Experiment-12

**Date**-June 24, 2021.

**AIM-** Implementation of Data encryption and decryption (Program for Caesar Cipher and Generalized Caesar Cipher).

**THEORY-** Caesar Cipher is a mono-alphabetic cipher wherein each letter of the plaintext is substituted by another letter to form the ciphertext. It is a simplest form of substitution cipher scheme. This cryptosystem is generally referred to as the Shift Cipher. The concept is to replace each alphabet by another alphabet which is ‘shifted’ by some fixed number between 0 and 25.

For this type of scheme, both sender and receiver agree on a ‘secret shift number’ for shifting the alphabet. This number which is between 0 and 25 becomes the key of encryption. The name ‘Caesar Cipher’ is occasionally used to describe the Shift Cipher when the ‘shift of three’ is used.

**Process**

* In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift.
* The plaintext letter is then encrypted to the ciphertext letter on the sliding ruler underneath. The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext ‘tutorial’ is encrypted to the ciphertext ‘wxwruldo’. Here is the ciphertext alphabet for a Shift of 3 −



* On receiving the ciphertext, the receiver who also knows the secret shift, positions his sliding ruler underneath the ciphertext alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.
* He then replaces the ciphertext letter by the plaintext letter on the sliding ruler underneath. Hence the ciphertext ‘wxwruldo’ is decrypted to ‘tutorial’. To decrypt a message encoded with a Shift of 3, generate the plaintext alphabet using a shift of ‘-3’ as shown below −



* For decryption just follow the reverse of encryption process.

**PROGRAM (JAVA)-**

import java.util.Scanner;

public class CaesarCipher {

public static final String ALPHABET = "abcdefghijklmnopqrstuvwxyz";

public static String encrypt(String plainText, int shiftKey) {

plainText = plainText.toLowerCase();

String cipherText = "";

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

int charPosition = ALPHABET.indexOf(plainText.charAt(i));

int keyVal = (shiftKey + charPosition) % 26;

char replaceVal = ALPHABET.charAt(keyVal);

cipherText += replaceVal;

}

return cipherText;

}

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

cipherText = cipherText.toLowerCase();

String plainText = "";

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

int charPosition = ALPHABET.indexOf(cipherText.charAt(i));

int keyVal = (charPosition - shiftKey) % 26;

if (keyVal < 0)

keyVal = ALPHABET.length() + keyVal;

char replaceVal = ALPHABET.charAt(keyVal);

plainText += replaceVal;

}

return plainText;

}

public static void main(String[] args) {

Scanner sc = new Scanner(System.in);

System.out.print("Enter the String for Encryption : ");

String message = sc.next();

System.out.print("Enter the key : ");

int key = sc.nextInt();

String encrypted = encrypt(message, key);

String decrypted = decrypt(encrypted , key);

System.out.println("\nEncrypted msg : " + encrypted);

System.out.println("Decrypted msg : " + decrypted);

}

}

**OUTPUT-**

