CSE 484 In-Class Worksheet #13 – Autumn 2018
Name: _____ UWNetID: _____ Date: _____
Email address: _____
Partner names for this activity: _____
Will you want to pick up your worksheet later? Circle one: Yes / No

Q1 (Diffie-Hellman): Let p = 11. Let g = 10. Compute g^1 mod p, g^2 mod p, g^3 mod p, …, g^{20} mod p. Also compute g^{5000} mod p. Don't use a calculator or computer.

Q2 (Diffie-Hellman): Let p = 11. Let g = 3. Compute g^1 mod p, g^2 mod p, g^3 mod p, …, g^{20} mod p. Also compute g^{5001} mod p. Don't use a calculator or computer.

Q3 (Diffie-Hellman): Let p = 11. Let g = 7. Alice's private key is x=3. Bob's private key is y=8. What is their shared key?

Q4 (RSA): Given these RSA parameters: p=5, q=7, e=5

What is N?

What is $\phi(N)$?

What is d?

Given these parameters, encrypt 16.

Given the parameters, decrypt 12.