IT\_120\_Module 5\_Lab\_4

Exercise 1: Caesar Cipher

**Encryption**



**Decryption**



I have written python code for encryption and decryption using Caesar Cipher.

**Code:**

#Caesar Encrypt

def caesarEncrypt(realText, step):

outText = []

cryptText = []

uppercase = ['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

lowercase = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']

for eachLetter in realText:

if eachLetter in uppercase: #Uppercase encryption

index = uppercase.index(eachLetter)

crypting = (index + step) % 26

cryptText.append(crypting)

newLetter = uppercase[crypting]

outText.append(newLetter)

elif eachLetter in lowercase: #Lowercase encryption

index = lowercase.index(eachLetter)

crypting = (index + step) % 26

cryptText.append(crypting)

newLetter = lowercase[crypting]

outText.append(newLetter)

else:

outText += eachLetter

return outText

print("\ncaesarEncrypt")

code = caesarEncrypt("MATH", 4)

print()

print("Encrypted message =", code)

print()

code = caesarEncrypt("CRYPTO", 6)

print()

print("Encrypted message =", code)

print()

# The Decryption Function

def cipher\_decrypt(ciphertext, key):

decrypted = ""

for c in ciphertext:

if c.isupper():

c\_index = ord(c) - ord('A')

# shift the current character to left by key positions to get its original position

c\_og\_pos = (c\_index - key) % 26 + ord('A')

c\_og = chr(c\_og\_pos)

decrypted += c\_og

elif c.islower():

c\_index = ord(c) - ord('a')

c\_og\_pos = (c\_index - key) % 26 + ord('a')

c\_og = chr(c\_og\_pos)

decrypted += c\_og

elif c.isdigit():

# if it's a number,shift its actual value

c\_og = (int(c) - key) % 10

decrypted += str(c\_og)

else:

# if its neither alphabetical nor a number, just leave it like that

decrypted += c

return decrypted

ciphertext = "QIIX PEXIV"

decrypted\_msg = cipher\_decrypt(ciphertext, 4)

print("The cipher text:\n", ciphertext)

print("The decrypted message is:\n",decrypted\_msg)

ciphertext = "SKKZ NKXK"

decrypted\_msg = cipher\_decrypt(ciphertext, 6)

print("The cipher text:\n", ciphertext)

print("The decrypted message is:\n",decrypted\_msg)

**Code Output**

caesarEncrypt

Encrypted message = ['Q', 'E', 'X', 'L']

Encrypted message = ['I', 'X', 'E', 'V', 'Z', 'U']

The cipher text:

QIIX PEXIV

The decrypted message is:

MEET LATER

The cipher text:

SKKZ NKXK

The decrypted message is:

MEET HERE

**Questions**

1. Encrypt the message MATH with the Caesar cipher with 4 as the key.

QEXL

2. Encrypt the message CRYPTO with the Caesar cipher with 6 as the key.

IXEVZU

3. The message QIIX PEXIV was encrypted using the Caesar cipher with 4 as the key. Decrypt the message.

MEET LATER

4. The message SKKZ NKXK was encrypted using a Caesar cipher. Decrypt the message.

MEET HERE

Exercise 2: Vignere cipher `

Formula of encryption is,

Ei = (Pi + Ki) mod 26

Formula of decryption is,

Di = (Ei - Ki) mod 26

**Code:**

def shift\_dict(Caesar, Shift):

dic\_len = len(Caesar)

Shift = Shift % dic\_len

list\_dic = [(k,v) for k, v in iter(Caesar.items())]

Shifted = {

list\_dic[x][0]: list\_dic[(x - Shift) % dic\_len][1]

for x in range(dic\_len)

}

return Shifted

Viginere = {

"A":0,

"B":1,

"C":2,

"D":3,

"E":4,

"F":5,

"G":6,

"H":7,

"I":8,

"J":9,

"K":10,

"L":11,

"M":12,

"N":13,

"O":14,

"P":15,

"Q":16,

"R":17,

"S":18,

"T":19,

"U":20,

"V":21,

"W":22,

"X":23,

"Y":24,

"Z":25

}

VFU = {

0:"A",

1:"B",

2:"C",

3:"D",

4:"E",

5:"F",

6:"G",

7:"H",

8:"I",

9:"J",

10:"K",

11:"L",

12:"M",

13:"N",

14:"O",

15:"P",

16:"Q",

17:"R",

18:"S",

19:"T",

20:"U",

21:"V",

22:"W",

23:"X",

24:"Y",

25:"Z"

}

VFL = {

0:"a",

1:"b",

2:"c",

3:"d",

4:"e",

5:"f",

6:"g",

7:"h",

8:"i",

9:"j",

10:"k",

11:"l",

12:"m",

13:"n",

14:"o",

15:"p",

16:"q",

17:"r",

18:"s",

19:"t",

20:"u",

21:"v",

22:"w",

23:"x",

24:"y",

25:"z"

}

Asker = int(input("Do you want to... 1. Encode, or 2. Decode? "))

X = 0

Lister = []

Text = list(str(input("")))

Key = list(str(input("")).upper())

Z = 0

if Asker == 1:

for i in range(len(Text)):

Shift = Viginere[Key[(Z % len(Key))]]

if Text[X].isalpha():

LetterNum = Viginere[Text[X].upper()]

Helper = (LetterNum + Shift) % 26

if Text[X].isupper():

Lister.append(VFU[Helper])

else:

Lister.append(VFL[Helper])

else:

Lister.append(Text[X])

Z -= 1

X += 1

Z += 1

print(\*Lister, sep = "")

elif Asker == 2:

for i in range(len(Text)):

Shift = Viginere[Key[(Z % len(Key))]]

if Text[X].isalpha():

LetterNum = Viginere[Text[X].upper()]

Helper = (LetterNum - Shift) % 26

if Text[X].isupper():

Lister.append(VFU[Helper])

else:

Lister.append(VFL[Helper])

else:

Lister.append(Text[X])

Z -= 1

X += 1

Z += 1

print(\*Lister, sep = "")

1. Encrypt FOLLO WTHEY ELLOW BRICK ROAD with the keyword OZ.

TNZKC VHGSX SKZNK AFHQJ FNOC

2. Decrypt LOSVW AZBSH DHQID ARSLG EL, encrypted with the Vignere cipher using SHOES as a key

THERE IS NO PLACE LIKE HOME

Exercise 3: Breaking the Caesar Cipher

These ciphers are broken using the codes already listed above.

1. Decrypt the message encrypted with a Caesar cipher: PAXG LAHNEW B KXMNKG

WHEN SHOULD I RETURN

2. Decrypt the message encrypted with a Caesar cipher: QUCN ZIL U JBIHY WUFF

WAIT FOR A PHONE CALL

3. Decrypt the message encrypted with a Caesar cipher: GUR ENOOVG PENJYRQ BHG BS VGF UBYR

THE RABBIT CRAWLED OUT OF ITS HOLE

4. Decrypt the message encrypted with a Caesar cipher:

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHKTHESE ARENT THEDR OIDSY OUREL OOKIN GFOR

THESE ARENT THE DROIDS YOURE LOOKING FOR.

Exercise 4: Breaking the Vignere Cipher `

1. Decrypt the following message, which was encrypted with a Vignere cipher of length 4: `

BCRRBCQORHKEPSLSLCWRWXXDESPEZMPYQWCEBCBOSFHCIZHSQWVHCBRWRVLNEGDRCKRRQS.

DO OR DO NOT THERE IS NO TRY JUDGE ME BY SIZE DO YOU RECKLESS IS HE NOW THINGS ARE WORSE.

2. Decrypt the following message, which was encrypted with a Vignere cipher of length 4: `

KBPYU BACDM LRQNM GOMLG VETQV PXUQZ LRZNM GOMLG VETQV PXYIM HDYQL BQUBR

YILRJ MTEGW YDQWE GUPGC UABRY ILRJM XNQKA MHJXJ KMYGV ETQVP XCRWV FQNBL

EZXBW TBRAQ MUCAM FGAXY UWGMH TBEJB BRYIL RJMLC CAHLQ NWYTS GCUAB RYILR

JMLNT QGEQN AMRMB RYILR JMPGP BXPQN WCUXT GT

IT WAS THE BEST OF TIMES IT WAS THE WORST OF TIMES IT WAS THE AGE OF WISDOM IT WAS THE AGE OF FOOLISHNESS

IT WAS THE EPOCH OF BELIEF IT WAS THE EPOCH OF INCREDULITY IT WAS THE SEASON OF LIGHT IT WAS THE SEASON OF

DARKNESS, IT WAS THE SPRING OF HOPE IT WAS THE WINTER OF DESPAIR.

Exercise 5

Use what you know to decrypt the following message. Note, the original word spacing is intact:

LKZB RMLK X JFAKFDEQ AOBXOV TEFIB F MLKABOBA TBXH XKA TBXOV LSBO JXKV X NRXFKQ

XKA ZROFLRP SLIRJB LC CLODLQQBK ILOB TEFIB F KLAABA KBXOIV KXMMFKD PRAABKIV

QEBOB ZXJB X QXMMFKD XP LC PLJB LKB DBKQIV OXMMFKD OXMMFKD XQ JV ZEXJYBO

ALLO Q FP PLJB SFPFQBO F JRQQBOBA QXMMFKD XQ JV ZEXJYBO ALLO LKIV QEFP XKA KLQEFKD JLOB

Decrypted Using Caesar Decrypt and K=3

ONCE UPON A MIDNIGHT DREARY WHILE I PONDERED WEAK AND WEARY OVER MANY A QUAINT AND CURIOUS VOLUME OF FORGOTTEN LORE WHILE I NODDED NEARLY NAPPING SUDDENLY THERE CAME A TAPPING AS OF SOME ONE GENTLY RAPPING RAPPING AT MY CHAMBER DOOR T IS SOME VISITER I MUTTERED TAPPING AT MY CHAMBER DOOR ONLY THIS AND NOTHING MORE