**CSE 484 In-section Worksheet #4**

Q1. Secret message:

EFVELEQHSCSYFMXICSYVXLYQFEXYWWMV
WEQTWSRMHSFMXIQCXLYQFWMV

Q2.Let p = 11. Let g = 10. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

Q3. Let p = 11. Let g = 7. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

Q4. Let p = 11. Let g = 3. Compute g1 mod p, g2 mod p, g3 mod p, …, g100 mod p.

Q5. Which symmetric encryption mode would you use for the following situations? Why?

 *You are going to send a small one-time command to fire to your nukes.*

 *You are living in the 1970s and want to send a long letter to your lover on ARPANET.*

 *You are sending lots of large message quickly and care about latency.*

 *Everything else (given the tools we’ve learned)*

Q5. What is a flaw with ECB encryption?