**CSE 484 In-class Worksheet – Lecture 10 – Spring 2017**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UW Student # : \_\_\_\_\_\_\_\_\_\_\_\_\_ 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 g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q3:** Let p = 11. Let g = 7. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q4:** Let p = 11. Let g = 3. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q5: Diffie-Hellman.** 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?