INFORMATION SECURITY

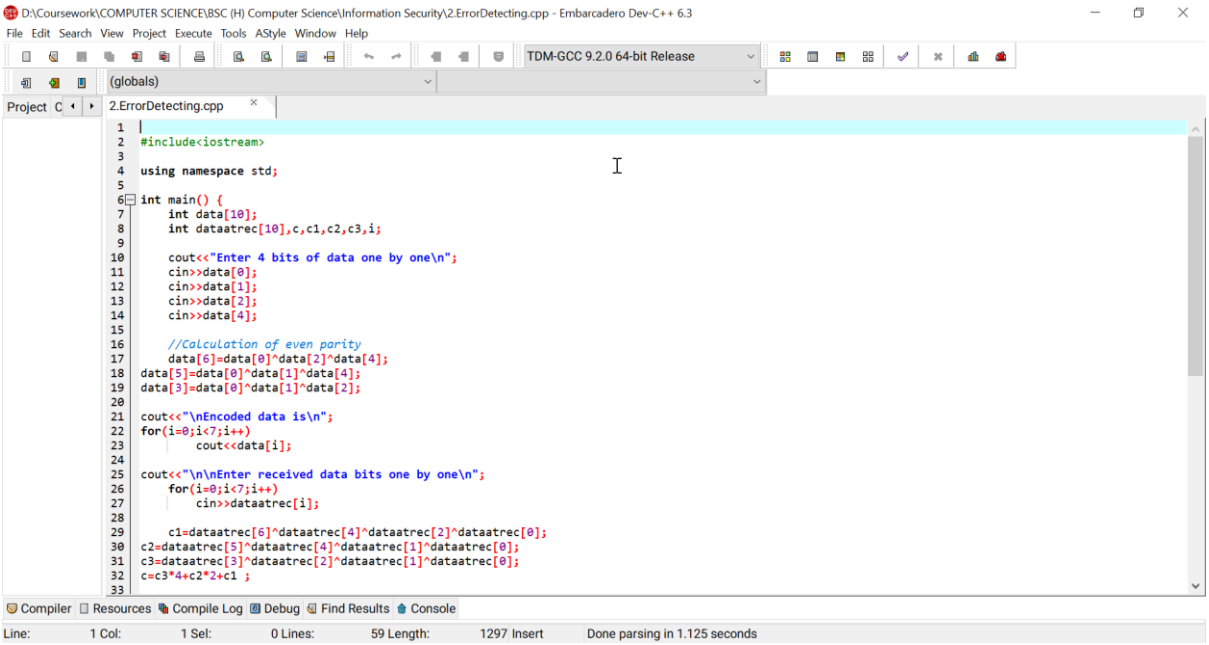
PRACTICAL FILE

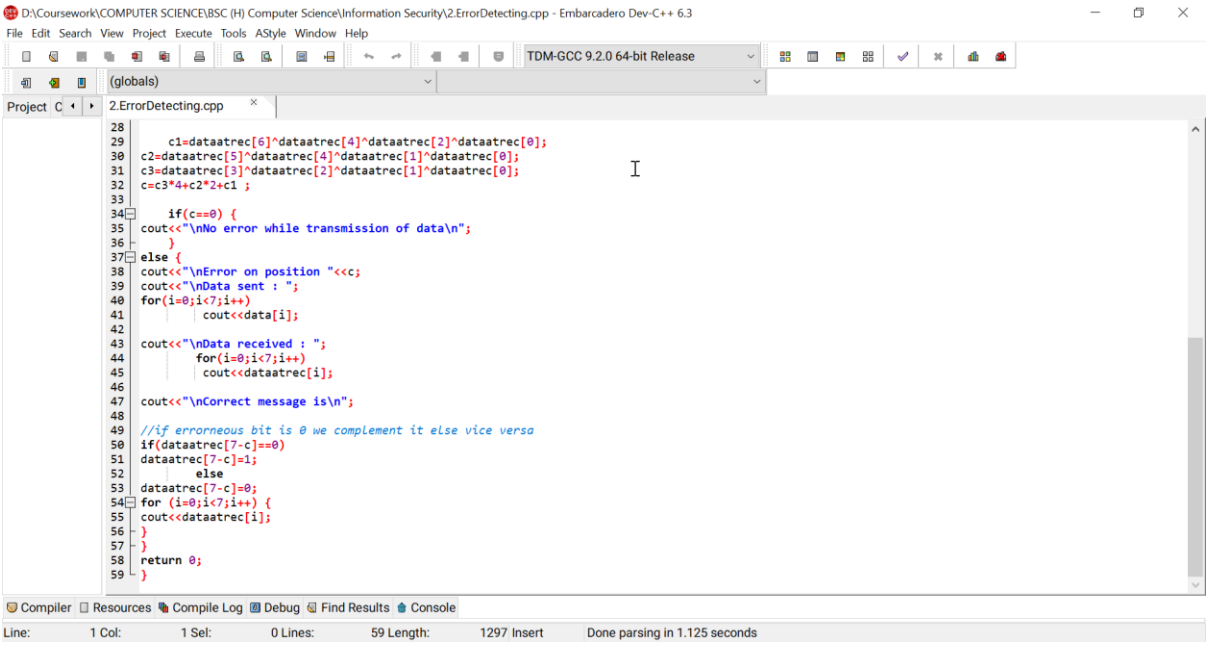
Shivam Saxena

BSc(H) Computer Science

20201423

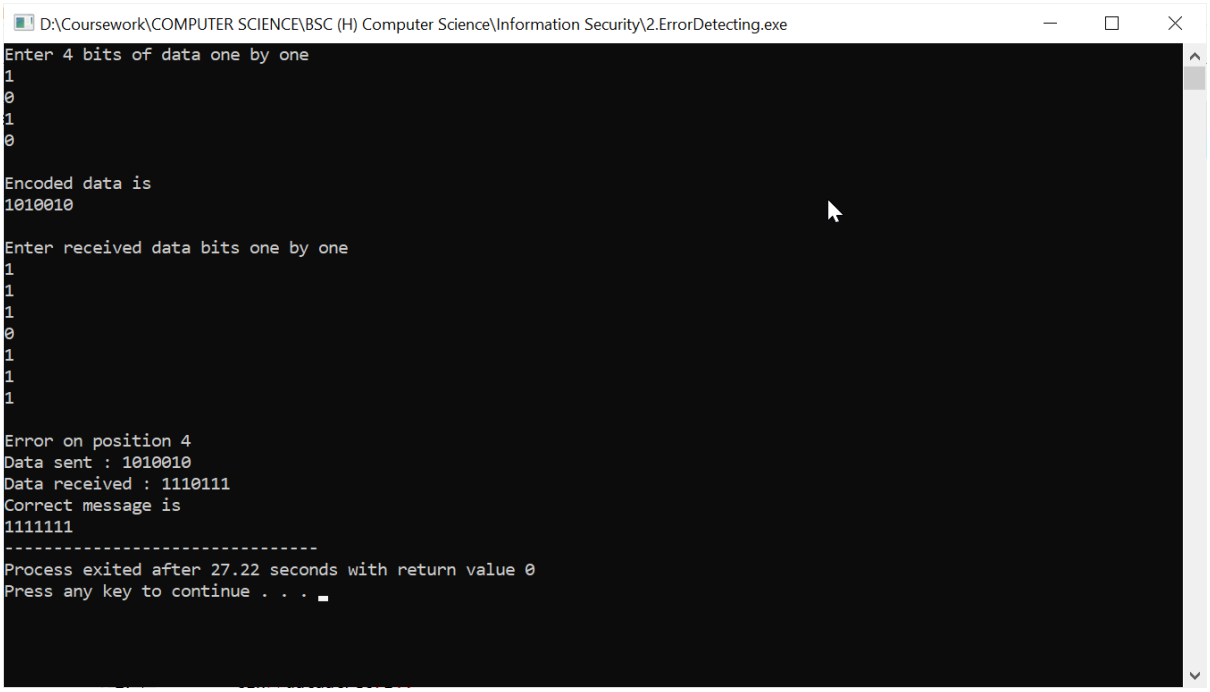
1. Implement the error detecting code





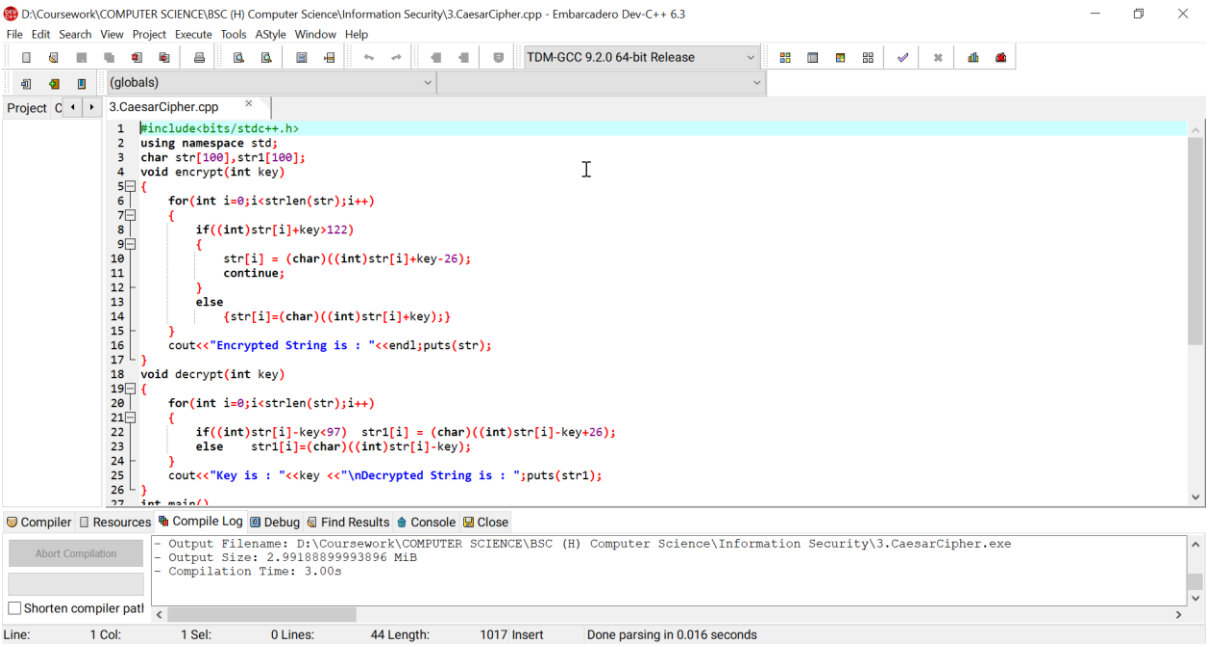
```
    c1=dataatrec[6]^dataatrec[4]^dataatrec[2]^dataatrec[0];
c2=dataatrec[5]^dataatrec[4]^dataatrec[1]^dataatrec[0];
c3=dataatrec[3]^dataatrec[2]^dataatrec[1]^dataatrec[0];
c=c3*4+c2*2+c1 ;

    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;
}
```

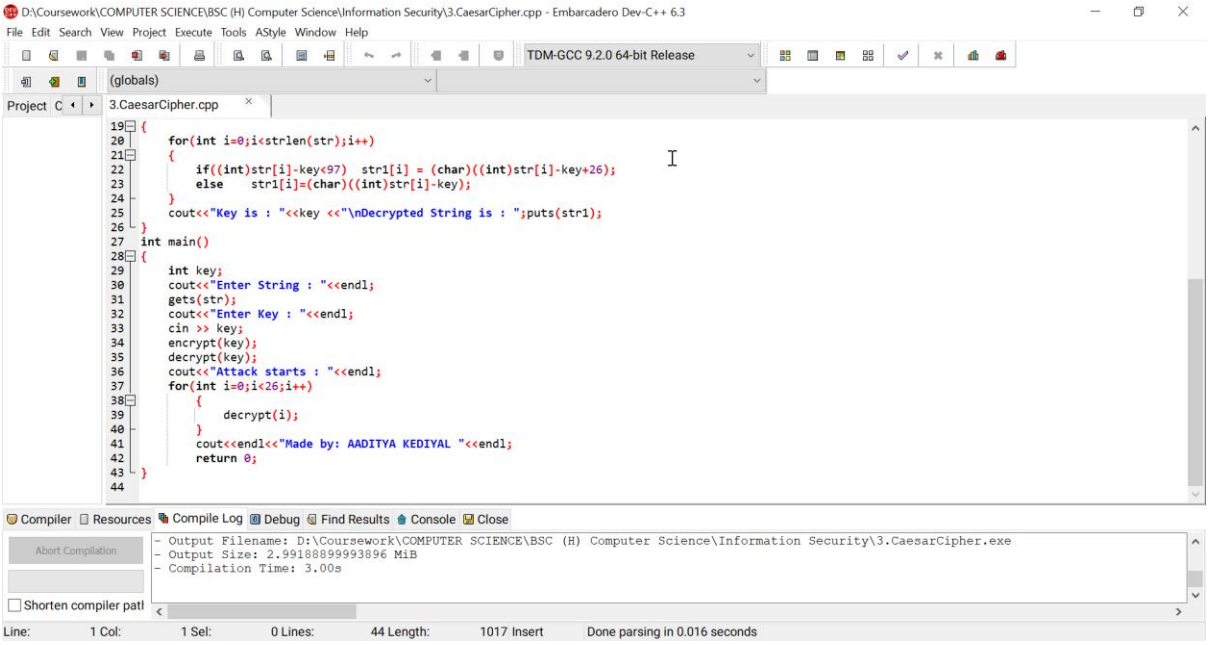
OUTPUT



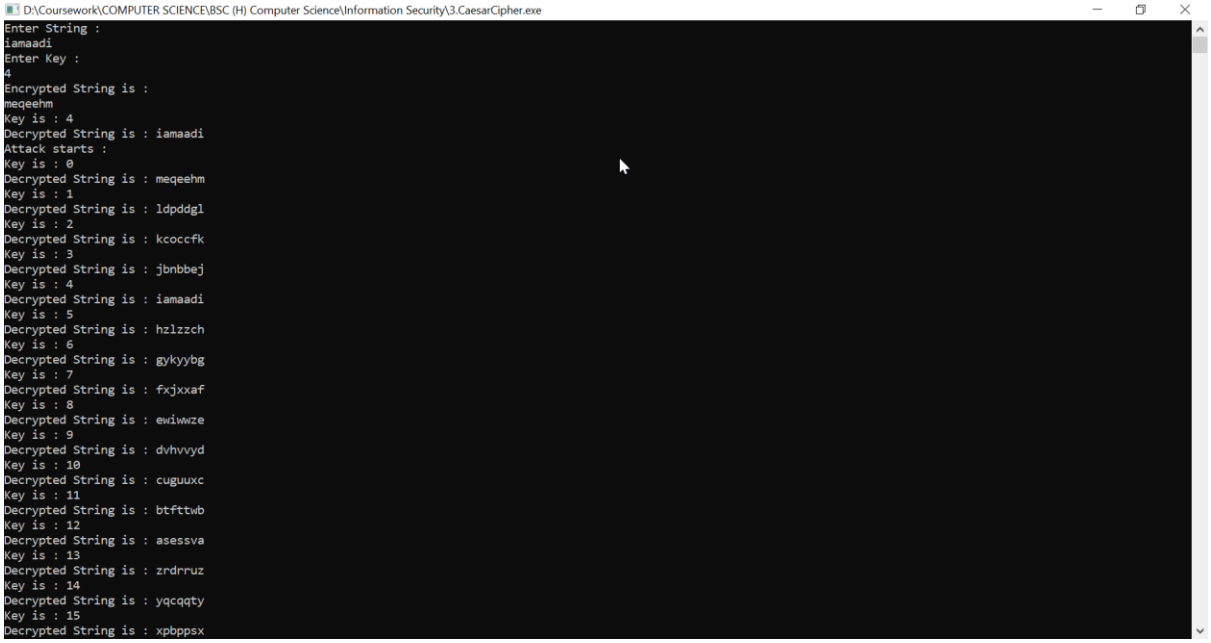
```
Enter 4 bits of data one by one
1
0
1
0

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 . . .
```

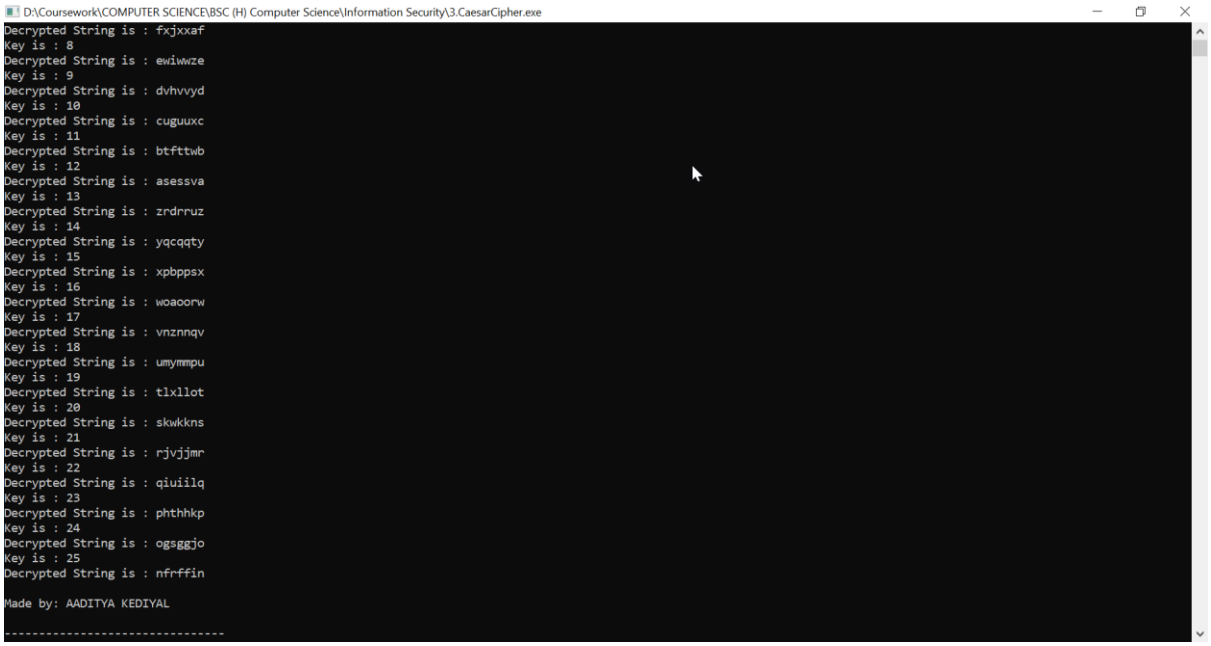
3. Implement caeser cipher substitution operation.





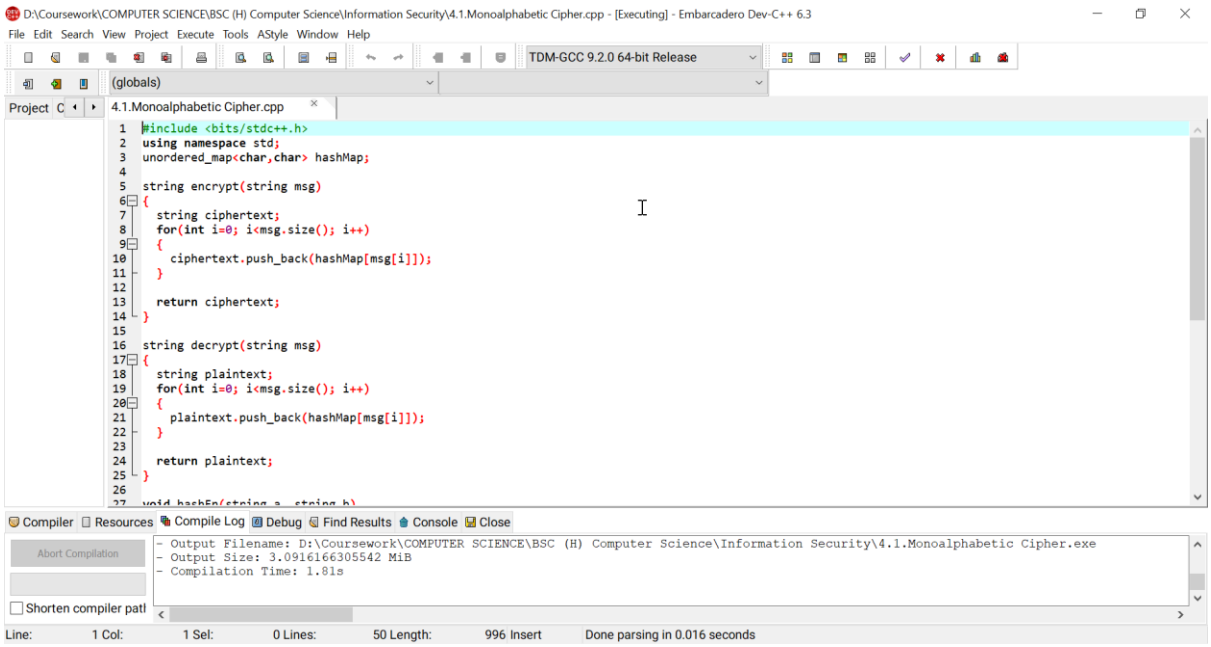
OUTPUT

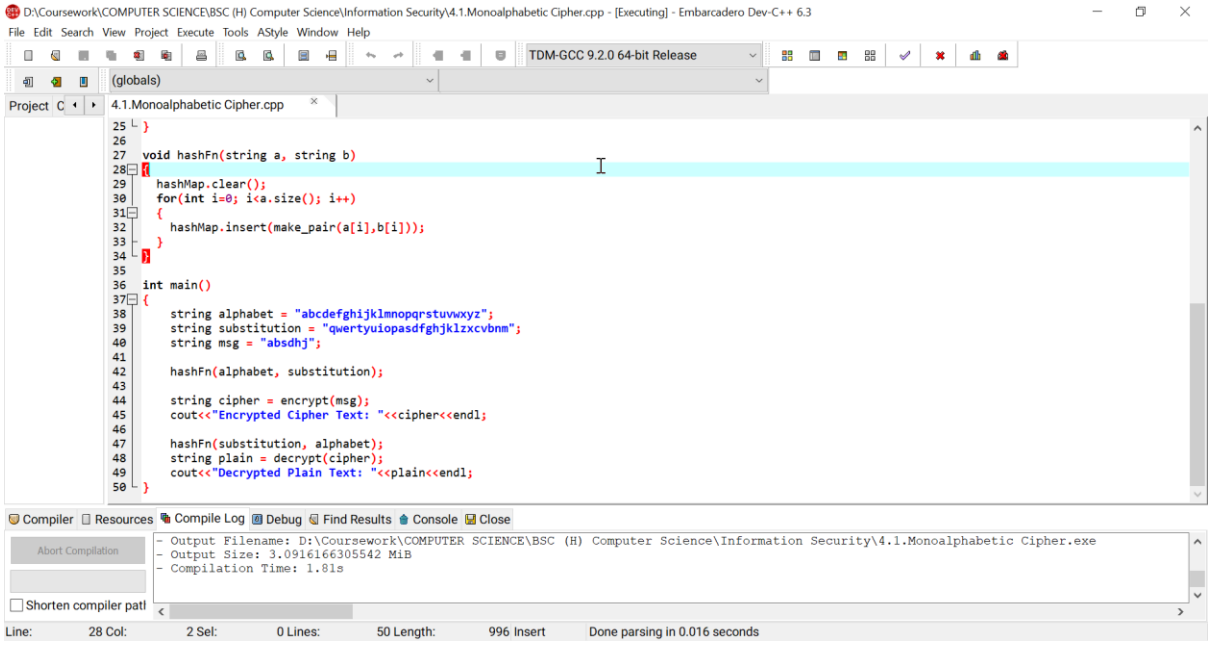

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\3.CaesarCipher.exe
Enter String :
iamaadi
Enter Key :
4
Encrypted String is :
meqeehm
Key is : 4
Decrypted String is : iamaadi
Attack starts :
Key is : 0
Decrypted String is : meqeehm
Key is : 1
Decrypted String is : ldpddgl
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

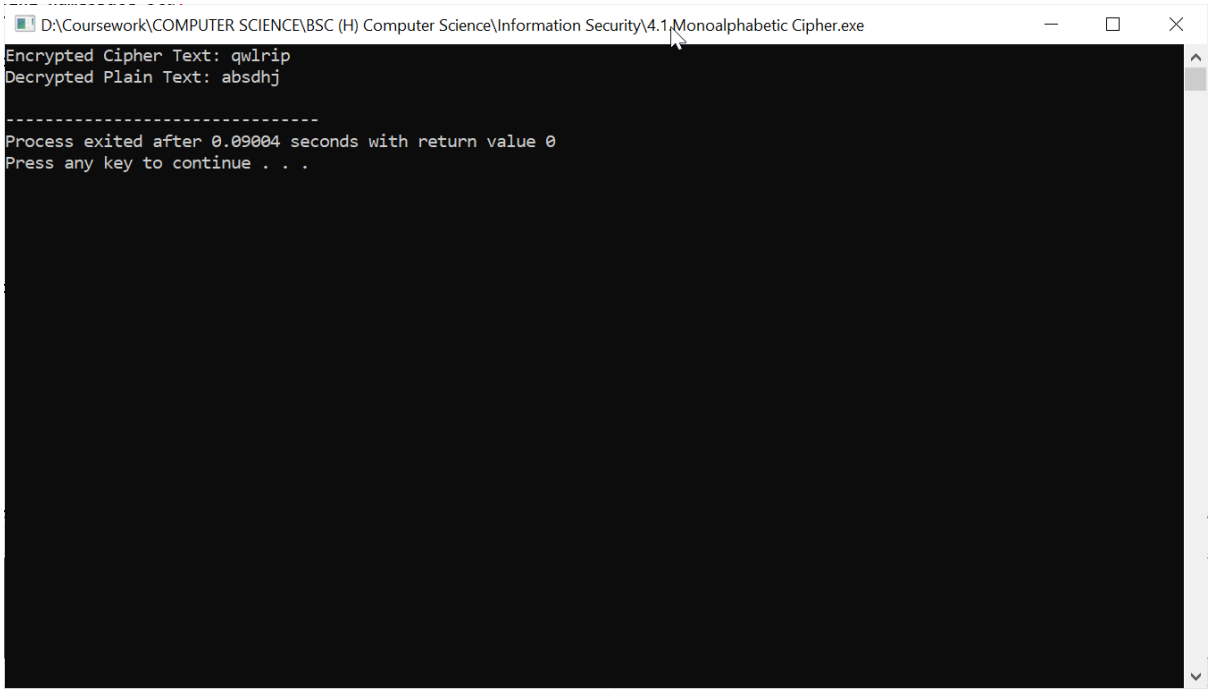
4.

4.1 . Implement monoalphabetic cipher substitution operation.

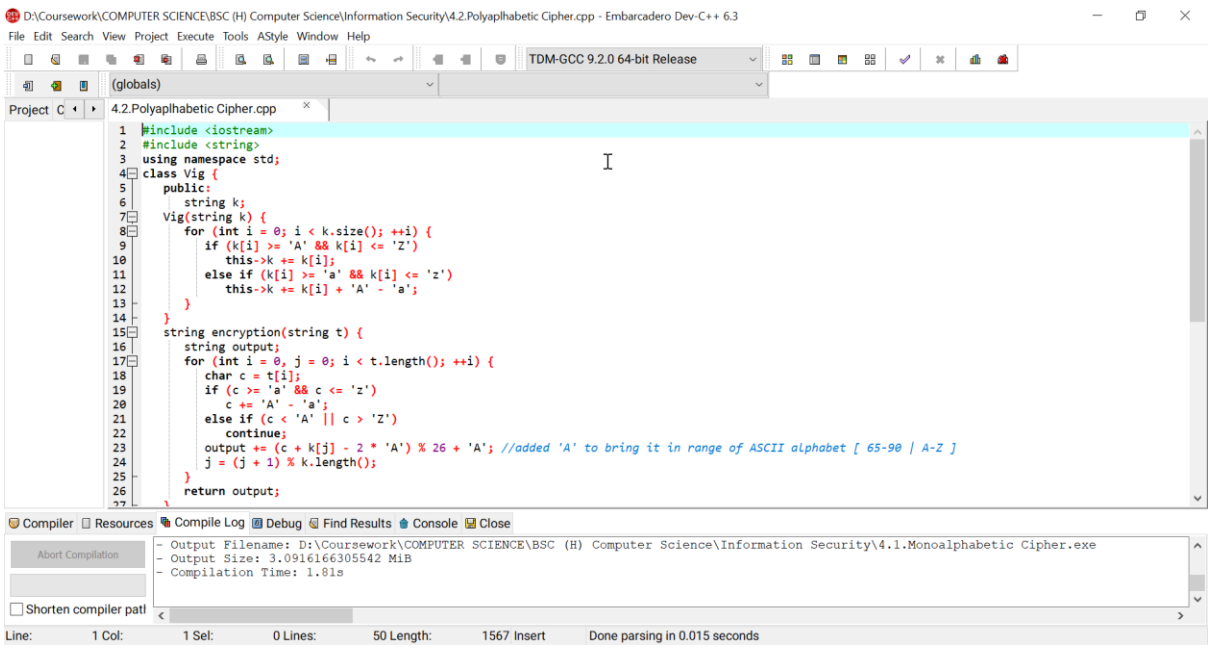


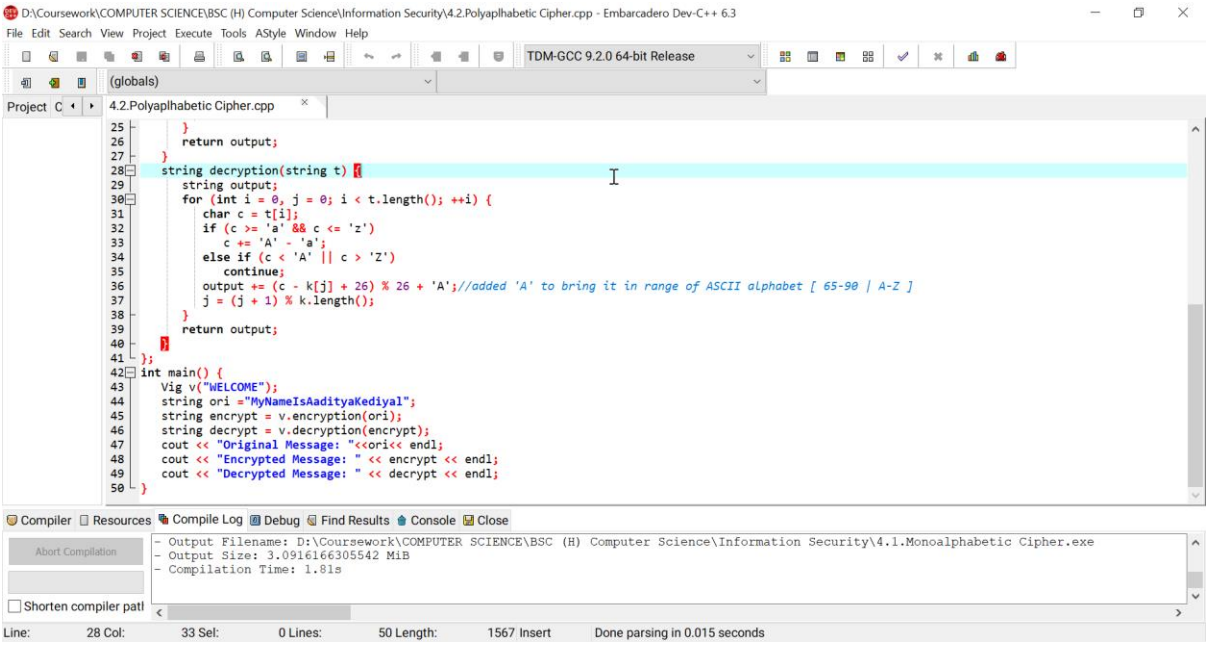


OUTPUT

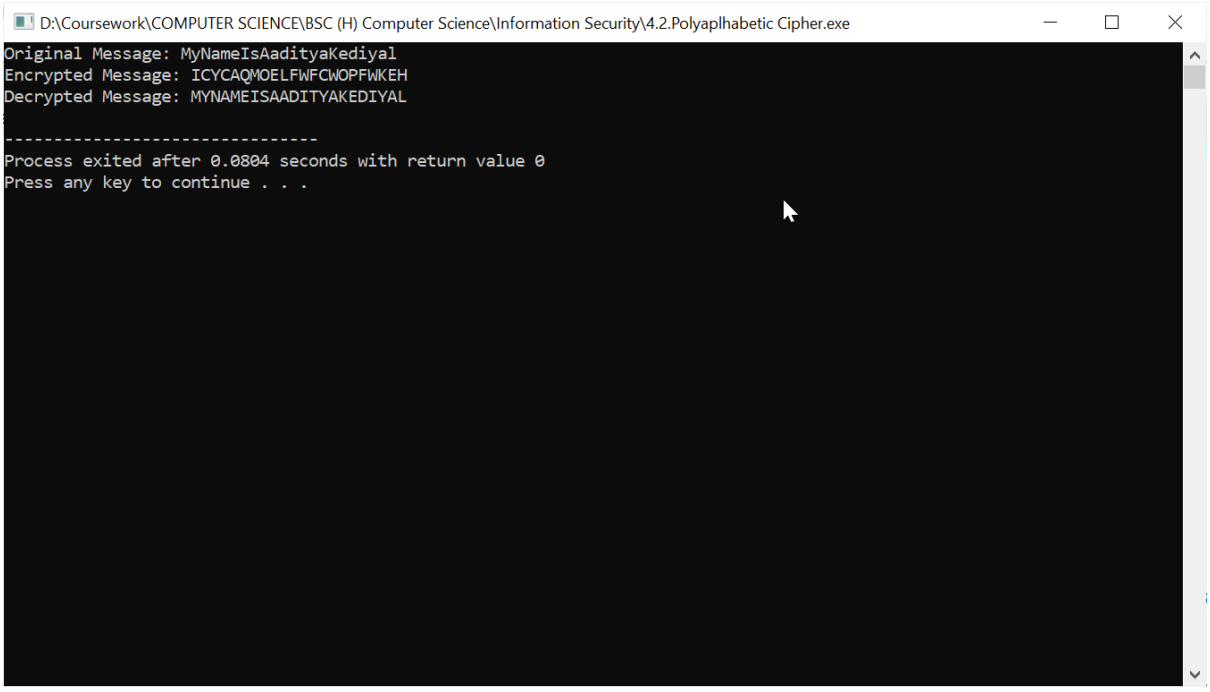


4.2 Implement polyalphabetic cipher substitution operation



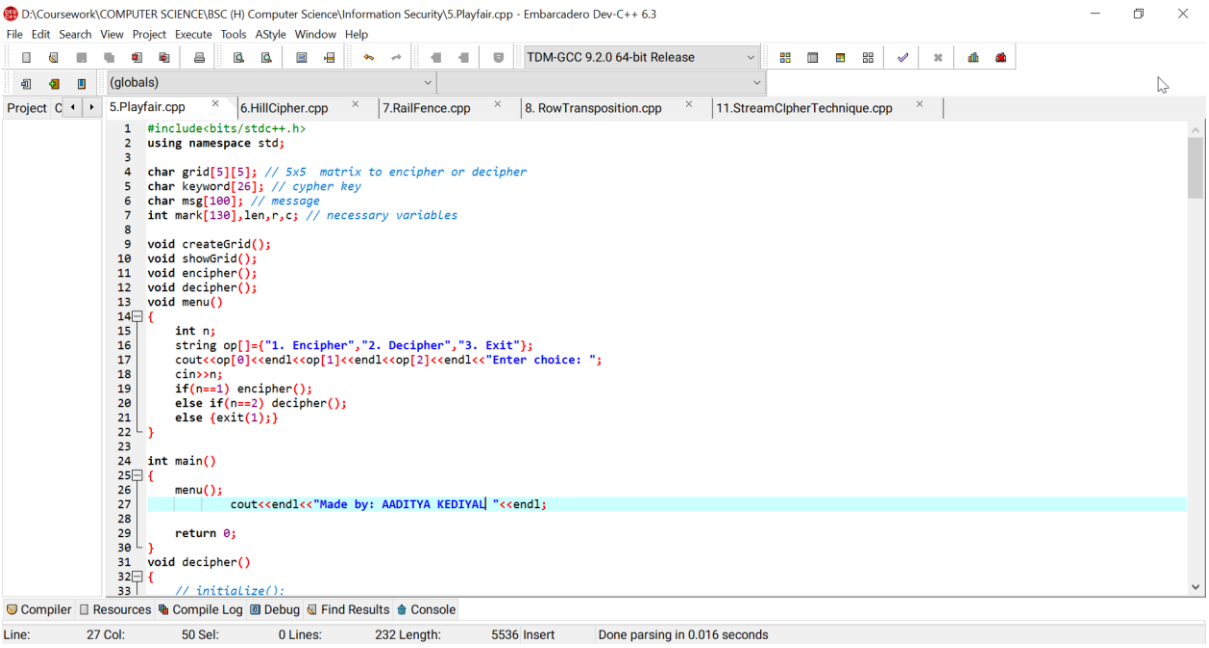

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\4.2.Polyaplhabetic Cipher.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
4.2.Polyaplhabetic Cipher.cpp
}
return output;
}
string 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
- 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
Shorten compiler path
Line: 28 Col: 33 Sel: 0 Lines: 50 Length: 1567 Insert Done parsing in 0.015 seconds

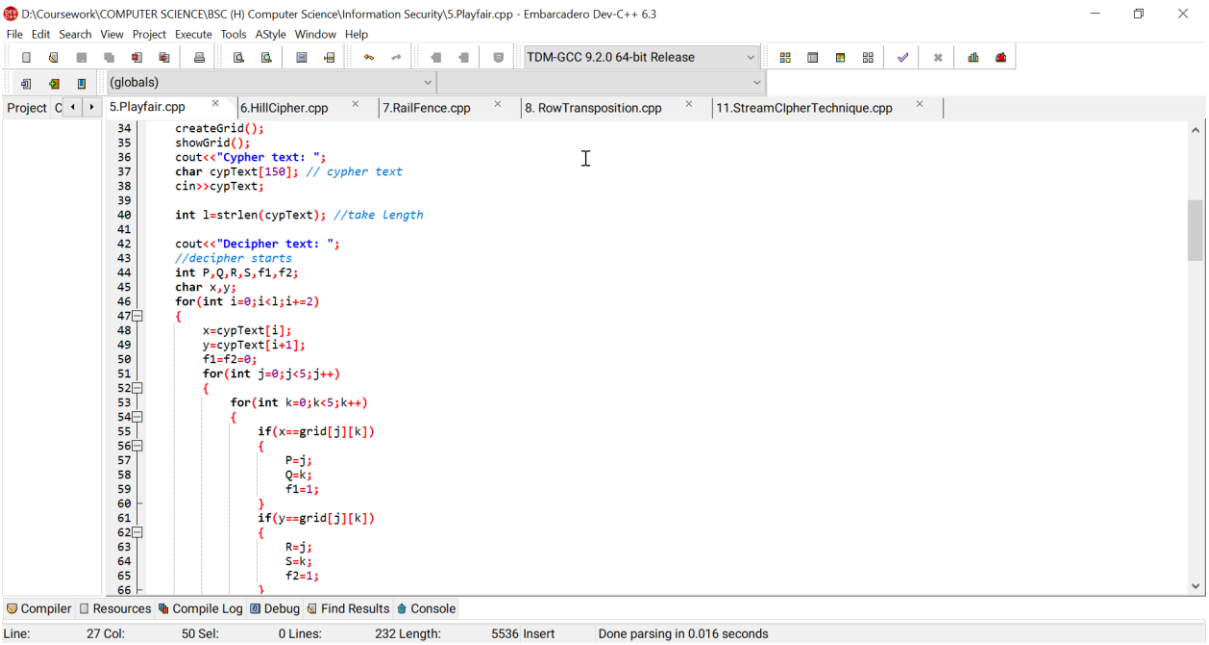
OUTPUT

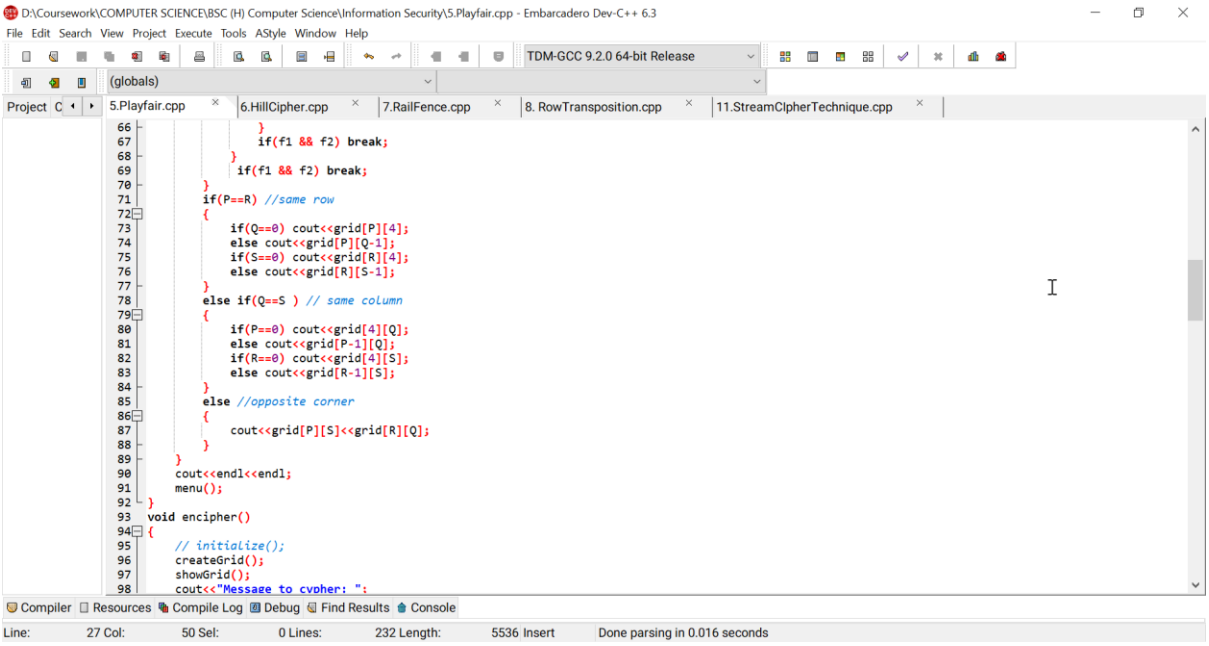

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\4.2.Polyaplhabetic Cipher.exe
Original Message: MyNameIsAadityaKediyal
Encrypted Message: ICYCAQMOELFWFCWOPFWKEH
Decrypted Message: MYNAMEISAADITYAKEDIYAL

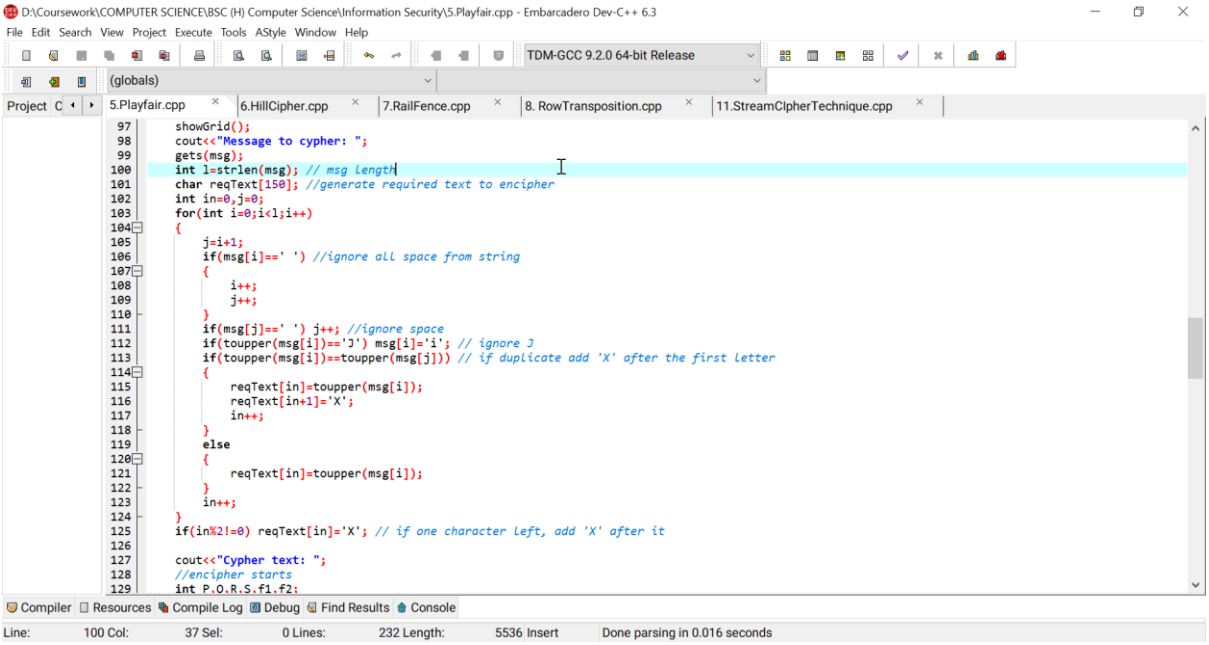
Process exited after 0.0804 seconds with return value 0
Press any key to continue . . .

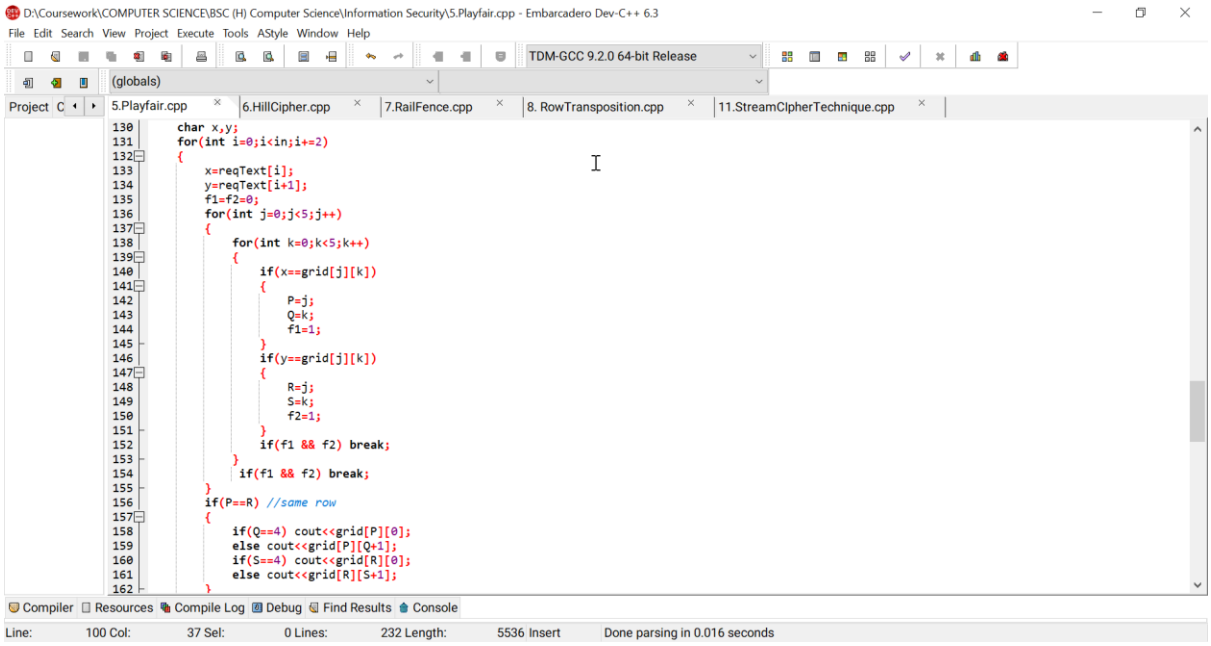
5. Implement playfair cipher substitution operation.

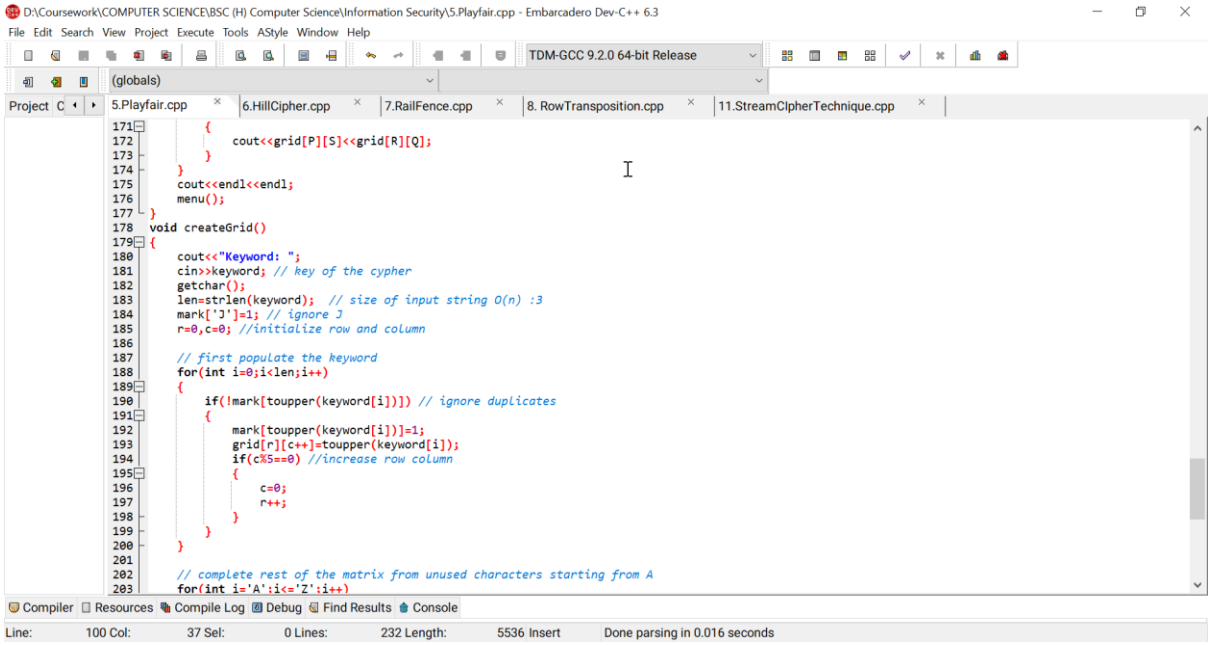


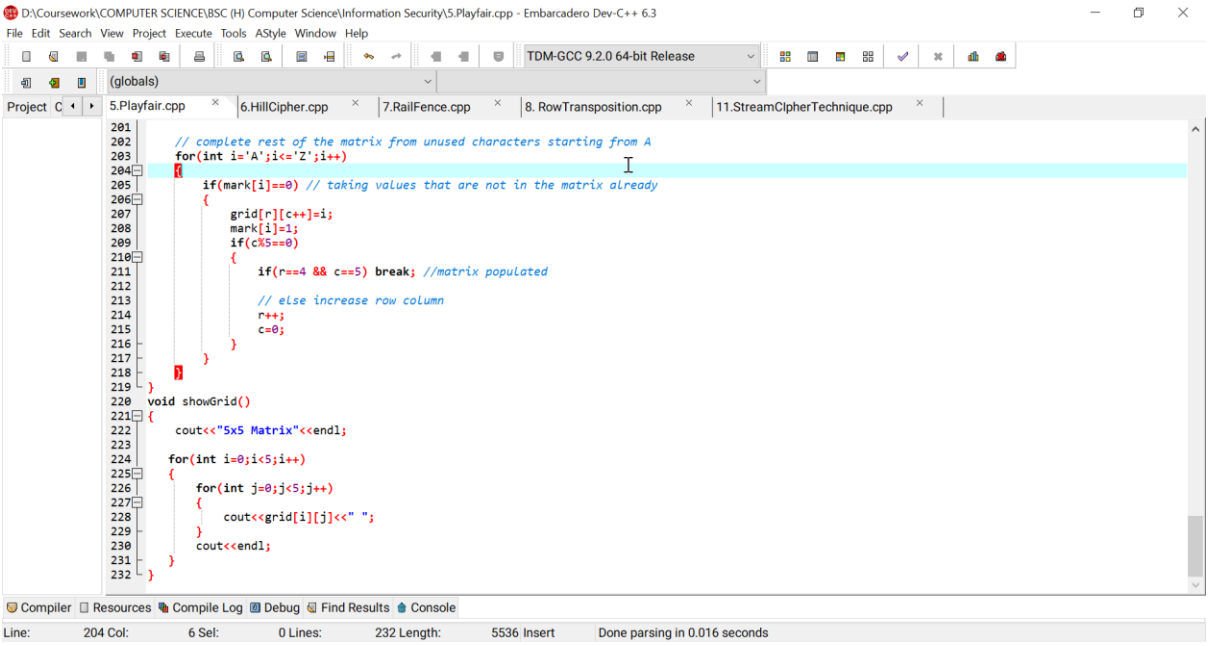



D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
5.Playfair.cpp
6.HillCipher.cpp
7.RailFence.cpp
8. RowTransposition.cpp
11.StreamClpherTechnique.cpp
}
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

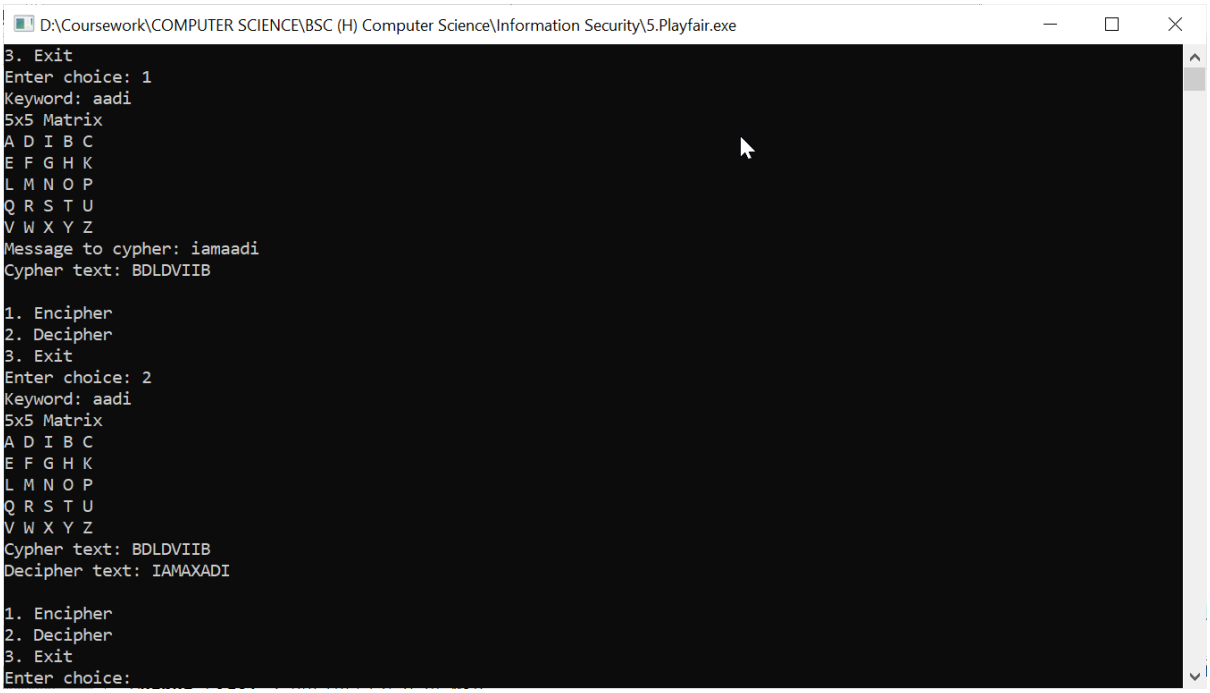

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
5.Playfair.cpp
6.HillCipher.cpp
7.RailFence.cpp
8. RowTransposition.cpp
11.StreamClpherTechnique.cpp
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
130 char x,y;
131 for(int i=0;i<in;i+=2)
132 {
133 x=reqText[i];
134 y=reqText[i+1];
135 f1=f2=0;
136 for(int j=0;j<5;j++)
137 {
138 for(int k=0;k<5;k++)
139 {
140 if(x==grid[j][k])
141 {
142 P=j;
143 Q=k;
144 f1=1;
145 }
146 if(y==grid[j][k])
147 {
148 R=j;
149 S=k;
150 f2=1;
151 }
152 if(f1 && f2) break;
153 }
154 if(f1 && f2) break;
155 }
156 if(P==R) //same row
157 {
158 if(Q==4) cout<<grid[P][0];
159 else cout<<grid[P][Q+1];
160 if(S==4) cout<<grid[R][0];
161 else cout<<grid[R][S+1];
162 }
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

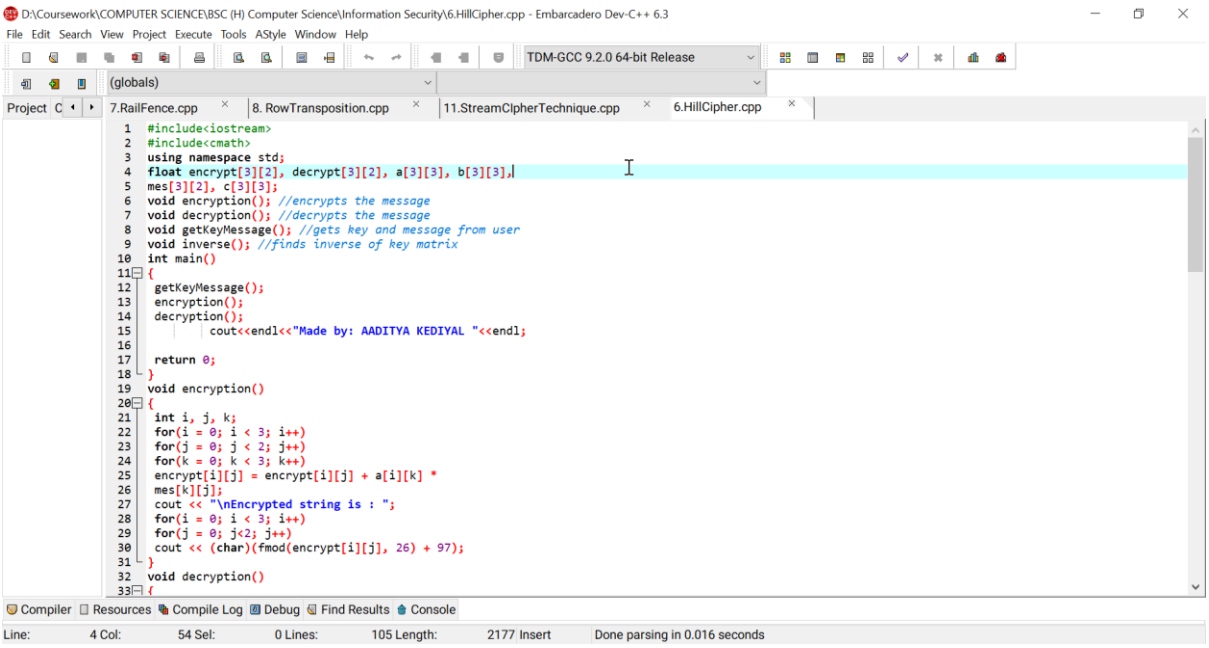

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
5.Playfair.cpp
6.HillCipher.cpp
7.RailFence.cpp
8. RowTransposition.cpp
11.StreamClpherTechnique.cpp
171 {
172 cout<<grid[P][S]<<grid[R][Q];
173 }
174 }
175 cout<<endl<<endl;
176 menu();
177 }
178 void createGrid()
179 {
180 cout<<"Keyword: ";
181 cin>>keyword; // key of the cypher
182 getchar();
183 len=strlen(keyword); // size of input string O(n) :3
184 mark['J']=1; // ignore J
185 r=0,c=0; //initialize row and column
186
187 // first populate the keyword
188 for(int i=0;i<len;i++)
189 {
190 if(!mark[toupper(keyword[i])]) // ignore duplicates
191 {
192 mark[toupper(keyword[i])]=1;
193 grid[r][c++]=toupper(keyword[i]);
194 if(c%5==0) //increase row column
195 {
196 c=0;
197 r++;
198 }
199 }
200 }
201
202 // complete rest of the matrix from unused characters starting from A
203 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

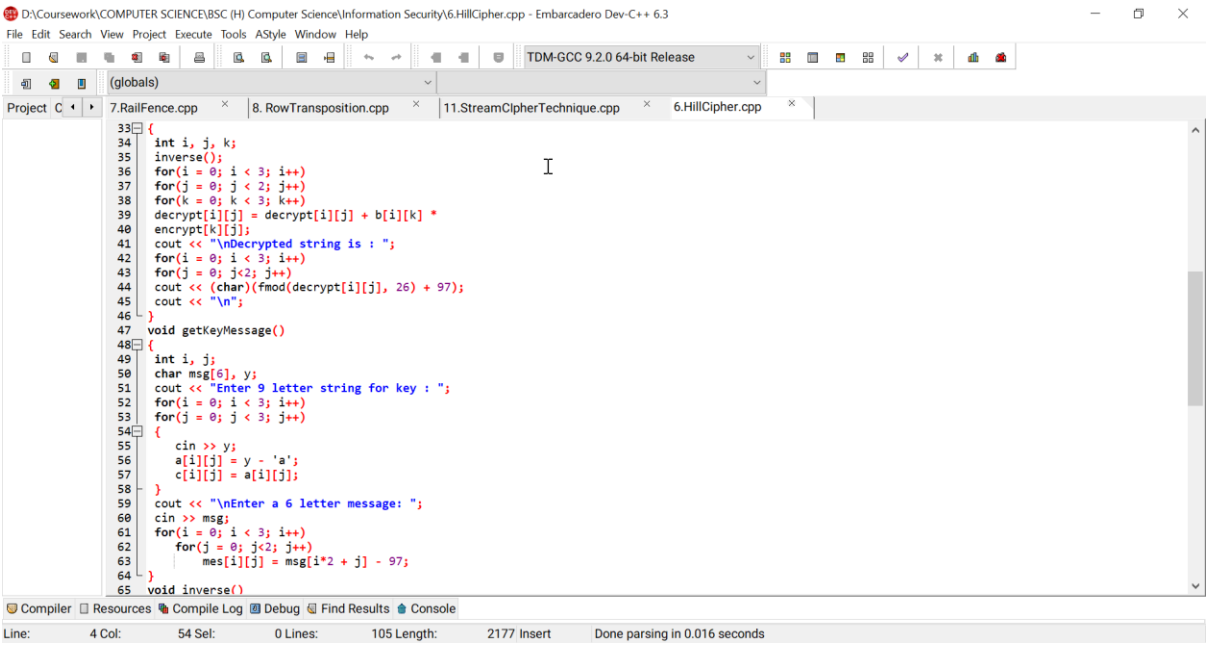

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\5.Playfair.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
5.Playfair.cpp
6.HillCipher.cpp
7.RailFence.cpp
8. RowTransposition.cpp
11.StreamCIpherTechnique.cpp
201 // complete rest of the matrix from unused characters starting from A
202 for(int i='A';i<='Z';i++)
203 {
204 if(mark[i]==0) // taking values that are not in the matrix already
205 {
206 grid[r][c++]=i;
207 mark[i]=1;
208 if(c%5==0)
209 {
210 if(r==4 && c==5) break; //matrix populated
211
212 // else increase row column
213 r++;
214 c=0;
215 }
216 }
217 }
218 }
219 void showGrid()
220 {
221 cout<<"5x5 Matrix"<<endl;
222
223 for(int i=0;i<5;i++)
224 {
225 for(int j=0;j<5;j++)
226 {
227 cout<<grid[i][j]<<" ";
228 }
229 cout<<endl;
230 }
231 }
232
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

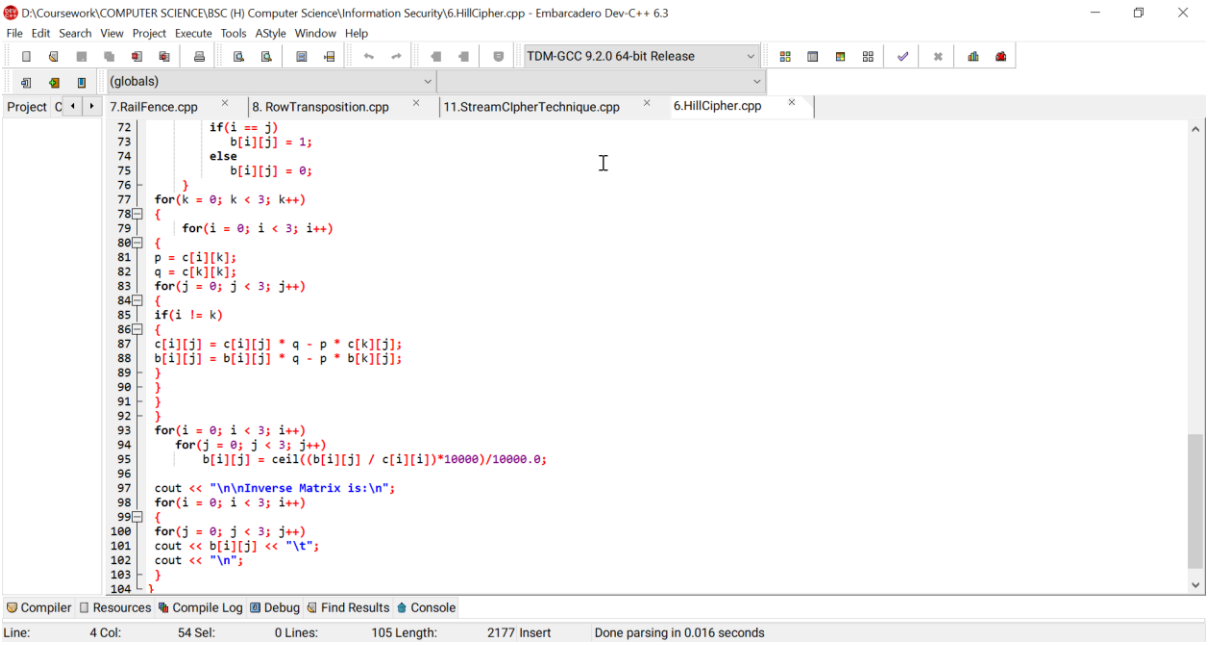
OUTPUT


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:

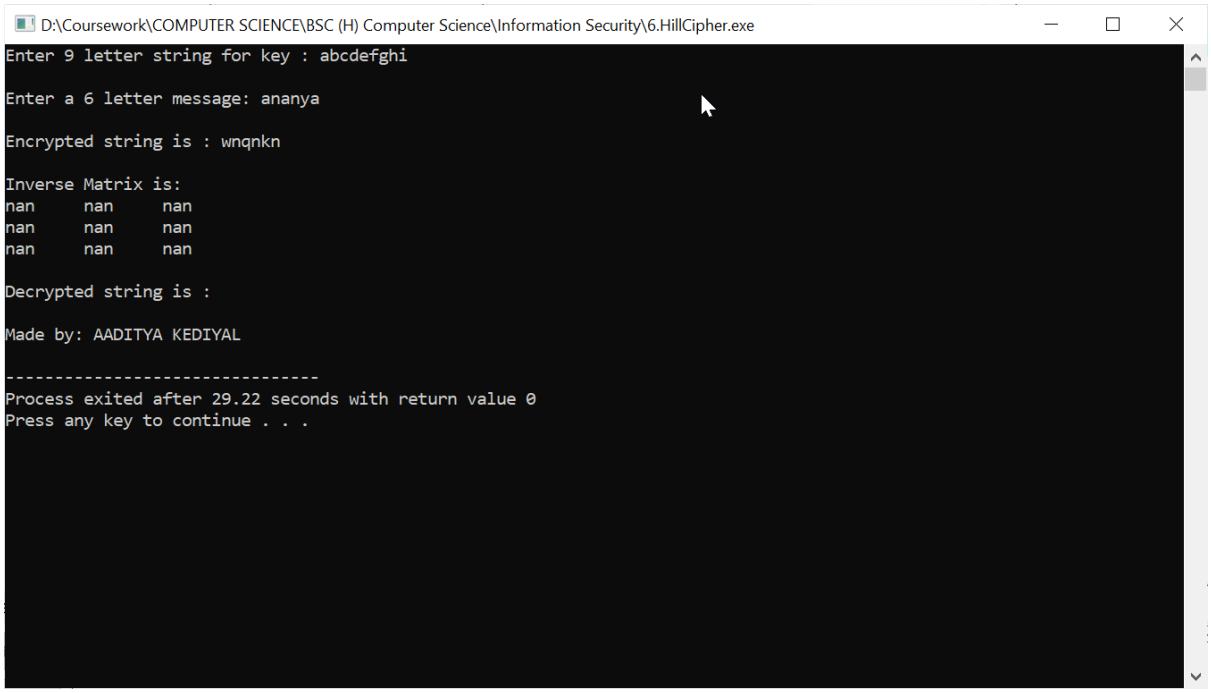
6. Implement hill cipher substitution operation



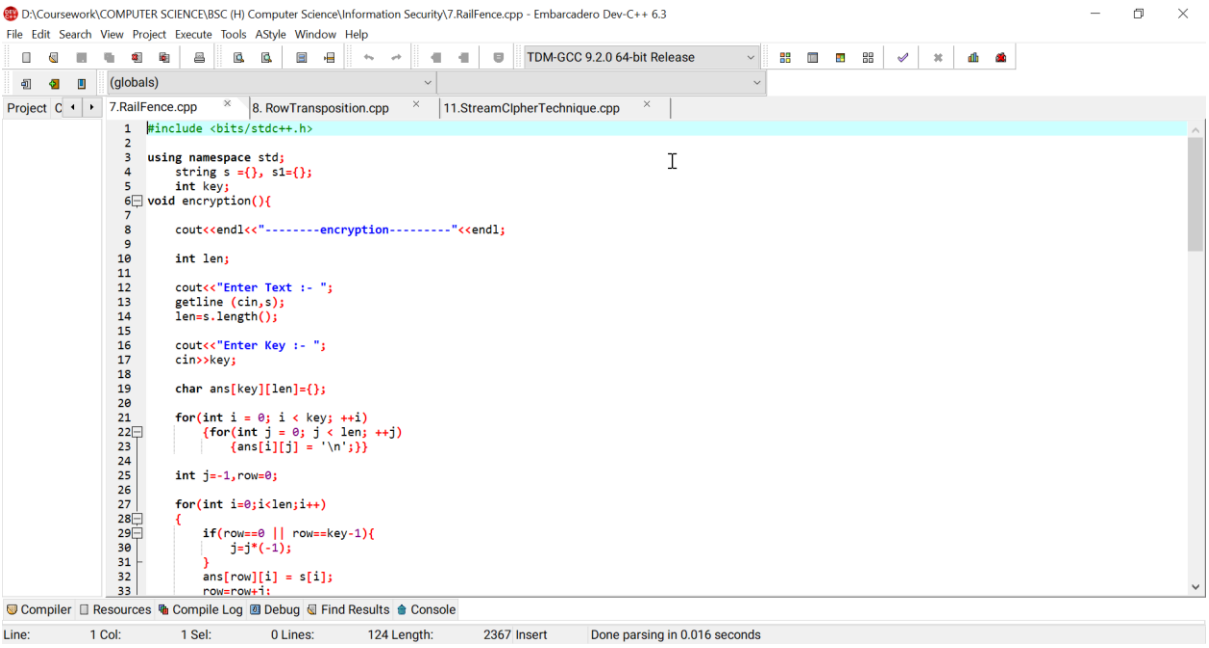


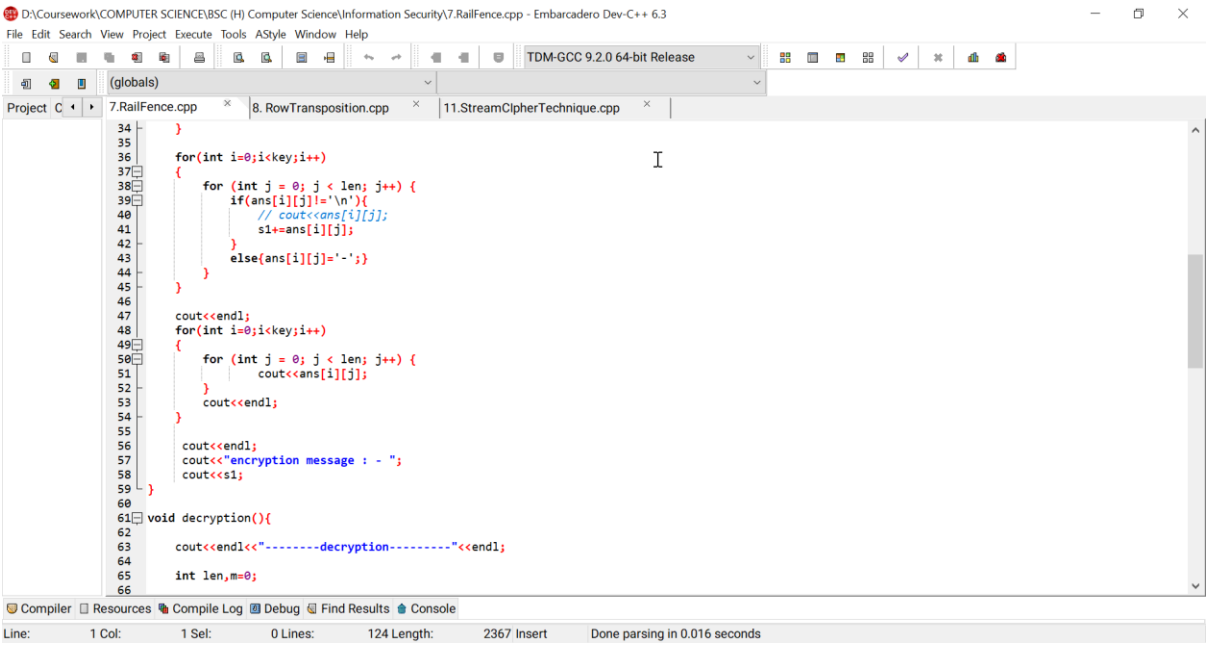

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\6.HillCipher.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
7.RailFence.cpp
8. RowTransposition.cpp
11.StreamCipherTechnique.cpp
6.HillCipher.cpp
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

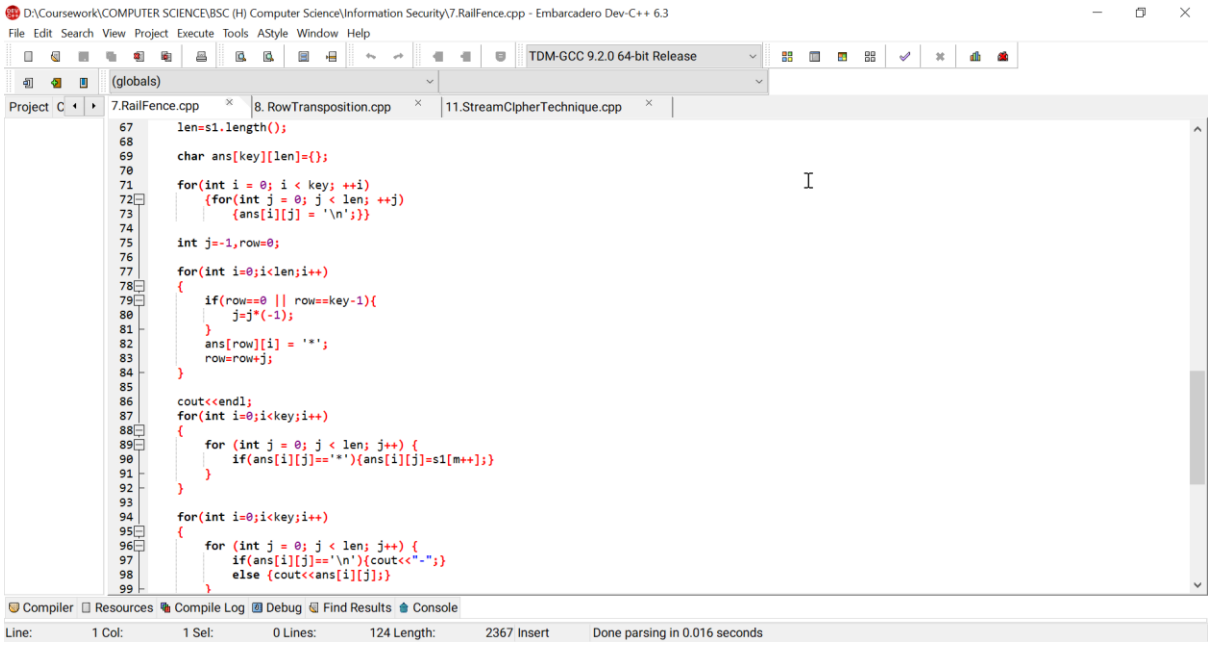
OUTPUT

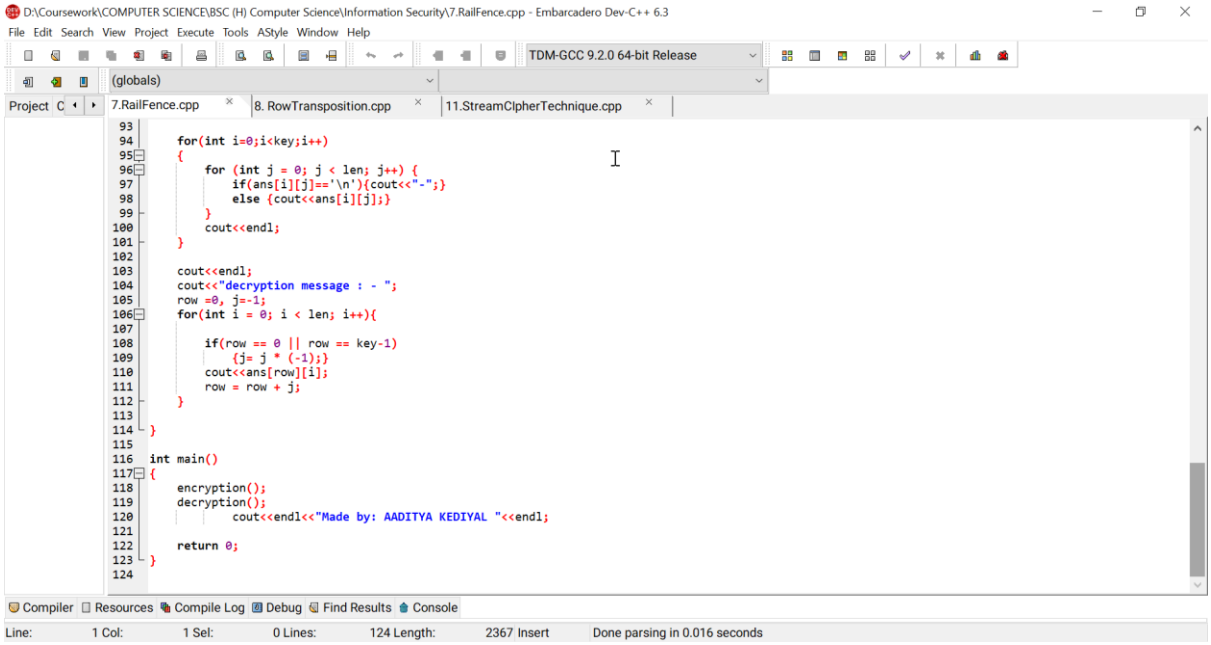

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\6.HillCipher.exe
Enter 9 letter string for key : abcdefghi
Enter a 6 letter message: ananya
Encrypted string is : wnqnkn
Inverse Matrix is:
nan nan nan
nan nan nan
nan nan nan
Decrypted string is :
Made by: AADITYA KEDIYAL
Process exited after 29.22 seconds with return value 0
Press any key to continue . . .

7. Implement rail fence cipher transposition operation.

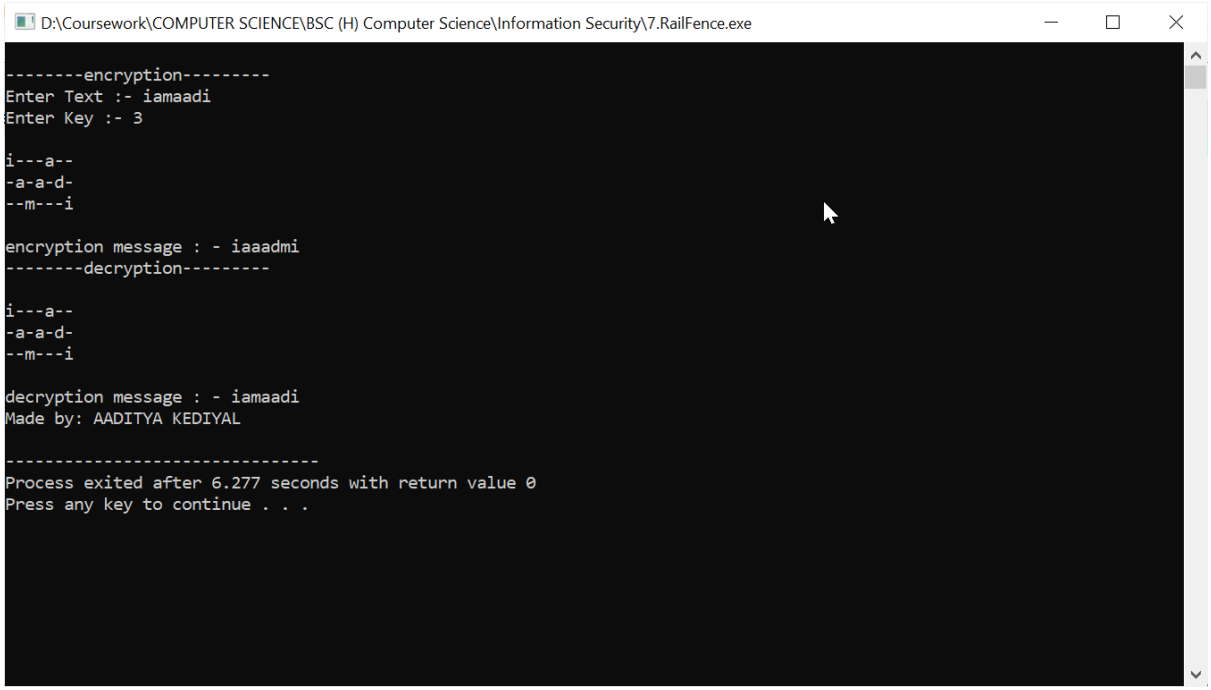




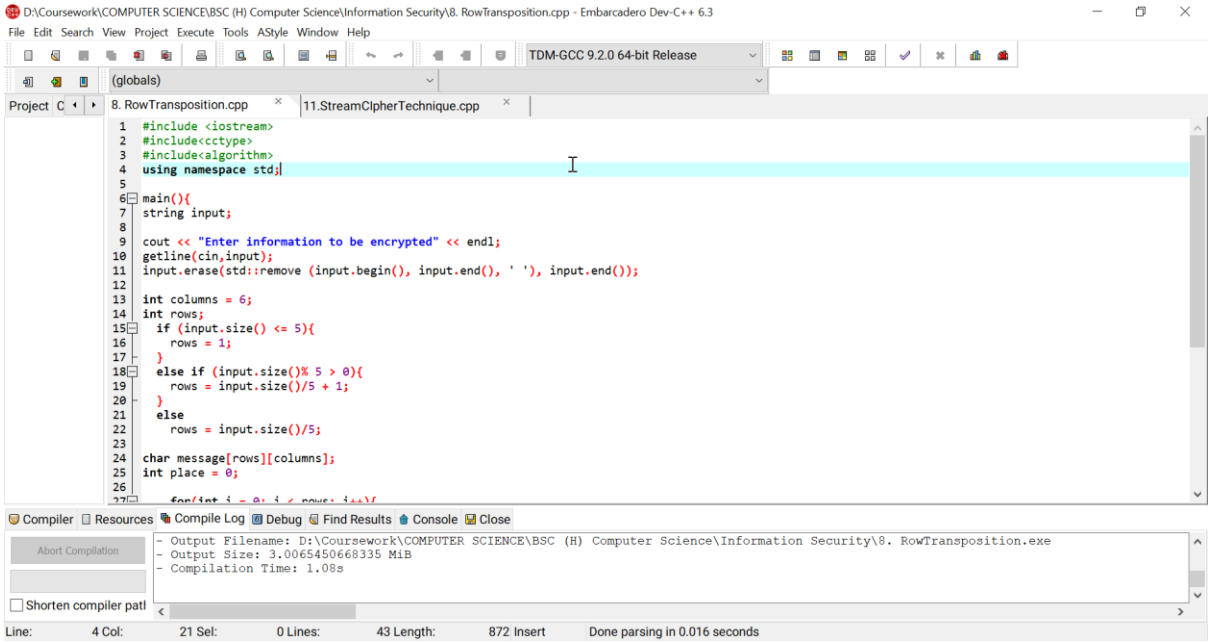

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\7.RailFence.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
7.RailFence.cpp
8. RowTransposition.cpp
11.StreamCIpherTechnique.cpp
len=s1.length();
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

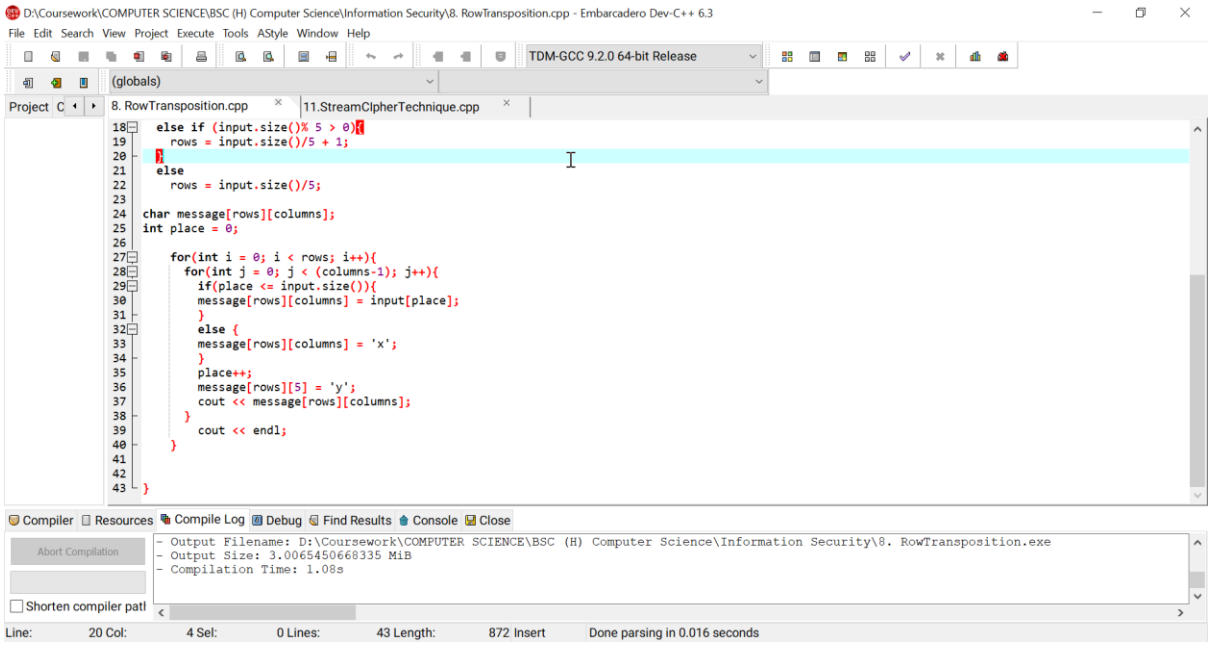

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\7.RailFence.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
7.RailFence.cpp
8. RowTransposition.cpp
11.StreamCIpherTechnique.cpp
for(int 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

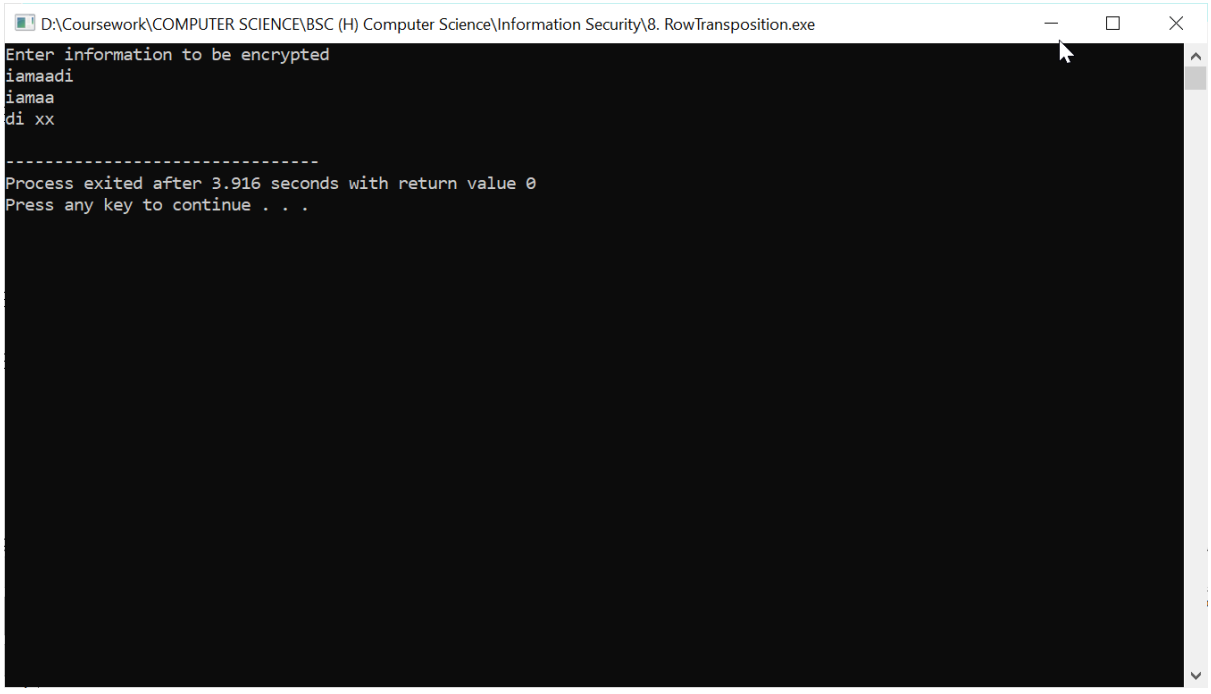


8 Implement row transposition cipher transposition operation.



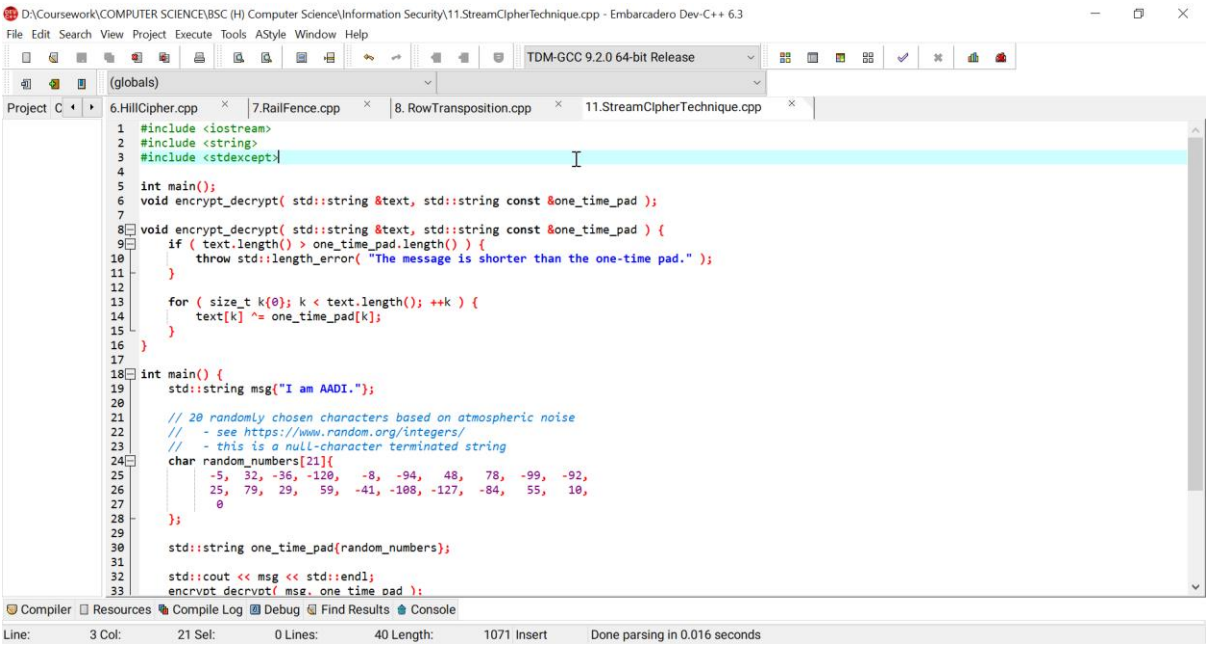

D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\8. RowTransposition.cpp - Embarcadero Dev-C++ 6.3
File Edit Search View Project Execute Tools AStyle Window Help
TDM-GCC 9.2.0 64-bit Release
(globals)
Project C
8. RowTransposition.cpp
11.StreamCipherTechnique.cpp
else if (input.size()% 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 path
- 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

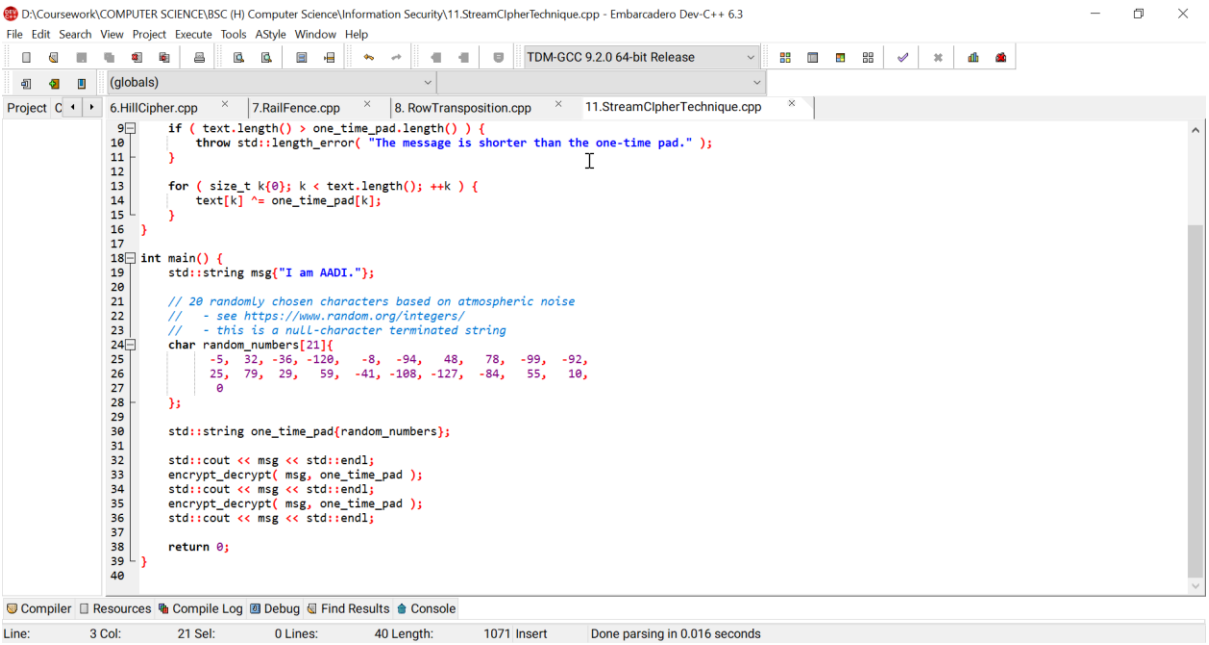
OUTPUT


D:\Coursework\COMPUTER SCIENCE\BSC (H) Computer Science\Information Security\8. RowTransposition.exe
Enter information to be encrypted
iamaadi
iamaa
di xx

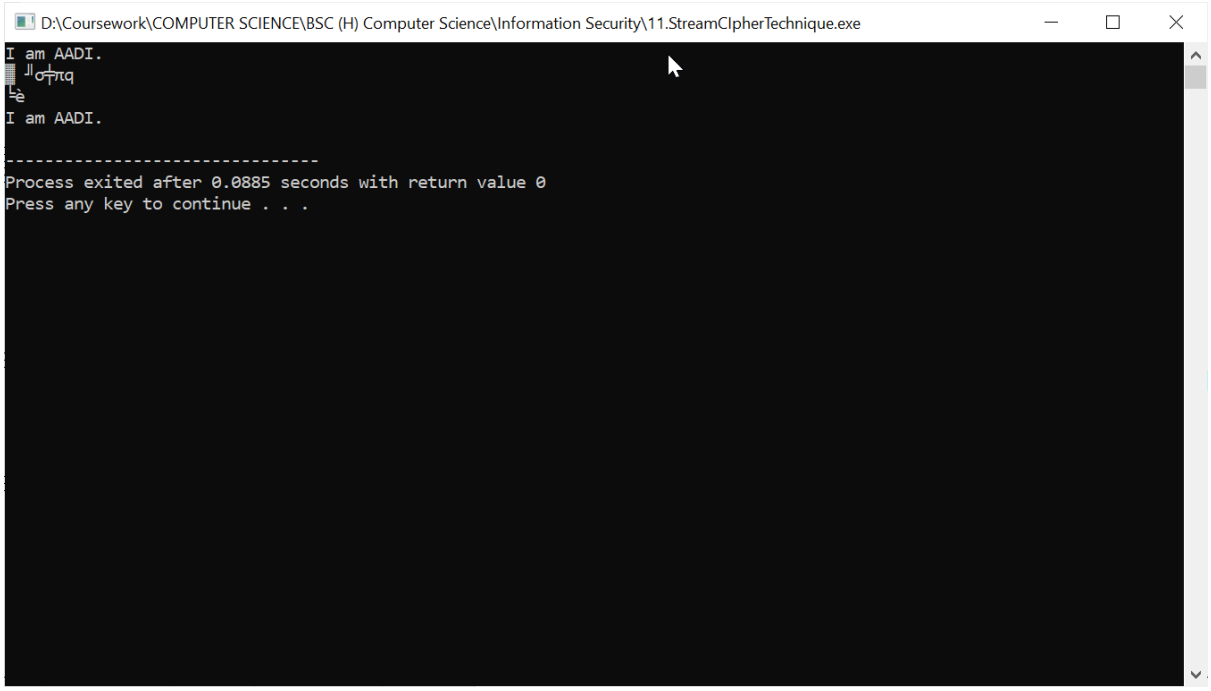
Process exited after 3.916 seconds with return value 0
Press any key to continue . . .

11. Implement a stream cipher technique





OUTPUT


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

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