LAB 3

Write a Program to do Encryption and Decryption using Vigenere Cipher. 2. Do the Cryptanalysis of Vigenere Cipher (Use sufficiently large CipherText). Use Index of Coincidence to verify the guessed Key Length. Use Mutual Index of Coincidence to guess the Key.

Code:

```
import string
values = dict()
for index, letter in enumerate(string.ascii_lowercase):
    values[letter] = index


def get(val):
    for key,value in values.items():
        if val == value:
            return key


def encryption(text,key):
    plength=len(text)
    pkey=len(key)
    temp = list()
    i=0
    for c in text:
        if(c!=' '):
            temp.append((values[c]+values[key[i % pkey]]) % 26)
            i = i+1
    ans = ""
    for p in temp:
```

```
        ans=ans+get(p)
    return ans

def decryption(text,key):
    temp=list()
    i=0
    plength=len(text)
    klength=len(key)
    for c in text:
        temp.append(values[c])
    ans=""
    for c in temp:
        m=(c-values[key[i%klength]])%26
        ans=ans+get(m)
        i=i+1
    return ans

frequency = [
        0.08167, 0.01492, 0.02782, 0.04253, 0.12702, 0.02228, 0.02015,
        0.06094, 0.06966, 0.00153, 0.00772, 0.04025, 0.02406, 0.06749,
        0.07507, 0.01929, 0.00095, 0.05987, 0.06327, 0.09056, 0.02758,
        0.00978, 0.02360, 0.00150, 0.01974, 0.00074]

def cal_IC(Lang):
    n = len(Lang)
    fre = cipher_f(Lang)
    Ic = sum([f*(f-1)/(n*n) for f in fre])
    return Ic

def find(t,l):
```

```
    for i in range(1,l):
        res=check(t, i)
        if res:
            return i


def check(t, l):
    IC=0.065
    limit=0.01
    Y = []
    Y_IC = []
    A = True
    c = ""
    for i in range(l):
        part = t[i::l]
        Y.append(part)
        temp = cal_IC(part)
        if abs(temp - IC) < limit:
            c += "1"
        else:
            c += "0"
            A=False
        Y_IC.append(temp)
    avg = sum(Y_IC)/len(Y_IC)
    m = 0.6
    if(c.count("1")/len(c) > m):
        A=True
    if abs(IC - avg) < limit and A:
        return True
    else:
        return False
```

```
def kasiski(cipherText):
    m=find(cipherText,26)
    return m

def cipher_f(cipherText):
    f=list()
    for index,letter in enumerate(string.ascii_lowercase):
        count=0
        for c in cipherText:
            if(c==letter):
                count += 1
        f.append(count)

    return f

def getProb(List1):
        L = [c for c in string.ascii_lowercase]
        n = len(List1)
        P = [List1.count(c)/n for c in L]
        return P

def MIC(LangX1, LangY1, maxChar=26):
    LangY1 = [c for c in LangY1]
    LangY2 = getProb(LangY1)
    buf = []
    for i in range(len(LangX1)):
        MI = sum([LangX1[j]*LangY2[j]
            for j in range(len(LangX1))])
        buf.append(MI)
```

```
        LangY2.append(LangY2.pop(0))
    max_MI = max(buf)
    key = buf.index(max_MI)
    print("MIC : ", max_MI, "\n Key alphabet :", get(key))
    return key


def getKey(t,l):
    secretKey=[]
    Y=[]
    for i in range(l):
        part=t[i::l]
        Y.append(part)
        temp= MIC(frequency,Y[i], 26)
        secretKey.append(get(temp))
    secretKey = "".join(secretKey)
    return secretKey


def cryptanalysis(t):
    m=kasiski(t)
    print("m:",m)
    key=getKey(t, m)
    print("Key by cryptanalysis:",key)
    return


text="perfect balance between art history and culture the extravaganza features
extraordinarily beautiful objects displaying the tribes history The performances that
complement these are works of art in motion While what might have been wars in ancient
times are recreated as mockfight dramas and are huge crowd pullers With war log drums
blazing shotguns backswords with bevels dao and spears performers stage fullblown mock
fights dressed in warrior costumes The shape pattern and carvings on traditional Naga
weapons differ from tribe to tribe Most of the performances are accompanied by live music
and rhythmic war cries HighlightsOrganised by the Government of Nagaland to promote
cultural heritage and encourage intertribal interactions the Hornbill Festival is the best way to
experience the rich culture of the state Some of the highlights of the festival are the
```

traditional Naga Morung exhibitions flower shows herbal medicine stalls fashion shows Naga wrestling indigenous games and musical concerts among others "

key = "india"

text = text.lower()

print("originalText: ")

print(text)

print("Key: ")

print(key)

cipherText = encryption(text,key)

print("encryption: ")

print(cipherText)

original = decryption(cipherText,key)

print("decryption: ")

print(original)

print("Cryptanalysis: ")

cryptanalysis(cipherText)

OUTPUT:

```
E:\SEM 6\NIS>13_vi.py
originalText:
perfect balance between art history and culture the extravaganza features extraordinarily beautiful objects displaying the tribes history the performances that complement these are works of art in motion while w
hat might have been wars in ancient times are recreated as mockfight dramas and are huge crowd pullers with war log drums blazing shotguns backswords with bevels dao and spears performers stage fullblown mock fi
ghts dressed in warrior costumes the shape pattern and carvings on traditional naga weapons differ from tribe to tribe most of the performances are accompanied by live music and rhythmic war cries highlightsorga
nised by the government of nagaland to promote cultural heritage and encourage intertribal interactions the hornbill festival is the best way to experience the rich culture of the state some of the highlights of
 the festival are the traditional naga morung exhibitions flower shows herbal medicine stalls fashion shows naga wrestling indigenous games and musical concerts among others
Key:
india
encryption:
krunekgeiliafmbmgzmevnubhqfwwrgnqlccywcrmgkmefguivitdvzishitcehaefguiozqlvazvogbmnxbinhowbrrfbslvvxlillvgbuhbrqohahqfwwrggkmpmeiwrunqkeagkitkbpxlmzhvtbuhaeieheozxvwfiewqnubwqovjkqlmjkituvjptpnymbmrqeazflvavplmnb
glueanumrmpumabrgisubfsfqtkbdznpisiagirmuxoekeredxhotezfzqtpjdzlwtgzuufetahvqospbwouvfeicsfzwrlfzqtpohdetfgioiagapmnuapmeiwruruasbnjmfcyojlwjquokxiqgpgvlrmfvmdqazirzvrzcwfwcmmfwpeaudxexnwbezadvdknudivtvwnbedliby
rvatadoaerdxovfgqfnrunrwzwzijrwwtzvemmwfwwfbuhxezsrzmiafmsiehickbpxavvhlbgyldeuhvqciagzhggkuikjdzczvhahqtktiouwaoztdviargjybuhoodruvmmawwfvnjiliagboxeruobrfclbhuilpruqtithinlrqkocedoeqawmrbeljatvqbeznfbiwavbhmur
znjvotfmfwqviylatpremsbjdgtwraxezvhvcmgkmrqpkkutgxzewswpeagdbeabpmongkmhqtktiouwaongkmfmfwqviydzebuhbriqlbiwadtnitduozhqoefuljibvrvsnyreezfkwwauhzbiypmdqplveagdtlasdahqbqahwjvvaonzzeagoqnovqliorqwuatdueanqlmcflk
atprvcmewaaubqoobuhzs
decryption:
perfectbalancebetweenarthistoryandculturetheextravaganzafeaturesextraordinarilybeautifulobjectsdisplayingthetribeshistorytheperformancesthatcomplementthesearworksofartinmotionwhilewhatmighthavebeenwarsinancient
timesarerecreatedasmockfightdramasandarehugecrowdpullerswithwarlogdrumsblazingshotgunsbackswordswithbevelsdaoandspearsperformersstagefullblownmockfightsdressedinwarriorcostumestheshapepatternandcarvingsontraditi
onalnagaweaponsdifferfromtribetotribemostoftheperformancesareaccompaniedbylivemusicandrhythmicwarcrieshighlightsorganisedbythegovernmentofnagalandtopromoteculturalheritageandencourageintertribalinteractionstheho
rnbillfestivalisthebestwaytoexperiencetherichcultureofthestatesomeofthehighlightsofthefestivalarethetraditionalnagamorungexhibitionsflowershowsherbalmedicinestallsfashionshowsnagawrestlingindigenousgamesandmusic
alconcertsamongothers
Cryptanalysis:
m: 5
MIC :  0.06261826585955376
 Key alphabet : i
MIC :  0.06423323699421966
 Key alphabet : n
MIC :  0.06614549132947978
 Key alphabet : d
MIC :  0.06291578034682081
 Key alphabet : i
MIC :  0.06533421965317919
 Key alphabet : a
Key by cryptanalysis: india

E:\SEM 6\NIS>
```

```
Cryptanalysis:
m: 5
MIC :  0.06261826589595376
 Key alphabet : i
MIC :  0.06423323699421966
 Key alphabet : n
MIC :  0.06614549132947978
 Key alphabet : d
MIC :  0.06291578034682081
 Key alphabet : i
MIC :  0.06533421965317919
 Key alphabet : a
Key by cryptanalysis: india

E:\SEM 6\NIS>
```