**CSE 484 In-class Worksheet – Lecture 11 – Spring 2017**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UW Student # : \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**Q1 (Refresher):** Let p = 11. Let g = 7. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q2 (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?

**Q3 (RSA):** Given these RSA parameters: p=5, q=7, e=5

What is N?

What is ϕ(N)?

What is d?

Given these parameters, encrypt 16.

Given the parameters, decrypt 12.

**Q4:** Is there anything in the crypto section of the course that was particularly confusing, or that you found particularly interesting? Is there anything else you’d like to share?