INFORMATION SECURITY

PRACTICAL FILE

AADITYA KEDIYAL

BSc(H) Computer Science

20201401

2. Implement the error detecting code

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\2.ErrorDetecting.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C

2.ErrorDetecting.cpp

```cpp
#include<iostream>

using namespace std;

int main() {
    int data[10];
    int dataatrec[10],c,c1,c2,c3,i;

    cout<<"Enter 4 bits of data one by one\n";
    cin>>data[0];
    cin>>data[1];
    cin>>data[2];
    cin>>data[4];

    //Calculation of even parity
    data[6]=data[0]^data[2]^data[4];
data[5]=data[0]^data[1]^data[4];
data[3]=data[0]^data[1]^data[2];

cout<<"\nEncoded data is\n";
for(i=0;i<7;i++)
        cout<<data[i];

cout<<"\n\nEnter received data bits one by one\n";
    for(i=0;i<7;i++)
        cin>>dataatrec[i];

    c1=dataatrec[6]^dataatrec[4]^dataatrec[2]^dataatrec[0];
c2=dataatrec[5]^dataatrec[4]^dataatrec[1]^dataatrec[0];
c3=dataatrec[3]^dataatrec[2]^dataatrec[1]^dataatrec[0];
c=c3*4+c2*2+c1 ;
```

Compiler Resources Compile Log Debug Find Results Console

Line: 1 Col: 1 Sel: 0 Lines: 59 Length: 1297 Insert Done parsing in 1.125 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\2.ErrorDetecting.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C

2.ErrorDetecting.cpp

```cpp

    c1=dataatrec[6]^dataatrec[4]^dataatrec[2]^dataatrec[0];
c2=dataatrec[5]^dataatrec[4]^dataatrec[1]^dataatrec[0];
c3=dataatrec[3]^dataatrec[2]^dataatrec[1]^dataatrec[0];
c=c3*4+c2*2+c1 ;

    if(c==0) {
cout<<"\nNo error while transmission of data\n";
    }
else {
cout<<"\nError on position "<<c;
cout<<"\nData sent : ";
for(i=0;i<7;i++)
        cout<<data[i];

cout<<"\nData received : ";
        for(i=0;i<7;i++)
        cout<<dataatrec[i];

cout<<"\nCorrect message is\n";

//if errorneous bit is 0 we complement it else vice versa
if(dataatrec[7-c]==0)
dataatrec[7-c]=1;
        else
dataatrec[7-c]=0;
for (i=0;i<7;i++) {
cout<<dataatrec[i];
}
}
return 0;
}
```

Compiler Resources Compile Log Debug Find Results Console

Line: 1 Col: 1 Sel: 0 Lines: 59 Length: 1297 Insert Done parsing in 1.125 seconds

OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\2.ErrorDetecting.exe

```
Enter 4 bits of data one by one
1
0
1
0

Encoded data is
1010010

Enter received data bits one by one
1
1
1
0
1
1
1

Error on position 4
Data sent : 1010010
Data received : 1110111
Correct message is
1111111
--------------------------------
Process exited after 27.22 seconds with return value 0
Press any key to continue . . .
```

3. Implement caeser cipher substitution operation.

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\3.CaesarCipher.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C

3.CaesarCipher.cpp

```cpp
#include<bits/stdc++.h>
using namespace std;
char str[100],str1[100];
void encrypt(int key)
{
    for(int i=0;i<strlen(str);i++)
    {
        if((int)str[i]+key>122)
        {
            str[i] = (char)((int)str[i]+key-26);
            continue;
        }
        else
            {str[i]=(char)((int)str[i]+key);}
    }
    cout<<"Encrypted String is : "<<endl;puts(str);
}
void decrypt(int key)
{
    for(int i=0;i<strlen(str);i++)
    {
        if((int)str[i]-key<97)  str1[i] = (char)((int)str[i]-key+26);
        else    str1[i]=(char)((int)str[i]-key);
    }
    cout<<"Key is : "<<key <<"\nDecrypted String is : ";puts(str1);
}
int main()
```

Compiler Resources Compile Log Debug Find Results Console Close

Abort Compilation

Shorten compiler patl

```
- Output Filename: D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\3.CaesarCipher.exe
- Output Size: 2.99188899993896 MiB
- Compilation Time: 3.00s
```

Line: 1 Col: 1 Sel: 0 Lines: 44 Length: 1017 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\3.CaesarCipher.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C

3.CaesarCipher.cpp

```cpp
{
    for(int i=0;i<strlen(str);i++)
    {
        if((int)str[i]-key<97)  str1[i] = (char)((int)str[i]-key+26);
        else    str1[i]=(char)((int)str[i]-key);
    }
    cout<<"Key is : "<<key <<"\nDecrypted String is : ";puts(str1);
}
int main()
{
    int key;
    cout<<"Enter String : "<<endl;
    gets(str);
    cout<<"Enter Key : "<<endl;
    cin >> key;
    encrypt(key);
    decrypt(key);
    cout<<"Attack starts : "<<endl;
    for(int i=0;i<26;i++)
        {
            decrypt(i);
        }
        cout<<endl<<"Made by: AADITYA KEDIYAL "<<endl;
        return 0;
}
```

Compiler Resources Compile Log Debug Find Results Console Close

Abort Compilation

Shorten compiler patl

```
- Output Filename: D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\3.CaesarCipher.exe
- Output Size: 2.99188899993896 MiB
- Compilation Time: 3.00s
```

Line: 1 Col: 1 Sel: 0 Lines: 44 Length: 1017 Insert Done parsing in 0.016 seconds

OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\3.CaesarCipher.exe

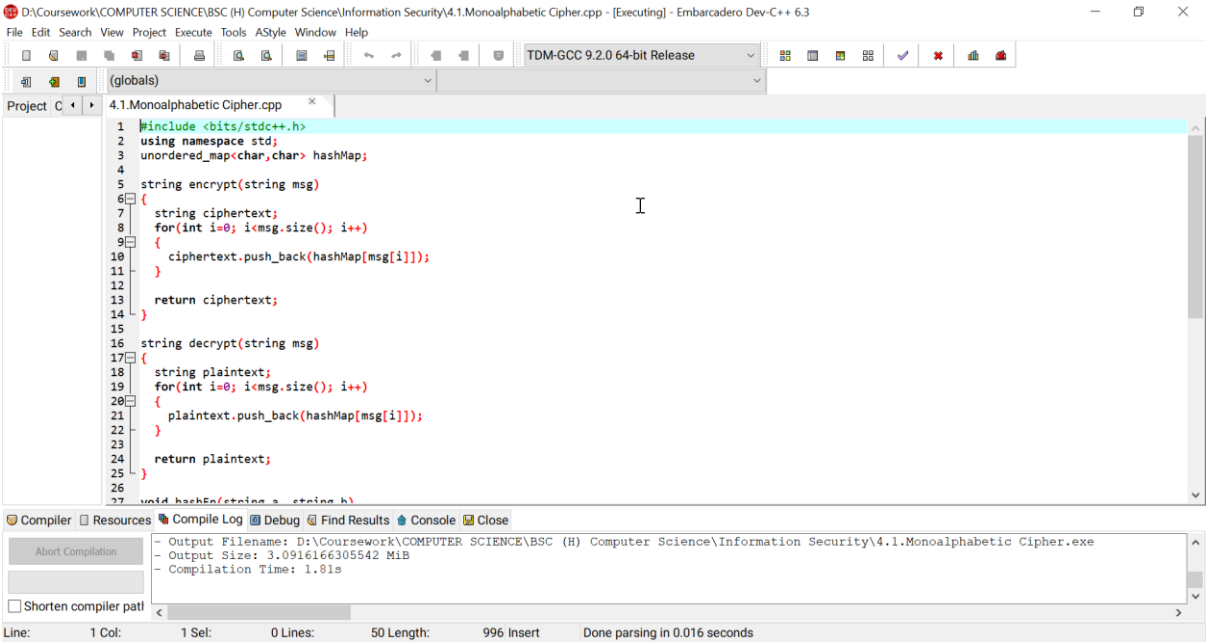
```
Enter String :
iamaadi
Enter Key :
4
Encrypted String is :
meqeehm
Key is : 4
Decrypted String is : iamaadi
Attack starts :
Key is : 0
Decrypted String is : meqeehm
Key is : 1
Decrypted String is : ldpddgl
Key is : 2
Decrypted String is : kcoccfk
Key is : 3
Decrypted String is : jbnbbej
Key is : 4
Decrypted String is : iamaadi
Key is : 5
Decrypted String is : hzlzzch
Key is : 6
Decrypted String is : gykyybg
Key is : 7
Decrypted String is : fxjxxaf
Key is : 8
Decrypted String is : ewiwwze
Key is : 9
Decrypted String is : dvhvvyd
Key is : 10
Decrypted String is : cuguuxc
Key is : 11
Decrypted String is : btfttwb
Key is : 12
Decrypted String is : asessva
Key is : 13
Decrypted String is : zrdrruz
Key is : 14
Decrypted String is : yqcqqty
Key is : 15
Decrypted String is : xpbppsx
```

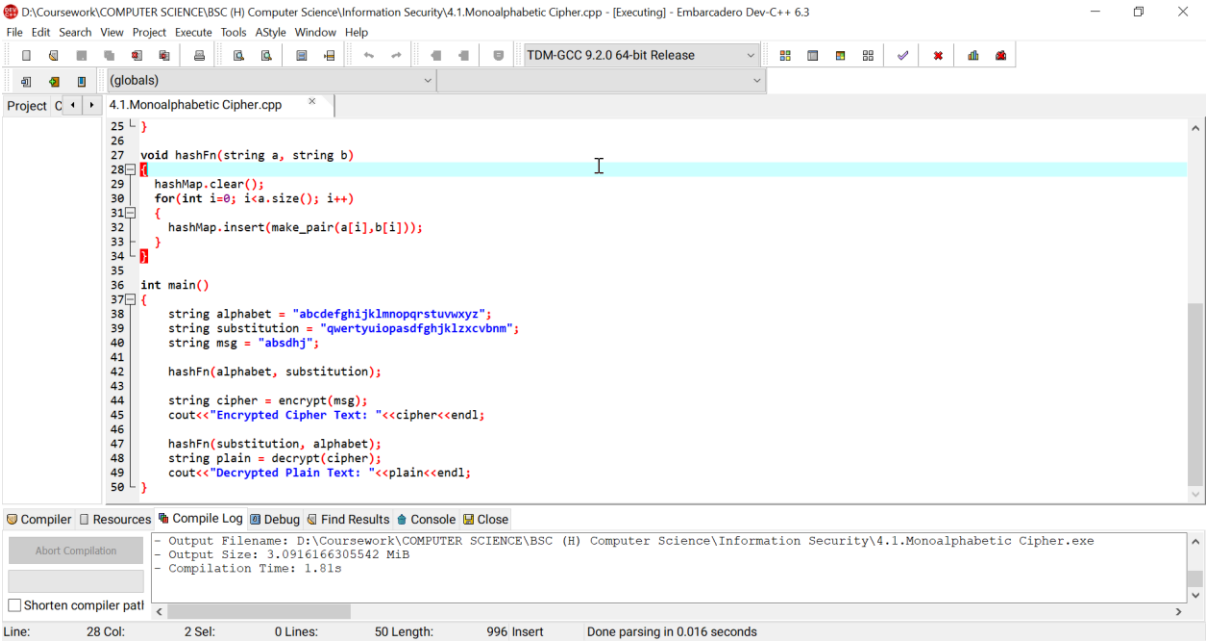
D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\3.CaesarCipher.exe

```
Decrypted String is : fxjxxaf
Key is : 8
Decrypted String is : ewiwwze
Key is : 9
Decrypted String is : dvhvvyd
Key is : 10
Decrypted String is : cuguuxc
Key is : 11
Decrypted String is : btfttwb
Key is : 12
Decrypted String is : asessva
Key is : 13
Decrypted String is : zrdrruz
Key is : 14
Decrypted String is : yqcqqty
Key is : 15
Decrypted String is : xpbppsx
Key is : 16
Decrypted String is : woaoorw
Key is : 17
Decrypted String is : vnznnqv
Key is : 18
Decrypted String is : umymmpu
Key is : 19
Decrypted String is : tlxllot
Key is : 20
Decrypted String is : skwkkns
Key is : 21
Decrypted String is : rjvjjmr
Key is : 22
Decrypted String is : qiuiilq
Key is : 23
Decrypted String is : phthhkp
Key is : 24
Decrypted String is : ogsggjo
Key is : 25
Decrypted String is : nfrffin

Made by: AADITYA KEDIYAL

--------------------------------
```

4.

4.1 . Implement monoalphabetic cipher substitution operation.





OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\4.1.Monoalphabetic Cipher.exe

```
Encrypted Cipher Text: qwlrip
Decrypted Plain Text: absdhj

--------------------------------
Process exited after 0.09004 seconds with return value 0
Press any key to continue . . .
```

4.2 Implement polyalphabetic cipher substitution operation

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\4.2.Polyaplhabetic Cipher.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 4.2.Polyaplhabetic Cipher.cpp

```cpp
#include <iostream>
#include <string>
using namespace std;
class Vig {
   public:
      string k;
   Vig(string k) {
      for (int i = 0; i < k.size(); ++i) {
         if (k[i] >= 'A' && k[i] <= 'Z')
            this->k += k[i];
         else if (k[i] >= 'a' && k[i] <= 'z')
            this->k += k[i] + 'A' - 'a';
      }
   }
   string encryption(string t) {
      string output;
      for (int i = 0, j = 0; i < t.length(); ++i) {
         char c = t[i];
         if (c >= 'a' && c <= 'z')
            c += 'A' - 'a';
         else if (c < 'A' || c > 'Z')
            continue;
         output += (c + k[j] - 2 * 'A') % 26 + 'A'; //added 'A' to bring it in range of ASCII alphabet [ 65-90 | A-Z ]
         j = (j + 1) % k.length();
      }
      return output;
```

Compiler | Resources | Compile Log | Debug | Find Results | Console | Close

Abort Compilation

Shorten compiler patl

```
- Output Filename: D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\4.1.Monoalphabetic Cipher.exe
- Output Size: 3.0916166305542 MiB
- Compilation Time: 1.81s
```

Line: 1 Col: 1 Sel: 0 Lines: 50 Length: 1567 Insert Done parsing in 0.015 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\4.2.Polyaplhabetic Cipher.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 4.2.Polyaplhabetic Cipher.cpp

```cpp
        }
        return output;
    }
    string decryption(string t) {
        string output;
        for (int i = 0, j = 0; i < t.length(); ++i) {
            char c = t[i];
            if (c >= 'a' && c <= 'z')
                c += 'A' - 'a';
            else if (c < 'A' || c > 'Z')
                continue;
            output += (c - k[j] + 26) % 26 + 'A';//added 'A' to bring it in range of ASCII alphabet [ 65-90 | A-Z ]
            j = (j + 1) % k.length();
        }
        return output;
    }
};
int main() {
    Vig v("WELCOME");
    string ori ="MyNameIsAadityaKediyal";
    string encrypt = v.encryption(ori);
    string decrypt = v.decryption(encrypt);
    cout << "Original Message: "<<ori<< endl;
    cout << "Encrypted Message: " << encrypt << endl;
    cout << "Decrypted Message: " << decrypt << endl;
}
```

Compiler | Resources | Compile Log | Debug | Find Results | Console | Close

Abort Compilation

Shorten compiler patl

```
- Output Filename: D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\4.1.Monoalphabetic Cipher.exe
- Output Size: 3.0916166305542 MiB
- Compilation Time: 1.81s
```

Line: 28 Col: 33 Sel: 0 Lines: 50 Length: 1567 Insert Done parsing in 0.015 seconds

OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\4.2.Polyaplhabetic Cipher.exe

```
Original Message: MyNameIsAadityaKediyal
Encrypted Message: ICYCAQMOELFWFCWOPFWKEH
Decrypted Message: MYNAMEISAADITYAKEDIYAL

--------------------------------
Process exited after 0.0804 seconds with return value 0
Press any key to continue . . .
```

5. Implement playfair cipher substitution operation.

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 5.Playfair.cpp | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamClpherTechnique.cpp

```cpp
#include<bits/stdc++.h>
using namespace std;

char grid[5][5]; // 5x5  matrix to encipher or decipher
char keyword[26]; // cypher key
char msg[100]; // message
int mark[130],len,r,c; // necessary variables

void createGrid();
void showGrid();
void encipher();
void decipher();
void menu()
{
    int n;
    string op[]={"1. Encipher","2. Decipher","3. Exit"};
    cout<<op[0]<<endl<<op[1]<<endl<<op[2]<<endl<<"Enter choice: ";
    cin>>n;
    if(n==1) encipher();
    else if(n==2) decipher();
    else {exit(1);}
}

int main()
{
    menu();
            cout<<endl<<"Made by: AADITYA KEDIYAL "<<endl;

    return 0;
}
void decipher()
{
    // initialize();
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 27 Col: 50 Sel: 0 Lines: 232 Length: 5536 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 5.Playfair.cpp | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamClpherTechnique.cpp

```cpp
    createGrid();
    showGrid();
    cout<<"Cypher text: ";
    char cypText[150]; // cypher text
    cin>>cypText;

    int l=strlen(cypText); //take length

    cout<<"Decipher text: ";
    //decipher starts
    int P,Q,R,S,f1,f2;
    char x,y;
    for(int i=0;i<l;i+=2)
    {
        x=cypText[i];
        y=cypText[i+1];
        f1=f2=0;
        for(int j=0;j<5;j++)
        {
            for(int k=0;k<5;k++)
            {
                if(x==grid[j][k])
                {
                    P=j;
                    Q=k;
                    f1=1;
                }
                if(y==grid[j][k])
                {
                    R=j;
                    S=k;
                    f2=1;
                }
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 27 Col: 50 Sel: 0 Lines: 232 Length: 5536 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 5.Playfair.cpp | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamClpherTechnique.cpp

```cpp
                }
                if(f1 && f2) break;
            }
            if(f1 && f2) break;
        }
        if(P==R) //same row
        {
            if(Q==0) cout<<grid[P][4];
            else cout<<grid[P][Q-1];
            if(S==0) cout<<grid[R][4];
            else cout<<grid[R][S-1];
        }
        else if(Q==S ) // same column
        {
            if(P==0) cout<<grid[4][Q];
            else cout<<grid[P-1][Q];
            if(R==0) cout<<grid[4][S];
            else cout<<grid[R-1][S];
        }
        else //opposite corner
        {
            cout<<grid[P][S]<<grid[R][Q];
        }
    }
    cout<<endl<<endl;
    menu();
}
void encipher()
{
    // initialize();
    createGrid();
    showGrid();
    cout<<"Message to cypher: ";
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 27 Col: 50 Sel: 0 Lines: 232 Length: 5536 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 5.Playfair.cpp | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamClpherTechnique.cpp

```cpp
    showGrid();
    cout<<"Message to cypher: ";
    gets(msg);
    int l=strlen(msg); // msg length
    char reqText[150]; //generate required text to encipher
    int in=0,j=0;
    for(int i=0;i<l;i++)
    {
        j=i+1;
        if(msg[i]==' ') //ignore all space from string
        {
            i++;
            j++;
        }
        if(msg[j]==' ') j++; //ignore space
        if(toupper(msg[i])=='J') msg[i]='i'; // ignore J
        if(toupper(msg[i])==toupper(msg[j])) // if duplicate add 'X' after the first letter
        {
            reqText[in]=toupper(msg[i]);
            reqText[in+1]='X';
            in++;
        }
        else
        {
            reqText[in]=toupper(msg[i]);
        }
        in++;
    }
    if(in%2!=0) reqText[in]='X'; // if one character left, add 'X' after it

    cout<<"Cypher text: ";
    //encipher starts
    int P,Q,R,S,f1,f2;
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 100 Col: 37 Sel: 0 Lines: 232 Length: 5536 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 5.Playfair.cpp | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamClpherTechnique.cpp

```cpp
    char x,y;
    for(int i=0;i<in;i+=2)
    {
        x=reqText[i];
        y=reqText[i+1];
        f1=f2=0;
        for(int j=0;j<5;j++)
        {
            for(int k=0;k<5;k++)
            {
                if(x==grid[j][k])
                {
                    P=j;
                    Q=k;
                    f1=1;
                }
                if(y==grid[j][k])
                {
                    R=j;
                    S=k;
                    f2=1;
                }
                if(f1 && f2) break;
            }
             if(f1 && f2) break;
        }
        if(P==R) //same row
        {
            if(Q==4) cout<<grid[P][0];
            else cout<<grid[P][Q+1];
            if(S==4) cout<<grid[R][0];
            else cout<<grid[R][S+1];
        }
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 100 Col: 37 Sel: 0 Lines: 232 Length: 5536 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 5.Playfair.cpp | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamClpherTechnique.cpp

```cpp
        {
            cout<<grid[P][S]<<grid[R][Q];
        }
    }
    cout<<endl<<endl;
    menu();
}
void createGrid()
{
    cout<<"Keyword: ";
    cin>>keyword; // key of the cypher
    getchar();
    len=strlen(keyword);  // size of input string O(n) :3
    mark['J']=1; // ignore J
    r=0,c=0; //initialize row and column

    // first populate the keyword
    for(int i=0;i<len;i++)
    {
        if(!mark[toupper(keyword[i])]) // ignore duplicates
        {
            mark[toupper(keyword[i])]=1;
            grid[r][c++]=toupper(keyword[i]);
            if(c%5==0) //increase row column
            {
                c=0;
                r++;
            }
        }
    }

    // complete rest of the matrix from unused characters starting from A
    for(int i='A';i<='Z';i++)
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 100 Col: 37 Sel: 0 Lines: 232 Length: 5536 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 5.Playfair.cpp | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp

```cpp
    // complete rest of the matrix from unused characters starting from A
    for(int i='A';i<='Z';i++)
    {
        if(mark[i]==0) // taking values that are not in the matrix already
        {
            grid[r][c++]=i;
            mark[i]=1;
            if(c%5==0)
            {
                if(r==4 && c==5) break; //matrix populated

                // else increase row column
                r++;
                c=0;
            }
        }
    }
}
void showGrid()
{
    cout<<"5x5 Matrix"<<endl;

    for(int i=0;i<5;i++)
    {
        for(int j=0;j<5;j++)
        {
            cout<<grid[i][j]<<" ";
        }
        cout<<endl;
    }
}
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 204 Col: 6 Sel: 0 Lines: 232 Length: 5536 Insert Done parsing in 0.016 seconds

OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.exe

```
3. Exit
Enter choice: 1
Keyword: aadi
5x5 Matrix
A D I B C
E F G H K
L M N O P
Q R S T U
V W X Y Z
Message to cypher: iamaadi
Cypher text: BDLDVIIB

1. Encipher
2. Decipher
3. Exit
Enter choice: 2
Keyword: aadi
5x5 Matrix
A D I B C
E F G H K
L M N O P
Q R S T U
V W X Y Z
Cypher text: BDLDVIIB
Decipher text: IAMAXADI

1. Encipher
2. Decipher
3. Exit
Enter choice:
```

6. Implement hill cipher substitution operation

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\6.HillCipher.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp | 6.HillCipher.cpp

```cpp
#include<iostream>
#include<cmath>
using namespace std;
float encrypt[3][2], decrypt[3][2], a[3][3], b[3][3],
mes[3][2], c[3][3];
void encryption(); //encrypts the message
void decryption(); //decrypts the message
void getKeyMessage(); //gets key and message from user
void inverse(); //finds inverse of key matrix
int main()
{
 getKeyMessage();
 encryption();
 decryption();
        cout<<endl<<"Made by: AADITYA KEDIYAL "<<endl;

 return 0;
}
void encryption()
{
 int i, j, k;
 for(i = 0; i < 3; i++)
 for(j = 0; j < 2; j++)
 for(k = 0; k < 3; k++)
 encrypt[i][j] = encrypt[i][j] + a[i][k] *
 mes[k][j];
 cout << "\nEncrypted string is : ";
 for(i = 0; i < 3; i++)
 for(j = 0; j<2; j++)
 cout << (char)(fmod(encrypt[i][j], 26) + 97);
}
void decryption()
{
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 4 Col: 54 Sel: 0 Lines: 105 Length: 2177 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\6.HillCipher.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp | 6.HillCipher.cpp

```cpp
{
 int i, j, k;
 inverse();
 for(i = 0; i < 3; i++)
 for(j = 0; j < 2; j++)
 for(k = 0; k < 3; k++)
 decrypt[i][j] = decrypt[i][j] + b[i][k] *
 encrypt[k][j];
 cout << "\nDecrypted string is : ";
 for(i = 0; i < 3; i++)
 for(j = 0; j<2; j++)
 cout << (char)(fmod(decrypt[i][j], 26) + 97);
 cout << "\n";
}
void getKeyMessage()
{
 int i, j;
 char msg[6], y;
 cout << "Enter 9 letter string for key : ";
 for(i = 0; i < 3; i++)
 for(j = 0; j < 3; j++)
 {
    cin >> y;
    a[i][j] = y - 'a';
    c[i][j] = a[i][j];
 }
 cout << "\nEnter a 6 letter message: ";
 cin >> msg;
 for(i = 0; i < 3; i++)
    for(j = 0; j<2; j++)
        mes[i][j] = msg[i*2 + j] - 97;
}
void inverse()
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 4 Col: 54 Sel: 0 Lines: 105 Length: 2177 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\6.HillCipher.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp | 6.HillCipher.cpp

```cpp
            if(i == j)
               b[i][j] = 1;
            else
               b[i][j] = 0;
         }
   for(k = 0; k < 3; k++)
   {
      for(i = 0; i < 3; i++)
   {
   p = c[i][k];
   q = c[k][k];
   for(j = 0; j < 3; j++)
   {
   if(i != k)
   {
   c[i][j] = c[i][j] * q - p * c[k][j];
   b[i][j] = b[i][j] * q - p * b[k][j];
   }
   }
   }
   }
   for(i = 0; i < 3; i++)
      for(j = 0; j < 3; j++)
         b[i][j] = ceil((b[i][j] / c[i][i])*10000)/10000.0;

   cout << "\n\nInverse Matrix is:\n";
   for(i = 0; i < 3; i++)
   {
   for(j = 0; j < 3; j++)
   cout << b[i][j] << "\t";
   cout << "\n";
   }
}
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 4 Col: 54 Sel: 0 Lines: 105 Length: 2177 Insert Done parsing in 0.016 seconds

OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\6.HillCipher.exe

```
Enter 9 letter string for key : abcdefghi

Enter a 6 letter message: ananya

Encrypted string is : wnqnkn

Inverse Matrix is:
nan     nan     nan
nan     nan     nan
nan     nan     nan

Decrypted string is :

Made by: AADITYA KEDIYAL

--------------------------------
Process exited after 29.22 seconds with return value 0
Press any key to continue . . .
```

7. Implement rail fence cipher transposition operation.

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\7.RailFence.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp

```cpp
#include <bits/stdc++.h>

using namespace std;
    string s ={}, s1={};
    int key;
void encryption(){

    cout<<endl<<"--------encryption---------"<<endl;

    int len;

    cout<<"Enter Text :- ";
    getline (cin,s);
    len=s.length();

    cout<<"Enter Key :- ";
    cin>>key;

    char ans[key][len]={};

    for(int i = 0; i < key; ++i)
        {for(int j = 0; j < len; ++j)
            {ans[i][j] = '\n';}}

    int j=-1,row=0;

    for(int i=0;i<len;i++)
    {
        if(row==0 || row==key-1){
            j=j*(-1);
        }
        ans[row][i] = s[i];
        row=row+j;
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 1 Col: 1 Sel: 0 Lines: 124 Length: 2367 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\7.RailFence.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp

```cpp
    }

    for(int i=0;i<key;i++)
    {
        for (int j = 0; j < len; j++) {
            if(ans[i][j]!='\n'){
                // cout<<ans[i][j];
                s1+=ans[i][j];
            }
            else{ans[i][j]='-';}
        }
    }

    cout<<endl;
    for(int i=0;i<key;i++)
    {
        for (int j = 0; j < len; j++) {
                cout<<ans[i][j];
        }
        cout<<endl;
    }

     cout<<endl;
     cout<<"encryption message : - ";
     cout<<s1;
}

void decryption(){

    cout<<endl<<"--------decryption---------"<<endl;

    int len,m=0;
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 1 Col: 1 Sel: 0 Lines: 124 Length: 2367 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\7.RailFence.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp

```cpp
    len=s1.length();

    char ans[key][len]={};

    for(int i = 0; i < key; ++i)
        {for(int j = 0; j < len; ++j)
            {ans[i][j] = '\n';}}

    int j=-1,row=0;

    for(int i=0;i<len;i++)
    {
        if(row==0 || row==key-1){
            j=j*(-1);
        }
        ans[row][i] = '*';
        row=row+j;
    }

    cout<<endl;
    for(int i=0;i<key;i++)
    {
        for (int j = 0; j < len; j++) {
            if(ans[i][j]=='*'){ans[i][j]=s1[m++];}
        }
    }

    for(int i=0;i<key;i++)
    {
        for (int j = 0; j < len; j++) {
            if(ans[i][j]=='\n'){cout<<"-";}
            else {cout<<ans[i][j];}
        }
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 1 Col: 1 Sel: 0 Lines: 124 Length: 2367 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\7.RailFence.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp

```cpp
    for(int i=0;i<key;i++)
    {
        for (int j = 0; j < len; j++) {
            if(ans[i][j]=='\n'){cout<<"-";}
            else {cout<<ans[i][j];}
        }
        cout<<endl;
    }

    cout<<endl;
    cout<<"decryption message : - ";
    row =0, j=-1;
    for(int i = 0; i < len; i++){

        if(row == 0 || row == key-1)
            {j= j * (-1);}
        cout<<ans[row][i];
        row = row + j;
    }

}

int main()
{
    encryption();
    decryption();
            cout<<endl<<"Made by: AADITYA KEDIYAL "<<endl;

    return 0;
}
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 1 Col: 1 Sel: 0 Lines: 124 Length: 2367 Insert Done parsing in 0.016 seconds

OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\7.RailFence.exe

```
--------encryption---------
Enter Text :- iamaadi
Enter Key :- 3

i---a--
-a-a-d-
--m---i

encryption message : - iaaadmi
--------decryption---------

i---a--
-a-a-d-
--m---i

decryption message : - iamaadi
Made by: AADITYA KEDIYAL

--------------------------------
Process exited after 6.277 seconds with return value 0
Press any key to continue . . .
```

8 Implement row transposition cipher transposition operation.

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\8. RowTransposition.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp

```cpp
#include <iostream>
#include<cctype>
#include<algorithm>
using namespace std;

main(){
string input;

cout << "Enter information to be encrypted" << endl;
getline(cin,input);
input.erase(std::remove (input.begin(), input.end(), ' '), input.end());

int columns = 6;
int rows;
  if (input.size() <= 5){
    rows = 1;
  }
  else if (input.size()% 5 > 0){
    rows = input.size()/5 + 1;
  }
  else
    rows = input.size()/5;

char message[rows][columns];
int place = 0;

    for(int i = 0; i < rows; i++){
```

Compiler | Resources | Compile Log | Debug | Find Results | Console | Close

Abort Compilation

Shorten compiler patl

```
- Output Filename: D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\8. RowTransposition.exe
- Output Size: 3.0065450668335 MiB
- Compilation Time: 1.08s
```

Line: 4 Col: 21 Sel: 0 Lines: 43 Length: 872 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\8. RowTransposition.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 8. RowTransposition.cpp | 11.StreamClpherTechnique.cpp

```cpp
  else if (input.size()% 5 > 0){
    rows = input.size()/5 + 1;
  }
  else
    rows = input.size()/5;

char message[rows][columns];
int place = 0;

    for(int i = 0; i < rows; i++){
      for(int j = 0; j < (columns-1); j++){
        if(place <= input.size()){
        message[rows][columns] = input[place];
        }
        else {
        message[rows][columns] = 'x';
        }
        place++;
        message[rows][5] = 'y';
        cout << message[rows][columns];
      }
        cout << endl;
    }


}
```

Compiler | Resources | Compile Log | Debug | Find Results | Console | Close

Abort Compilation

Shorten compiler patl

```
- Output Filename: D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\8. RowTransposition.exe
- Output Size: 3.0065450668335 MiB
- Compilation Time: 1.08s
```

Line: 20 Col: 4 Sel: 0 Lines: 43 Length: 872 Insert Done parsing in 0.016 seconds

OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\8. RowTransposition.exe

```
Enter information to be encrypted
iamaadi
iamaa
di xx

--------------------------------
Process exited after 3.916 seconds with return value 0
Press any key to continue . . .
```

11. Implement a stream cipher technique

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\11.StreamCIpherTechnique.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp

```cpp
#include <iostream>
#include <string>
#include <stdexcept>

int main();
void encrypt_decrypt( std::string &text, std::string const &one_time_pad );

void encrypt_decrypt( std::string &text, std::string const &one_time_pad ) {
    if ( text.length() > one_time_pad.length() ) {
        throw std::length_error( "The message is shorter than the one-time pad." );
    }

    for ( size_t k{0}; k < text.length(); ++k ) {
        text[k] ^= one_time_pad[k];
    }
}

int main() {
    std::string msg("I am AADI.");

    // 20 randomly chosen characters based on atmospheric noise
    //   - see https://www.random.org/integers/
    //   - this is a null-character terminated string
    char random_numbers[21]{
          -5,  32, -36, -120,   -8,  -94,   48,   78,  -99,  -92,
          25,  79,  29,   59,  -41, -108, -127,  -84,   55,   10,
           0
    };

    std::string one_time_pad{random_numbers};

    std::cout << msg << std::endl;
    encrypt_decrypt( msg, one_time_pad );
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 3 Col: 21 Sel: 0 Lines: 40 Length: 1071 Insert Done parsing in 0.016 seconds

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\11.StreamCIpherTechnique.cpp - Embarcadero Dev-C++ 6.3

File Edit Search View Project Execute Tools AStyle Window Help

TDM-GCC 9.2.0 64-bit Release

(globals)

Project C | 6.HillCipher.cpp | 7.RailFence.cpp | 8. RowTransposition.cpp | 11.StreamCIpherTechnique.cpp

```cpp
    if ( text.length() > one_time_pad.length() ) {
        throw std::length_error( "The message is shorter than the one-time pad." );
    }

    for ( size_t k{0}; k < text.length(); ++k ) {
        text[k] ^= one_time_pad[k];
    }
}

int main() {
    std::string msg("I am AADI.");

    // 20 randomly chosen characters based on atmospheric noise
    //   - see https://www.random.org/integers/
    //   - this is a null-character terminated string
    char random_numbers[21]{
          -5,  32, -36, -120,   -8,  -94,   48,   78,  -99,  -92,
          25,  79,  29,   59,  -41, -108, -127,  -84,   55,   10,
           0
    };

    std::string one_time_pad{random_numbers};

    std::cout << msg << std::endl;
    encrypt_decrypt( msg, one_time_pad );
    std::cout << msg << std::endl;
    encrypt_decrypt( msg, one_time_pad );
    std::cout << msg << std::endl;

    return 0;
}
```

Compiler | Resources | Compile Log | Debug | Find Results | Console

Line: 3 Col: 21 Sel: 0 Lines: 40 Length: 1071 Insert Done parsing in 0.016 seconds

OUTPUT

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\11.StreamCIpherTechnique.exe

```
I am AADI.
╝┌┼┐q
└┘
I am AADI.

--------------------------------
Process exited after 0.0885 seconds with return value 0
Press any key to continue . . .
```