**Assignment 1 solutions.**

**Ques 1:**

1. No, brute forcing the cipher by running it through all possible keys from 0-25, one can encrypt it. Hence, it is not perfectly secret.
2. Vignere cipher : have different keys for different letters and/or positions.

**Ques 2 :**

a)

def Enc(m,k):

result = ""

for i in range(len(m)):

char = m[i]

if (char == ' '):

result += ' '

elif (char.isupper()):

result += chr((ord(char) + k-65) % 26 + 65)

else:

result += chr((ord(char) + k - 97) % 26 + 97)

return result

m1 = "iitk is better than iitd and iitb"

k1 = 9

m2 = 'lets learn cryptography'

k2 = 25

print ("Text : " + m1)

print ("Shift : " + str(k1))

print ("Cipher: " + Enc(m1,k1))

print ("Text : " + m2)

print ("Shift : " + str(k2))

print ("Cipher: " + Enc(m2,k2))

b)

def Dec(m):

for i in range(26):

print("Orignal Text is " + Enc(m,-i))

print("The key is " , i)

m3 = 'bm ptl wtfg xtlr tztbg'

m4 = 'rc fjb mjvw njbh’

Dec(m3)

Key was 19;

Dec(m4)

Key was 9;