Homework 2

Please put your solutions in a .doc, .docx or .pdf to CSNS by 11:59pm, Monday 02/12.

Total points: 5

---

1 (2pt) This problem provides a numerical example of encryption using a one-round version of DES. Suppose both the key and the output of the initial p-box are:

1010 1101 0101 0110 1100 1001 1101 1010 1001 0001 1011 1011 0001 1001 1011 1010

a. Derive k1, the first round key
b. Derive L0, R0
c. Expand R0 to get E[R0] using the Expansion P-box
d. Calculate A = E[R0] XOR K1
e. Group the 48-bit result of (d) into sets of 6 bits and get the corresponding S-box substitutions
f. Concatenate the results of (e) to get a 32-bit results, B
g. Apply the permutation to get P(B)
h. Calculate R1 = P(B) XOR L0
i. Write down the output of the first round.

2.(1pt) For the group G = $<Z_{26^*}, x>$

a. Find the order of the group

b. Find the order of each element in the group

c. Is the group is a cyclic group? Prove your answer and find the generator(s) if the answer is yes.

3(2pt) Using the irreducible polynomial $f(x) = x^5+x^4+x^3+x^2+1$ to

a) generate the elements of the field $GF(2^5)$

b) **based on the results of a)**, calculate the followings in $GF(2^5)$

b.1) $(x^4 - x + 1)^{-1}$

b.2) $(x^3 - x + 1) * (x^4 + x^2 - x + 1)$

b.3) $(x^4 - x^3 + 1) / (x^2 + x + 1)$

Note: You won't get credit if you don't use the results of a) to do b)
