Name: Rutikesh Sawant
Batch: B2
Subject: CNS Lab
PRN: 2019BTECS00034

Assignment 2

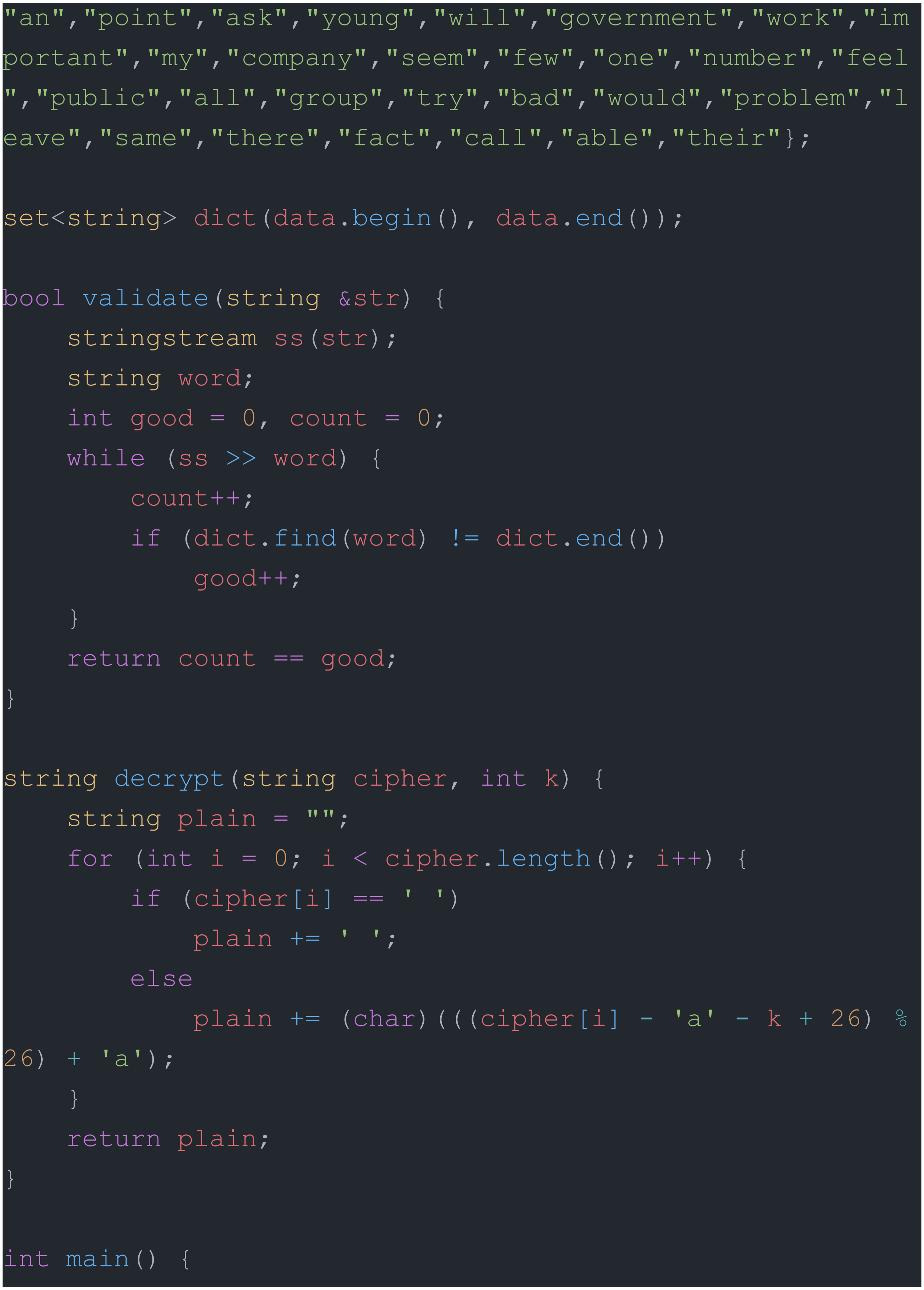
Aim: Given a cipher text which is encrypted using caesar cipher. Find plain text using cryptanalysis method.

Theory:

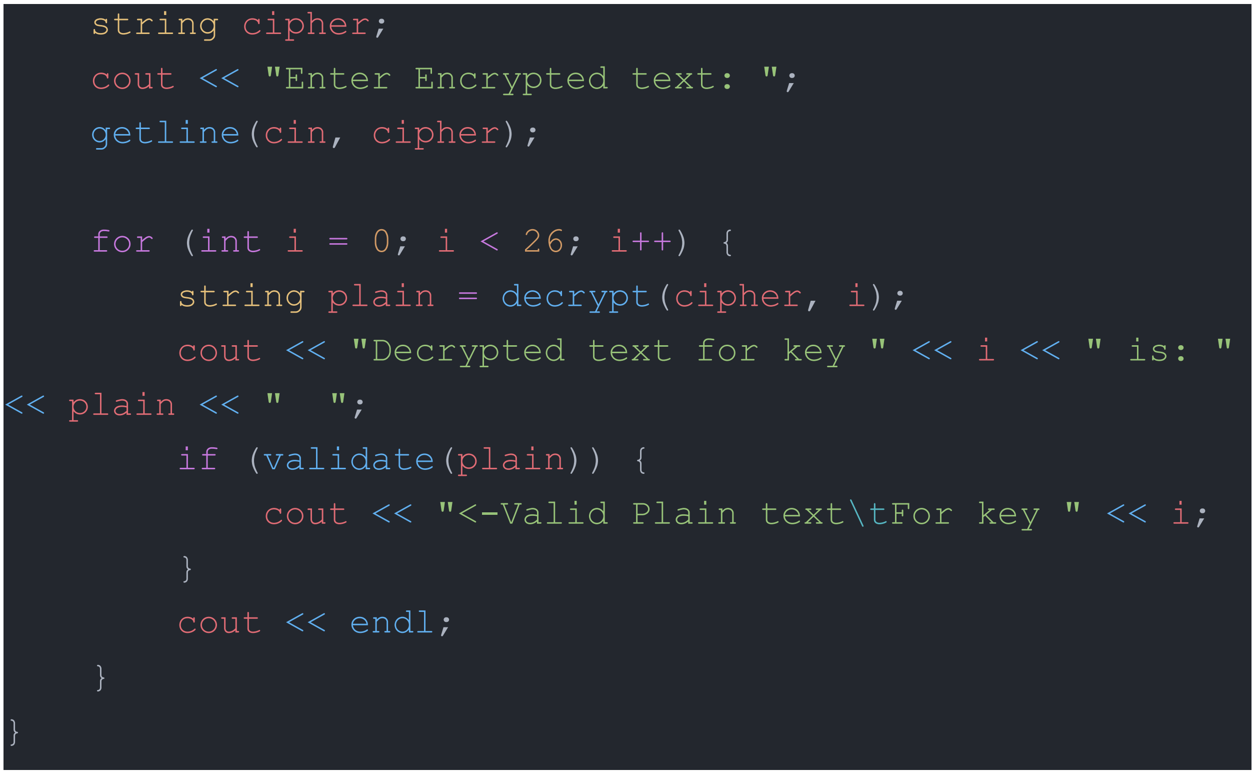
Caesar cipher is a substitution cipher in which we replace every character with another character in alphabetical order with a common difference.
Cryptanalysis is a technique in which we find a plain text from given cipher text and method of encryption.

Code:

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

vector<string> data =
{"time","be","good","am","to","the","person","have","new"
,"of","and","year","do","first","in","a","way","say","las
t","for","that","day","get","long","on","i","thing","make
","great","with","it","man","go","little","at","not","wor
ld","know","own","by","he","life","take","other","from","
as","hand","see","old","up","you","part","come","right","
about","this","child","think","big","into","but","eye","l
ook","high","over","his","woman","want","different","afte
r","they","place","give","small","her","work","use","larg
e","she","week","find","next","or","case","tell","early",
```

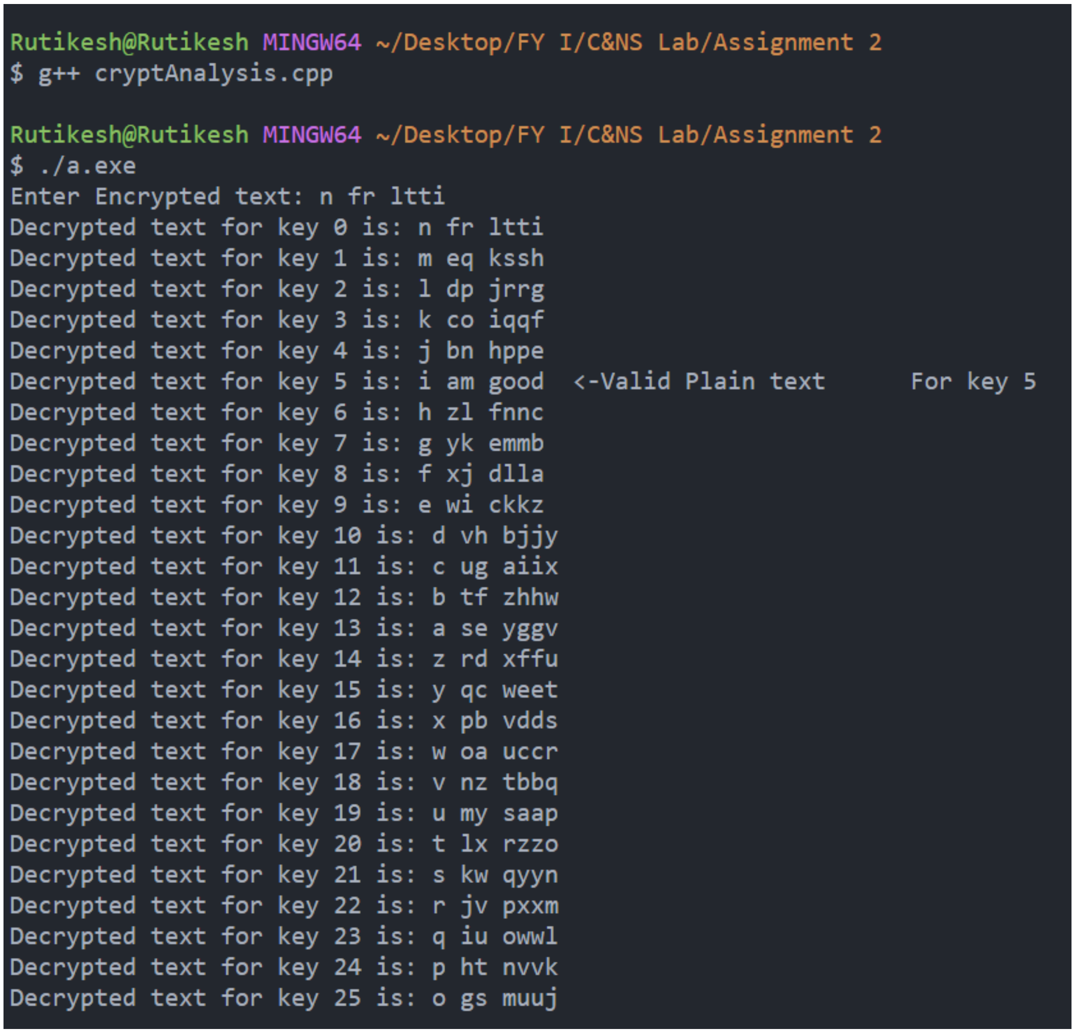


```
"an","point","ask","young","will","government","work","important","my","company","seem","few","one","number","feel","public","all","group","try","bad","would","problem","leave","same","there","fact","call","able","their"};

set<string> dict(data.begin(), data.end());

bool validate(string &str) {
    stringstream ss(str);
    string word;
    int good = 0, count = 0;
    while (ss >> word) {
        count++;
        if (dict.find(word) != dict.end())
            good++;
    }
    return count == good;
}

string decrypt(string cipher, int k) {
    string plain = "";
    for (int i = 0; i < cipher.length(); i++) {
        if (cipher[i] == ' ')
            plain += ' ';
        else
            plain += (char)(((cipher[i] - 'a' - k + 26) % 26) + 'a');
    }
    return plain;
}

int main() {
```



```
    string cipher;
    cout << "Enter Encrypted text: ";
    getline(cin, cipher);

    for (int i = 0; i < 26; i++) {
        string plain = decrypt(cipher, i);
        cout << "Decrypted text for key " << i << " is: "
<< plain << "  ";
        if (validate(plain)) {
            cout << "<-Valid Plain text\tFor key " << i;
        }
        cout << endl;
    }
}
```

Output:



```
Rutikesh@Rutikesh MINGW64 ~/Desktop/FY I/C&NS Lab/Assignment 2
$ g++ cryptAnalysis.cpp

Rutikesh@Rutikesh MINGW64 ~/Desktop/FY I/C&NS Lab/Assignment 2
$ ./a.exe
Enter Encrypted text: n fr ltti
Decrypted text for key 0 is: n fr ltti
Decrypted text for key 1 is: m eq kssh
Decrypted text for key 2 is: l dp jrrg
Decrypted text for key 3 is: k co iqqf
Decrypted text for key 4 is: j bn hppe
Decrypted text for key 5 is: i am good  <-Valid Plain text      For key 5
Decrypted text for key 6 is: h zl fnnc
Decrypted text for key 7 is: g yk emmb
Decrypted text for key 8 is: f xj dlla
Decrypted text for key 9 is: e wi ckkz
Decrypted text for key 10 is: d vh bjjy
Decrypted text for key 11 is: c ug aiix
Decrypted text for key 12 is: b tf zhhw
Decrypted text for key 13 is: a se yggv
Decrypted text for key 14 is: z rd xffu
Decrypted text for key 15 is: y qc weet
Decrypted text for key 16 is: x pb vdds
Decrypted text for key 17 is: w oa uccr
Decrypted text for key 18 is: v nz tbbq
Decrypted text for key 19 is: u my saap
Decrypted text for key 20 is: t lx rzzo
Decrypted text for key 21 is: s kw qyyn
Decrypted text for key 22 is: r jv pxxm
Decrypted text for key 23 is: q iu owwl
Decrypted text for key 24 is: p ht nvvk
Decrypted text for key 25 is: o gs muuj
```