Final Year B. Tech., Sem VII 2022-23

Cryptography And Network Security

PRN/ Roll No: 2020BTECS00206

Full Name: SAYALI YOGESH DESAI

Batch: B4

Assignment No. 2

---

1. **Aim:**

   Given a cipher text, encrypted Caesar using, cryptanalysis find the plain text.

2. **Theory:**

   Caesar Cipher: It is a substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet We will decrypt using all the possible key, and find the most relative plain text.

3. **Code:**

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

using namespace std;

int main()

{

set<string> dict;

dict.insert("i");

dict.insert("am");

dict.insert("in");

dict.insert("cns");

dict.insert("lab");

dict.insert("for");

dict.insert("LA");

string s, org;
```

```cpp
cout << "Enter Cipher text" << endl;

getline(cin, s);

string x;

int k = 0;

cout << "\nCipher text is: " << s << endl << endl;

org = s;

for (int k = 0; k < 26; k++)

{

cout << "Keep Key as: " << k << endl;

s = org;

string word = "";

int flg = 0;

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

{

if (s[i] == ' ')

{

if (dict.find(word) == dict.end())

{

flg = 1;

break;

}

word = "";

continue;

}

int val = s[i] - 'a';

val = (val - k + 26) % 26;

char ch = 'a' + val;
```

```
word += ch;

s[i] = ch;

}

if (dict.find(word) == dict.end())

{

flg = 1;

}

if (flg == 0)

cout << s << endl << endl;

}

}
```
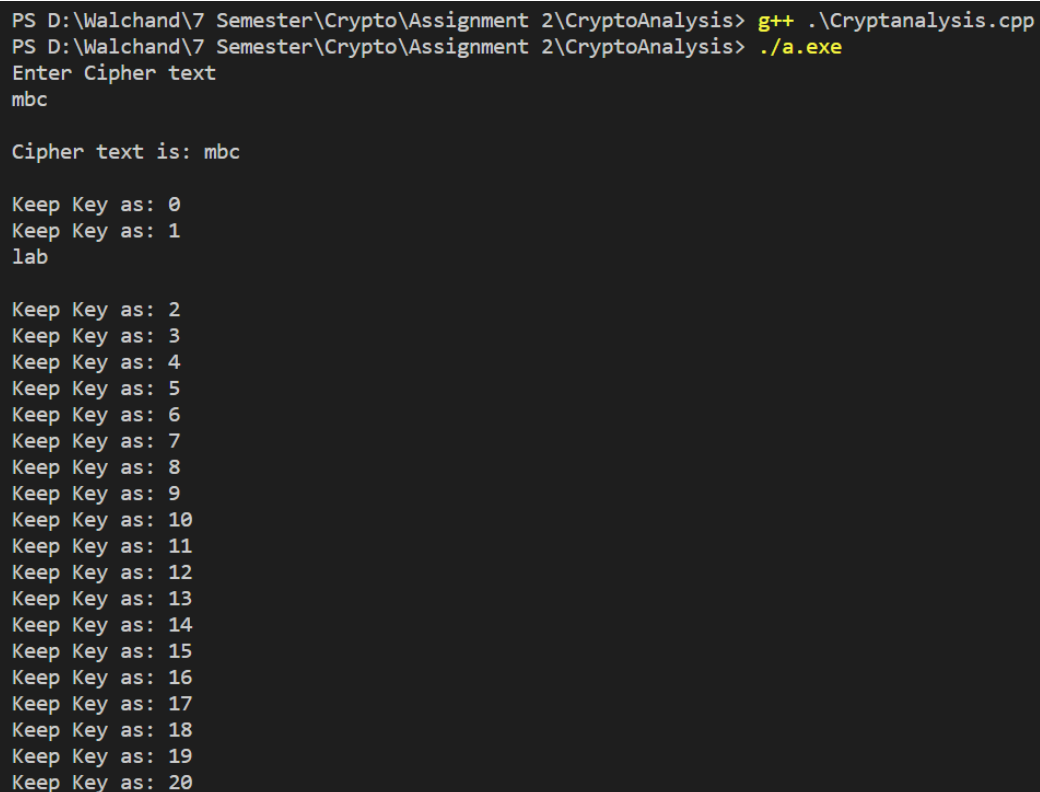
4. **Output:**

```
PS D:\Walchand\7 Semester\Crypto\Assignment 2\CryptoAnalysis> g++ .\Cryptanalysis.cpp
PS D:\Walchand\7 Semester\Crypto\Assignment 2\CryptoAnalysis> ./a.exe
Enter Cipher text
mbc

Cipher text is: mbc

Keep Key as: 0
Keep Key as: 1
lab

Keep Key as: 2
Keep Key as: 3
Keep Key as: 4
Keep Key as: 5
Keep Key as: 6
Keep Key as: 7
Keep Key as: 8
Keep Key as: 9
Keep Key as: 10
Keep Key as: 11
Keep Key as: 12
Keep Key as: 13
Keep Key as: 14
Keep Key as: 15
Keep Key as: 16
Keep Key as: 17
Keep Key as: 18
Keep Key as: 19
Keep Key as: 20
```

5. **Conclusion:**

Successfully decrypted the cipher text and displayed plain text using cryptanalysis.