In this lab you will implement the simplified DES that we discussed in Lecture 6. Refer to the wire diagrams shown below.

Li-1

Ri-1

Li

Ri

⊕

f

Ki

Ri-1

S2

⊕

E(Ri-1)

Ki

S1

Return f(Ri-1, Ki)

For this assignment use the functions **expand()** and **Sbox1()** (we called this S11\_function() in homework5) to do the following:

1. Create a second function for substitution box **Sbox2()** that replicates the **Sbox1()**  your wrote for homework 5 except that it uses the following substitution boxes: S11 contains the binary of the numbers (4, 0, 6, 5, 7, 1, 3 2) and S12 contains those for (5, 3, 0, 7, 6, 2, 1, 4). (20 points)
2. Create a round function called **round1()** that takes a binary character vector of length 12 and key K of length 9 and does the following: (20 points total)
   1. Divide the block into two equal halves called L0 and R0.
   2. Create two sub keys K1 containing the first 8 digits of K and K2 that contains the last 8 digits of K.
   3. Expand R0 from 6 t o 8 bits and call it ER0.
   4. Take the XOR of the result of ER0 with K1. Store the first 4 bits in a variable called block1 and the last 4 bits in a variable called block2.
   5. Call Sbox1() with block1 as its parameter.
   6. Call Sbox2() with block2 as its parameter.
   7. Concatenate the results of e) and f) and store the result in a variable called FR0.
   8. Take the XOR of FR0 and L0 and store the results in R1.
   9. Store R0 to L1.
   10. Return L1 concatenated to R1.
   11. Test the function round1() with the following input parameters: round1('000001010111', "001101100")
3. Write a second function called **round2()** that is similar to **round1()**  except that it uses K2 and returns the concatenation of R2 and L2. (20 points)
4. Write an encryption function: des\_ecrypt() by using the work from 1-3 above.. Encrypt the message” “Wire $2000 to Bob” using the functions you wrote above following the simplified DES discussed in the class. (20 points)
5. Write a decryption function des\_decrypt() as follows. Modify the functions **round1()** and **round2()** such that they can be used for decryption. [Hint: for decryption use K2 instead of K1 for **round1()** and K1 instead of K2 for **round2()**]. (20 points)