

EX NO:03

Encrypt and decrypt a message with Hill cipher substitution techniques.

DATE:21.02.24

**Aim:** To write a c program to encrypt and decrypt a message with Hill cipher substitution techniques.

**Algorithm:**

1. Include necessary header files (<stdio.h> and <string.h>).
2. Declare character arrays for the original message (msg), encryption key (key), new key (newKey), encrypted message (encryptedMsg), and decrypted message (decryptedMsg).
3. Declare integer variables msgLen, keyLen, i, and j for storing lengths and loop indices.
4. Initialize msg and key with the original message and encryption key.
5. Calculate msgLen and keyLen using strlen.
6. Use a loop to generate the new key (newKey) based on the original key (key).
7. Initialize i and j to 0.
8. Use a loop to iterate over each character in the original message (msg).
9. Combine it with the corresponding character from the new key (newKey) using modular arithmetic.
10. Add a null terminator at the end of the decrypted message.

**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;
}
```

## Input and Output:

The screenshot shows a C++ IDE with the following code in `hill_cipher.cpp`:

```
42 }
43 }
44 }
45
46 int main() {
47     int cipherMatrix[NAX][NAX] = {{6, 24, 1}, {13, 16, 10}, {20, 17, 15}};
48     char message[NAX + 1];
49     int messageVector[NAX], encryptedVector[NAX], decryptedVector[NAX];
50
51     printf("Enter a message (3 lowercase alphabets): ");
52     scanf("%s", message);
53
54     convertStringToVector(message, messageVector);
55
56     encrypt(cipherMatrix, messageVector, encryptedVector);
57
58     printf("Encrypted message: %s\n", message);
59     printf("Encrypted message in numbers: ");
60     for (int i = 0; i < NAX; i++) {
61         printf("%d ", encryptedVector[i]);
62     }
63     printf("\n");
64
65     decrypt(cipherMatrix, encryptedVector, decryptedVector);
66
67     convertVectorToString(decryptedVector, message);
68     printf("Decrypted message: %s\n", message);
69
70     return 0;
71 }
72
73 }
```

The terminal window shows the following output:

```
Enter a message (3 lowercase alphabets): key
Encrypted message: key
Encrypted message in numbers: 24 18 4
Decrypted message: lqo
.....
Process exited after 8.93 seconds with return value 0
Press any key to continue . . .
```

The compilation results at the bottom show:

```
-----
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\aiswarya\Desktop\hill_cipher 2.exe
- Output Size: 130,943,593,75 KiB
- Compilation Time: 0.50s
```

**Result:** A c program to encrypt and decrypt a message with Hill cipher substitution techniques is successfully executed.

**SAVEETHA SCHOOL OF ENGINEERING**

**SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES**