CSE 484 In-Class Worksheet #10 – Spring 2019

Name: ____________________________ UWNetID: _____________ Date: ____________
Email address: ____
Partner names for this activity: ____________________________________
Will you want to pick up your worksheet later? Circle one: Yes / No

Q1: What problem do you see with the "Encrypt-and-MAC" approach for authenticated encryption?

Q2 (Diffie-Hellman): Let p = 11. Let g = 2. Alice's private key is x=9. Bob's private key is y=4. What is their shared key?