NAME: POOJA.S

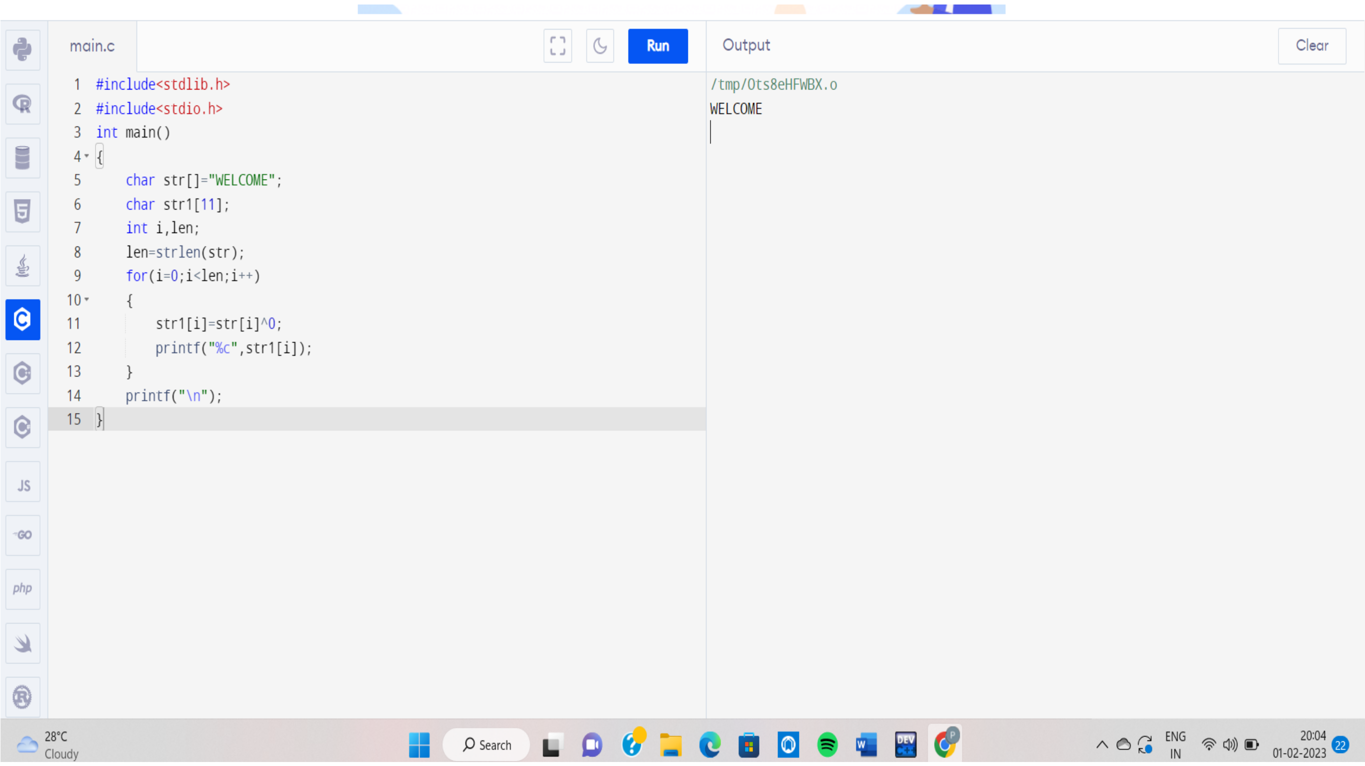
REG NO:192121001

COURSE CODE: CSA5166

COURSE NAME: CRYPTOGRAPHY AND NETWORK SECURITY WITH AUTHENTICATION SCHEMES

DAY-1

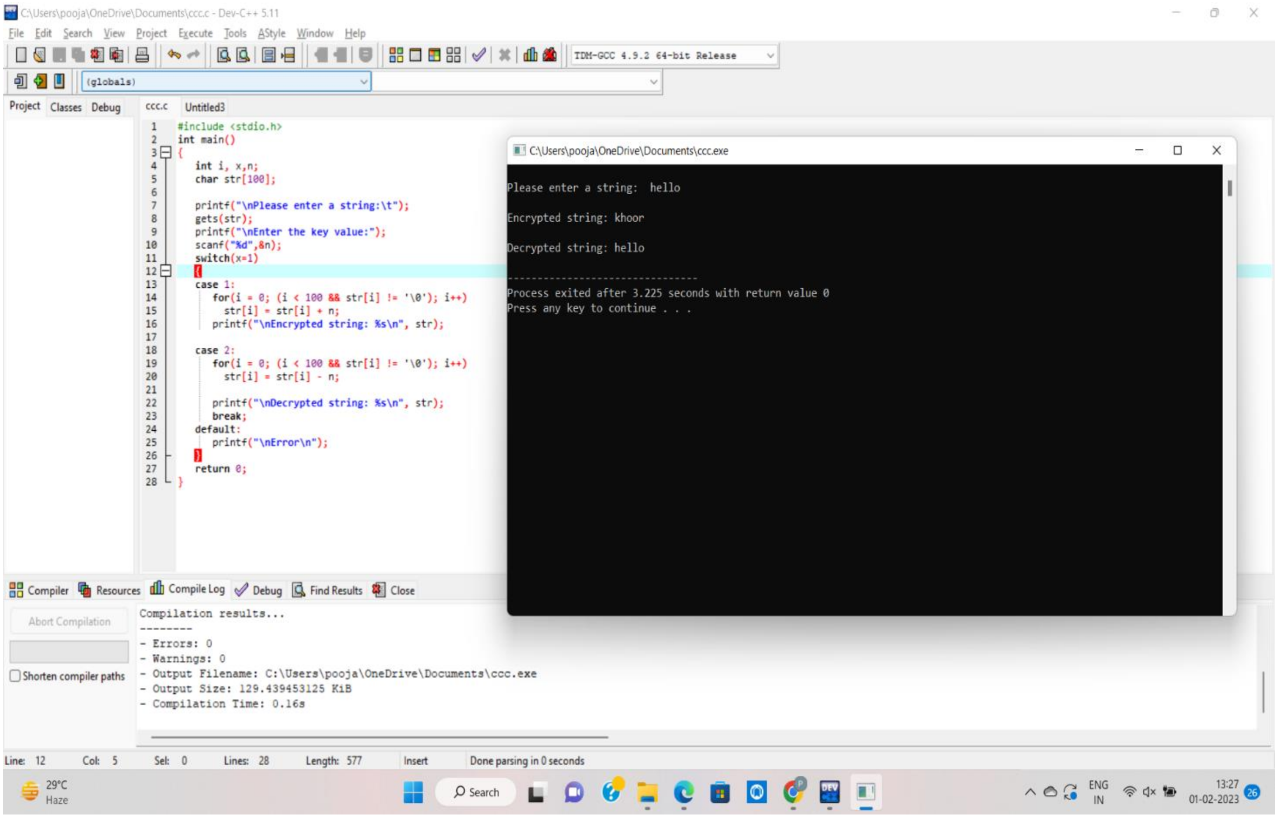
1. Write a C program that contains a string (char pointer)with a value\ “Hello world”. The program should XOR each character in this string with 0 and displays the result.



```c
#include<stdlib.h>
#include<stdio.h>
int main()
{
    char str[]="WELCOME";
    char str1[11];
    int i,len;
    len=strlen(str);
    for(i=0;i<len;i++)
    {
        str1[i]=str[i]^0;
        printf("%c",str1[i]);
    }
    printf("\n");
}
```

```
/tmp/Ots8eHFWBX.o
WELCOME
```

2. Write a C program for Caesar cipher involves replacing each letter of the alphabet with the letter stan places further down the alphabet, for k in the range 1 through 25.



C:\Users\pooja\OneDrive\Documents\ccc.c - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 4.9.2 64-bit Release
(globals)
Project Classes Debug
ccc.c Untitled3

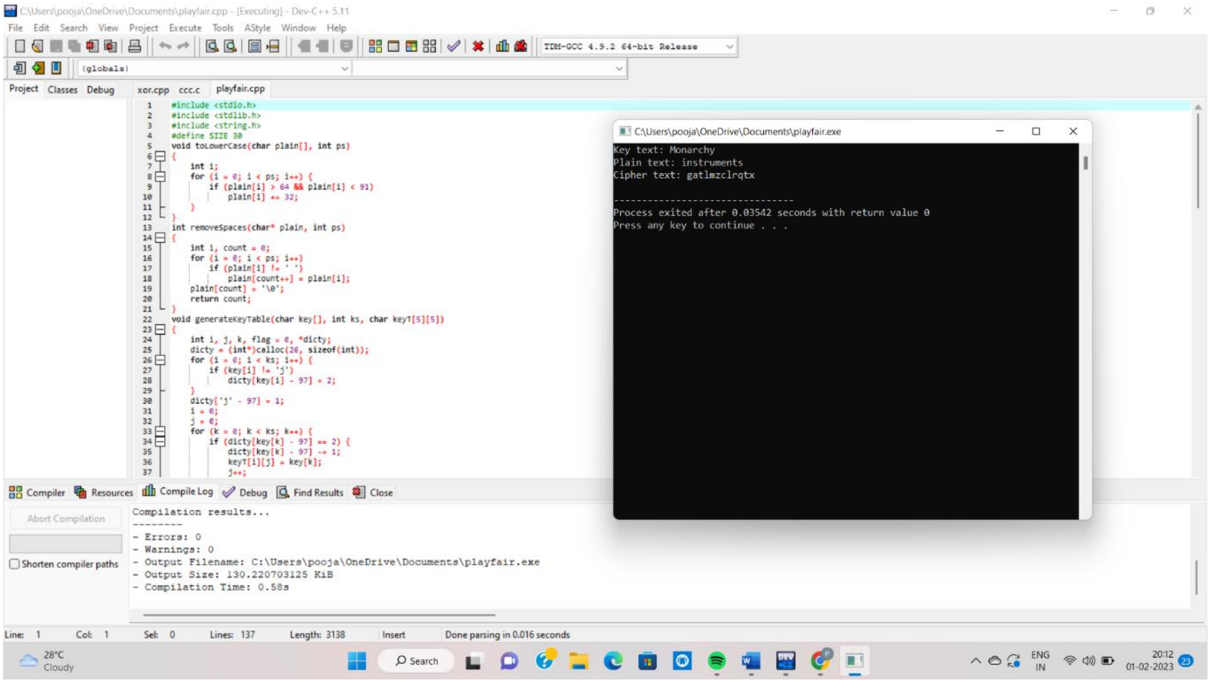
```c
#include <stdio.h>
int main()
{
   int i, x,n;
   char str[100];

   printf("\nPlease enter a string:\t");
   gets(str);
   printf("\nEnter the key value:");
   scanf("%d",&n);
   switch(x=1)
   {
   case 1:
      for(i = 0; (i < 100 && str[i] != '\0'); i++)
        str[i] = str[i] + n;
      printf("\nEncrypted string: %s\n", str);

   case 2:
      for(i = 0; (i < 100 && str[i] != '\0'); i++)
        str[i] = str[i] - n;

      printf("\nDecrypted string: %s\n", str);
      break;
   default:
      printf("\nError\n");
   }
   return 0;
}
```

C:\Users\pooja\OneDrive\Documents\ccc.exe

```
Please enter a string:  hello

Encrypted string: khoor

Decrypted string: hello

--------------------------------
Process exited after 3.225 seconds with return value 0
Press any key to continue . . .
```

```
Compilation results...
--------
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\pooja\OneDrive\Documents\ccc.exe
- Output Size: 129.439453125 KiB
- Compilation Time: 0.16s
```

3. Write a C program for Playfair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix.

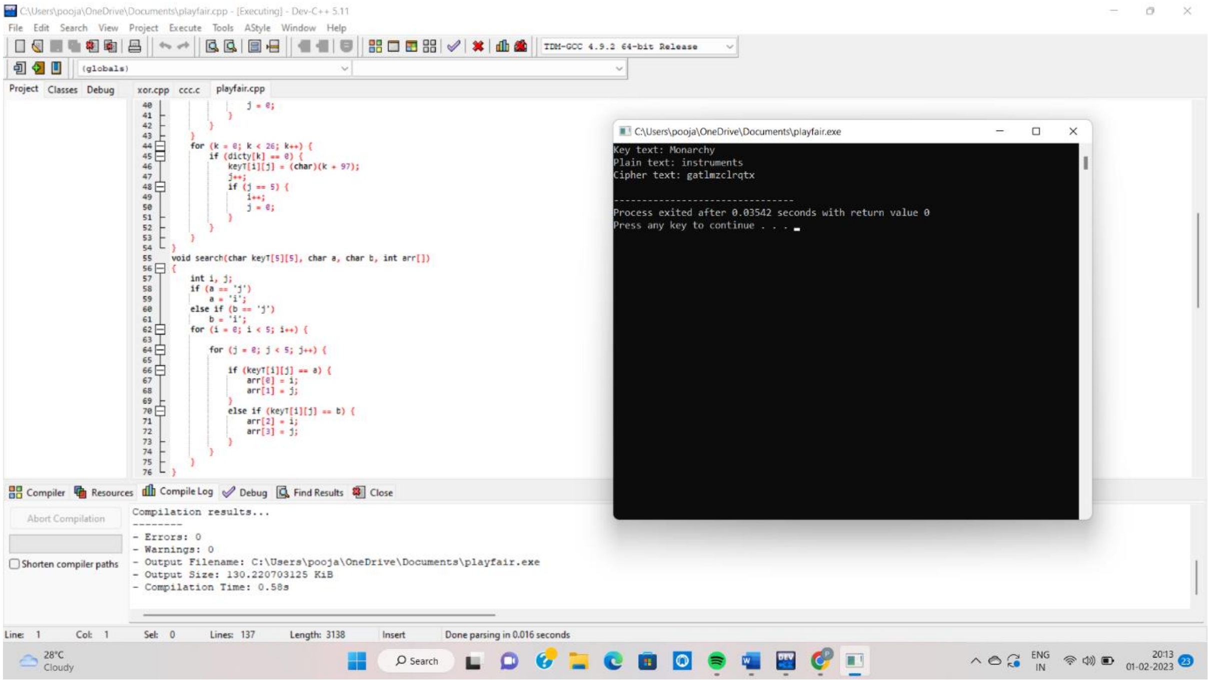


```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#define SIZE 30
void toLowerCase(char plain[], int ps)
{
    int i;
    for (i = 0; i < ps; i++) {
        if (plain[i] > 64 && plain[i] < 91)
            plain[i] += 32;
    }
}
int removeSpaces(char* plain, int ps)
{
    int i, count = 0;
    for (i = 0; i < ps; i++)
        if (plain[i] != ' ')
            plain[count++] = plain[i];
    plain[count] = '\0';
    return count;
}
void generateKeyTable(char key[], int ks, char keyT[5][5])
{
    int i, j, k, flag = 0, *dicty;
    dicty = (int*)calloc(26, sizeof(int));
    for (i = 0; i < ks; i++) {
        if (key[i] != 'j')
            dicty[key[i] - 97] = 2;
    }
    dicty['j' - 97] = 1;
    i = 0;
    j = 0;
    for (k = 0; k < ks; k++) {
        if (dicty[key[k] - 97] == 2) {
            dicty[key[k] - 97] -= 1;
            keyT[i][j] = key[k];
            j++;
```

```
Key text: Monarchy
Plain text: instruments
Cipher text: gatlmzclrqtx

--------------------------------
Process exited after 0.03542 seconds with return value 0
Press any key to continue . . .
```

```
Compilation results...
--------
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\pooja\OneDrive\Documents\playfair.exe
- Output Size: 130.220703125 KiB
- Compilation Time: 0.58s
```

C:\Users\pooja\OneDrive\Documents\playfair.cpp - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 4.9.2 64-bit Release
(globals)
Project Classes Debug
xor.cpp ccc.c playfair.cpp
C:\Users\pooja\OneDrive\Documents\playfair.exe
Compiler Resources Compile Log Debug Find Results Close
Abort Compilation
Shorten compiler paths
Line: 1 Col: 1 Sel: 0 Lines: 137 Length: 3138 Insert Done parsing in 0.016 seconds
28°C Cloudy
Search
ENG IN
20:12 01-02-2023

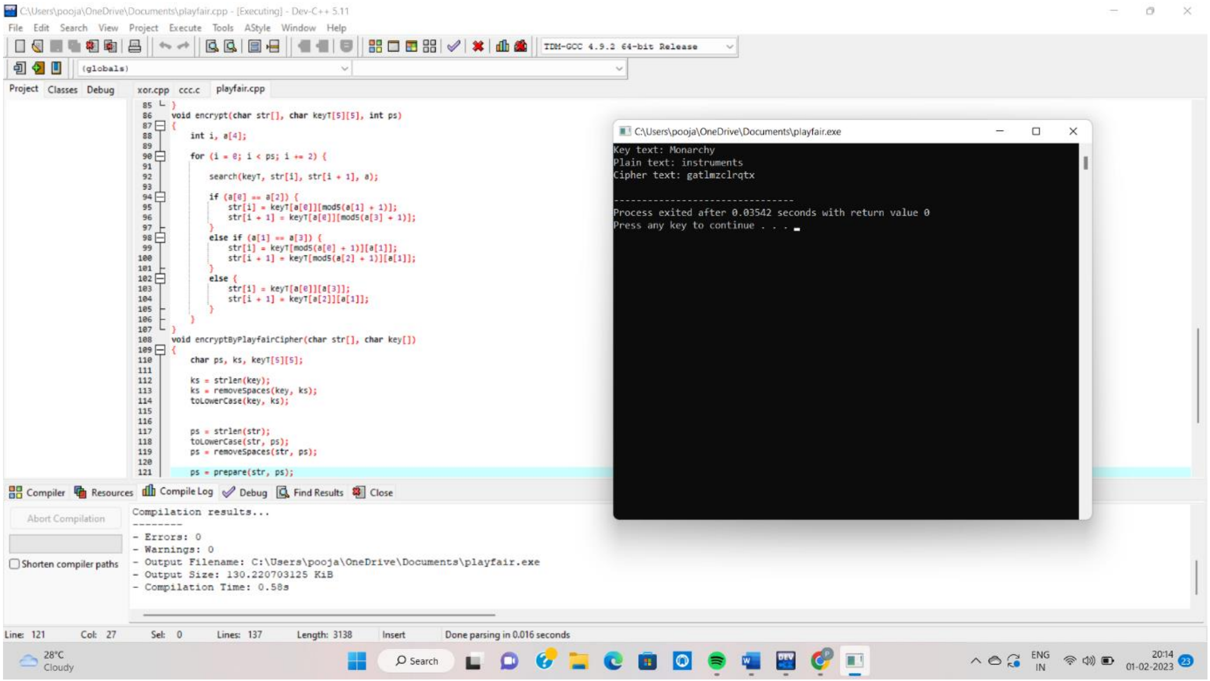


```
                j = 0;
            }
        }
    }
    for (k = 0; k < 26; k++) {
        if (dicty[k] == 0) {
            keyT[i][j] = (char)(k + 97);
            j++;
            if (j == 5) {
                i++;
                j = 0;
            }
        }
    }
}
void search(char keyT[5][5], char a, char b, int arr[])
{
    int i, j;
    if (a == 'j')
        a = 'i';
    else if (b == 'j')
        b = 'i';
    for (i = 0; i < 5; i++) {

        for (j = 0; j < 5; j++) {

            if (keyT[i][j] == a) {
                arr[0] = i;
                arr[1] = j;
            }
            else if (keyT[i][j] == b) {
                arr[2] = i;
                arr[3] = j;
            }
        }
    }
}
```

```
Key text: Monarchy
Plain text: instruments
Cipher text: gatlmzclrqtx

--------------------------------
Process exited after 0.03542 seconds with return value 0
Press any key to continue . . .
```

```
Compilation results...
--------
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\pooja\OneDrive\Documents\playfair.exe
- Output Size: 130.220703125 KiB
- Compilation Time: 0.58s
```

C:\Users\pooja\OneDrive\Documents\playfair.cpp - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 4.9.2 64-bit Release
(globals)
Project Classes Debug
xor.cpp ccc.c playfair.cpp
C:\Users\pooja\OneDrive\Documents\playfair.exe
Compiler Resources Compile Log Debug Find Results Close
Abort Compilation
Shorten compiler paths
Line: 1 Col: 1 Sel: 0 Lines: 137 Length: 3138 Insert Done parsing in 0.016 seconds
28°C Cloudy
Search
ENG IN
20:13 01-02-2023

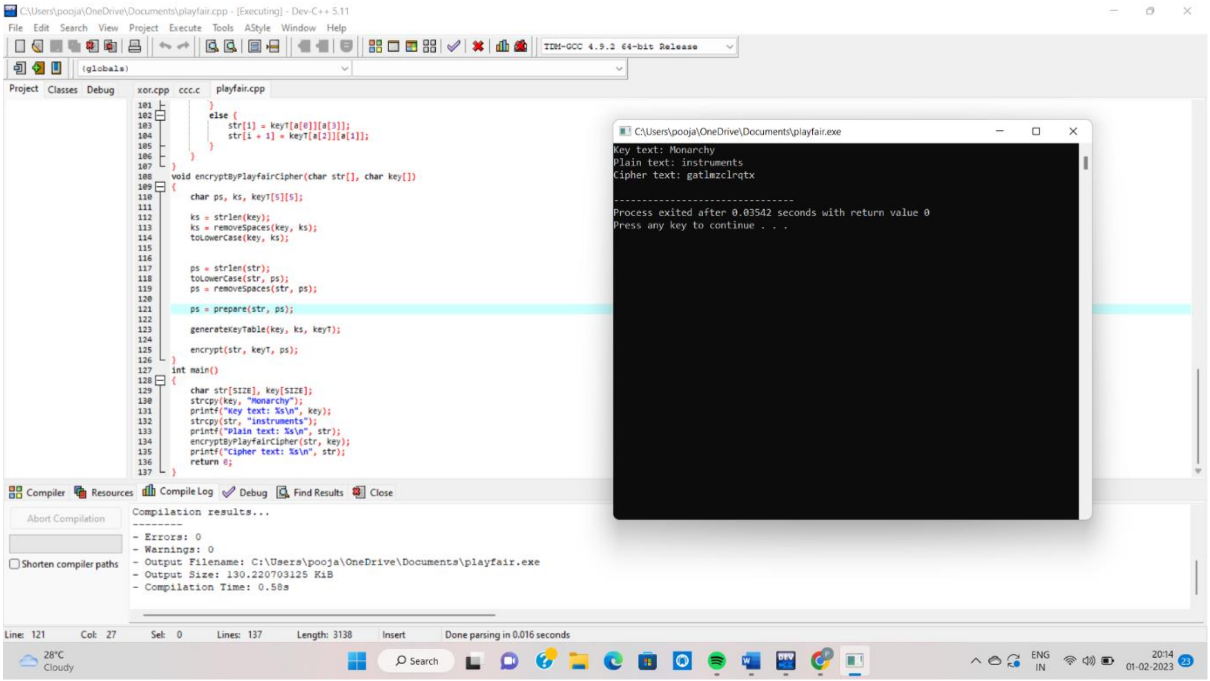

C:\Users\pooja\OneDrive\Documents\playfair.cpp - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 4.9.2 64-bit Release
(globals)
Project Classes Debug
xor.cpp ccc.c playfair.cpp
Compiler Resources Compile Log Debug Find Results Close
Abort Compilation
□ Shorten compiler paths
Line: 121 Col: 27 Sel: 0 Lines: 137 Length: 3138 Insert Done parsing in 0.016 seconds
28°C Cloudy
Search
ENG IN
20:14 01-02-2023

```
}
void encrypt(char str[], char keyT[5][5], int ps)
{
    int i, a[4];

    for (i = 0; i < ps; i += 2) {

        search(keyT, str[i], str[i + 1], a);

        if (a[0] == a[2]) {
            str[i] = keyT[a[0]][mod5(a[1] + 1)];
            str[i + 1] = keyT[a[0]][mod5(a[3] + 1)];
        }
        else if (a[1] == a[3]) {
            str[i] = keyT[mod5(a[0] + 1)][a[1]];
            str[i + 1] = keyT[mod5(a[2] + 1)][a[1]];
        }
        else {
            str[i] = keyT[a[0]][a[3]];
            str[i + 1] = keyT[a[2]][a[1]];
        }
    }
}
void encryptByPlayfairCipher(char str[], char key[])
{
    char ps, ks, keyT[5][5];

    ks = strlen(key);
    ks = removeSpaces(key, ks);
    toLowerCase(key, ks);


    ps = strlen(str);
    toLowerCase(str, ps);
    ps = removeSpaces(str, ps);

    ps = prepare(str, ps);
```

C:\Users\pooja\OneDrive\Documents\playfair.exe

```
Key text: Monarchy
Plain text: instruments
Cipher text: gatlmzclrqtx

--------------------------------
Process exited after 0.03542 seconds with return value 0
Press any key to continue . . .
```

```
Compilation results...
--------
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\pooja\OneDrive\Documents\playfair.exe
- Output Size: 130.220703125 KiB
- Compilation Time: 0.58s
```


C:\Users\pooja\OneDrive\Documents\playfair.cpp - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 4.9.2 64-bit Release
(globals)
Project Classes Debug
xor.cpp ccc.c playfair.cpp
Compiler Resources Compile Log Debug Find Results Close
Abort Compilation
□ Shorten compiler paths
Line: 121 Col: 27 Sel: 0 Lines: 137 Length: 3138 Insert Done parsing in 0.016 seconds
28°C Cloudy
Search
ENG IN
20:14 01-02-2023

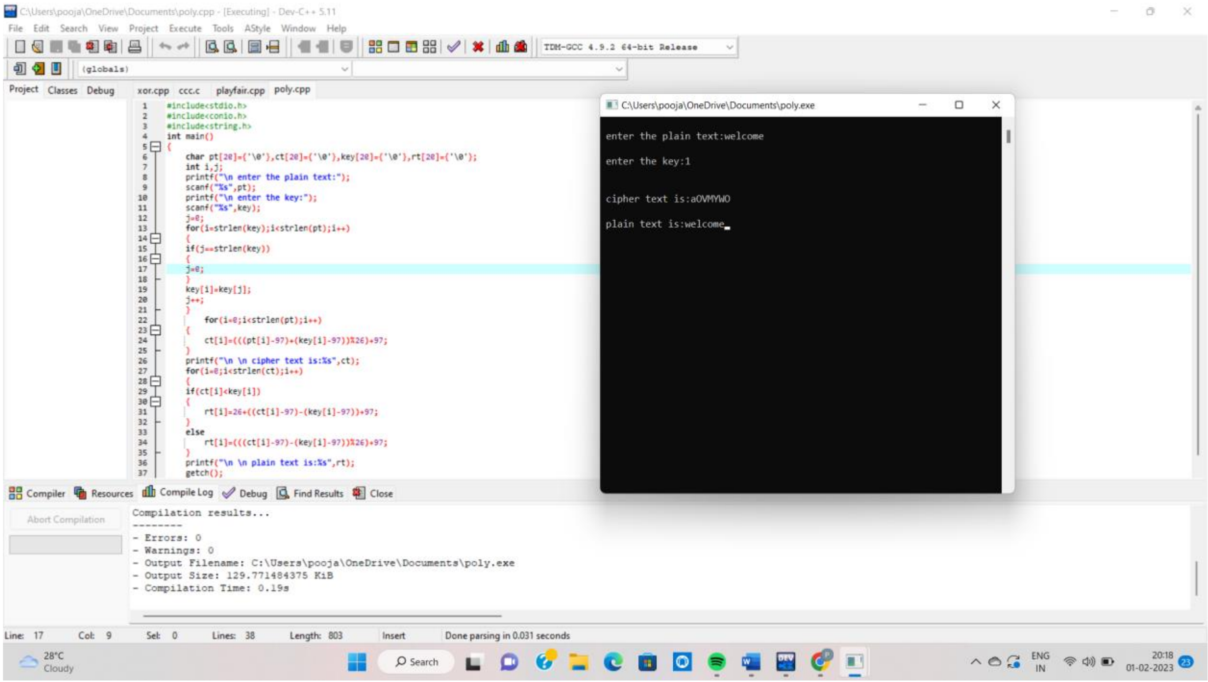
```
        }
        else {
            str[i] = keyT[a[0]][a[3]];
            str[i + 1] = keyT[a[2]][a[1]];
        }
    }
}
void encryptByPlayfairCipher(char str[], char key[])
{
    char ps, ks, keyT[5][5];

    ks = strlen(key);
    ks = removeSpaces(key, ks);
    toLowerCase(key, ks);


    ps = strlen(str);
    toLowerCase(str, ps);
    ps = removeSpaces(str, ps);

    ps = prepare(str, ps);

    generateKeyTable(key, ks, keyT);

    encrypt(str, keyT, ps);
}
int main()
{
    char str[SIZE], key[SIZE];
    strcpy(key, "Monarchy");
    printf("Key text: %s\n", key);
    strcpy(str, "instruments");
    printf("Plain text: %s\n", str);
    encryptByPlayfairCipher(str, key);
    printf("Cipher text: %s\n", str);
    return 0;
}
```

C:\Users\pooja\OneDrive\Documents\playfair.exe

```
Key text: Monarchy
Plain text: instruments
Cipher text: gatlmzclrqtx

--------------------------------
Process exited after 0.03542 seconds with return value 0
Press any key to continue . . .
```

```
Compilation results...
--------
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\pooja\OneDrive\Documents\playfair.exe
- Output Size: 130.220703125 KiB
- Compilation Time: 0.58s
```

4. Write a C program for polyalphabetic substitution cipher uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.


C:\Users\pooja\OneDrive\Documents\poly.cpp - [Executing] - Dev-C++ 5.11
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 4.9.2 64-bit Release
(globals)
Project Classes Debug
xor.cpp ccc.c playfair.cpp poly.cpp
C:\Users\pooja\OneDrive\Documents\poly.exe
Compiler Resources Compile Log Debug Find Results Close
Abort Compilation
Line: 17 Col: 9 Sel: 0 Lines: 38 Length: 803 Insert Done parsing in 0.031 seconds
28°C Cloudy
Search
ENG IN
20:18 01-02-2023

```c
#include<stdio.h>
#include<conio.h>
#include<string.h>
int main()
{
    char pt[20]={'\0'},ct[20]={'\0'},key[20]={'\0'},rt[20]={'\0'};
    int i,j;
    printf("\n enter the plain text:");
    scanf("%s",pt);
    printf("\n enter the key:");
    scanf("%s",key);
    j=0;
    for(i=strlen(key);i<strlen(pt);i++)
    {
    if(j==strlen(key))
    {
    j=0;
    }
    key[i]=key[j];
    j++;
    }
        for(i=0;i<strlen(pt);i++)
    {
        ct[i]=(((pt[i]-97)+(key[i]-97))%26)+97;
    }
    printf("\n \n cipher text is:%s",ct);
    for(i=0;i<strlen(ct);i++)
    {
    if(ct[i]<key[i])
    {
        rt[i]=26+((ct[i]-97)-(key[i]-97))+97;
    }
    else
        rt[i]=(((ct[i]-97)-(key[i]-97))%26)+97;
    }
    printf("\n \n plain text is:%s",rt);
    getch();
```

```
enter the plain text:welcome

enter the key:1


cipher text is:aOVMYWO

plain text is:welcome
```

```
Compilation results...
--------
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\pooja\OneDrive\Documents\poly.exe
- Output Size: 129.771484375 KiB
- Compilation Time: 0.19s
```