COE 449: Network Security Engineering
HW 5 – Chapter 9, 10, 11, 12
Posted: 3 January 2009 Due: 12 January 2009

1- Reconsider the case of Alice and her stockbroker, Bob. Suppose they decide not to use a session key. Instead, Alice pads the message (BUY or SELL) with random data.
   a. Explain under what conditions this approach would be effective?
   b. Discuss how the length of the block affects your answer?

2- Consider the following authentication protocol, which uses a classical cryptosystem. Alice generates a random message *r*, enciphers it with the key *k* she shares with Bob, and sends the enciphered message *{r}k* to Bob. Bob deciphers it, adds 1 to *r*, and sends *{r + 1}k* back to Alice. Alice deciphers the message and compares it with *r*. If the difference is 1, she knows that her correspondent shares the same key *k* and is therefore Bob. If not, she assumes that her correspondent does not share the key *k* and so is not Bob. Does this protocol authenticate Bob to Alice? Why or why not?

3- Referring to cipher techniques (Ch 10), give an example to each of the three attacks below:
   a. Precomputing the Possible Messages
   b. Misordered Blocks
   c. Statistical Regularities

4- Explain in your words (half a page minimum) IPsec??

5- What are the 7 checkers that must be met for successful proactive passwords??

6- Relating to salting a password
   a. What is it and what is its benefit?
   b. Why should salts be chosen at random?
   c. Does using passwords with salts make attacking a specific account more difficult than using passwords without salts? Explain why or why not?

7- What are the two problems involved in implementing password aging?

8- Classify the following proposed passwords as good choices or poor choices, and justify your reasoning.
   a. Mary
   b. go2work
   c. cat&dog
   d. 3.1515pi

9- A computer system uses biometrics to authenticate users. Discuss ways in which an attacker might try to spoof the system under each of the following conditions.
   a. The biometric hardware is directly connected to the system, and the authentication software is loaded onto the system.
   b. The biometric hardware is on a stand-alone computer connected to the system, and the authentication software on the stand-alone computer sends a "yes" or "no" to the system indicating whether or not the user has been authenticated.

10- Give an example in your words for each of the 8 principles of secure designs?