Alice. Alice then computes $a^{-1} \equiv 15619 \pmod{p-1}$ then $w = v^{15619} \equiv 27257 \pmod{32611}$ and sends $w = 27257$ to Bob. Finally, Bob computes $b^{-1} \equiv 31883 \pmod{p-1}$ then $w^{31883} \pmod{32611}$ and recovers the value 11111 of Alice's message.

1. Describe a version of this cryptosystem that uses the elliptic curve discrete log problem. It will start with them agreeing on an elliptic curve E over $\mathbb{F}_p$ for some prime p and some point $P \in E(\mathbb{F}_p)$. Assume that they both know the order of P in $E(\mathbb{F}_p)$.