Final Year B. Tech. (CSE) – I: 2022-23

4CS451: Cryptography and Network Security Lab

Assignment No. 2

PRN: 2019BTECS00077 **Batch: B7**

Full name: Biradar Avinash Vishnu

Title: Cryptanalysis of Caesar cipher algorithm.

Objective: Crack the given code and output the corresponding plain text.

Introduction & Theory:

In this we have write a code to crack the given Cipher Text where key is not provided and produce Output as plain Text.

Steps I have done:

1) I have taken a text file of 10000 English common words.
2) Produces the 25 possibilities and calculated the associated score of each possibility.
3) The max score possibility plain text is our expected ans.

Code:

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

unordered_set<string> uset;


// Capitalize the string
void capitalize(string &str){
    for(char &c:str){
      if(c>=97 && c<=122)
        c-=32;
    }
}

int score(string text){
```

```
  string word="";
  int score=0;
  for(char &c:text){
    if(c==32){
        if(uset.find(word)!=uset.end())
           score++;
        word.clear();
        continue;
      }
      word.push_back(c);
    }
    if(uset.find(word)!=uset.end())
        score++;
    return score;
}

void decryptCrackit(string &cypherText){

  string ans="";
  int maxScore=0;
  for(int i=0;i<26;i++){
    string tmp=cypherText;
    for(char &c:tmp){
      if(c==32)
        continue;
      c=((c-'A'-i+26)%26+'A');
    }
    if(score(tmp) > maxScore){
       maxScore=score(tmp);
       ans=tmp;
    }
    cout<<i<<": "<<tmp<<" "<<score(tmp)<<"\n";
  }

  cout<<"\n\nFinal output of crack the code:\n"<<ans<<endl;
}

string encrypt(string plainText,int pos){

   int n=plainText.size();
   for(int i=0;i<n;i++){
      if(plainText[i]==32)
        continue;
      if(plainText[i]>96 && plainText[i]<=122)
         plainText[i]-=32;
      plainText[i]+=pos;
```

```
      if(plainText[i]>90)
         plainText[i]=(plainText[i]%90+64);
   }
   cout<<"\nCypher Text :\n"<<plainText<<"\n\n";
   return plainText;
}


int main(){

    freopen("input.txt", "r", stdin);
    freopen("output.txt", "w", stdout);

    string plainText;
    getline(cin,plainText);
    capitalize(plainText);
    int pos;
    cin>>pos;

    string cypherText=encrypt(plainText,pos);

    ifstream file;
    file.open ("words.txt");

    string word;
    while (file >> word){
      capitalize(word);
      uset.insert(word);
    }
    decryptCrackit(cypherText);

    return 0;
}
```

Result:
File input output:

input.txt

```
is this algorithm is correct
28
```

output.txt

```

Cypher Text :
KU VJKU CNIQTKVJO KU EQTTGEV

0: KU VJKU CNIQTKVJO KU EQTTGEV 0
1: JT UIJT BMHPSJUIN JT DPSSFDU 0
2: IS THIS ALGORITHM IS CORRECT 5
3: HR SGHR ZKFNQHSGL HR BNQQDBS 2
4: GQ RFGQ YJEMPGRFK GQ AMPPCAR 0
5: FP QEFP XIDLOFQEJ FP ZLOOBZQ 2
6: EO PDEO WHCKNEPDI EO YKNNAYP 0
7: DN OCDN VGBJMDOCH DN XJMMZXO 0
8: CM NBCM UFAILCNBG CM WILLYWN 2
9: BL MABL TEZHKBMAF BL VHKKXVM 2
10: AK LZAK SDYGJALZE AK UGJJWUL 2
11: ZJ KYZJ RCXFIZKYD ZJ TFIIVTK 0
12: YI JXYI QBWEHYJXC YI SEHHUSJ 0
13: XH IWXH PAVDGXIWB XH RDGGTRI 0
14: WG HVWG OZUCFWHVA WG QCFFSQH 0
15: VF GUVF NYTBEVGUZ VF PBEERPG 0
16: UE FTUE MXSADUFTY UE OADDQOF 0
17: TD ESTD LWRZCTESX TD NZCCPNE 2
18: SC DRSC KVQYBSDRW SC MYBBOMD 2
19: RB CQRB JUPXARCQV RB LXAANLC 2
20: QA BPQA ITOWZQBPU QA KWZZMKB 0
21: PZ AOPZ HSNVYPAOT PZ JVYYLJA 0
```

```
22: OY ZNOY GRMUXOZNS OY IUXXKIZ 0
23: NX YMNX FQLTWNYMR NX HTWWJHY 0
24: MW XLMW EPKSVMXLQ MW GSVVIGX 2
25: LV WKLV DOJRULWKP LV FRUUHFW 0


Final output of crack the code:
IS THIS ALGORITHM IS CORRECT

```

Console Input Output:

```
PS E:\College\Final year\C&NS\practical> cd "e:\College\Final year\C&NS\p
} ; if ($?) { .\Cryptanalysis }
Department of CSE walchand college of engineering sangli
7

Cypher Text :
KLWHYATLUA VM JZL DHSJOHUK JVSSLNL VM LUNPULLYPUN ZHUNSP

0: KLWHYATLUA VM JZL DHSJOHUK JVSSLNL VM LUNPULLYPUN ZHUNSP 0
1: JKVGXZSKTZ UL IYK CGRINGTJ IURRKMK UL KTMOTKKXOTM YGTMRO 2
2: IJUFWYRJSY TK HXJ BFQHMFSI HTQQJLJ TK JSLNSJJWNSL XFSLQN 0
3: HITEVXQIRX SJ GWI AEPGLERH GSPPIKI SJ IRKMRIIVMRK WERKPM 0
4: GHSDUWPHQW RI FVH ZDOFKDQG FROOHJH RI HQJLQHHULQJ VDQJOL 2
5: FGRCTVOGPV QH EUG YCNEJCPF EQNNGIG QH GPIKPGGTKPI UCPINK 0
6: EFQBSUNFOU PG DTF XBMDIBOE DPMMFHF PG FOHJOFFSJOH TBOHMJ 2
7: DEPARTMENT OF CSE WALCHAND COLLEGE OF ENGINEERING SANGLI 5
8: CDOZQSLDMS NE BRD VZKBGZMC BNKKDFD NE DMFHMDDQHMF RZMFKH 2
9: BCNYPRKCLR MD AQC UYJAFYLB AMJJCEC MD CLEGLCCPGLE QYLEJG 2
10: ABMXOQJBKQ LC ZPB TXIZEXKA ZLIIBDB LC BKDFKBBOFKD PXKDIF 2
```

```
11: ZALWNPIAJP KB YOA SWHYDWJZ YKHHACA KB AJCEJAANEJC OWJCHE 2
12: YZKVMOHZIO JA XNZ RVGXCVIY XJGGZBZ JA ZIBDIZZMDIB NVIBGD 2
13: XYJULNGYHN IZ WMY QUFWBUHX WIFFYAY IZ YHACHYYLCHA MUHAFC 0
14: WXITKMFXGM HY VLX PTEVATGW VHEEXZX HY XGZBGXXKBGZ LTGZEB 0
15: VWHSJLEWFL GX UKW OSDUZSFV UGDDWYW GX WFYAFWWJAFY KSFYDA 0
16: UVGRIKDVEK FW TJV NRCTYREU TFCCVXV FW VEXZEVVIZEX JREXCZ 2
17: TUFQHJCUDJ EV SIU MQBSXQDT SEBBUWU EV UDWYDUUHYDW IQDWBY 2
18: STEPGIBTCI DU RHT LPARWPCS RDAATVT DU TCVXCTTGXCV HPCVAX 2
19: RSDOFHASBH CT QGS KOZQVOBR QCZZSUS CT SBUWBSSFWBU GOBUZW 2
20: QRCNEGZRAG BS PFR JNYPUNAQ PBYYRTR BS RATVARREVAT FNATYV 2
21: PQBMDFYQZF AR OEQ IMXOTMZP OAXXQSQ AR QZSUZQQDUZS EMZSXU 2
22: OPALCEXPYE ZQ NDP HLWNSLYO NZWWPRP ZQ PYRTYPPCTYR DLYRWT 0
23: NOZKBDWOXD YP MCO GKVMRKXN MYVVOQO YP OXQSXOOBSXQ CKXQVS 0
24: MNYJACVNWC XO LBN FJULQJWM LXUUNPN XO NWPRWNNARWP BJWPUR 0
25: LMXIZBUMVB WN KAM EITKPIVL KWTTMOM WN MVOQVMMZQVO AIVOTQ 2


Final output of crack the code:
DEPARTMENT OF CSE WALCHAND COLLEGE OF ENGINEERING SANGLI
```