|  |  |  |  |
| --- | --- | --- | --- |
| **Ex. No. 02** | **Frequency Analysis on Caesar Cipher** | | |
| Date of Exercise | 13 – 01 - 2015 | Date of Output Verification | 20 – 01 - 2015 |

**Question**

The following message was received by Rose, PHHW PH DIWHU WKH WRJD SDUWB. If the message is encrypted by using Caesar cipher. Find out the original plaintext using brute-force attack

**Procedure**

* Take the input from the user as a cipher text
* Analyze the input for each character, counting the repetitions of each character
* Now take the most repeating charterer and match with the statistical values
* Find the difference between them and di the shifting operations appropriately

**Program**

import java.util.Scanner;

import static javafx.application.Platform.exit;

public class NetworkSecurityLabExp2FrequencyAnalysisOnCaesarCipher {

public static int n, t = 0, max, op, sno, sp = 0;

public static Scanner in = new Scanner(System.in);

public static char stats[] = new char[]{'e', 't', 'a', 'o', 'i', 'n', 's', 'h', 'r', 'd', 'l', 'c', 'u', 'm', 'w', 'f', 'g', 'y', 'p', 'b', 'v', 'k', 'j', 'x', 'q', 'z'};

public static String ciphertext = "", output;

public static char[][] charcounts = new char[100][2];

public static void main(String[] args) {

System.out.println("Enter Cipher Text");

ciphertext = in.nextLine();

System.out.println(ciphertext);

n = ciphertext.length();

charcount();

charsort();

probabilities();

}

public static void charcount() {

t = 0;

for (int i = 0; i < n; i++) {

char a = ciphertext.charAt(i);

int p = 0;

for (int r = 0; r < t; r++) {

if (charcounts[r][0] == a && t != 0) {

charcounts[r][1] = (char) (charcounts[r][1] + 1);

p = 1;

}

if (a == ' ') {

p = 1;

}

}

if (p == 0) {

charcounts[t][0] = (char) (a);

charcounts[t][1] = '1';

t++;

}

}

System.out.println("\n--------Before Sort--------");

for (int i = 0; i < t; i++) {

System.out.print(charcounts[i][0] + " - " + charcounts[i][1] + "\n");

}

}

public static void charsort() {

char a0, a1;

for (int i = 0; i < t; i++) {

for (int j = 0; j < t; j++) {

if (charcounts[i][1] > charcounts[j][1]) {

a0 = charcounts[i][0];

a1 = charcounts[i][1];

charcounts[i][0] = charcounts[j][0];

charcounts[i][1] = charcounts[j][1];

charcounts[j][0] = a0;

charcounts[j][1] = a1;

}

}

}

max = charcounts[0][1];

System.out.println("\n---------After Sort--------");

for (int i = 0; i < t; i++) {

System.out.print(charcounts[i][0] + " - " + charcounts[i][1] + "\n");

}

}

public static void frequencymatch() {

System.out.println("\n\n\n-----Frequency Match " + (sp + 1) + "-----");

sno = stats[sp] - charcounts[0][0];

System.out.println("Differenece: " + sno);

if (sno < 0) {

op = 2;

sno = 0 - sno;

System.out.println("Shift Operation: Left");

} else {

op = 1;

System.out.println("Shift Operation: Right");

}

System.out.println("Shift Number: " + sno);

sp++;

}

public static void decode() {

System.out.println("\n--------Decode-------");

output = "";

if (op == 1) {

left();

} else if (op == 2) {

right();

}

System.out.println("Decoded Text: " + output);

}

public static void left() {

int j;

for (char i : ciphertext.toCharArray()) {

j = i;

if (Character.isLowerCase(i)) {

j = i - sno;

if (j < 97) {

j += 26;

}

}

if (Character.isUpperCase(i)) {

j = i - sno;

if (j < 65) {

j += 26;

}

}

output = output + (char) j;

}

}

public static void right() {

for (char i : ciphertext.toCharArray()) {

if (Character.isLowerCase(i)) {

output = output + (char) ((i - 97 + sno) % 26 + 97);

} else if (Character.isUpperCase(i)) {

output = output + (char) ((i - 65 + sno) % 26 + 65);

} else {

output = output + i;

}

}

}

public static void probabilities() {

int pr = 0;

do {

pr = 0;

frequencymatch();

decode();

System.out.println("\n----Verification-----\n1.Check The Next Possiility\n2.Exit");

pr = in.nextInt();

in.nextLine();

if (pr == 2) {

break;

}

} while (pr == 1);

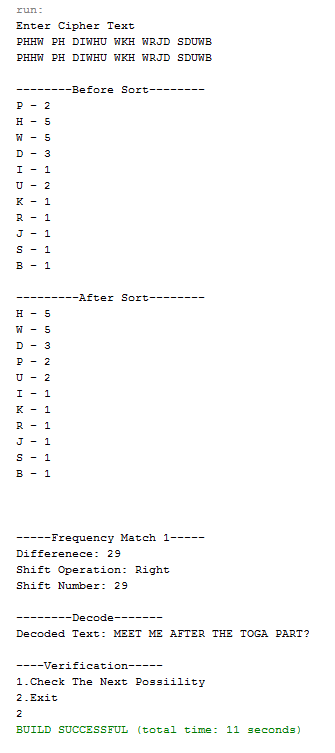
}

}

**Input**

PHHW PH DIWHU WKH WRJD SDUWB

**Output**



**Result**

The frequency analysis on Caesar cipher is successfully implemented.

[Signature of the Staff In-charge]

Name of the Staff In – charge: Mr. Manoj Kumar

Date: 20 – 01 - 2015