CS 178 Intro to Crypto

1. In the DES algorithm, compute the following:

$$IP(1248842112488421)$$

$$E(84211248) \quad P(12488421)$$

$$S_i(110011) \text{ for } i = 1, 2, \ldots, 8$$

   All numbers are hex or binary.

2. Consider the DES algorithm.
   (1) Suppose that $K_1 = K_2 = \cdots = K_{16}$. Show that all bits in C_1 are equal and all bits in D_1 are equal.
   (2) Show that there are exactly 4 DES keys for which all round keys are the same. They are called *weak DES keys*.
   (3) Determine these 4 weak DES keys.

3. Consider the Cipher Feedback (CFB) mode of the DES algorithm. Answer the following questions:
   (1) Assume $s = 4$. The 4-bit ciphertext C_2 is corrupted during the transmission, and the recipient has the incorrect value of C_2. How many plaintext values starting from M_2 will be incorrectly computed?
   (2) Assume $s = 8$. A single DES encryption takes 16 cycles, and an 8-bit shift takes just one cycle. How many cycles are needed to encrypt 1024 bits of data?

4. There are other modes of block cipher besides the ones we have learned. One of these modes is named Plaintext Block Chaining (PBC) Mode. On the encryption side, the following is executed to obtain the nth ciphertext: $C_n := E_k(M_n) \oplus M_{n-1}$. Suppose that we need to encrypt $M_1, \ldots, M_5$ using the PBC mode. Show the explicit formulas to obtain $C_1, \ldots, C_5$. What do you need to use for M_0? Also, show the steps on the decryption side to obtain $M_1, \ldots, M_5$.