Rashtriya Raksha University

**School of Information Technology, Artificial Intelligence & Cyber Security (SITAICS)**

At- Lavad, Dahegam, Gandhinagar, Gujarat-382305

# Practical File

## (Introduction to Cryptography)

Name: Sarthak Sanay
Enrollment No: 230031101611051
Subject Name: Introduction to Cryptography
Subject Code: G4A19ITC
Program: B.Tech CSE (with specialization in Cyber Security)
Year: 2nd year (Semester-IV)

This is certifying that Mr. Sarthak Sanay has satisfactorily completed all experiments in the practical work prescribed by SITAICS in the ITC laboratory.

Dr. Ashish Revar
SUBJECT INCHARGE

# PRACTICAL - 5

## AIM: TO IMPLEMENT COLUMNAR CIPHER

## BRIEF :-

The Columnar Transposition Cipher is a way to hide a message by writing its letters into rows beneath a chosen keyword. You fill the grid row by row, adding extra filler characters at the end if needed so the last row is full. To make the ciphertext, you number the keyword's letters by their order in the alphabet and then read the letters down each numbered column in turn.

To decrypt, you rebuild the same grid shape using the keyword, fill in each column from the ciphertext in the right order, and then read the message off row by row, removing any filler. This simple reversal shows how the same steps in opposite order recover the original text. It's a straightforward manual method that anyone can work out with pen and paper.

Although the columnar cipher mixes up letters and hides obvious word patterns, it is still easy for modern programs to break. Attackers can try different key lengths or look for common words running down columns. Even so, it remains a useful teaching tool, demonstrating how moving letters (a transposition) can form the building blocks of more complex encryption systems.

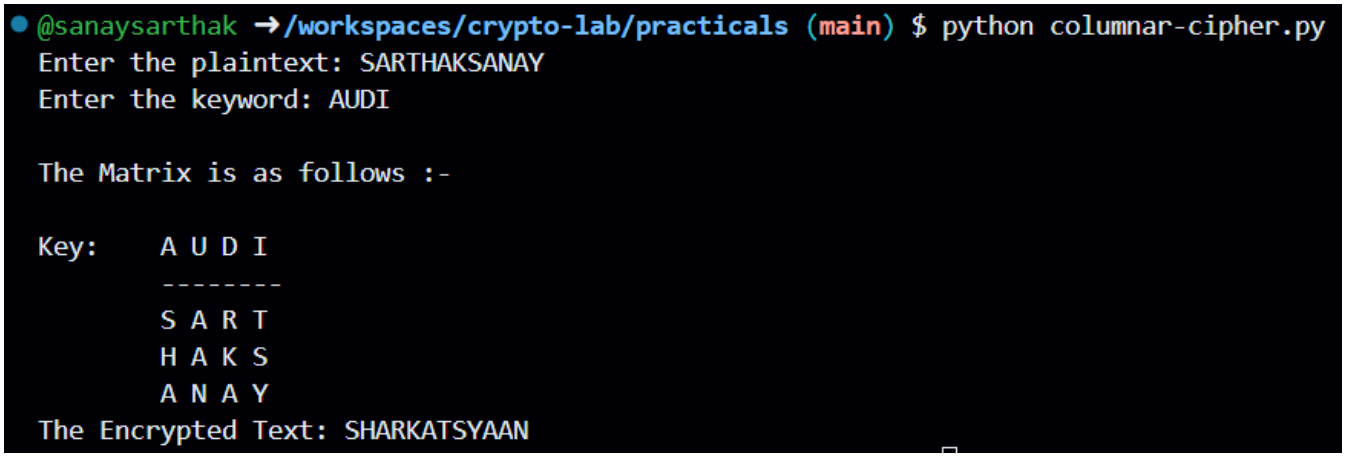
# ALGORITHM / PSEUDOCODE :-

```
repeat
    print menu
    read ch

    if ch == 1 then
        read plain_text
        read key

        text ← removeSpaces(plain_text)
        cols ← length(key)

        matrix ← EMPTY LIST
        for i from 0 to length(text)-1 step cols do
            append text[i..i+cols-1] as list to matrix
        end for

        print "The Matrix is as follows :-"
        print "Key:    " + join(key, " ")
        print "        " + repeat("-", 2 * cols)
        for each row in matrix do
            print "        " + join(row, " ")
        end for

        order ← getOrder(key)

        cipher_text ← ""
        for num from 1 to cols do
            colIndex ← indexOf(order, num)
            for each row in matrix do
                if colIndex < length(row) then
                    cipher_text ← cipher_text + row[colIndex]
                end if
            end for
        end for

        print "Encrypted Text: " + cipher_text

    else if ch == 0 then
        exit loop

    else
        print "Invalid choice"
    end if

until ch == 0
```

# CODE :-

```
# Program in Python to implement Columnar Cipher

def encrypt(text, key):
    text = text.replace(" ", "")
    cols = len(key)
    matrix = build_matrix(text, cols)
    print_matrix(matrix, key)

    order = get_order(key)
    cipher = ""

    for num in range(1, cols + 1):
        col = order.index(num)
        for row in matrix:
            if col < len(row):
                cipher += row[col]
    return cipher

def build_matrix(text, width):
    matrix = []
    for i in range(0, len(text), width):
        matrix.append(list(text[i:i+width]))
    return matrix

def print_matrix(matrix, key):
    print("\nThe Matrix is as follows :-\n")
    print("Key:   ", " ".join(key))
    print("        " + ('-' * (len(key)*2)))
    for row in matrix:
        print("       ", " ".join(row))

def get_order(key):
    order = []
    for i, ch in enumerate(key):
        count = 1
        for j in range(i):
            if key[j] <= ch:
                count += 1
            else:
                order[j] += 1
        order.append(count)
    return order

text = input("Enter the plaintext: ")
key = input("Enter the keyword: ")
result = encrypt(text, key)
print("The Encrypted Text:", result)
```

# OUTPUT :-


@sanaysarthak ➜/workspaces/crypto-lab/practicals (main) $ python columnar-cipher.py
Enter the plaintext: SARTHAKSANAY
Enter the keyword: AUDI
The Matrix is as follows :-
Key: A U D I
S A R T
H A K S
A N A Y
The Encrypted Text: SHARKATSYAAN