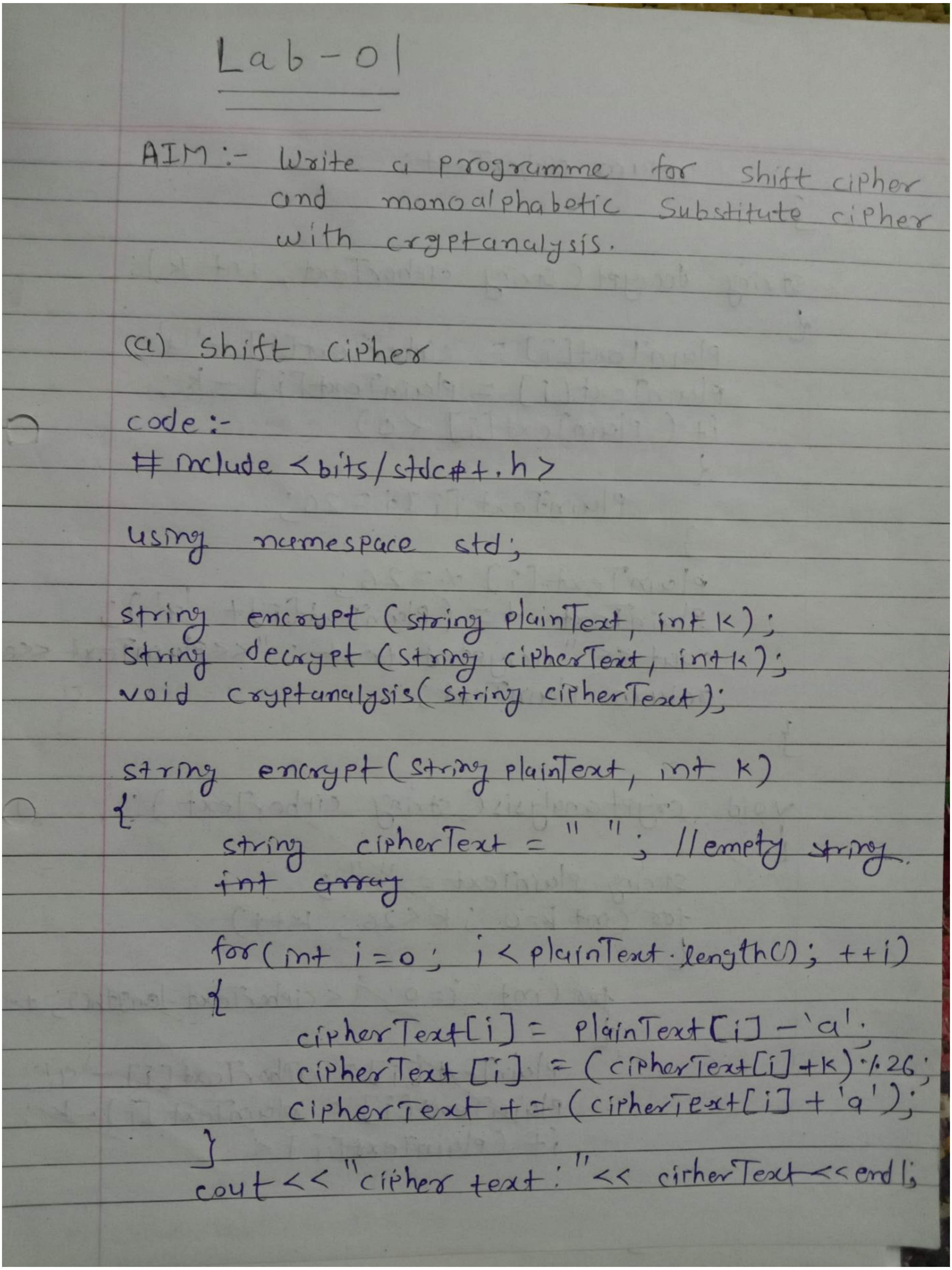


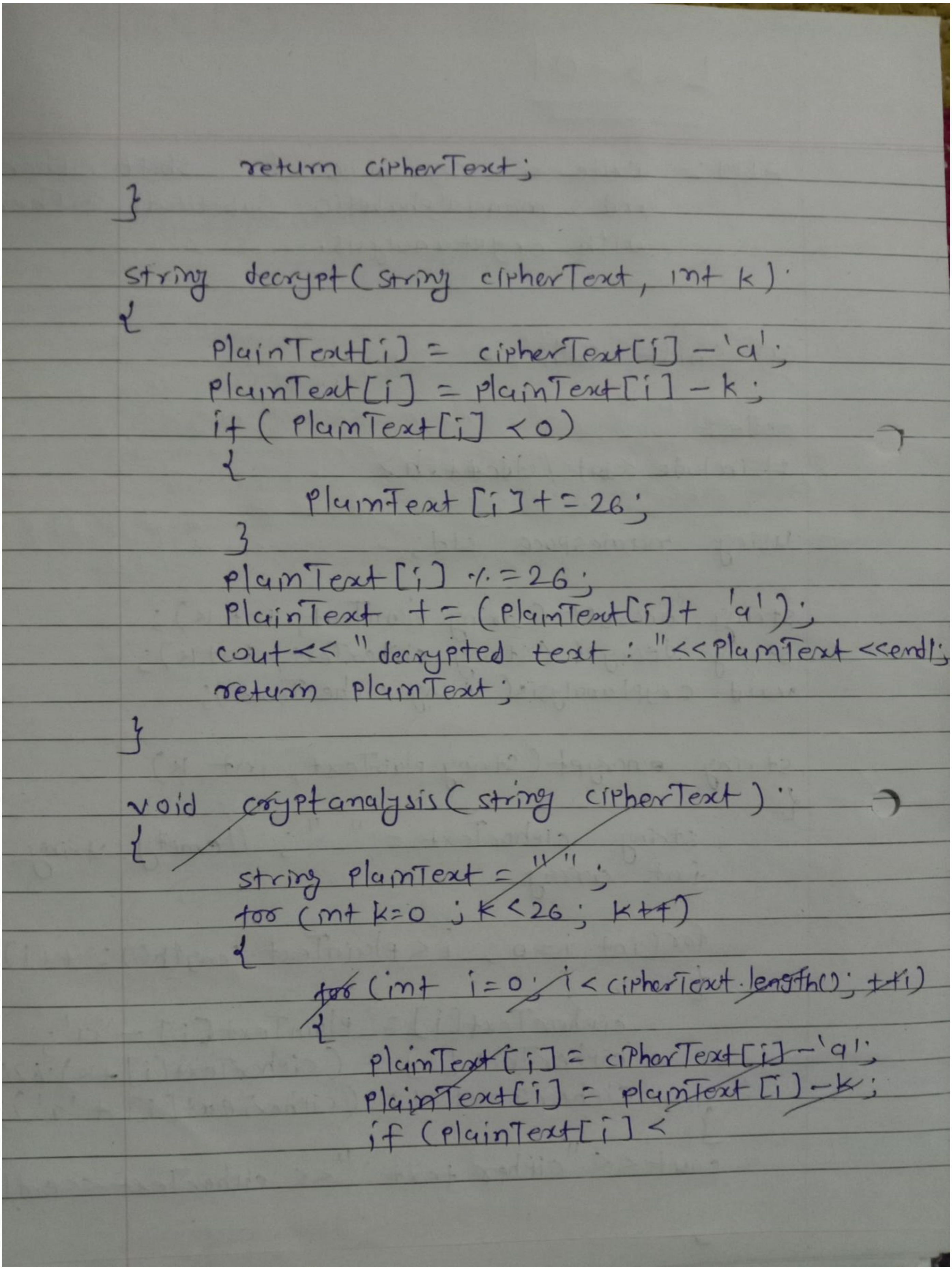
Lab-01

AIM :- Write a programme for shift cipher and monoalphabetic Substitute cipher with cryptanalysis.

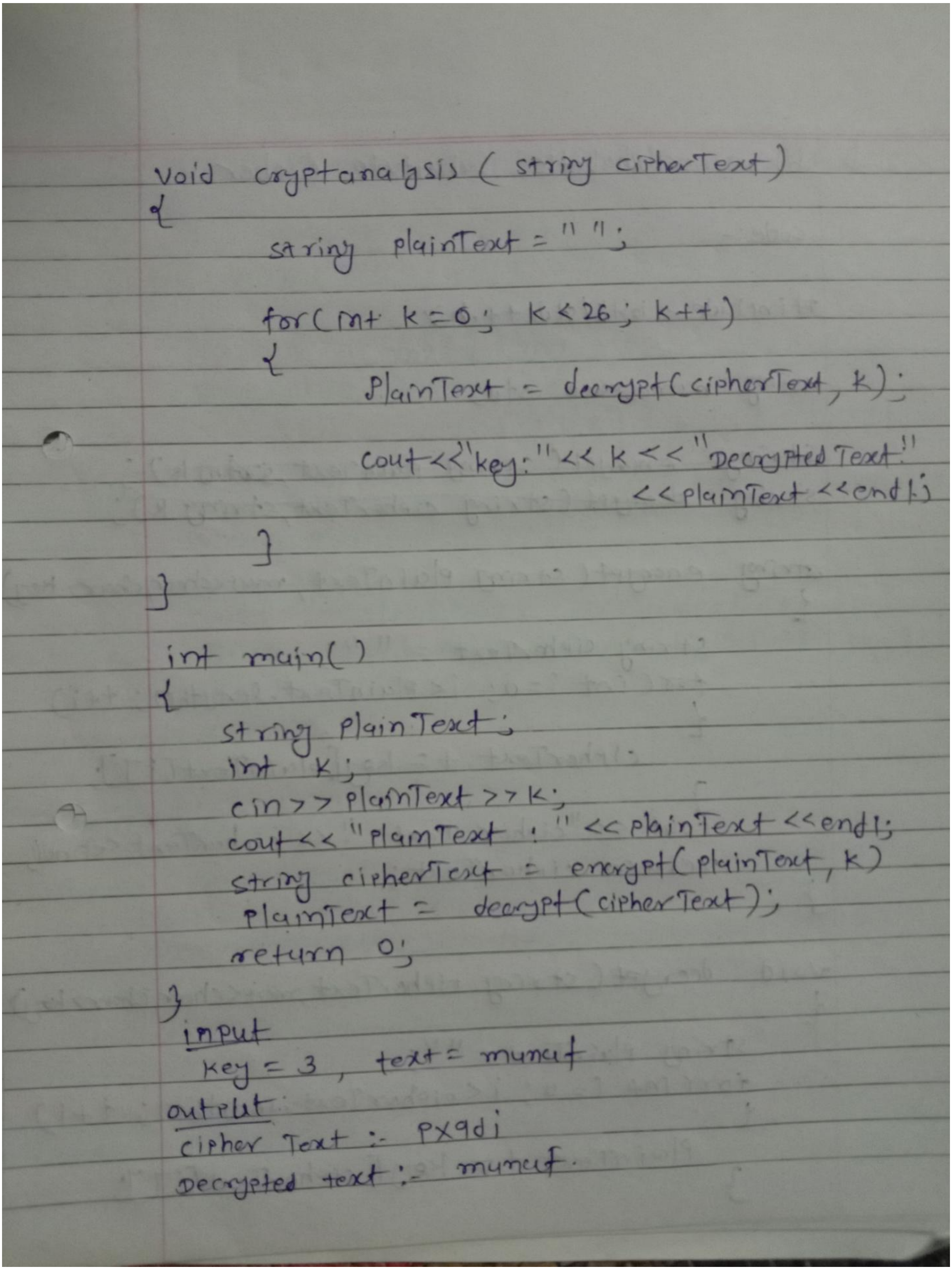
(a) Shift cipher

code:-

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

using namespace std;

string encrypt (string plainText, int k);
string decrypt (string cipherText, int k);
void cryptanalysis( string cipherText);

string encrypt(string plainText, int k)
{
        string cipherText = " "; //empty string.
        ~~int array~~

        for(int i=0; i<plainText.length(); ++i)
        {
                cipherText[i] = plainText[i] - 'a';
                cipherText[i] = (cipherText[i]+k)%26;
                cipherText += (cipherText[i] + 'a');
        }
        cout<< "cipher text:"<< cipherText<<endl;
```



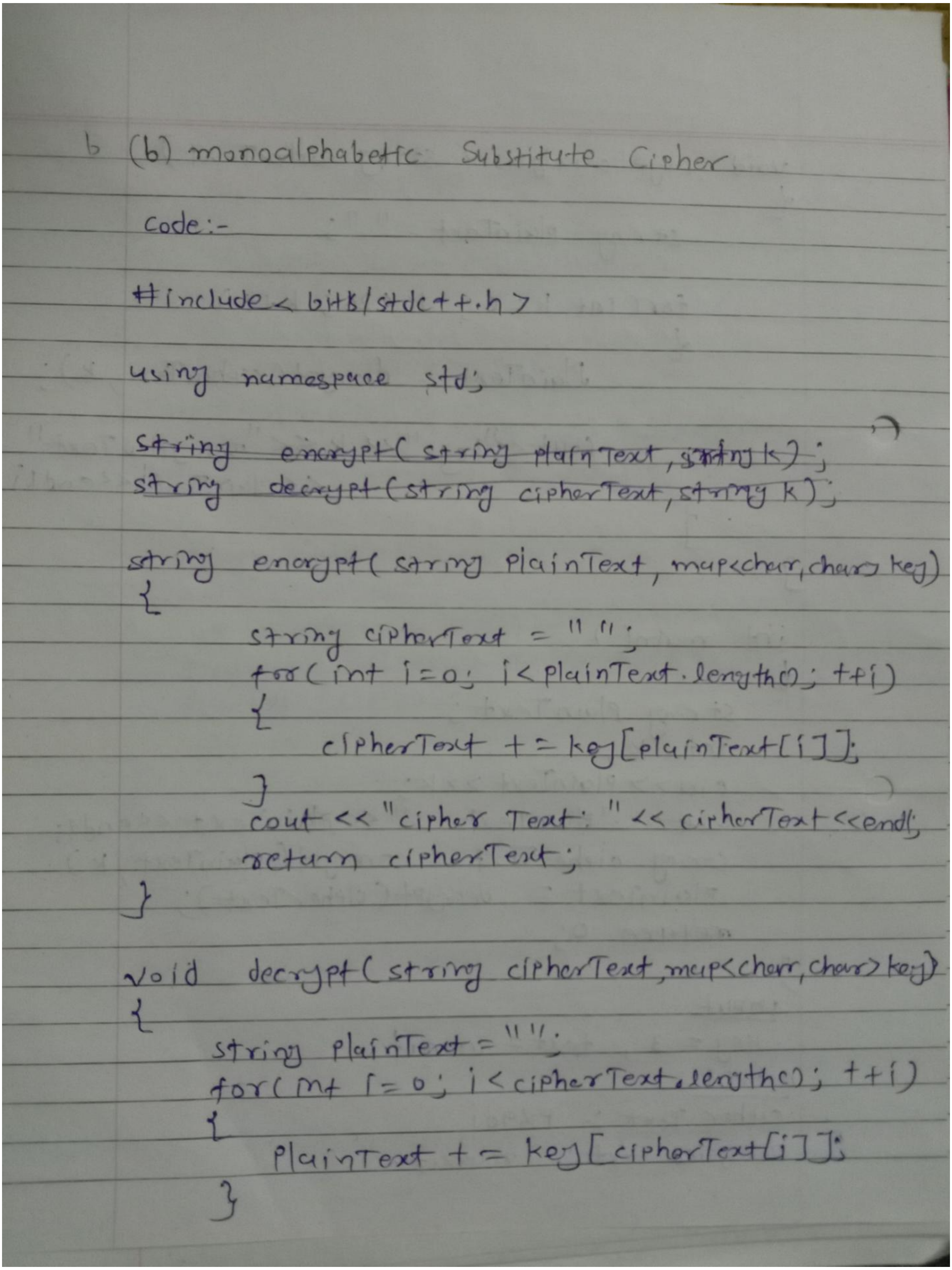
```
        return cipherText;
}

string decrypt(string cipherText, int k)
{
      PlainText[i] = cipherText[i] - 'a';
      plainText[i] = plainText[i] - k;
      if ( PlainText[i] < 0)
       {
           PlainText [i] += 26;
       }
       plainText[i] %= 26;
       PlainText += (PlainText[i] + 'a');
       cout<< "decrypted text : "<<PlainText <<endl;
       return plainText;
}

void cryptanalysis(string cipherText)
{
       string plainText = "";
       for (int k=0 ; k<26; k++)
       {
            for (int i=0; i<cipherText.length(); ++i)
            {
                 plainText[i] = ciphorText[i] - 'a';
                 plainText[i] = plainText[i] - k;
                 if (plainText[i] <
```



```
void cryptanalysis ( string cipherText)
{
        string plainText = " ";

        for(int k=0; k<26; k++)
        {
              PlainText = decrypt(cipherText, k);

              cout<<"key:"<< k << "Decrypted Text:"
                                   <<plainText <<endl;
        }
}

int main()
{
      string PlainText;
      int k;
      cin>>plainText>>k;
      cout<<"plainText : "<<plainText<<endl;
      string cipherText = encrypt(plainText, k)
      plainText = decrypt(cipherText);
      return 0;
}
```

input
key = 3, text = munaf

output
cipher Text :- pxqdi
Decrypted text :- munaf.



b (b) monoalphabetic Substitute Cipher

Code:-

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

using namespace std;

~~string encrypt(string plainText, string k);~~
string decrypt(string cipherText, string k);

string encrypt(string plainText, map<char,char> key)
{
        string cipherText = "";
        for(int i=0; i<plainText.length(); ++i)
        {
            cipherText += key[plainText[i]];
        }
        cout << "cipher Text: " << cipherText <<endl;
        return cipherText;
}

void decrypt(string cipherText, map<char, char> key)
{
    string plainText = "";
    for(int i = 0; i<cipherText.length(); ++i)
    {
        plainText += key[cipherText[i]];
    }
```

```
        cout<<"Decrypted text: "<<plainText<<endl;
}

int main()
{
   // this is a random key
   map<char,char> key{
                    {'a';'z'},{'b','y'},{'c';'x'},
                    {'d','w'},{'e''v'},.....
                    {'x','c'},{'y','b'},{'z','a'}};
   string plainText;
   cin>>plainText;
   cout<<"original msg: "<<plaintext<<endl;
   string cipherText = encrypt(PlainText,key);
   decrypt (cipherText, key);
   return 0;
}
```

Input: munaf

output:

```
Original text: munaf
Cipher text: nfmzu
Decrypted text: munaf.
```