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

Q1. Using modular exponentiation and without evaluating the exponent directly, what is 35 mod 11?

Q2. In one Diffie-Hellman exchange, which variables are public? What does Alice know? Bob?

(some options: p, g, x, y) What do they send to each other? What is the shared key?

Q3. What does Zp\* represent? What is the mathematical definition of co-primality for p and q?

Q4.Let p = 11. Let g = 5. Alice’s private key is x=4. Bob’s private key is y=8. What is their shared key?

Q5. What does Euler’s Totient function compute for some integer p? What is ϕ(35)?

Q6. What is the public key in RSA? The private key? (some options: p, q, n, e, d)

Q7. In a RSA communication, Alice is trying to send a message with value 16 to Bob. Her public key is (5,35) and his private key is (5,35). What is the resulting cipher text? How do we decrypt this?

Q8. Given that Alice generates the (large) prime numbers p=5 and q=7. What do we choose for e? What are its bounds? What is a value for d that works? Why not 3?

Q9. Are RSA or Diffie-Hellman sufficient for all of our security needs? Which cryptography goals do they meet?