Assignment 1 solutions.

Q1

a) No, if subjected to brute force algorithms it can be cracked.
b) Yes what we can do is have different keys for different letters or positions. This way the key will also be as long as the message.

Q2

a)

```
def Enc(m,k):
    result = ""

    for i in range(len(m)):
        char = m[i]
        if (char == ' '):
            result += ' '


        # Encrypt uppercase characters
        elif (char.isupper()):
            result += chr((ord(char) + k-65) % 26 + 65)

        # Encrypt lowercase characters
        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;
```