1. In the DES algorithm, compute the following:
   (1) IP(1248842112488421)
   (2) E(84211248)
   (3) P(12488421)
   (4) S_i(110011) 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. 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 $M_1, \ldots, M_5$.

4. (9 pts) Consider the AES/Rijndael algorithm and its Galois field GF(2^8).
   (a) Compute the sum (`a7`) + (`5c`) in GF(2^8)
   (b) Compute the product (`a7`) × (`5c`) in GF(2^8)
   (c) Compute S(`a7`)
   (d) Compute S^{-1}(`5c`)

5. The definition of the SubBytes function is given as $f(a) = A\ a^{-1} \oplus d$ for a fixed 8×8 matrix A and 8×1 vector d. Let $a = x + 1$. Compute $f(a)$ using the SubBytes lookup table and then using the above definition. Show that these values are equal.