# Cryptography---19CS412-classical-techqniques

# Name:SARWESHVARAN A

# Regno:212223230198

# Hill Cipher

Hill Cipher using with different key values

# AIM:

To develop a simple C program to implement Hill Cipher.

## DESIGN STEPS:

### Step 1:

Design of Hill Cipher algorithnm

### Step 2:

Implementation using C or pyhton code

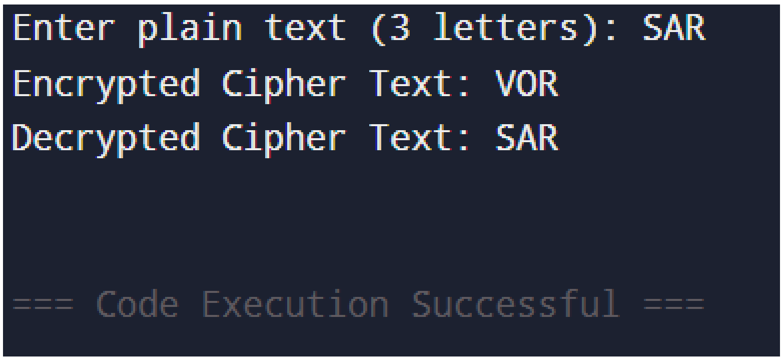
### Step 3:

Testing algorithm with different key values. ALGORITHM DESCRIPTION: The Hill cipher is a substitution cipher invented by Lester S. Hill in 1929. Each letter is represented by a number modulo 26. To encrypt a message, each block of n letters is multiplied by an invertible n × n matrix, again modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26). The cipher can, be adapted to an alphabet with any number of letters. All arithmetic just needs to be done modulo the number of letters instead of modulo 26.

## PROGRAM:

```
#include <stdio.h>

int key[3][3] = {
    {6, 24, 1},
    {13, 16, 10},
    {20, 17, 15}
};

int inverseKey[3][3] = {
    {8, 5, 10},
    {21, 8, 21},
    {21, 12, 8}
};

int main() {
    char msg[4];
    unsigned int enc[3] = {0}, dec[3] = {0};

    printf("Enter plain text (3 letters): ");
    scanf("%3s", msg);
    msg[3] = '\0';

    // Convert to uppercase
    for (int i = 0; i < 3; i++) {
        if (msg[i] >= 'a' && msg[i] <= 'z') {
            msg[i] -= 32;
        }
    }

    // Encryption
    for (int i = 0; i < 3; i++) {
        enc[i] = 0;
        for (int j = 0; j < 3; j++) {
            enc[i] += key[i][j] * (msg[j] - 'A');
        }
        enc[i] = enc[i] % 26;
    }

    printf("Encrypted Cipher Text: %c%c%c\n", enc[0] + 'A', enc[1] + 'A', enc[2] + 'A');

    // Decryption
    for (int i = 0; i < 3; i++) {
        dec[i] = 0;
        for (int j = 0; j < 3; j++) {
            dec[i] += inverseKey[i][j] * enc[j];
        }
        dec[i] = (dec[i] % 26 + 26) % 26;
    }

    printf("Decrypted Cipher Text: %c%c%c\n", dec[0] + 'A', dec[1] + 'A', dec[2] + 'A');

    return 0;
}
```

## OUTPUT:



```
Enter plain text (3 letters): SAR
Encrypted Cipher Text: VOR
Decrypted Cipher Text: SAR



=== Code Execution Successful ===
```

## RESULT:

The program is executed successfully