**CSE 484 In-class Worksheet #0x76736577 (Fall 2016)**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UWNetID: \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student ID #: \_\_\_\_\_\_\_\_\_\_\_

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

**Q1:** Hashes are one-way, which means it’s better to store a hash of a password than the password itself on a server. But let’s say someone steals a multiple databases of millions of hashed passwords, and wants to find out what peoples’ passwords were. What might the attacker do? Why is this approach weak?

**Q2:** Why might cryptographers not like Encrypt-and-MAC mode for authenticated encryption?

**Q3:** Let p = 11. Let g = 10. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q4:** Let p = 11. Let g = 7. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q5:** Let p = 11. Let g = 3. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

**Q6:** Let p = 11. Let g = 7. Alice’s private key is x=4. Bob’s private key is y=8. What is their shared secret?