Tutorial 2: Symmetric Key Crypto

1. This problem deals with a Feistel Cipher.

   a. Give the definition of a Feistel Cipher.
   b. Is DES a Feistel Cipher?
   c. Is AES a Feistel Cipher?
   d. Why is the Tiny Encryption Algorithm, TEA, "almost" a Feistel Cipher?

2. Consider a Feistel cipher with four rounds. Then the plaintext is denoted as *P* = (Lo, Ro) and the corresponding ciphertext is C = (L_4, R_4). What is the ciphertext C, in terms of *Lo,* Ro*,* and the subkey, for each of the following round functions?

   a. $\mathbf{F(R_{i-1},K_i) = 0}$
   b. $\mathbf{F(R_{i-1},K_i) = R_{i-1}}$
   c. $\mathbf{F(R_{i-1},K_i) = K_i}$
   d. $\mathbf{F(R_{i-1},K_i) = R_{i-1} \oplus K_i}$

3. This problem deals with the DES cipher.

   a. How many bits in each plaintext block?
   b. How many bits in each ciphertext block?
   c. How many bits in the key?
   d. How many bits in each subkey?
   e. How many rounds?
   f. How many S-boxes?
   g. An S-box requires how many bits of input?
   h. An S-box generates how many bits of output?

4. AES consists of four functions in three layers.

   a. Which of the four functions are primarily for confusion and which are primarily for diffusion? Justify your answer.
   b. Which of the three layers are for confusion and which are for diffusion? Justify your answer.