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

**MAC & Hashing**

Q1. What security goal are we able to achieve by the use of MAC?

Q2. After submitting your lab1 md5 hashes, you decide to modify the solution without the TAs knowing. Which known cryptographic vulnerability of md5 can you take advantage of?

**Number Theory**

Q3. Using modular exponentiation and without evaluating the exponent directly, what is 35 mod 11?

Q4. Produce the generating sequence for g = 4 and p = 7. What order is it?

**Diffie-Hellman**

Q5. In one Diffie-Hellman exchange, which variables are public? What does Alice know? Bob?

(some options: p, g, x, y)

1. What do they send to each other?
2. What is the shared key?
3. What makes it secure?

Q6.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?

**RSA**

Q7. What does Euler’s Totient function compute for some integer p? What is ϕ(35)?

Q8. 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?

Q9. 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?

**Security Goals Review**

Q10. What are the 4 security goals that we are trying to achieve?

|  |
| --- |
|  |
|  |
|  |
|  |

Q11. Are RSA or Diffie-Hellman sufficient for all of our security needs? Which security goals do they meet?