***SAVEETHA SCHOOL OF ENGINEERING***

***SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCE***

**EXP NO 3: Encrypt and decrypt a message with Hill cipher substitution techniques**

**AIM**

To write a C program to Encrypt and decrypt a message with Hill cipher substitution techniques

**PROCEDURE**

* Download and install any c application.
* Choose a key matrix of size *n*×*n*, where *n* is an integer.
* Ensure that the determinant of the key matrix is relatively prime to 26
* Ensure that all calculations involving letters are modulo 26 to handle wrapping around the alphabet.
* Convert the resulting numerical values back to letters to get the ciphertext.
* Convert the resulting numerical values back to letters to get the original plaintext.

**PROGRAM**

#include <stdio.h>

#include <stdlib.h>

#include <string.h>

#include <math.h>

#define MAX 3

void encrypt(int cipherMatrix[MAX][MAX], int messageVector[MAX], int encryptedVector[MAX]) {

int i, j;

for (i = 0; i < MAX; i++) {

encryptedVector[i] = 0;

for (j = 0; j < MAX; j++) {

encryptedVector[i] += cipherMatrix[i][j] \* messageVector[j];

}

encryptedVector[i] %= 26;

}

}

void decrypt(int cipherMatrix[MAX][MAX], int encryptedVector[MAX], int decryptedVector[MAX]) {

int i, j;

int inverseMatrix[MAX][MAX] = {{6, 24, 1}, {13, 16, 10}, {20, 17, 15}};

for (i = 0; i < MAX; i++) {

decryptedVector[i] = 0;

for (j = 0; j < MAX; j++) {

decryptedVector[i] += inverseMatrix[i][j] \* encryptedVector[j];

}

decryptedVector[i] = (decryptedVector[i] + 26) % 26;

}

}

void convertStringToVector(char \*str, int \*vector) {

int i;

for (i = 0; i < MAX; i++) {

vector[i] = str[i] - 'a';

}

}

void convertVectorToString(int \*vector, char \*str) {

int i;

for (i = 0; i < MAX; i++) {

str[i] = vector[i] + 'a';

}

str[i] = '\0';

}

int main() {

int cipherMatrix[MAX][MAX] = {{6, 24, 1}, {13, 16, 10}, {20, 17, 15}};

char message[MAX + 1];

int messageVector[MAX], encryptedVector[MAX], decryptedVector[MAX];

printf("Enter a message (3 lowercase alphabets): ");

scanf("%s", message);

convertStringToVector(message, messageVector);

encrypt(cipherMatrix, messageVector, encryptedVector);

printf("Encrypted message: %s\n", message);

printf("Encrypted message in numbers: ");

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

printf("%d ", encryptedVector[i]);

}

printf("\n");

decrypt(cipherMatrix, encryptedVector, decryptedVector);

convertVectorToString(decryptedVector, message);

printf("Decrypted message: %s\n", message);

return 0;

}

**OUTPUT**

