**Practical III**

**Roll No: 07 Date: 01/10/22**

**Aim: Cryptanalysis of Caesar Cipher**

**CODE**

package prac3;

import java.util.Scanner;

import java.util.Arrays;

\* @author Shubham Khedaskar

public class Prac3 {

/\*\*

\* @param args the command line arguments

\*/public static final String ALPHA = "abcdefghijklmnopqrstuvwxyz";

public static void main(String[] args) {

// TODO code application logic here

Scanner sc = new Scanner(System.in);

char[] alpha = {'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'};

System.out.println("Enter frequency character: ");

char freq = sc.next().charAt(0);

System.out.println("Enter cipher text: ");

String quote = sc.next();

quote = quote.toLowerCase().replaceAll("[^a-z]", "");

int[] frequencies = new int[26];

for (char c : quote.toCharArray()) {

frequencies[c - 'a'] = frequencies[c - 'a'] + 1;

}

System.out.println(Arrays.toString(frequencies));

int max = Integer.MIN\_VALUE;

int index = -1;

for(int i = 0; i < frequencies.length; i ++){

if(max < frequencies[i]){

max = frequencies[i];

index = i;

}

}

System.out.println(alpha[index]+" has maximum frequency");

int key = index - ALPHA.indexOf(freq);

System.out.println(key+" can be a shift key");

String decText = decrypt(quote, key);

System.out.println("Cryptanalysis of cipher text is : "+decText);

}

public static String decrypt(String message, int shiftKey) {

int i = 0;

char replaceVal = ' ';

message = message.toLowerCase();

String plainText = "";

for (int jj = 0; jj < message.length(); jj++) {

int charPosition = ALPHA.indexOf(message.charAt(jj));

int keyVal = ( charPosition - shiftKey) % 26;

if(keyVal < 0){

i = 26 - (-keyVal);

replaceVal = ALPHA.charAt(i);

} else{

replaceVal = ALPHA.charAt(keyVal);

}

plainText += replaceVal;

}

return plainText;

}

}

**OUTPUT**

Enter frequency character:

e

Enter cipher text:

usftwstwklewlzgvxgjlzwkqklweozauzusffglmkwsfqugehdauslwvugvafylwuzfaimwk

[4, 0, 0, 1, 3, 6, 5, 1, 1, 1, 5, 7, 2, 0, 1, 0, 2, 0, 5, 2, 7, 3, 9, 1, 1, 5]

w has maximum frequency

18 can be a shift key

Cryptanalysis of cipher text is : canbeabestmethodforthesystemwhichcannotuseanycomplicatedcodingtechniques

BUILD SUCCESSFUL (total time: 7 seconds)