1. Show that DES decryption can be done by applying the DES encryption Algorithm to the ciphertext with the key schedule reversed.

2. Describe How DES can be used for message authentication.

3. Suppose, the text Alice sends Bob is not encrypted, how would you Make sure that the text Alice sends Bob is encrypted and authenticated?

4. If the input to S-box S1 is 011010
   a) What bits select the row? Column?
   b) What is the output?