Part A:

Cease Cipher

**Code:**

#include<iostream>

using namespace std;

void CeaserCipher()

{

string text="Internet Security difficult subject";

string result\_encrypt = "";

string result\_decrypt = "";

int s = 1;

for (int i=0;i<text.length();i++)

{

result\_encrypt += char(int(text[i]+s-97)%26 +97);

}

cout << "Text : " << text<<"\n";

cout<<"Result: "<<result\_encrypt<<endl;

for (int i=0;i<text.length();i++)

{

result\_decrypt += char(int(text[i]+s-97)%26 +97)-s;

}

cout<<"Decrypt : "<<result\_decrypt;

}

void CeaserRow()

{

int i,j,row,col=0;

char message[10][10];

char temp[10][10];

cout<<"Enter number of rows:";

cin>>row;

cout<<"\nEnter number of columns:";

cin>>col;

cout<<"Enter plain text("<<row\*col<<" characters):";

for(i=0;i<row;i++){

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

cin>>message[i][j];

}

}

for(i=0;i<row;i++){

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

cout<<"\n["<<i<<"]["<<j<<"]:"<<message[i][j]<<"\t";

}

cout<<"\n";

}

for(i=0;i<row;i++){

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

temp[i+1][j]=message[i][j];

if(i==row-1){

temp[0][j]=message[i][j];

}

}

}

cout<<"\n ROW TRANSPOSE ARRAY";

for(i=0;i<row;i++){

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

cout<<"\n["<<i<<"]["<<j<<"]:"<<temp[i][j]<<"\t";

}

cout<<"\n";

}

}

void CeaserColumn()

{

int i,j,row,col=0;

char message[10][10];

char temp[10][10];

cout<<"Enter number of rows:";

cin>>row;

cout<<"\nEnter number of columns:";

cin>>col;

cout<<"Enter plain text("<<row\*col<<" characters):";

for(i=0;i<row;i++){

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

cin>>message[i][j];

}

}

for(i=0;i<row;i++){

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

cout<<"\n["<<i<<"]["<<j<<"]:"<<message[i][j]<<"\t";

}

cout<<"\n";

}

for(i=0;i<row;i++){

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

temp[i][j+1]=message[i][j];

if(j==col-1){

temp[i][0]=message[i][j];

}

}

}

cout<<"\nCOLUMN TRANSPOSE ARRAY";

for(i=0;i<row;i++){

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

cout<<"\n["<<i<<"]["<<j<<"]:"<<temp[i][j]<<"\t";

}

cout<<"\n";

}

}

int main()

{

char choice;

cout<<"Enter your choice..\na. Substitution Cipher.\nb. Row Transposition Cipher. \nc. Column Transposition Cipher. \n";

cin>>choice;

switch(choice)

{

case 'a':

CeaserCipher();

break;

case 'b':

CeaserRow();

break;

case 'c':

CeaserColumn();

break;

default:

cout<<"Enter valid option\n";

}

}

**Output:**

Enter your choice..

a. Substitution Cipher.

b. Row Transposition Cipher.

c. Column Transposition Cipher.

a

Text : Internet Security difficult subject

Result: JoufsofuUTfdvsjuzUejggjdvmuUtvckfdu

Decrypt : InternetTSecurityTdifficultTsubject

Enter your choice..

a. Substitution Cipher.

b. Row Transposition Cipher.

c. Column Transposition Cipher.

b

Enter number of rows:3

Enter number of columns:3

Enter plain text(9 characters):

m

a

t

b

a

t

c

a

t

[0][0]:m

[0][1]:a

[0][2]:t

[1][0]:b

[1][1]:a

[1][2]:t

[2][0]:c

[2][1]:a

[2][2]:t

ROW TRANSPOSE ARRAY

[0][0]:c

[0][1]:a

[0][2]:t

[1][0]:m

[1][1]:a

[1][2]:t

[2][0]:b

[2][1]:a

[2][2]:t

Enter your choice..

a. Substitution Cipher.

b. Row Transposition Cipher.

c. Column Transposition Cipher.

c

Enter number of rows:3

Enter number of columns:3

Enter plain text(9 characters):

m

a

t

b

a

t

c

a

t

[0][0]:m

[0][1]:a

[0][2]:t

[1][0]:b

[1][1]:a

[1][2]:t

[2][0]:c

[2][1]:a

[2][2]:t

COLUMN TRANSPOSE ARRAY

[0][0]:t

[0][1]:m

[0][2]:a

[1][0]:t

[1][1]:b

[1][2]:a

[2][0]:t

[2][1]:c

[2][2]:a

Part B:

Diffie Hellman key exchange algorithm

**Code:**

#include<iostream>

#include <cmath>

using namespace std;

int main()

{

int p, g, x, a, y, b, ka, kb;

cout<<"Enter the value of the prime modulus and generator on which both Alice and Bob will agree publicly:\n";

cin>>p;

cin>>g;

cout<<"Enter private key of Alice:\n";

cin>>a;

x = (int)pow(g, a)%p;

cout<<"Enter private key of Bob:\n";

cin>>b;

y = (int)pow(g, b)%p;

ka = (long)pow(y, a)%p;

kb = (long)pow(x, b)%p;

cout<<"\nSecret key of Alice:"<<ka;

cout<<"\nSecret key of Bob:"<<kb;

return 0;

}

**Output:**

Enter the value of the prime modulus and generator on which both Alice and Bob will agree publicly:

11

7

Enter private key of Alice:

3

Enter private key of Bob:

6

Secret key of Alice: 9

Secret key of Bob:9