**Practical 1**

**AIM: Implement Caesar cipher encryption-decryption.**

Caesar cipher is one of the simplest and oldest method of encrypting message.

It was developed by Julius Caesar to protect military communication.

This technique involves shifting the letter of alphabet by fix number. which is known as “Shift/Key”.

It’s simplest type of substitution Cipher. In which each letter of given text is replaced by a shift or key position alphabet.

**CODE:**

def caesar\_cipher\_encrypt(msg, shift):

ciphertext = ""

for char in msg:

if char.isalpha():

if char.isupper(): #Checks if the character is alphabetic

shifted\_char = chr((ord(char) - ord('A') + shift) % 26 + ord('A'))

else:

shifted\_char = chr((ord(char) - ord('a') + shift) % 26 + ord('a'))

ciphertext += shifted\_char

else:

ciphertext += char

return ciphertext

def caesar\_cipher\_decrypt(ciphertext, shift):

msg = ""

for char in ciphertext:

if char.isalpha():

if char.isupper():

shifted\_char = chr((ord(char) - ord('A') - shift) % 26 + ord('A'))

else:

shifted\_char = chr((ord(char) - ord('a') - shift) % 26 + ord('a'))

msg += shifted\_char

else:

msg += char

return msg

msg = input("Enter the message: ")

shift = int(input("Enter the shift value: "))

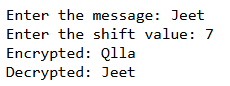
encrypted\_text = caesar\_cipher\_encrypt(msg, shift)

print("Encrypted:", encrypted\_text)

decrypted\_text = caesar\_cipher\_decrypt(encrypted\_text, shift)

print("Decrypted:", decrypted\_text)

**OUTPUT:**

****

**Practical 2**

**AIM: Implement Monoalphabetic cipher encryption-decryption.**

Monoalphabetic cipher is substitution technique in which a single alphabet is used for message.

It provides protection from brute force attack.

In Monoalphabetic cipher the mapping is done randomly not in uniform format.

**CODE:**

import numpy as np

import random

import string

def generate\_monoalphabetic\_key():

"""Generate a random Monoalphabetic cipher key."""

letters = list(string.ascii\_uppercase)

key = {}

for char in string.ascii\_uppercase:

random\_char = random.choice(letters)

key[char] = random\_char

letters.remove(random\_char) # Remove selected character to ensure unique mapping

return key

def encrypt\_monoalphabetic(message, key):

"""Encrypt a message using a Monoalphabetic cipher."""

encrypted\_message = []

capitalization\_info = []

for char in message:

if char.upper() in key:

encrypted\_char = key[char.upper()]

encrypted\_message.append(encrypted\_char)

capitalization\_info.append(char.isupper())

else:

encrypted\_message.append(char) # if character is not in the key, add it as-is

capitalization\_info.append(False) # mark as non-alphabetic or lowercase

return ''.join(encrypted\_message), capitalization\_info

def decrypt\_monoalphabetic(encrypted\_message, capitalization\_info, key):

"""Decrypt a message encrypted with a Monoalphabetic cipher."""

decrypted\_message = []

reverse\_key = {v: k for k, v in key.items()} # create reverse key for decryption

for i, char in enumerate(encrypted\_message):

if char.upper() in reverse\_key:

decrypted\_char = reverse\_key[char.upper()]

if capitalization\_info[i]:

decrypted\_char = decrypted\_char.upper()

else:

decrypted\_char = decrypted\_char.lower()

decrypted\_message.append(decrypted\_char)

else:

decrypted\_message.append(char) # if character is not in the key, add it as-is

return ''.join(decrypted\_message)

def analyze\_frequency(message):

"""Analyze the frequency of characters in a message."""

frequency = np.zeros((26,), dtype=int)

for char in message.upper():

if char.isalpha():

frequency[ord(char) - ord('A')] += 1

return frequency

# Generate a random Monoalphabetic key

key = generate\_monoalphabetic\_key()

print("Generated Monoalphabetic Key:")

print(key)

# Encrypt a message

message = input("Enter the message: ")

encrypted\_message, capitalization\_info = encrypt\_monoalphabetic(message, key)

print("Original Message:", message)

print("Encrypted Message:", encrypted\_message)

# Decrypt the message

decrypted\_message = decrypt\_monoalphabetic(encrypted\_message, capitalization\_info, key)

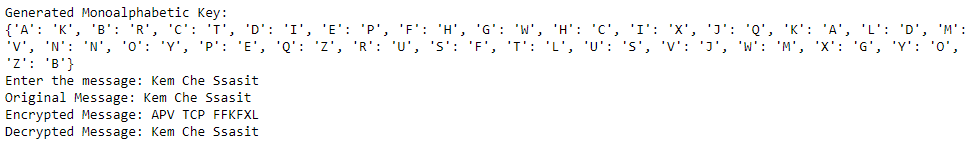
print("Decrypted Message:", decrypted\_message)

# Analyze the frequency of characters in the original and encrypted messages

original\_frequency = analyze\_frequency(message)

encrypted\_frequency = analyze\_frequency(encrypted\_message)

**OUTPUT:**



**Practical 3**

**AIM: Implement Playfair cipher encryption-decryption.**

Playfair cipher was invented by Charles Wheatstone. But later in 90’s lord playfair make it more useful and popular, so the name “Playfair cipher”.

It’s also substitution technique. Unlike a single alphabet substitution in encryption it replaces pair of alphabet.

**Encryption:**

**Steps:**

1) Generate a key square of 5x5 for encryption the plain text. In this table we have to omit any single character and consider as “J”.

2) Keep the alphabet in the key square unit. That no alphabet should be repeated. Place the key first in the key square and then remaining alphabet in order.

3) Encrypt the plain text. The plain text is split into pair of two letter called “Diagraph”.

* No alphabet remain single. It makes the plain text of even. Suppose any plain text has odd number then add any dummy letter.
* If any letter appears more than one time, then side by side then place any dummy letter to make it unique.
* If both the letter are in the same column take the letter below each one. If it’s bottom, then take it to top.
* If both the letter are in the same row take the letter to the immediate right of each one. If it’s at last position, then take it back to the first.
* If neither of the above rule is true form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

**Decryption:**

It is same as encryption but the steps are applied in reverse order.

**Steps:**

1) Split the plain text into diagraph.

2) Construct the 5x5 key matrix.

3) It will traverse the key matrix step by step and find the corresponding encipher for the pair.

**CODE:**

def generate\_key\_matrix(key):

key = key.upper().replace('J', 'I')

matrix = []

used = set()

# Add unique letters from the key

for char in key:

if char not in used and char.isalpha():

used.add(char)

matrix.append(char)

# Add remaining letters of the alphabet

for char in 'ABCDEFGHIKLMNOPQRSTUVWXYZ':

if char not in used:

used.add(char)

matrix.append(char)

# Convert to 5x5 matrix

return [matrix[i:i+5] for i in range(0, 25, 5)]

def print\_matrix(matrix):

for row in matrix:

print(' '.join(row))

print() # For better readability

def preprocess\_text(text):

text = text.upper().replace('J', 'I')

text = ''.join(filter(str.isalpha, text))

digraphs = []

i = 0

while i < len(text):

if i + 1 < len(text):

if text[i] == text[i + 1]:

digraphs.append(text[i] + 'X')

i += 1

else:

digraphs.append(text[i] + text[i + 1])

i += 2

else:

digraphs.append(text[i] + 'X')

i += 1

return digraphs

def find\_position(matrix, char):

for r, row in enumerate(matrix):

if char in row:

return (r, row.index(char))

return None

def encrypt\_digraph(matrix, digraph):

pos1 = find\_position(matrix, digraph[0])

pos2 = find\_position(matrix, digraph[1])

if pos1[0] == pos2[0]:

return matrix[pos1[0]][(pos1[1] + 1) % 5] + matrix[pos2[0]][(pos2[1] + 1) % 5]

elif pos1[1] == pos2[1]:

return matrix[(pos1[0] + 1) % 5][pos1[1]] + matrix[(pos2[0] + 1) % 5][pos2[1]]

else:

return matrix[pos1[0]][pos2[1]] + matrix[pos2[0]][pos1[1]]

def decrypt\_digraph(matrix, digraph):

pos1 = find\_position(matrix, digraph[0])

pos2 = find\_position(matrix, digraph[1])

if pos1[0] == pos2[0]:

return matrix[pos1[0]][(pos1[1] - 1) % 5] + matrix[pos2[0]][(pos2[1] - 1) % 5]

elif pos1[1] == pos2[1]:

return matrix[(pos1[0] - 1) % 5][pos1[1]] + matrix[(pos2[0] - 1) % 5][pos2[1]]

else:

return matrix[pos1[0]][pos2[1]] + matrix[pos2[0]][pos1[1]]

def playfair\_cipher(key, text, mode='encrypt'):

matrix = generate\_key\_matrix(key)

digraphs = preprocess\_text(text)

if mode == 'encrypt':

print("Key Matrix:")

print\_matrix(matrix)

process\_digraph = encrypt\_digraph

elif mode == 'decrypt':

process\_digraph = decrypt\_digraph

else:

raise ValueError("Mode must be 'encrypt' or 'decrypt'")

processed\_text = ''.join(process\_digraph(matrix, digraph) for digraph in digraphs)

return processed\_text

key = input("Enter the key: ")

plaintext = input("Enter the message: ")

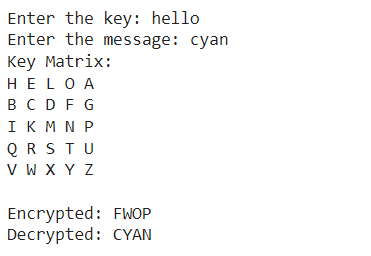
ciphertext = playfair\_cipher(key, plaintext, mode='encrypt')

print("Encrypted:", ciphertext)

decrypted\_text = playfair\_cipher(key, ciphertext, mode='decrypt')

print("Decrypted:", decrypted\_text)

**OUTPUT:**



**Practical 4**

**AIM: Implement hill cipher encryption-decryption.**

Hill cipher is polygraphic substitution cipher, based on linear algebra. This algorithm use matrix multiplication, and factorization.

**Encryption:**

**Step:**

1) Create the matrix of a key and convert that, into a numerical value.

2) Convert plain text into vector form and do the matrix multiplication.

3) Multiply the key matrix with each plain text vector and take the modulo of result, then concate the result to get the cipher text.

**CODE:**

import numpy as np

# Helper function to convert text to numbers and vice versa

def text\_to\_numbers(text):

return [ord(char) - ord('A') for char in text.upper()]

def numbers\_to\_text(numbers):

return ''.join(chr(num + ord('A')) for num in numbers)

# Encrypt function

def hill\_encrypt(plaintext, key\_matrix):

plaintext\_numbers = text\_to\_numbers(plaintext)

plaintext\_vector = np.array(plaintext\_numbers).reshape(-1, 5)

ciphertext\_vector = np.dot(plaintext\_vector, key\_matrix) % 26

ciphertext\_numbers = ciphertext\_vector.flatten()

return numbers\_to\_text(ciphertext\_numbers)

# Decrypt function

def hill\_decrypt(ciphertext, key\_matrix):

ciphertext\_numbers = text\_to\_numbers(ciphertext)

ciphertext\_vector = np.array(ciphertext\_numbers).reshape(-1, 5)

# Calculate inverse of the key matrix modulo 26

determinant = int(round(np.linalg.det(key\_matrix)))

determinant\_inv = pow(determinant, -1, 26)

key\_matrix\_inv = determinant\_inv \* np.round(determinant \* np.linalg.inv(key\_matrix)).astype(int) % 26

plaintext\_vector = np.dot(ciphertext\_vector, key\_matrix\_inv) % 26

plaintext\_numbers = plaintext\_vector.flatten()

return numbers\_to\_text(plaintext\_numbers)

# Function to input the 5x5 key matrix from user

def input\_key\_matrix():

print("Enter the 5x5 key matrix (each row separated by a space):")

matrix = []

for i in range(5):

row = list(map(int, input(f"Row {i+1}: ").strip().split()))

if len(row) != 5:

raise ValueError("Each row must have exactly 5 integers.")

matrix.append(row)

return np.array(matrix)

# Function to input the plaintext from user

def input\_plaintext():

plaintext = input("Enter the plaintext: ").upper().replace(" ", "")

if len(plaintext) % 5 != 0:

padding\_length = 5 - (len(plaintext) % 5)

plaintext += 'X' \* padding\_length

return plaintext

# Main function to execute the encryption and decryption

def main():

key\_matrix = input\_key\_matrix()

plaintext = input\_plaintext()

ciphertext = hill\_encrypt(plaintext, key\_matrix)

decrypted\_text = hill\_decrypt(ciphertext, key\_matrix)

print(f"\nPlaintext: {plaintext}")

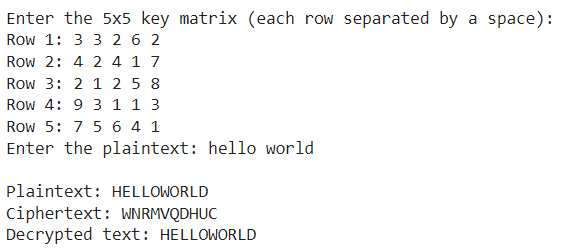
print(f"Ciphertext: {ciphertext}")

print(f"Decrypted text: {decrypted\_text}")

if \_\_name\_\_ == "\_\_main\_\_":

main()

**OUTPUT:**

****

**Practical 5**

**AIM: Implement polyalphabetic Cipher.**

Polyalphabetic cipher is a substitution alphabetic technique using multiple substitution alphabet. We can use more than one substitution for the same alphabet.

Encryption= Ei =(Pi+ki) mod 26

Decryption= Di = Ei-Ki

There are various technique to implement poly alphabetic. One of them is Vigenere . Which is Simplest and most popular method. Whenever a vigenere table is not given then it will be performed by formula given.

**CODE:**

def generate\_vigenere\_table():

"""Generate a Vigenère cipher table."""

table = []

for i in range(26):

row = [(chr((j + i) % 26 + ord('A'))) for j in range(26)]

table.append(row)

return table

def vigenere\_encrypt(plaintext, keyword):

"""Encrypt plaintext using the Vigenère cipher with the given keyword."""

table = generate\_vigenere\_table()

plaintext = plaintext.upper()

keyword = keyword.upper()

encrypted\_text = []

keyword\_length = len(keyword)

keyword\_index = 0

for char in plaintext:

if char.isalpha():

row = ord(keyword[keyword\_index]) - ord('A')

col = ord(char) - ord('A')

encrypted\_char = table[row][col]

encrypted\_text.append(encrypted\_char)

keyword\_index = (keyword\_index + 1) % keyword\_length

else:

encrypted\_text.append(char)

return ''.join(encrypted\_text)

def vigenere\_decrypt(ciphertext, keyword):

"""Decrypt ciphertext using the Vigenère cipher with the given keyword."""

table = generate\_vigenere\_table()

ciphertext = ciphertext.upper()

keyword = keyword.upper()

decrypted\_text = []

keyword\_length = len(keyword)

keyword\_index = 0

for char in ciphertext:

if char.isalpha():

row = ord(keyword[keyword\_index]) - ord('A')

col = table[row].index(char)

decrypted\_char = chr(col + ord('A'))

decrypted\_text.append(decrypted\_char)

keyword\_index = (keyword\_index + 1) % keyword\_length

else:

decrypted\_text.append(char)

return ''.join(decrypted\_text)

# Example usage

key = input("Key: ")

plaintext = input("Plaintext: ")

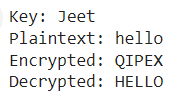
encrypted = vigenere\_encrypt(plaintext, key)

print("Encrypted:", encrypted)

decrypted = vigenere\_decrypt(encrypted, key)

print("Decrypted:", decrypted)

**OUTPUT:**

****