CS 372 Introduction to Computer Networks
Self-Check Exercises: Lecture 42

1) What is message encryption? (High-level is OK)

2) How would encryption work with public key encryption?

3) Use the RSA algorithm discussed in lecture to develop a public key and a private key for public-key encryption. Let $p = 5$, $q = 11$, $e = 7$, m is the original message, c is the encrypted message.
   a. $n =$

   b. $z =$

   c. $d =$

   d. $c = \text{Kpublic}(m) =$

   e. $\text{Kprivate}(c) =$

   f. $\text{Kprivate}(\text{Kpublic}(m)) =$

4) How might authentication work with public key encryption? (Textbook will be helpful here)