CSE 484 In-class Worksheet #5 (Spring 2016)
Name: _____ UWNetID: _____ Date: _____
Email address: _____
Partner names for this activity: _____

Q1: Why might cryptographers not like Encrypt-and-MAC mode for authenticated encryption?

Q2: Let p = 11. Let g = 10. Compute g^1 mod p, g^2 mod p, g^3 mod p, …, g^{100} mod p.

Q3: Let p = 11. Let g = 7. Compute g^1 mod p, g^2 mod p, g^3 mod p, …, g^{100} mod p.

Q4: Let p = 11. Let g = 3. Compute g^1 mod p, g^2 mod p, g^3 mod p, …, g^{100} mod p.

Q5: Let p = 11. Let g = 7. Alice's private key is x=4. Bob's private key is y=8. What is their shared key?