Homework Assignment 7
ECE 151 / CMPSC 171 - Spring 2013
Due Tuesday, May 28
Note: Monday, May 27, is Memorial Day (a Holiday)

1. (a) Explain the difference between confidentiality and integrity. Can we have one without the other?

(b) Explain the difference between integrity and authentication. Can we have one without the other?

2. Consider the RSA algorithm, described in Lecture 12, Slides 18 and 19, which is used for public key cryptography.

(a) Given the values $p = 7$ and $q = 13$, find the smallest legitimate value of d and the corresponding value of e.

(b) Using the RSA algorithm and the value of e that you found, encrypt "ACE" where A is represented by 1, C is represented by 3, and E is represented by 5.

3. (a) Explain the "key" difference between symmetric cryptography and asymmetric cryptography.

(b) Discuss the advantages and disadvantages of symmetric cryptography and asymmetric cryptography.

4. Consider the Needham-Schroeder protocol for authentication, as corrected with the additional nonce RB1, given in Lecture 12, Slide 30.

(a) Why is the additional nonce RB1 necessary?

(b) The KDC puts B (Bob) into its reply message and A (Alice) into the ticket. Why does the KDC do so?

(c) In the KDC's message to Alice, the ticket is encrypted with the shared secret key $K_{A,KDC}$. Why is it necessary to encrypt the ticket?

5. In public-key cryptography, explain the difference in the use of the public key and the private key for (a) secrecy and (b) authentication.

6. Consider the Diffie Hellman Key Exchange as given in Lecture 13, Slide 22.

(a) Construct an example consisting of specific numbers n, g, x and y.

(b) Show the specific numbers that Alice and Bob send to each other in Steps (1) and (2) of the algorithm.

(c) Show that Alice and Bob constract the same shared secret key in Steps (3) and (4) of the algorithm.