

**CSE 484 In-class Worksheet #5**

Name: \_\_\_\_\_ UWNNetID: \_\_\_\_\_ 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  $g^1 \bmod p$ ,  $g^2 \bmod p$ ,  $g^3 \bmod p$ , ...,  $g^{100} \bmod p$ .

**Q3:** Let  $p = 11$ . Let  $g = 7$ . Compute  $g^1 \bmod p$ ,  $g^2 \bmod p$ ,  $g^3 \bmod p$ , ...,  $g^{100} \bmod p$ .

**Q4:** Let  $p = 11$ . Let  $g = 3$ . Compute  $g^1 \bmod p$ ,  $g^2 \bmod p$ ,  $g^3 \bmod p$ , ...,  $g^{100} \bmod p$ .

**Q5:** 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?