CS 372 Introduction to Computer Networks

Self-Check Exercises: Lecture 42 **Solutions**

1) What is message encryption? (High-level is OK)
Altering the contents of a message so that it is difficult (or impossible) to ascertain the original message, unless you are the intended recipient, by means of cryptography.

2) How would encryption work with public key encryption?
Sender encrypts with recipient's registered public key. Recipient decrypts with their own private key.

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 = pq = 5 x 11 = 55

b. z = (p-1)(q-1) = 4 x 10 = 40

c. d = 23
There are several possibilities. Choose d so that ed-1 is exactly divisible by z.
If we choose d = 23, ed-1 = 7 x 23 – 1 = 160, which is divisible by 40.

d. c = Kpublic(m) = m^e mod n

e. Kprivate(c) = c^d mod n

f. Kprivate(Kpublic(m)) = m

4) How might authentication work with public key encryption? (Textbook will be helpful here)
Sender encrypts a signature with a registered private key, and distributes public key. If this known public key correctly decrypts the signature, we know the sender to be who we think they are.