CSE 484 In-class Worksheet – Lecture 11 – Fall 2017

Name: ________________ UW Student # : _____________ Date: __________________

Email address: ____

Partner names for this activity: ____________________________________

Q1 (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?

Q2 (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.