Assignment 1
Vernam Cipher

Vernam cipher is the **symmetric key** algorithm. In this, a key K is used for encryption and the same key for decryption. Consider a Message 'M' that consists of characters and a Key 'K' which is used for encryption using the defined algorithm then after encryption we get a ciphertext which is **E=K(M)** and then the receiver uses the same kay and a different algorithm to decrypt the message and get the original message as **D=K(K(M))**.

The algorithm used for Encryption:

1. Convert the plain text and key from characters to numbers like **'a' -> 0, 'b -> 1,…., 'z' -> 25** and let us name them P and K for Plain text and key respectively.
2. Add then add P and K and if any addition is greater than 26 subtract 26 from it.
3. Then send this message as Ciphertext.

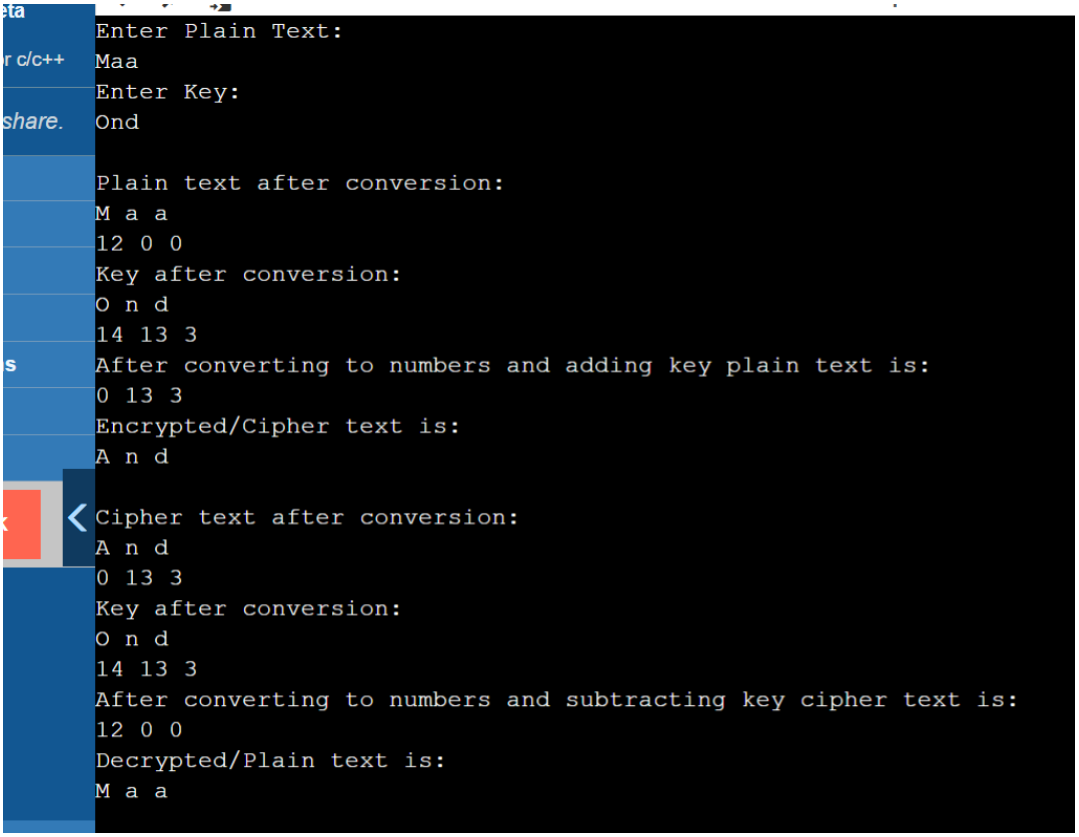
The algorithm used for Decryption:

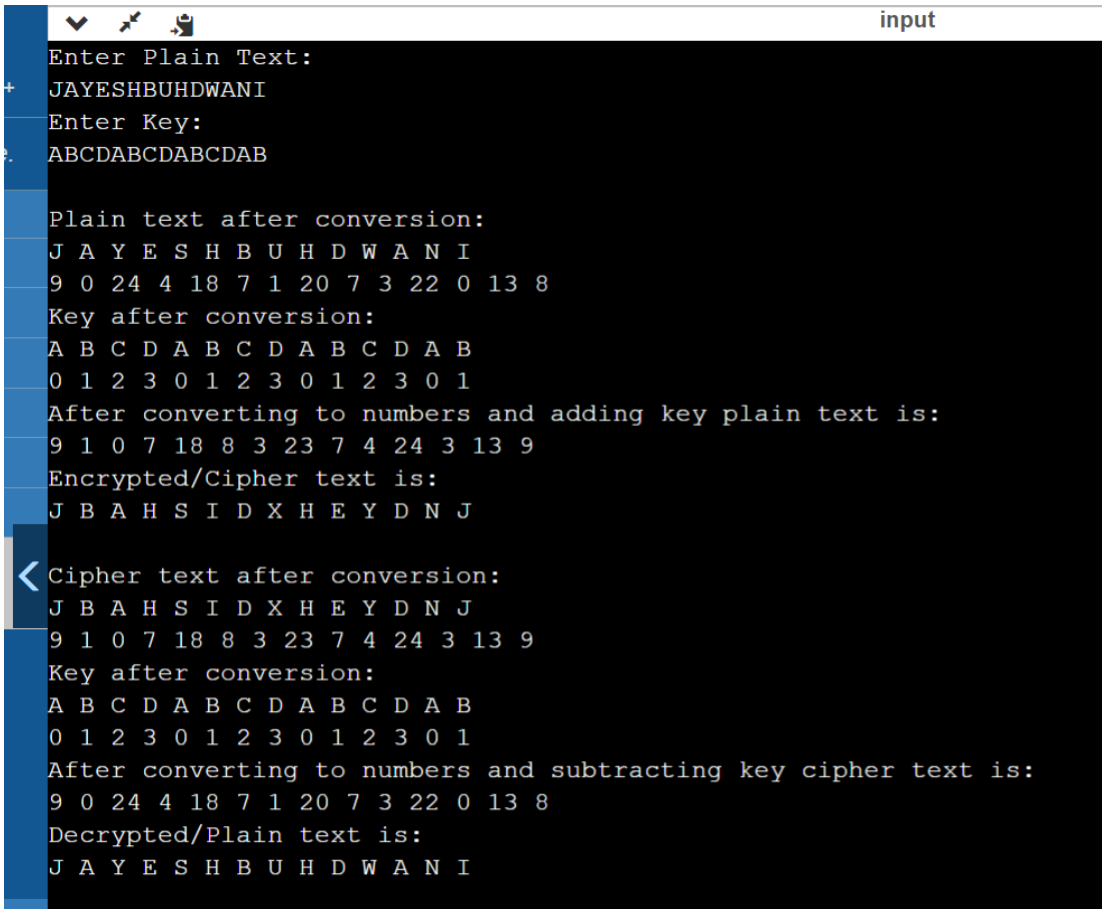
1. Convert the ciphertext and key from characters to numbers like **'a' -> 0, 'b -> 1,…., 'z' -> 25** and let us name them C and K for Plain text and key respectively.
2. Add then subtract C and K and if any subtraction is less than 0 add 26 to it.
3. This is the message sent by the sender.

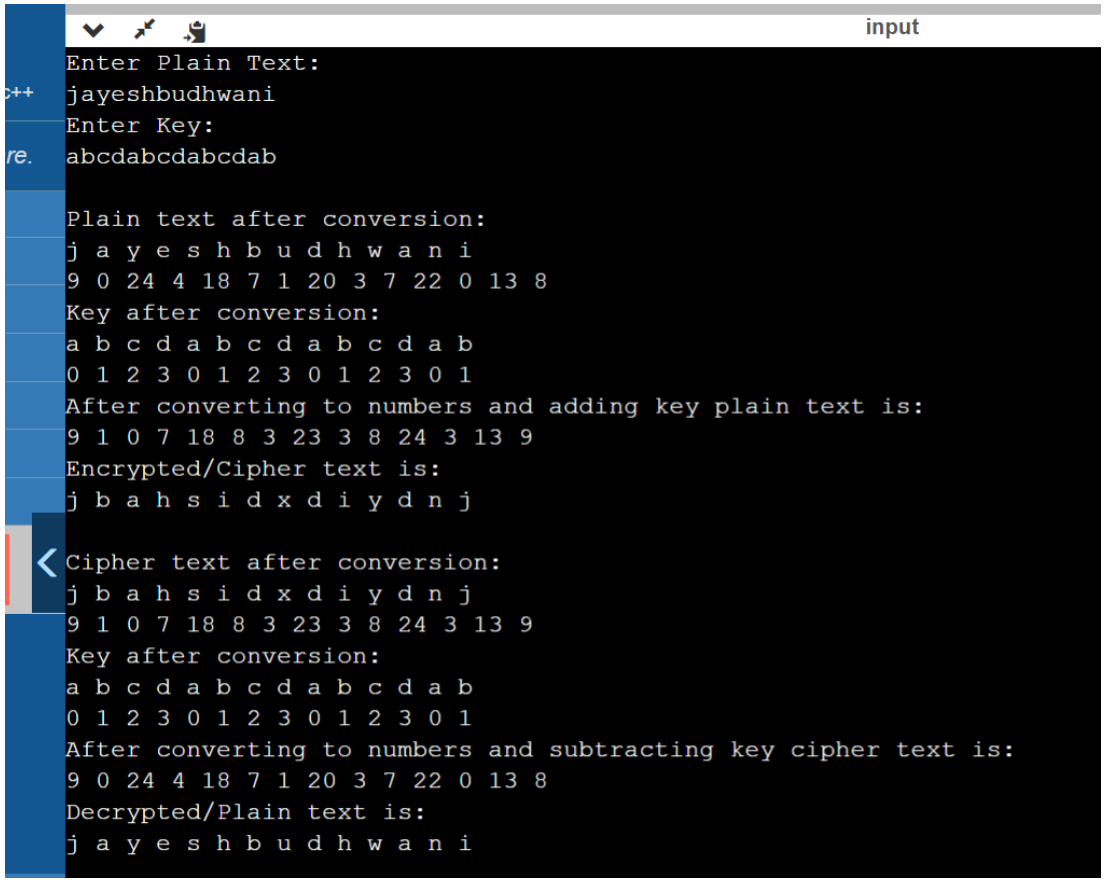
Code Implementation:

1. There are two functions **Encrypt** and **Decrypt** defined for encryption and decryption, which takes two strings message and key as input and provide the respective output string.
2. The two functions defined as Text_to_Numbers and Numbers_to_Text are defined to convert char to numbers and from numbers to char.
3. Finally, the conversion takes place as the algorithm is defined.

OUTPUTS




input
Enter Plain Text:
JAYESHBUHDWANI
Enter Key:
ABCDABCDABCDAB
Plain text after conversion:
J A Y E S H B U H D W A N I
9 0 24 4 18 7 1 20 7 3 22 0 13 8
Key after conversion:
A B C D A B C D A B C D A B
0 1 2 3 0 1 2 3 0 1 2 3 0 1
After converting to numbers and adding key plain text is:
9 1 0 7 18 8 3 23 7 4 24 3 13 9
Encrypted/Cipher text is:
J B A H S I D X H E Y D N J
Cipher text after conversion:
J B A H S I D X H E Y D N J
9 1 0 7 18 8 3 23 7 4 24 3 13 9
Key after conversion:
A B C D A B C D A B C D A B
0 1 2 3 0 1 2 3 0 1 2 3 0 1
After converting to numbers and subtracting key cipher text is:
9 0 24 4 18 7 1 20 7 3 22 0 13 8
Decrypted/Plain text is:
J A Y E S H B U H D W A N I


input
Enter Plain Text:
jayeshbudhwani
Enter Key:
abcdabcdabcdab
Plain text after conversion:
j a y e s h b u d h w a n i
9 0 24 4 18 7 1 20 3 7 22 0 13 8
Key after conversion:
a b c d a b c d a b c d a b
0 1 2 3 0 1 2 3 0 1 2 3 0 1
After converting to numbers and adding key plain text is:
9 1 0 7 18 8 3 23 3 8 24 3 13 9
Encrypted/Cipher text is:
j b a h s i d x d i y d n j
Cipher text after conversion:
j b a h s i d x d i y d n j
9 1 0 7 18 8 3 23 3 8 24 3 13 9
Key after conversion:
a b c d a b c d a b c d a b
0 1 2 3 0 1 2 3 0 1 2 3 0 1
After converting to numbers and subtracting key cipher text is:
9 0 24 4 18 7 1 20 3 7 22 0 13 8
Decrypted/Plain text is:
j a y e s h b u d h w a n i

PROGRAM:

```
#include<iostream>
#include<bits/stdc++.h>
using namespace std;
void print_vector(vector<int> v)
{
   for(int i=0;i<v.size()-1;i++)
   {
      cout<<v[i]<<" ";
   }
   cout<<v[v.size()-1]<<endl;
}
void print_string(string v)
{
   for(int i=0;i<v.size()-1;i++)
   {
      cout<<v[i]<<" ";
   }
   cout<<v[v.size()-1]<<endl;
}
vector<int> Text_to_Numbers(string x)
{
   int i;
   vector<int> t;
   for(i=0;i<x.size();i++)
   {
      if(x[i]>='A' && x[i]<='Z')
      t.push_back(x[i]-'A');
      else if(x[i]>='a' && x[i]<='z')
      t.push_back(x[i]-'a');
   }
   return t;
}
string Numbers_to_Text(vector<int> t,string x)
{
   int i;
   string s;
   for(i=0;i<t.size();i++)
   {
      if(x[i]>='A' && x[i]<='Z')
      s+=(char)(t[i]+'A');
      else if(x[i]>='a' && x[i]<='z')
      s+=(char)(t[i]+'a');
   }
   return s;
}
string Encrypt(string pl,string key)
{
   int i,sum;
   vector<int> p,k,d;
   string s;
   p=Text_to_Numbers(pl);
   k=Text_to_Numbers(key);
   for(i=0;i<p.size();i++)
   {
      sum=p[i]+k[i];
      if(sum>=26)
      sum=sum-26;
      d.push_back(sum);
```

```
    }
    cout<<"Plain text after conversion:"<<endl;
    print_string(pl);
    print_vector(p);
    cout<<"Key after conversion:"<<endl;
    print_string(key);
    print_vector(k);
    cout<<"After converting to numbers and adding key plain text is: "<<endl;
    print_vector(d);
    s=Numbers_to_Text(d,pl);
    return s;
}
string Decrypt(string ct,string key)
{
    int i,diff;
    vector<int> c,k,s;
    string s1;
    c=Text_to_Numbers(ct);
    k=Text_to_Numbers(key);
    for(i=0;i<c.size();i++)
    {
        diff=c[i]-k[i];
        if(diff<0)
        diff=diff+26;
        s.push_back(diff);
    }
    cout<<"Cipher text after conversion:"<<endl;
    print_string(ct);
    print_vector(c);
    cout<<"Key after conversion:"<<endl;
    print_string(key);
    print_vector(k);
    cout<<"After converting to numbers and subtracting key cipher text is: "<<endl;
    print_vector(s);
    s1=Numbers_to_Text(s,ct);
    return s1;
}
int main()
{
    string p,k,c,x;
    cout<<"Enter Plain Text:"<<endl;
    cin>>p;
    cout<<"Enter Key:"<<endl;
    cin>>k;
    cout<<endl;
    if(p.size()!=k.size())
    {
        cout<<"The Size of Key and Plain text do not match try again..."<<endl;
    }
    else
    {
        c=Encrypt(p,k);
        cout<<"Encrypted/Cipher text is: "<<endl;
        print_string(c);
        cout<<endl;
        x=Decrypt(c,k);
        cout<<"Decrypted/Plain text is: "<<endl;
        print_string(x);
        cout<<endl;
```

```
    }
    return 0;
}
```