There is no need to turn in your solution of HW6. The solution of HW6 will be posted on 28th April, 2011. There are 5 questions from chapter 8.

Chapter 8

P762 P5,
P762 P6,
P763 P7,
P763 P10,
P764 P12

P5. Consider the block cipher in Figure 8.5. For a given "key" Alice and Bob would need to keep eight tables, each 8 bits by 8 bits. For Alice (or Bob) to store all eight tables, how many bits of storage are necessary? How does this number compare with the number of bits required for a full-table 64-bit block cipher?

P6. Consider the 3-bit block cipher in Table 8.1. Suppose the plaintext is 100100100.
   a) Initially assume that CBC is not used. What is the resulting ciphertext?
   b) Suppose Trudy sniffs the cipher text. Assuming she knows that a 3-bit block cipher without CBC is being employed (but doesn’t know the specific cipher), what can she surmise?
   c) Now suppose that CBC is used with IV=111. What is the resulting ciphertext?

P7.
   a) Using RSA, choose p=3 and q=11, and encode the word "dog" by encrypting each letter separately. Apply the decryption algorithm to the encrypted version to recover the original plaintext message.
   b) Repeat part (a) but now encrypt “dog” as one message m.

P10. Suppose Alice wants to communicate with Bob using symmetric key cryptography using a session key $K_s$. In Section 8.2, we learned how public-key cryptography can be used to distribute the session key from Alice to Bob. In this problem, we explore how the session key can be distributed- without public key cryptography- using a Key
Distribution Center (KDC). The KDC is a server that shares a unique secret symmetric key with each registered user. For Alice and Bob, denote these keys by $K_{A,KDC}$ and $K_{B,KDC}$. Design a scheme that uses the KDC to distribute $K_s$ to Alice and Bob. Your scheme should use three messages to distribute the session key: a message from Alice to the KDC, a message from the KDC to Alice, and finally a message from Alice to Bob. The first message is $K_{A,KDC}(A,B)$. Using the notation, $K_{A,KDC}$, $K_{B,KDC}$, $S$, $A$ and $B$ answer the following questions.

a. What is the second message?
b. What is the third message?

P12. Suppose Alice and Bob share two secret keys: an authentication key $S_1$ and a symmetric encryption key $S_2$. Augment Figure 8.9 so that both integrity and confidentiality are provided.