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

K1 = 1001 0111 1000 1011 1011 1011

0100 0010 1101 1101 1011 0001

b. Derive L0, R0

L0 = 0000 1110 1111 1010 0000 0011 0111 0101

R0 = 1011 1101 1010 0001 1110 1101 1010 1010

c. Expand R0 to get E[R0] using the Expansion P-box

EXP(R0) = 010111 111011 110100 000011 111101 011011 110101 010101

d. Calculate A = E[R0]    XOR  K1

010010 000011 011010 111000 101101 110110 000011 100100

e. Group the 48-bit result of (d) into sets of 6 bits and get the corresponding S-box substitutions

110010 = s1 = row 2 col 9 = 12; 000011=s2= row1 col 1 = 13; 011010 =s3=row 0 col13; 111000=s4=row 2 col 12 = 5; 101101=s5=row 3 col 6 =2; 110110=s6=row 2 col 11=10; 000011=row 1 col 1=0; 100100=row 2 col 2=4;

1100 1101 0100 0101 0010 1010 0000 0100

f. Concatenate the results of (e) to get a 32-bit results, B

1100 1101 0100 0101 0010 1010 0000 0100

g. Apply the permutation to get P(B)

P(B) = 1001 0000 1010 1001 1100 0000 1001 0000

h. Calculate R1 = P(B)  XOR  L0

1001 1110 0101 0011 1100 0011 1110 0101

i. Write down the output of the first round.

L1 = R0;

L1ConcatR1= 1011 1101 1010 0001 1110 1101 1010 1010

1001 1110 0101 0011 1100 0011 1110 0101 ;

CIPHERTEXT(after final permutation):

0111 1110 1010 1001 1100 0110 1100 0101

1110 0000 0101 0111 0010 1110 1101 1111

OR 7EA9C6C5E0572EDF

3(2pt)  Using the irreducible polynomial  f(x) = x5+x4+x3+x2+1 to

1. generate the elements of the field GF(25)

g5 = g4+g3+g2+1

|  |  |  |
| --- | --- | --- |
| 0 = | 0 = | 00000 |
| g0 = | g0 = | 00001 |
| g1 = | g1 = | 00010 |
| g2 = | g2 = | 00100 |
| g3 = | g3 = | 01000 |
| g4 = | g4 = | 10000 |
| g5 = | g4+ g3+ g2+ 1 | 11101 |
| g6 = | g2 + g | 00101 |
| g7 = | G3 +g2 | 01010 |
| g8 = | G4 + g2 | 10100 |
| g9 = | G4+g2+1 | 10101 |
| g10 = | G4+g2+1+g | 10111 |
| g11 = | G4 + 1+g | 10011 |
| g12 = | G4+g3+1+g | 11011 |
| g13 = | g3+1+g | 01011 |
| g14 = | G4+g2+g | 10110 |
| g15 = | G4+1 | 10001 |
| g10 = | G4+g3+g2+1+g | 11111 |
| G11= | 1 + g | 00011 |
| G12= | G2+g | 00110 |
| G13 | G3+g2 | 01100 |
| G14= | G4+g3 | 11000 |
| G15= | g3+g2+1 | 01101 |
| G16= | G4+g3+g | 11010 |
| G17= | g3+1 | 01010 |
| G18= | G4+g | 10010 |
| G19= | G4+g3+1 | 11001 |
| G20= | G3+g2+g+1 | 01111 |
| G21= | G4+g3+g2+g | 11110 |
| G22= | 1 | 00001 |
| G23 | G | 00010 |
| G24 |  |  |

b) **based on the results of a)**, calculate the followings in GF(25)

   b.1) (x4 - x+ 1)-1

   b.2) (x3- x + 1) \* (x4 + x2 - x + 1)

   b.3) (x4- x3 + 1) / (x2 + x + 1)