EX. NO: 1(E)

IMPLEMENTATION OF RAIL FENCE – ROW & COLUMN TRANSFORMATION TECHNIQUE

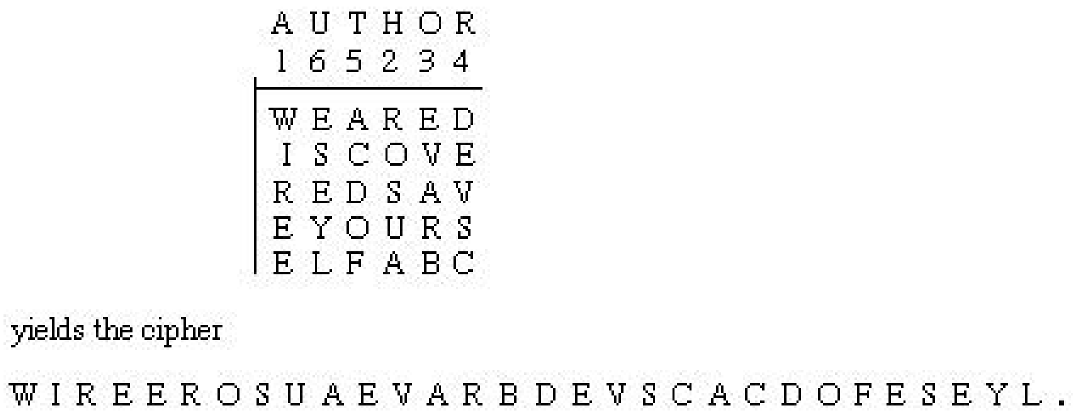
AIM:

To write a C program to implement the rail fence transposition technique.

DESCRIPTION:

In the rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.

EXAMPLE:



A	U	T	H	O	R
1	6	5	2	3	4
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	S	A	V
E	Y	O	U	R	S
E	L	F	A	B	C

yields the cipher

WIREEROSUAEVARBDEVSCACDOFESEYL.

ALGORITHM:

STEP-1: Read the Plain text.

STEP-2: Arrange the plain text in row columnar matrix format.

STEP-3: Now read the keyword depending on the number of columns of the plain text.

STEP-4: Arrange the characters of the keyword in sorted order and the corresponding columns of the plain text.

STEP-5: Read the characters row wise or column wise in the former order to get the cipher text.

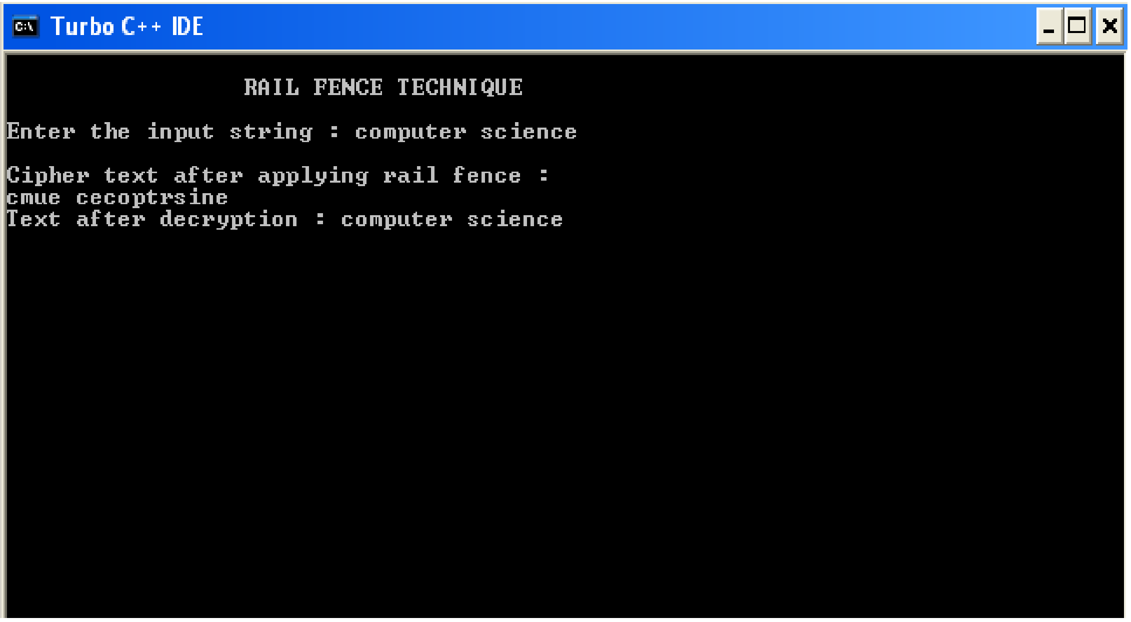
PROGRAM: (Rail Fence)

```
#include<stdio.h>
#include<conio.h>
#include<string.h>
void main()
{
     int i,j,k,l;
     char a[20],c[20],d[20];
     clrscr();
     printf("\n\t\t RAIL FENCE TECHNIQUE");
     printf("\n\nEnter the input string : ");
     gets(a);
     l=strlen(a);

/*Ciphering*/
for(i=0,j=0;i<l;i++)
{
     if(i%2==0)
     c[j++]=a[i];
}
for(i=0;i<l;i++)
{
     if(i%2==1)
     c[j++]=a[i];
}
c[j]='\0';
printf("\nCipher text after applying rail fence :");
printf("\n%s",c);

/*Deciphering*/
if(l%2==0)
     k=l/2;
else
     k=(l/2)+1;
for(i=0,j=0;i<k;i++)
{
    d[j]=c[i];
    j=j+2;
}
for(i=k,j=1;i<l;i++)
{
    d[j]=c[i];
    j=j+2;
}
d[l]='\0';
printf("\nText after decryption : ");
printf("%s",d);
getch();
}
```

OUTPUT:



```
                 RAIL FENCE TECHNIQUE
Enter the input string : computer science
Cipher text after applying rail fence :
cmue cecoptrsine
Text after decryption : computer science
```

VIVA QUESTIONS

1. Where do you apply PGP?
2. List out the basic tasks in Public Key Encryption in key distribution.
3. Give an example for Simple Hash Function.
4. List out the two methods of operations in Authentication Header (AH) and Encapsulating Security Payload (ESP).
5. Enumerate the functions provided by S/MIME.
6. List out the two ways in which password can be protected.
7. Which attack is related to integrity?
8. Which public key cryptosystem can be used for digital signature?
9. Expand: S/MIME.
10. What is the use of trusted system?

RESULT:

The rail fence algorithm had been executed successfully.