MODEL LAB

1. **Write a program to perform rotate word and substitute byte for key generation in AES**

Code :

```
h = ['0','1','2','3','4','5','6','7','8','9','a','b','c','d','e','f']
s_box = [['63', '7c',    '77',    '7b',    'f2',    '6b',    '6f',    'c5',    '30',    '01',    '67',
          '2b',    'fe',    'd7',    'ab',    '76'],['ca',    '82',    'c9',    '7d',    'fa',    '59',
          '47',    'f0',    'ad',    'd4',    'a2',    'af',    '9c',    'a4',    '72',    'c0'],['b7',
          'fd',    '93',    '26',    '36',    '3f',    'f7',    'cc',    '34',    'a5',    'e5',    'f1',
          '71',    'd8',    '31',    '15'],['04',    'c7',    '23',    'c3',    '18',    '96',    '05',
          '9a',    '07',    '12',    '80',    'e2',    'eb',    '27',    'b2',    '75'],['09',    '83',
          '2c',    '1a',    '1b',    '6e',    '5a',    'a0',    '52',    '3b',    'd6',    'b3',    '29',
          'e3',    '2f',    '84'],['53',    'd1',    '00',    'ed',    '20',    'fc',    'b1',    '5b',
          '6a',    'cb',    'be',    '39',    '4a',    '4c',    '58',    'cf'],['d0',    'ef',    'aa',
          'fb',    '43',    '4d',    '33',    '85',    '45',    'f9',    '02',    '7f',    '50',    '3c',
          '9f',    'a8'],['51',    'a3',    '40',    '8f',    '92',    '9d',    '38',    'f5',    'bc',
          'b6',    'da',    '21',    '10',    'ff',    'f3',    'd2'],['cd',    '0c',    '13',    'ec',
          '5f',    '97',    '44',    '17',    'c4',    'a7',    '7e',    '3d',    '64',    '5d',    '19',
          '73'],['60',    '81',    '4f',    'dc',    '22',    '2a',    '90',    '88',    '46',    'ee',
          'b8',    '14',    'de',    '5e',    '0b',    'db'],['e0',    '32',    '3a',    '0a',    '49',
          '06',    '24',    '5c',    'c2',    'd3',    'ac',    '62',    '91',    '95',    'e4',
          '79'],['e7',    'c8',    '37',    '6d',    '8d',    'd5',    '4e',    'a9',    '6c',    '56',
          'f4',    'ea',    '65',    '7a',    'ae',    '08'],['ba',    '78',    '25',    '2e',    '1c',
          'a6',    'b4',    'c6',    'e8',    'dd',    '74',    '1f',    '4b',    'bd',    '8b',
          '8a'],['70',    '3e',    'b5',    '66',    '48',    '03',    'f6',    '0e',    '61',    '35',
          '57',    'b9',    '86',    'c1',    '1d',    '9e'],['e1',    'f8',    '98',    '11',    '69',
          'd9',    '8e',    '94',    '9b',    '1e',    '87',    'e9',    'ce',    '55',    '28',
          'df'],['8c',    'a1',    '89',    '0d',    'bf',    'e6',    '42',    '68',    '41',    '99',
          '2d',    '0f',    'b0',    '54',    'bb',    '16']]
r_key =
[['01','00','00','00'],['02','00','00','00'],['04','00','00','00'],['08','00','00','00'],['10','00','00','00'],
['20','00','00','00'],['40','00','00','00'],['80','00','00','00'],['1B','00','00','00'],['36','00','00','00']]
print("Enter round key : ")
l2=[]
for i in range(4):
    l2+=[input().split()]
idx = 0
```

```
l3=[]
a=[]
i=3
for j in range(3):
    l3+=[l2[(j+1)][i]]
l3+=[l2[0][3] ]
print("Rotated column = ",l3)
for j in l3:
    a.append(s_box[h.index(j[0])][h.index(j[1])])
print("Substitution = ",a)
```

Output :

```
Enter round key :
a0 b1 c2 d3
e4 f5 a3 b4
c5 d6 e7 f8
a4 b5 c6 d7
Rotated column =  ['b4', 'f8', 'd7', 'd3']
Substitution =  ['8d', '41', '0e', '66']


...Program finished with exit code 0
Press ENTER to exit console.
```

2. **To implement dictionary attack**

Code :

```
import itertools
d={}
s="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890
"
two_letter=list(itertools.permutations(s,2))
#print(two_letter)
three_letter=list(itertools.permutations(s,3))
#print(three_letter)
passwords=two_letter+three_letter
for i in passwords:
    word="".join(i)
    d[hash(word)]=word
```

```
#print(d)
choice=int(input("Enter 1-Password to hash conversion  2-Password crack using hash value    0-Exit  : "))
while(choice!=0):
   if(choice==1):
      password=str(input("Ente password : "))
      print("Hash of password = ",hash(password))
   if(choice==2):
      hash_val=int(input("Enter hash value : "))
      print("password = ",d[hash_val])
   choice=int(input("Enter 1-Password to hash conversion  2-Password crack using hash value    0-Exit  : "))
```

Output :

```
Enter 1-Password to hash conversion  2-Password crack using hash value    0-Exit  : 1
Ente password : ISH
Hash of password =  -8711691796656064244
Enter 1-Password to hash conversion  2-Password crack using hash value    0-Exit  : 2
Enter hash value : -8711691796656064244
password =  ISH
Enter 1-Password to hash conversion  2-Password crack using hash value    0-Exit  : 0


...Program finished with exit code 0
Press ENTER to exit console.
```