# INTRODUCTION TO CRYPTOGRAPHY – PROJECT 2

## B.Tech. Computer Science and Engineering (Cybersecurity)

| | |
|---|---|
| Name: Anish Sudhan Nair | Roll No.: K041 |
| Batch: K2/A2 | Date of submission: 12/12/2021 |

**Code:**

Language: C

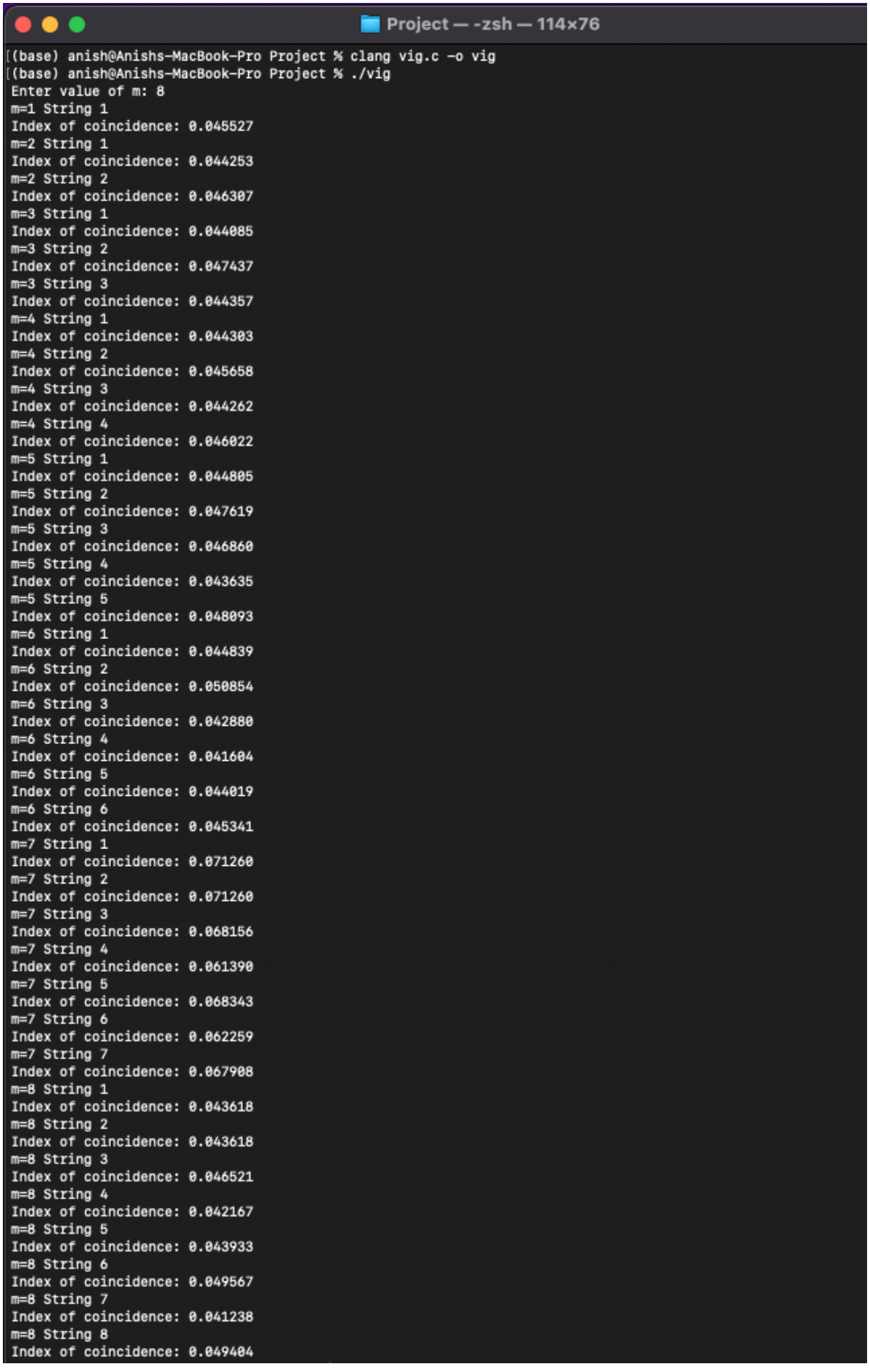
Editor: Atom

Compiler: clang/ZSH

Part 1: Verification of keyword length assumption through Index of Coincidences method

IMAGE ON NEXT PAGE

Via the diagram we can confirm that the Indices of the strings of m=7 are much closer to 0.065 than those of any other string.


Project — -zsh — 114×76
[(base) anish@Anishs-MacBook-Pro Project % clang vig.c -o vig
[(base) anish@Anishs-MacBook-Pro Project % ./vig
Enter value of m: 8
m=1 String 1
Index of coincidence: 0.045527
m=2 String 1
Index of coincidence: 0.044253
m=2 String 2
Index of coincidence: 0.046307
m=3 String 1
Index of coincidence: 0.044085
m=3 String 2
Index of coincidence: 0.047437
m=3 String 3
Index of coincidence: 0.044357
m=4 String 1
Index of coincidence: 0.044303
m=4 String 2
Index of coincidence: 0.045658
m=4 String 3
Index of coincidence: 0.044262
m=4 String 4
Index of coincidence: 0.046022
m=5 String 1
Index of coincidence: 0.044805
m=5 String 2
Index of coincidence: 0.047619
m=5 String 3
Index of coincidence: 0.046860
m=5 String 4
Index of coincidence: 0.043635
m=5 String 5
Index of coincidence: 0.048093
m=6 String 1
Index of coincidence: 0.044839
m=6 String 2
Index of coincidence: 0.050854
m=6 String 3
Index of coincidence: 0.042880
m=6 String 4
Index of coincidence: 0.041604
m=6 String 5
Index of coincidence: 0.044019
m=6 String 6
Index of coincidence: 0.045341
m=7 String 1
Index of coincidence: 0.071260
m=7 String 2
Index of coincidence: 0.071260
m=7 String 3
Index of coincidence: 0.068156
m=7 String 4
Index of coincidence: 0.061390
m=7 String 5
Index of coincidence: 0.068343
m=7 String 6
Index of coincidence: 0.062259
m=7 String 7
Index of coincidence: 0.067908
m=8 String 1
Index of coincidence: 0.043618
m=8 String 2
Index of coincidence: 0.043618
m=8 String 3
Index of coincidence: 0.046521
m=8 String 4
Index of coincidence: 0.042167
m=8 String 5
Index of coincidence: 0.043933
m=8 String 6
Index of coincidence: 0.049567
m=8 String 7
Index of coincidence: 0.041238
m=8 String 8
Index of coincidence: 0.049404

Part 2:

```
Enter correct length of keyword to continue : 7

Table:
g       Vg1             Vg2             Vg3             Vg4             Vg5             Vg6             Vg7
0       0.0407          0.0331          0.0453          0.0409          0.0476          0.0312          0.0350
1       0.0355          0.0377          0.0354          0.0386          0.0351          0.0396          0.0386
2       0.0369          0.0354          0.0314          0.0428          0.0324          0.0400          0.0323
3       0.0425          0.0313          0.0370          0.0333          0.0379          0.0477          0.0392
4       0.0662          0.0338          0.0666          0.0440          0.0672          0.0362          0.0432
5       0.0375          0.0432          0.0393          0.0396          0.0391          0.0442          0.0362
6       0.0334          0.0444          0.0322          0.0461          0.0352          0.0389          0.0402
7       0.0327          0.0378          0.0296          0.0366          0.0301          0.0460          0.0411
8       0.0400          0.0423          0.0410          0.0363          0.0407          0.0355          0.0471
9       0.0298          0.0423          0.0318          0.0294          0.0286          0.0367          0.0407
10      0.0350          0.0408          0.0371          0.0351          0.0380          0.0319          0.0364
11      0.0362          0.0380          0.0381          0.0421          0.0394          0.0352          0.0298
12      0.0331          0.0333          0.0368          0.0365          0.0318          0.0358          0.0352
13      0.0361          0.0308          0.0376          0.0425          0.0349          0.0335          0.0404
14      0.0397          0.0373          0.0405          0.0303          0.0410          0.0402          0.0354
15      0.0493          0.0361          0.0468          0.0350          0.0483          0.0319          0.0412
16      0.0405          0.0365          0.0389          0.0412          0.0391          0.0384          0.0337
17      0.0415          0.0441          0.0424          0.0628          0.0429          0.0415          0.0304
18      0.0383          0.0344          0.0384          0.0356          0.0384          0.0637          0.0350
19      0.0491          0.0284          0.0440          0.0319          0.0425          0.0383          0.0656
20      0.0379          0.0402          0.0376          0.0352          0.0381          0.0350          0.0427
21      0.0339          0.0683          0.0334          0.0465          0.0338          0.0314          0.0314
22      0.0305          0.0417          0.0342          0.0342          0.0339          0.0425          0.0289
23      0.0406          0.0311          0.0388          0.0337          0.0363          0.0345          0.0509
24      0.0306          0.0337          0.0341          0.0370          0.0353          0.0365          0.0350
25      0.0336          0.0451          0.0328          0.0339          0.0335          0.0347          0.0355


Keyword:
EVEREST
```

Keyword: Everest

Part 3: Plaintext

```
The plain text is: thedepartmentofjusticehasbeenandwillalwaysbecommittedtoprotectingthelibertyandsecurityofthosewhomweservei
nrecentmonthshoweverwehaveonanewscaleseenmainstreamproductsandservicesdesignedinawaythatgivesuserssolecontroloveraccesstothe
irdataasaresultlawenforcementissometimesunabletorecoverthecontentofelectroniccommunicationsfromthetechnologyprovidereveninre
sponsetoacourtorderorduly authorizedwarrantissuedbyafederaljudgeforexamplemanycommunicationsservicesnowencryptcertaincommunic
ationsbydefaultwiththekeynecessarytodecryptthecommunicationssolelyinthehandsoftheenduserthisappliesbothwhenthedataisinmotion
overelectronicnetworksoratrestonanelectronicdeviceifthecommunicationsproviderisservedwithawarrantseekingthosecommunicationst
heprovidercannotprovidethedatabecauseithasdesignedthetechnologysuchthatitcannotbeaccessedbyanythirdpartywedonothaveanysilver
bulletsandthediscussionswithintheexecutivebrancharestillongoingwhiletherehasnotyetbeenadecisionwhethertoseeklegislationwemus
tworkwithcongressindustryacademicsprivacygroupsandotherstocraftanapproachthataddressesallofthemultiplecompetingconcernsthath
avebeenthefocusofsomuchdebatebutwecanallagreethatwewillneedongoinghonestandinformedpublicdebateabouthowbesttoprotectlibertya
ndsecurityinbothourlawsandourtechnology
```

<u>Formatted Plaintext:</u>

The department of justice has been and will always be committed to protecting the liberty and security of those whom we serve. In recent months, however, we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data. As a result, law enforcement is sometimes unable to recover the content of electronic communications from the technology provider even in response to a court order or duly authorized warrant issued by a federal judge. For example, many communications services now encrypt certain communications by default, with the key necessary to decrypt the communications solely in the hands of the end user. This applies both when the data is in motion over electronic networks, or at rest on an electronic device. If the communications provider is served with a warrant seeking those communications, the provider cannot provide the data because it has designed the technology such that it cannot be accessed by any third party. We do not have any silver bullets and the discussions within the executive branch are still ongoing. While there has not yet been a decision whether to seek legislation, we must work with congress, industry, academics, privacy groups and others to craft an approach that addresses all of the multiple, competing concerns that have been the focus of so much debate. But we can all agree that we will need ongoing honest and informed public debate about how best to protect liberty and security in both our laws and our technology.

## Code:

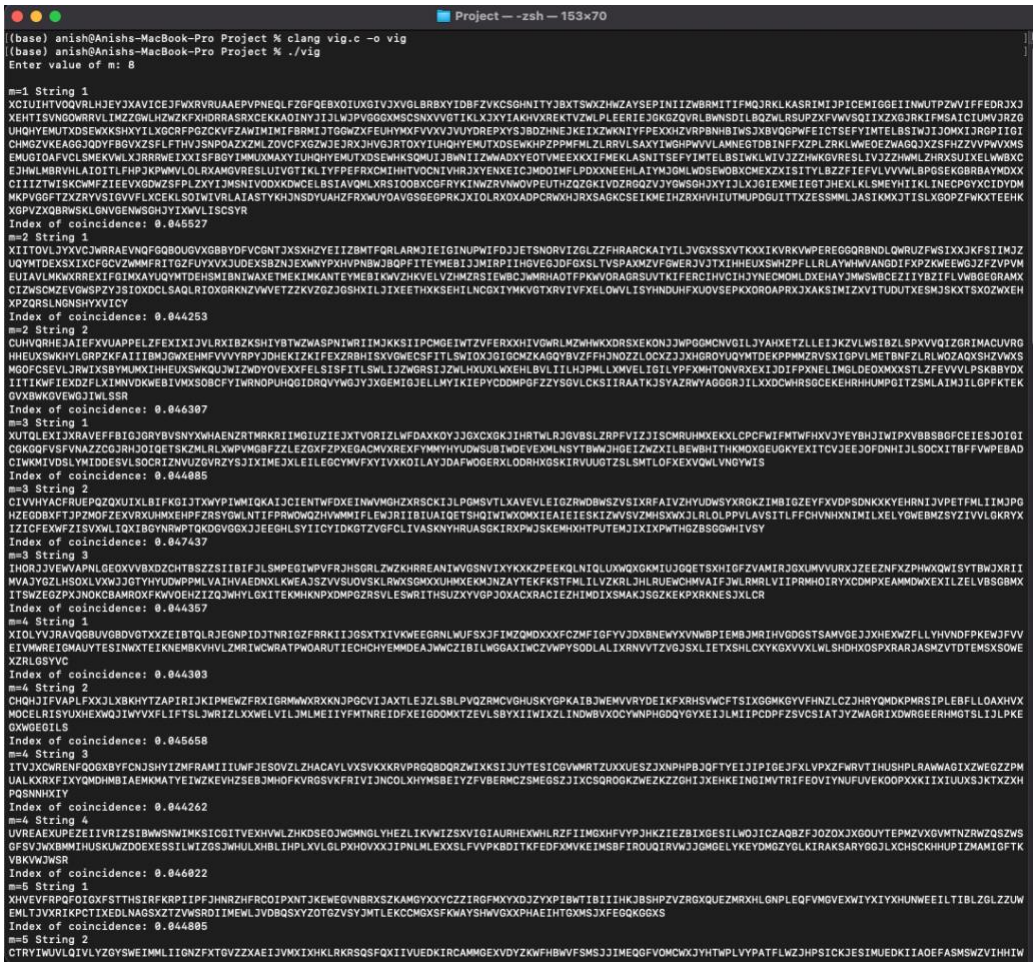
```c
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <ctype.h>
char
cipher_text[]="XCIUIHTVOQVRLHJEYJXAVICEJFWXRVRUAAEPVPNEQLFZGFQEBXOIUXGIVJXVGLBRBXYIDBFZVKCSGHNITYJBXTSWXZHWZAYSEPINIIZWBRMITIFMQJ
RKLKASRIMIJPICEMIGGEIINWUTPZWVIFFEDRJXJXEHTISVNGOWRRVLIMZZGWLHZWZKFXHDRRASRXCEKKAOINYJIJLWJPVGGGXMSCSNXVVGTIKLXJXYIAKHVXREKTVZWLP
LEERIEJGKGZQVRLBWNSDILBQZWLRSUPZXFVWVSQIIXZXGJRKIFMSAICIUMVJRZGUHQHYEMUTXDSEWXKSHXYILXGCRFPGZCKVFZAWIMIMIFBRMIJTGGWZXFEUHYMXFVVXV
JVUYDREPXYSJBDZHNEJKEIXZWKNIYFPEXXHZVRPBNHBIWSJXBVQGPWFEICTSEFYIMTELBSIWJIJOMXIJRGPIIGICHMGZVKEAGGJQDYFBGVXZSFLFTHVJSNPOAZXZMLZOV
CFXGZWJEJRXJHVGJRTOXYIUHQHYEMUTXDSEWKHPZPPMFMLZLRRVLSAXYIWGHPWVVLAMNEGTDBINFFXZPLZRKLWWEOEZWAGQJXZSFHZZVVPWVXMSEMUGIOAFVCLSMEKVWL
XJRRRWEIXXISFBGYIMMUXMAXYIUHQHYEMUTXDSEWHKSQMUIJBWNIIZWWADXYEOTVMEEXKXIFMEKLASNITSEFYIMTELBSIWKLWIVJZZHWKGVRESLIVJZZHWMLZHRXSUIXE
LWWBXCEJHWLMBRVHLAIOITLFHPJKPWMVLOLRXAMGVRESLUIVGTIKLIYFPEFRXCMIHHTVOCNIVHRJXYENXEICJMDOIMFLPDXXNEEHLAIYMJGMLWDSEWOBXCMEXZXISITYL
BZZFIEFVLVVWLBPGSEKGBRBAYMDXXCIIIZTWISKCWMFZIEEVXGDWZSFPLZXYIJMSNIVODXKDWCELBSIAVQMLXRSIOOBXCGFRYKINWZRVNWOVPEUTHZQZGKIVDZRGQZVJ
YGWSGHJXYIJLXJGIEXMEIEGTJHEXLKLSMEYHIIKLINECPGYXCIDYDMMKPVGGFTZXZRYVSIGVVFLXCEKLSOIWIVRLAIASTYKHJNSDYUAHZFRXWUYOAVGSGEGPRKJXIOLRX
OXADPCRWXHJRXSAGKCSEIKMEIHZRXHVHIUTMUPDGUITTXZESSMMLJASIKMXJTISLXGOPZFWKXTEEHKXGPVZXQBRWSKLGNVGENWSGHJYIXWVLISCSYR";
// char
cipher_text[]="DBMOKWWODJPAOPEPHGQAHWVUJNXDZAIAQMRPNEMHGPERZOVKRVLWUGAEOPXEHMXDVBXDDVKOYQHJJBLWKXIJDVUQDBIPCMAWTBLATKSIZJEYFBSIZB
SZVG";
float
p[]={0.082,0.015,0.028,0.043,0.127,0.022,0.020,0.061,0.070,0.002,0.008,0.040,0.024,0.067,0.075,0.019,0.001,0.060,0.063,0.091,0.02
8,0.010,0.023,0.001,0.020,0.001};
char alphabet[]="ABCDEFGHIJKLMNOPQRSTUVWXYZ";
float* q[26];
float* Vg[26];
char* stringY[36];
float ioc[100];
float ioc_diff[100];
int keyword[10];

int findIndex(char n){
  for (int i = 0; i < 26; i++) {
    if(n==alphabet[i])
      return i;
  }
  return 0;
}

float IoC(char y_string[1300]){
  int temp[26]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0};
  int b = strlen(y_string);
  int sum=0;

  for (int i = 0; i<b; i++) {
    for (int j = 0; j < 27; j++) {
      if (y_string[i]==alphabet[j]) {
        temp[j]+=1;
      }
    }
  }
  for (int a = 0; a <26; a++) {
  }

  for (int i = 0; i < 26; i++) {
    if (temp[i]>0) {
      sum+=(temp[i]*(temp[i]-1));
    }
  }

  float ioc = (float) sum/(b*(b-1));
  printf("Index of coincidence: %f\n",ioc );
  return ioc;
}


int stringGenerator(int m){
  int key, k=0;
  char string_Y[1300];
  int w=0,z,p,count=0, l;
  for (int a = 1; a <= m; a++) {
    for (int i = 0; i < a; i++) {
      for (int j = i, k = 0; j < strlen(cipher_text); ) {
        string_Y[k]=cipher_text[j];
        j+=a,k++;
        l=k;
      }
      string_Y[l]='\0';
      printf("m=%d String %d \n",a, i+1);
      printf("%s\n",stringY[k]);
      k++;
      ioc[w]=IoC(string_Y);
      w++;
      count++;
    }
  }

  printf("\n\nEnter correct length of keyword to continue : ");
  scanf("%d", &key);
  return key;
}

int main() {
  int m;
  printf("Enter value of m: ");
  scanf("%d",&m);
  printf("\n" );

  int counter=0;
  int num=m;
  while (num!=0) {
    counter=counter+num;
    num--;
  }

  for (int i = 0; i < 36; i++) {
    stringY[i] = malloc(sizeof(char)*1300);
  }
```

```
      int z=0;
      for (int a = 1; a <= m; a++) {
        for (int i = 0; i < a; i++) {
          char* p=stringY[z];
          for (int j = i; j < strlen(cipher_text); ) {
            *p=cipher_text[j];
            j+=a,p++;
          }
          *p='\0';
        z++;
        }

      }

    int key=stringGenerator(m);

    counter=0;
    num=key;
    while (num!=0) {
      counter=counter+num;
      num--;
    }

    for (int i = 0; i < key; i++) {
      q[i] = malloc(sizeof(float)*26);
    }

    int string_counter=(counter-key);

    z=0;
    for (int a = 1; a <= key; a++) {
      int temp[26]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0};
      int b = strlen(stringY[string_counter]);
      float* arr=q[z];

      for (int i = 0; i < b; i++) {
        for (int j = 0; j < 27; j++) {
          if(stringY[string_counter][i]==alphabet[j]) {
            temp[j]+=1;
          continue;
          }
        }
      }
      for (int k = 0; k < 26; k++) {
        *arr=(float)temp[k]/b;
        arr++;
      }
        z++;
        string_counter++;
      }

      for (int i = 0; i < 7; i++) {
```

```
        Vg[i] = malloc(sizeof(float)*26);
      }

      /*
    vg  0   1   2   3
    g=0 x   y   z   w   -> x = Sum of 26 vals use v_shift, sum it, input in vg
    g=1 x   y   z   w
    g=2 x   y   z   w
      */

      //creating the table

      z=0;
      int ind=0;
      for (int a = 1; a <= key; a++) {
        float* v=Vg[z];

        for (int g = 0; g < 26; g++) {
          float v_shift[26]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0};
          float v_sum=0;
          for (int i = 0; i < 26; i++) {
            v_shift[i]=q[ind][(i+g)%26];
            v_shift[i]=v_shift[i]*p[i];
            // printf("The q index : %d \t", ind );
            // printf("The i val: %d \t",i );
            // printf("The g val: %d \n", g);
            // printf("The index val: %d \t",(i+g) );
            // printf("The q array val: %f \t", q[ind][(i+g)%26]);
            // printf("The prod val: %f\n", v_shift[i]);
          }
          for (int i = 0; i < 26; i++) {
            v_sum+=v_shift[i];
          }
          *v=v_sum;
          v++;
        }
        z++;
        ind++;
      }

      //finding keyword

      for (int i = 0; i < key; i++) {
        // printf("\n\nVg for String %d V\n",i+1);
        float max=Vg[i][0];
        int max_i=0;
        for (int j = 0; j < 26; j++) {
          // printf("%f\n",Vg[i][j]);
          if (Vg[i][j]>max) {
            max=Vg[i][j];
            max_i=j;
          }
        }
```

```
        keyword[i]=max_i;
    }

    //print table

    printf("\nTable: \n");

    int index=0;

    printf("g \t Vg1 \t\t Vg2 \t\t Vg3 \t\t Vg4 \t\t Vg5 \t\t Vg6 \t\t Vg7\n" );
    for (int g = 0; g < 26; g++) {
      printf("%d \t %.4f \t %.4f \t %.4f \t %.4f \t %.4f \t %.4f \t %.4f\t\n",g,
      Vg[index][g],Vg[index+1][g],Vg[index+2][g],Vg[index+3][g],Vg[index+4][g],Vg[index+5][g],Vg[index+6][g]);
    }

    printf("\n\nKeyword: \n" );
    for (int i = 0; i < key; i++) {
      printf("%c", alphabet[keyword[i]]);
    }

    //decryption

        int temp;
        char new_txt[1300]="";
        char ch;

        for (int i=0,j=0;cipher_text[i]!='\0';i++,j++)
        {
            if(j==key)
              j=0;
            ch = cipher_text[i];
            int posn = findIndex(ch);
            int key_posn = keyword[j];
            temp = (posn - key_posn)%26;
            if (temp<0)
              temp= (26 - key_posn + posn);
            temp+='a';
            new_txt[i]= temp;
        }
        printf("\n\nThe plain text is: ");
        printf("%s", new_txt);

    return 0;
}
```

## Complete Output:



```
Project — -zsh — 153×70
(base) anish@Anishs-MacBook-Pro Project % clang vig.c -o vig
(base) anish@Anishs-MacBook-Pro Project % ./vig
Enter value of m: 8

m=1 String 1
XCIUIHTVOQVRLHJEYJXAVICEJFWXRVRUAAEPVPNEQLFZGFQEBXOIUXGIVJXVGLBRBXYIDBFZVKCSGHNITYJBXTSWXZHWZAYSEPINIIZWBRMITIFMQJRKLKASRIMIJPICEMIGGEIINWUTPZWVIFFEDRJXJ
XEHTISVNGOWRRVLIMZZGWLHZWZKFXHDRRASRXCEKKAOINYJILWJPVGGGXMSCSNXVVGTIKLXJXYIAKHVXREKTVZWLPLEERIEJGKGZQVRLBWNSDILBQZWLRSUPZXFVWVSQIIXZXGJRKIFMSAICIUMVJRZG
UHQHYEMUTXDSEWXKSHXYILXGCRFPGZCKVFZAWIMIMIFBRMIJTGGWZXFEUHYMXFVVXVJVUYDREPXYSJBDZHNEJKEIXZWKNIYFPEXXHZVRPBNHBIWSJXBVQGPWFEICTSEFYIMTELBSIWJIJOMXIJRQPIIGI
CHMGZVKEAGGJQDYFBGVXZSFLFTHVJSNPOAZXZMLZOVCFXGZWJERXJHVGJRTOXYIUHQHYEMUTXDSEWKHPZPMFMLZLRRVLSAXYIWGHPWVVLAMNEGTDBINFFXZPLZRKLWWEOEZWAGQJXZSFHZZVVPWVXMS
EMUGIOAFVCLSMEKVWLXJRRRWEIXXISFBGYIMMUXMAXYIUHQHYEMUTXDSEWHKSQMUIJBWNIIZWWADXYEOTVMEEXKXIFMEKLASNITSEFYIMTELBSIWKLWIVJZZHWKGVRESLIVJZZHWMLZHRXSUIXELWWBXC
EJHWLMBRVHLAIOITLFHPJKPWMVLOLRXAMGVRESLUIVGTIKLIYFPEFRXCMIHHTVOCNIVHRJXYENXEICJMDOIMFLPDXXNEEHLAIYMJGMLWDSEWOBXCMEXZXISITYLBZZFIEFVLVVVWLBPGSEKGBRBAYMDXX
CIIIZTWISKCWMFZIEEVXGDWZSFPLZXYIJMSNIVODXKDWCELBSIAVQMLXRSIOOBXCGFRYKINWZRVNWOVPEUTHZQZGKIVDZRGQZVJYGWSGHJXYIJLXJGIEXMEIEGTJHEXLKLSMEYHIIKLINECPGYXCIDYDM
MKPVGGFTZXZRYVSIGVVFLXCEKLSOIWIVRLAIASTYKHJNSDYUAHZFRXWUYOAVGSGEGPRKJXIOLRXOXADPCRWXHJRXSAGKCSEIKMEIHZRXHVHIUTMUPDGUITTXZESSMMLJASIKMXJTISLXGOPZFWKXTEEHK
XGPVZXQBRWSKLGNVGENWSGHJYIXWVLISCSYR
Index of coincidence: 0.045527
m=2 String 1
XIITOVLJYXVCJWRRAEVNQFGQBOUGVXGBBYDFVCGNTJXSXHZYEIIZBMTFQRLARMJIEIGINUPWIFDJJETSNORVIZGLZZFHRARCKAIYILJVGXSSXVTKXXIKVRKVWPEREGGQRBNDLQWRUZFWSIXXJKFSIIMJZ
UQYMTDEXSXIXCFGCVZWMMFRITGZFUYXVXJUDEXSBZNJEXWNYPXHVPNBWJBQPFITEYMEBIJJMIRPIIHGVEGJDFGXSLTVSPAXMZVFGWERJVJTXIHHEUXSWHZPFLLRLAYWHWVANGDIFXPZKWEEWGJZFZVPVM
EUIAVLMKWXRREXIFGIMXAYUQYMTDEHSMIBNIWAXETMEKIMKANTEYMEBIKWVZHKVELVZHMZRSIEWBCJWMRHAOTFPKWVORAGRSUVTKIFERCIHVCIHJYNECMOMLDXEHAYJMWSWBCEZIIYBZIFLVWBGEGRAMX
CIZWSCMZEVGWSPZYJSIOXDCLSAQLRIOXGRKNZVWVETZZKVZGZJGSHXILJIXEETHXKSEHILNCGXIYMKVGTXRVIVFXELOWVLISYHNDUHFXUOVSEPKXOROAPRXJXAKSIMIZXVITUDUTXESMJSKXTSXOZWXEH
XPZQRSLN0NSHYXVICY
Index of coincidence: 0.044253
m=2 String 2
CUHVQRHEJAIEFXVUAPPELZFEXIXIJVLRXIBZKSHIYBTWZWASPNIWRIIMJKKSIIPCMGEIWTZVFERXXHIVGWRLMZWHWXDRSXEKONJJWPQGMCNVGILJYAHXETZLLEIJKZVLWSIBZLSPXVVQIZGRIMACUVRG
HHEUXSWKHYLGRPZKFAIIIBMJGWXEHMFVVYRPYJDHEKIZKIFEXZRBHISXVGWECSFITLSWIOXJGIGCMZKAGQYBVZFFHJNQZZLOCXZJJXHGROYUQYMTDEKPMMZRVSXIGPVLMETBNFZLRLWOZAQXSHZVWXS
MGOFCSEVLJRWIXSBYMUMXIHHEUXSWKQUJWIZWDYOVEXXFELSISFITLSWLIJZWGRSIJZWLHXULWKEHLBVLIILHJPWLLXMVELIGILYPFXMHTONVRXEXIJDIFPXNELIMGLDEOXMXXSTLZFEVVVLPSKBBYDX
IITIKWFIEXDZFLXIMNVDKWEBIVMXSOBCFYIWRNOPUHQGIDRQVYWGJYJXGEMIGJELLMYIKIEPYCDDMPGFZZYSGVLCKSIIRAAATKJSYAZRWYAGGGRJILXXDCWHRSGCEKEHRHHUMPGITZSMLAIMJILGPFKTEK
GVXBWKGVEWGJIWLSSR
Index of coincidence: 0.046307
m=3 String 1
XUTQLEXIJXRAVEFFBIGJGRYBVSNYXWHAENZRTMRKRIIMGIUZIEJXTVQRIZLWFDAXKOYJJGXCXGKJIHRTWLRJGVBSLZRPFVIZJISCMRUHMXEKXLCPCFWIFMTWFHXVJYEYBHJIWIPXVBBSBGFCEIESJOIGI
CGKGQFVSFVNAZZCGJRHJOIQETSKZMLRLXWPVMGBFZZLEZGXFZPXEGACMVXREXFYMMYHYUDWSUBIWDEVEXMLNSYTBWWJHGEIZWZXILBEWBIHTHKMOXGEUGKYEXITCVJEEJOFDNHIJLSOCXITBFFVWPEBAD
CIWKMIVDSLYMIDDESVLSOCRIZNVUZGVRZYSJIXIMEJXLEILEGCYMVFXYIVXKOILAYJDAFWOGERXLODRHXGSKIRVUUGTZSLSMTLOFXEXVQWLVNGYWIS
Index of coincidence: 0.044085
m=3 String 2
CIVVHYACFRUEPQZQXUIXLBIFKGIJTXWYPIWMIQKAIJCIENTWFDXEINWVMGHZXRSCKIJLPGMSVTLXAVEVLEIGZRWDBWSZVSIXRFAIVZHYUDWSYXRGKZIMBIGZEYFXVDPSDNKXKYEHRNIJVPETFMLIIMJPG
HZEGDBXFTJPZMOFZEXVRXUHMXEHPFZRSYGWLNTIFPRWOWQZHVWMMIFLEWJRIIBIUAIQETSHQIWIWXOMXIEAIEIESKIZWVSVZMHSXWXJLRLOLPPVLAVSITLFFCHVNHXNIMILXELYGWEBMZSYZIVVLGKRYX
IZICFEXWFZISVXWLIQXIBGYNRWPTQKDGVGGXJJEEGHLSYIICYIDKGTZVGFCLIVASKNYHRUASGKIRXPWJSKEMHXHTPUTEMJIXIXPWTHGZBSGGWHIVSY
Index of coincidence: 0.047437
m=3 String 3
IHORJJVEWVAPNLGEOXVVBXDZCHTBSZZSIIBIFJLSMPEGIWPVFRJHSGRLZWZKHRREANIWVGSNVIXYKXKZPEEKQLNIQLUXWQXGKMIUJGQETSXHIGFZVAMIRJGXUMVVURXJZEEZNFXZPHWXQWISYTBWJXRII
MVAJYGZLHSOXLVXWJJGTYHYUDWPPMLVAIHVAEDNXLKWEAJSZVVSUOVSKLRWXSGMXXUHMXEKMJNZAYTEKFKSTFMLLVZKRLJHLRUEWCHMVAIFJWLRMRLVIIPRMHOIRYXCDMPXEAMMDWXEXILZELVBSGBMX
ITSWZEGZPXJNOKCBAMROXFKWVOEHZIZQJWHYLGXITEKMHKNPXDMPGZRSVLESWRITHSUZXYVGPJOXACXRACIEZHIMDIXSMAKJSGZKEKPXRKNESJXLCR
Index of coincidence: 0.044357
m=4 String 1
XIOLYVJRAVQGBUVGBDVGTXXZEIBTQLRJEGNPIDJTNRIGZFRRKIIJGSXTXIVKWEEGRNLWUFSXJFIMZQMDXXXFCZMFIGFYVJDXBNEWYXVNWBPIEMBJMRIHVGDGSTSAMVGEJJXHEXWZFLLYHVNDFPKEWJFVV
EIVMWREIGMAUYTESINWXTEIKNEMBKVHVLZMRIWCWRATPWOARUTIECHCHYEMMDEAJWWCZIBILWGGAXIWCZWPYSODLALIXRNVVTZVGJSXLIETXSHLCXYKGXVVXLWLSHDHXOSPXRARJASMZVTDTEMSXSOWE
XZRLGSYVC
Index of coincidence: 0.044303
m=4 String 2
CHQHJIFVAPLFXXJLXBKHYTZAPIRIJKIPMEWZFRXIGRMWWXRXKNJPGCVIJAXTLEJZLSBLPVQZRMCVGHUSKYGPKAIBJWEMVVRYDEIKFXRHSVWCFTSIXGGMKGYVFHNZLCZJHRYQMDKPMRSIPLEBFLLOAXHVX
MOCELRISYUXHEXWQJIWYVXFLIFTSLJWRIZLXXWELVILJMLMEIIYFMTNREIDFXEIGDOMXTZEVLSBYXIIWIXZLINDWBVXOCYWNPHGDQYGYXEIJLMIIPCDPFZSVCSIATJYZWAGRIXDWRGEERHMGTSLIJLPKE
GXWGEGILS
Index of coincidence: 0.045658
m=4 String 3
ITVJXCWRENFQQGXBYFCNJSHYIZMFRAMIIIUWFJESOVZLZHACAYLVXSVKXKRVPRGQBDQRZWIXKSIJUYTESICGVWMRTZUXXUESZJXNPHPBJQFTYEIJIPIGEJFXLVPXZFWRVTIHUSHPLRAWWAGIXZWEGZZPM
UALKXRXFIXYQMDHMBIAEMKMATYEIWZKEVHZSEBJMHOFKVRGSVKFRIVIJNCOLXHYMSBEIYZFVBERMCZSMEGSZJIXCSQROGKZWEZKZZGHIJXEHKEINGIMVTRIFEOVIYNUFUVEKOOPXXKIIXIUUXSJKTXZXH
PQSNNHXIY
Index of coincidence: 0.044262
m=4 String 4
UVREAEXUPEZEIIVRIZSIBWWSNWIMKSICGITVEXHVWLZHKDSEOJWGMNGLYHEZLIKVWIZSXVIGIAURHEXWHLRZFIIMGXHFVYPJHKZIEZBIXGESILWOJICZAQBZFJOZOXJXGOUYTEPMZVXGVMTNZRWZQSZWS
GFSVJWXBMMIHUSKUWZDOEXESSILWIZGSJWHULXHBLIHPLXVLGLPXHOVXXJIPNLMLEXXSLFVVPKBDITKFEDFXMVKEIMSBFIROUQIRVWJJGMGELYKEYDMGZYGLKIRAKSARYGGJLXCHSCKHHUPIZMAMIGFTK
VBKVWZWSR
Index of coincidence: 0.046022
m=5 String 1
XHVEVFRPQFOIGXFSTTHSIRFKRPIIPFJHNRZHFRCOIPXNTJKEWEGVNBRXSZKAMGYXXYCZZIRGFMXYXDJZYXPIBWTIBIIIHKJBSHPZVZRGXQUEZMRXHLGNPLEQFVMGVEXWIYXIYXHUNWEEILTIBLZGLZZUW
EMLTJVXRIKPCTIXEDLNAGSXZTZVWSRDIIMEWLJVDBQSXYZOTGZVSYJMTLEKCCMGXSFKWAYSHWVGXXPHAEIHTGXMSJXFEGQKGGXS
Index of coincidence: 0.044805
m=5 String 2
CTRYIWUVLQIVLYZGYSWEIMMLIIGNZFXTGVZZXAEIJVMXIXHKLRKRSQSFQXIIVUEDKIRCAMMGEXVDYZKWFHBWVFSMSJJIMEQGFVOMCWXJYHTWPLVYPATFLWZJHPSICKJESIMUEDKIIAOEFASMSWZVIHHIW
```

```
JBALKLAEVLEMVVYIOPEIMECXYFLLEBXISFVZZMOWSMICKRVHKRJGIGEJKYLPIMGZILLIIKDZUGPIOCJGIHVMUZMITGWEPBLEHWC
Index of coincidence: 0.047619
m=5 String 3
IVLJCXAPFEUJBIVHJWZPZIQKMCGWWEJIOLGWHSKNLGSVKYVTPIGLDZUVIGFCJHMSSLFKWIIWUFJRSHEKPZNSQEETIORGGADVLJALFJJRIYXKPZLIWMDFZWWXZWEOLVRIFMAHMSSJIDTXMSETIIHRVWRXB
HRIFPOMSGIFIOHECIDEYLWMILIVBKAXZKZXSXSDCILOGIVPZIGYHJIIHLHIGDKFRGXSVAHYFYSROXRRKKZHUIELKIOKHVRGNJVS
Index of coincidence: 0.046860
m=5 String 4
UOHXERANZBXXRDKNBXAIWTJAIEEUVDXSWIWZDRKYWGCVLIXVLEZBIWPWIJMIRQUEHXPVIFJZHVVEJNINEVHJGIFEWMGIZGYXFSZZXEHTUEDHMLSWVNBXREAZZVMASWRXBMXQUEQBZXVKENFEWVWEJMXEX
WVOHWLGLTYRHCRNJMXHMWOESBEVPGYCTCIGFYNXEAXOFNNEQVQGJLEEESINYYPTYVCORSJUROGKLAWXCMRIPTSJMSPXKZWNWYLY
Index of coincidence: 0.043635
m=5 String 5
IQJAJVEEGXGVBBCIXZYNBIRSJMITIREVRMLKRXAJJGSGXARZEJQWLLZVXRSUZHTWXGGFMBTXYVUPBEXIXRBXPCYLJXPCVGFZTNXOGJVOHMSPFRAGVEIZKOGSVXUFMLRXGUYHTWMWWYMXKIYLKJKSZLSLC
LHIPMRVUIFXHNJXMFXLJDBXIZFVGBMIWWEDPIIKLVRBRWWUZDZWXXXGXMIEXDVZVVEILTNAXAEJRDXSSEXUDTSAXLZTXXSVSIIR
Index of coincidence: 0.048093
m=6 String 1
XTLXJRVFBGGYVNXHEZTRRIGUIJTOILFAKYJXXKIRWRGBLRFIJSMUMEXCCWFTFXJEBJWPVBBFEEJIIGGFSVAZGRJIESZLLWVGFZEGFPEAMXEFMYYDSBWEEMNYBWHEZZIBWHTKOGUKEICJEODHJSCIBFWEA
CWMVSYIDSLORZVZVZSIIEXELGYVXIXOLYDFOEXORXSIVUTSSTOXXQLNYI
Index of coincidence: 0.044839
m=6 String 2
CVHAFUPZXILIKITWPWIKICETFXIWMHXSKJPMVLAELIZWBSVIRAVHUWYRKIBGEFVPDKKERIVEFLIJGZGBFJZOZXRUMEPZSGLTFROQHWMFEJIBUIESQWWOXEIISIWSZHXXLLLPLVILFHNXIIXLGEMSZVLKY
IIFXFIVWIXBYRPQDVGJEGLYIYDGZGCIAKYRAGIXWSEHHPTMIIPTGBGWIS
Index of coincidence: 0.050854
m=6 String 3
IOJVWANGOVBDCTSZIBFLMEIPFJSRZZHRAIVSVXKKPEQNQUWXKIJQTXIFVMRGUVUXZENXPWQIYBJRIVJGLSXVWJTHUWPLAHADXKEJZVUVKRXGXUMEMNATKKTMIVKLHRECMAFWRRVIRHIYCMXAMWEIZLBGM
ISZGPJOCARXKVEZZJHLXTKHNXMGRVEWIHUXVPOAXAIZIDXMKSZEPRNSXC
Index of coincidence: 0.042880
m=6 String 4
UQEIXAEFIJRBSYWANRMKIMIZEXVRZWDXOJGCGJHTLJVSZPVZICRHXKLPFIMWHVYYHIIXBSGCISOGCKQVFNZCJHOQTKMRXPMBZLZXZXGCVRXYMHUWUIDVXLSTWJGIWXLEBIHMXEGYXTVEJFNILOXTFVPBD
IKIDLMDEVSCINUGRYJXMJLIECMFYVKIAJAWGRLDHGKRUGZLMLFEVWVGWS
Index of coincidence: 0.041604
m=6 String 5
IVYCREQQUXBFGJXYIMQAJINWDENVGZRCILGSTXVVEGRDWZSXFIZYDSXGZMIZYXDSNXYHNJPTMIMPHEDXTPMFEVXHXHFRYWNIPWWZVMILWRIIAQTHIIXMIAEEKZVVMSWJROPVASTFCVHNMLEYWBZYIVGRX
ZCEWZSXLQIGNWTKGGXJEHSICIKTVFLVSNHUSKRPJKMXTUEJXWHZSGHVY
Index of coincidence: 0.044019
m=6 String 6
HRJEVPLEXVXZHBZSIIJSPGWVRHGLWKRENWGNIYXZEKLILXQGMUGESHGZAIJXMVRJEZFZHXWSTWXIMAYZHOLXJGYYDPMVIVENLWASVSOSLWSMXHXKJZYEFSFLLZRJLUWHVIJLMLIPMORXDPEMDXXLEVSBX
TWEZXNKBMOFWOHIQWYGIEMKPDPZSLSRTSZYGJXCRCEHMISAJGKKXKEJLR
Index of coincidence: 0.045341
m=7 String 1
XVJIRPFXVRFHXWIRQSIEPEEGIHHXIWXVXHVEGWQPSGSVQXSGCIRWYVEDEIHHBEYSMIGGGFPLGXTQXPLSHMILEQZXISXIGMQXSWAVISYSVGVLIXMIPLGIIXVREIXIWXIZLPRXWFGLSKSXXIWHVVHXEEEIX
MTSXIIJHYEIAHKEVPXLXGXGRVHL
Index of coincidence: 0.071260
m=7 String 2
COECVVZOJBZNTZNMJRCIZDHOMZDCNJMVJVZRZNZZQJAJHDHCKMMZMJPZIYZBVIIIXIZJVTOZZJOHDZZAPNNZOJZMOMJXYAHDQNDMFNIIJVJZXCBOJOVVYCOJIMNYDCSZVGBCIZDZNDIRCNOZDJJJIXYNC
KZICWANZOGODJCIHDZJJOTPWGJI
Index of coincidence: 0.071260
m=7 String 3
IQYERPGIXXVISAIIRIEIWRTWZWREYPSGXXWIQSWXIRIRYSXRVIIXXVXHXFVIQCMWIGVQXHAOWHXYSPLXWEFREXVSAERXIXYSMIXEMIMWZRZHEERIKLRGFMCXCFEMSMIFVSAISIWXIWASGWVQZYXGELHEI
PXGEISSFAPLPRSHIGEATPEVSEYS
Index of coincidence: 0.068156
m=7 String 4
UVJJUNFUVYKTWYITKMMNVJIRZZRKJVCTYRLEVDLFIKCZEEYFFMJFFUYNZPRWGTTJJIKDZVZVJVYEEPRYVGFKZZVEFKRIMYEEUIYEETTKZEZRLJVTPRETPINYJLEJEETIVEYIKEZYVCVIFZPZRGYIGKICD
VZVKVTDRVRRCXEZUUSSIZEZKNIC
Index of coincidence: 0.061390
m=7 String 5
IRXFAEQXDICYXSZILIIWIXSRGKAKIGSIIEPJRIRVXIIGMWIPZITEVYSEWEPSPSEIRCEYSJXCEGIMWMRIVTXLWSPMVVRSMIMWIZEXKSELHSHXWHHLWXSIEHIEMPHGWXYEWKMICESIOEQORREGGWIETLIPY
GRVLRYYXGKXRSIRTISISFHXLWXS
Index of coincidence: 0.068343
m=7 String 6
HLAWAQEGLDSJZEWFKJGUFJVVWFSAJGNKAKLGLLSWZFUUUXLGAFGUVDJJKXBJWELJGHAFFSZFJJUUKFVWLDZWAFWUCWWFUUUHJWOKLELWWLWSWWLFMALKFHVNDDLMOZLFLGDZWVFJDLMOYVUKQSJXJSKGD
GYFSLKUWSJOWAKXMTMKLWKQGSWY
Index of coincidence: 0.062259
m=7 String 7
THVXELBIBBGBHPBMAPGTFXNLLXROLGXLKTEKBBUVXMMHTKXZWBGHXRBKNXNXFFBOPMGBLNMXRRHTHMLGABPWGHVGLLEBXHTKBWTXAFBIKIMUBLAHVMULRTHXOXALBXBVBBXTMXPMXBLBKNTIZGLMHMLYM
FVLOAHAUGXXXGMHUTMMXKXBNGVR
Index of coincidence: 0.067908
m=8 String 1
XOYJAQBVBVTXEBQRENIJNIZRKIGXXVWERLUSJIZMXXCMIFVDBEYVWPEBMIVDSSMGJXEWFLHNFKWFVIMRIMUTSNXEKEBVVZRWWAPORTEHHEMEJWZBLGAICVPSDAIRVTVJXITSLXKXVLLHHOPRRAMVDESSW
XRGYC
Index of coincidence: 0.043618
```

```
m=8 String 2
CQJFALXJXKYZPRJIMWFXGMWRKJGVJXLJLBPQRCGUKGKIJEVRDIFRSWFSXGKYFNLZHYMKMSPEFLAHXOERSUHXQIYXLFSJRZXWLIJLEIFTRIFEGOXZVSYIWXLNWVOYNHDYYEJMICPZVSAJZARXWGEHGSILK
GWEIS
Index of coincidence: 0.043618
m=8 String 3
IVXWEFOXYCJHIMRMIUFEOZZAALXVXRPGBQZIKIUTSCVMTUXEZXPPJFYIIIEFLPZWVIUHLAWGXWGZMAKRFXQDMIEKAYIZEHSBMOKRSKRVJCLHMBIZVEMZMGZICQOKWZZGIXHENIVRFOINFVKOXKIIUSKXX
PSNXY
Index of coincidence: 0.046521
m=8 String 4
URAXPZIVISBWNIKIGTEHWZKSOWMGYELKWZXIIUHXHRFIGHVPHZEBXEIWJCABFOOJGUTPZXVTZWQZSFVWBMHSUZOXSIWZSWUXBIPXLLXOXJPLLXSFVKDTFDXVEMBIOQRWJMEYEDGYLIASRGJXHCHUIMMGT
VKWWR
Index of coincidence: 0.042167
m=8 String 5
ILVRVGUGDGXZITLJGPDTRGFRIJSTIKEGNWFXFMQDXFZFGYJXNWXNBIMJRHGGTAVEJHXZLYVDPEJVEVWEGAYEIWTINMKHLMICRTWAUICCYMDAWCIIWGXWZWYOLLXNVZGSLEXHCYGVXWSDXSXAJSZTTMXOE
ZLSV
Index of coincidence: 0.043933
m=8 String 6
HHIVPFXLBHTAIIKPEZRIRWXXNPCIATEZSLVZMVHSYPABWMVYEKXHVCTIGMGVHZCJRQDPRILBLOXVMCLIYXEWJWVFITLWILXEVLMMIYMNEDXIDMTELBXIIZIDBXCWPGQGXILIPDFSCITYWGIDRERMTLJPE
XGGL
Index of coincidence: 0.049567
m=8 String 7
TJCRNQGBFNSYZFAIIWJSVLHCYVSKKVRQDRWXSJYEIGWRZXUSJNHBQTEJPGJXVXFRTHSPRWAIZEZPULXXIYMHBAMMTEWKVZEJHFVGVFIINOXYSEYFBRCSESJXSRGZEKZHJEKIGMTIEVYUUEOPXIXUXJTZH
QNHI
Index of coincidence: 0.041238
m=8 String 8
VEEUEEIRZIWSWMSCIVXVLHDEJGNLHZIVISVGAREWLZIMXFYJKIZIGSLOIZQZJZXXOYEMVGMNRZSWGSJXMIUKWDEESLIGJHLHLHLVGPHVXINMEXLVPBIKEFMKISFRUIVJGGLKYMZGKRKAYGLCSKHPZAIFK
BVJS
Index of coincidence: 0.049404


Enter correct length of keyword to continue : 7

Table:
g        Vg1             Vg2             Vg3             Vg4             Vg5             Vg6             Vg7
0        0.0407          0.0331          0.0453          0.0409          0.0476          0.0312          0.0350
1        0.0355          0.0377          0.0354          0.0386          0.0351          0.0396          0.0386
2        0.0369          0.0354          0.0314          0.0428          0.0324          0.0400          0.0323
3        0.0425          0.0313          0.0370          0.0333          0.0379          0.0477          0.0392
4        0.0662          0.0338          0.0666          0.0440          0.0672          0.0362          0.0432
5        0.0375          0.0432          0.0393          0.0396          0.0391          0.0442          0.0362
6        0.0334          0.0444          0.0322          0.0461          0.0352          0.0389          0.0402
7        0.0327          0.0378          0.0296          0.0366          0.0301          0.0460          0.0411
8        0.0400          0.0423          0.0410          0.0363          0.0407          0.0355          0.0471
9        0.0298          0.0423          0.0318          0.0294          0.0286          0.0367          0.0407
10       0.0350          0.0408          0.0371          0.0351          0.0380          0.0319          0.0364
11       0.0362          0.0380          0.0381          0.0421          0.0394          0.0352          0.0298
12       0.0331          0.0333          0.0368          0.0365          0.0318          0.0358          0.0352
13       0.0361          0.0308          0.0376          0.0425          0.0349          0.0335          0.0404
14       0.0397          0.0373          0.0405          0.0303          0.0410          0.0402          0.0354
15       0.0493          0.0361          0.0468          0.0350          0.0483          0.0319          0.0412
16       0.0405          0.0365          0.0389          0.0412          0.0391          0.0384          0.0337
17       0.0415          0.0441          0.0424          0.0628          0.0429          0.0415          0.0304
18       0.0383          0.0344          0.0384          0.0356          0.0384          0.0637          0.0350
19       0.0491          0.0284          0.0440          0.0319          0.0425          0.0383          0.0656
20       0.0379          0.0402          0.0376          0.0352          0.0381          0.0350          0.0427
21       0.0339          0.0683          0.0334          0.0465          0.0338          0.0314          0.0314
22       0.0305          0.0417          0.0342          0.0342          0.0339          0.0425          0.0289
23       0.0406          0.0311          0.0388          0.0337          0.0363          0.0345          0.0509
24       0.0306          0.0337          0.0341          0.0370          0.0353          0.0365          0.0350
25       0.0336          0.0451          0.0328          0.0339          0.0335          0.0347          0.0355


Keyword:
EVEREST

The plain text is: thedepartmentofjusticehasbeenandwillalwaysbecommittedtoprotectingthelibertyandsecurityofthosewhomweserveinrecentmonthshoweverwehaveona
newscaleseenmainstreamproductsandservicesdesignedinawaythatgivesuserssolecontroloveraccesstotheirdataasaresultlawenforcementissometimesunabletorecoverthe
contentofelectroniccommunicationsfromthetechnologyproviderevenifinresponsetoacourtorderorduly authorizedwarrantissuedbyafederaljudgeforexamplemanycommunicat
ionsservicesnowencryptcertaincommunicationsbydefaultwiththekeynecessarytodecryptthecommunicationssolelyinthehandsoftheenduserthisappliesbothwhenthedatais
inmotionoverelectronicnetworksoratrestonanelectronicdeviceifthecommunicationsproviderisservedwithawarrantseekingthosecommunicationstheprovidercannotprovi
dethedatabecauseithasdesignedthetechnologysuchthatitcannotbeaccessedbyanythirdpartywedonothaveanysilverbulletsandthediscussionswithintheexecutive(base) a
nish@Anishs-MacBook-Pro Project % (base) anish@Anishs-MacBook-Pro Project % (base) anish@Anishs-MacBook-(base) anish@Anishs-M(base) anish@A(base) (base)
```