**CSE 484 In-class Worksheet #0xFFFFFFFF (Fall 2016)**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UWNetID: \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student ID #: \_\_\_\_\_\_\_\_\_\_\_

Partner names for this activity: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Q1:** Let p = 11. Let g = 10. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q2:** Let p = 11. Let g = 7. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q3:** Let p = 11. Let g = 3. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q5:** Why is the statement “the Discrete Logarithm problem is hard” not enough to guarantee that “Diffie-Hellman is secure”?

**Q6:** Let p = 11. Let g = 7. Alice’s private key is x=4. Bob’s private key is y=8. What is their shared secret?