FINAL EXAM

Paul Vrbik : 301056796 : MATH 800 : Fall 2006

December 8, 2006

Question 1.7

For $m = 30$ there are $30 \cdot \phi(2 \cdot 3 \cdot 5) = 240$ keys, for $m = 100$ there are $100 \cdot \phi(2^2 \cdot 5^2) = 4000$ keys, and for $m = 1225$ there are $1225 \cdot \phi(5^2 \cdot 7^2) = 1029000$ keys.

Question 1.9

```
seq((1/i) mod 29,i=1..28);

1, 15, 10, 22, 6, 5, 25, 11, 13, 3, 8, 17, 9, 27,
2, 20, 12, 21, 26, 16, 18,  4, 24, 23, 7, 19, 14, 28
```

So the inverses of $1, 2, 3, ..., 28$ in $\mathbb{Z}_{29}$ are

$$1, 15, 10, 22, 6, 5, 25, 11, 13, 3, 8, 17, 9, 27, 2, 20, 12, 21, 26, 16, 18, 4, 24, 23, 7, 19, 14, 28$$

respectively.

Question 1.13

```
NonSingMat := proc(n) local a,b,c,d,count ::int;
    count:=0;
    for a from 1 to n do
        for b from 1 to n do
            for c from 1 to n do
                for d from 1 to n do
                    if (gcd((a*d-b*c) mod n,n)=1) then
                        count:=count+1
                    end if;
                end do;
             end do;
        end do;
    end do;
    return(count);
end proc:

NonSingMat(6);
                              288
NonSingMat(9);
                              3888
NonSingMat(26);
                             157248
```

So by this maple code there are 288 invertible matrices in $\mathbb{Z}_6$, 3888 in $\mathbb{Z}_9$ and 157248 in $\mathbb{Z}_26$.

Question 1.16

(a) The inverse for $x \in [1, 8]$ is given by:

$$\pi^{-1}[x] = [2, 4, 6, 1, 8, 3, 5, 7]$$

i.e. $\pi^{-1}[3] = 6$.

(b)

```
Citxt:="TGEEMNELNNTDROEOAAHDOETCSHAEIRLM";
               "TGEEMNELNNTDROEOAAHDOETCSHAEIRLM"
Plntxt:="";
                               ""
d:=array(0..7,[2,4,6,1,8,3,5,7]);

A:=[Citxt[1..8],Citxt[9..16],Citxt[17..24],Citxt[25..32]];
        ["TGEEMNEL", "NNTDROEO", "AAHDOETC", "SHAEIRLM"]

decrypt:=proc(A) local i,j::int, pln::string;
    pln:="";
    for j from 1 to 4 do
        for i from 0 to 7 do pln:=cat(pln,A[j][d[i]]); end do;
    end do
end proc:

decrypt(A);
               "GENTLEMENDONOTREADEACHOTHERSMAIL"
```

Question 1.21

(a) After much time investment, using the information found below the decrypted message is:

```
i may not be able to grow flowers but my garden produces
just as many dead leaves old over shoes pieces of rope
and bushels of dead grass as anybodys and today i bought
a wheel barrow to help in clearing it up i have always loved
and respected the wheel barrow it is the one wheeled vehicle
of which i am perfect master
```

with the following key:

```
A -> V | C -> E | D -> B | E -> I |
F -> W | G -> A | H -> F | I -> D |
J -> C | K -> S | L -> Y | M -> M |
N -> L | O -> N | P -> U | S -> O |
U -> T | W -> G | X -> P | Y -> R |
Z -> H


Sigma:="ABCDEFGHIJKLMNOPQRSTUVWXYZ":

Citxt:=
"EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCKQPKUGKMGOLICGINCGACKSNI
SACYKZSCKXECJCKSHYSXCGOIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZUGFZC
CNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNSACIGOIYCKXCJUCIUZCFZCCNDGYYS
FEUEKUZCSOCFZCCNCIACZEJNCSHFZEJZEGMXCYHCJUMGKUCY":

T:=table();

for i from 1 to length(Sigma) do T[Sigma[i]]:=0; od:
for i from 1 to length(Citxt) do T[Citxt[i]]:=T[Citxt[i]]+1: od:
```

```
seq(printf("%c    %d     %f\n",Sigma[i],T[Sigma[i]],T[Sigma[i]]/length(Citxt)),i=1..26);
A    5     0.019531
B    0     0.000000
C    37     0.144531
D    8     0.031250
E    12     0.046875
F    9     0.035156
G    24     0.093750
H    5     0.019531
I    15     0.058594
J    7     0.027344
K    18     0.070312
L    7     0.027344
M    5     0.019531
N    13     0.050781
O    10     0.039062
P    6     0.023438
Q    1     0.003906
R    0     0.000000
S    20     0.078125
T    0     0.000000
U    14     0.054688
V    0     0.000000
W    5     0.019531
X    7     0.027344
Y    15     0.058594

Di:=table();

for i from 1 to length(Citxt)-1 do Di[Citxt[i..i+1]]:=0 od:
for i from 1 to length(Citxt)-1 do Di[Citxt[i..i+1]]:=Di[Citxt[i..i+1]]+1 od:
for i from 1 to length(Citxt)-1 do
    if (Di[Citxt[i..i+1]]>2) then
        printf("(%s %d)   ",Citxt[i..i+1],Di[Citxt[i..i+1]]);
    end if
end do;
(MG 3)   (GL 3)   (CG 7)   (NC 5)   (US 3)   (YS 5)   (SF 4)   (SF 4)   (CY 4)   (GY 4)   (IC 3)   (YS 5)
(CK 5)   (KU 3)   (GK 4)   (MG 3)   (GO 5)   (IC 3)   (CG 7)   (NC 5)   (CG 7)   (AC 5)   (CK 5)   (KS 3)
(CY 4)   (CK 5)   (XE 3)   (CJ 3)   (CK 5)   (KS 3)   (SH 3)   (YS 5)   (XC 3)   (CG 7)   (GO 5)   (OI 3)
(CN 5)   (KS 3)   (SH 3)   (IC 3)   (CG 7)   (GK 4)   (KG 3)   (GK 4)   (KG 3)   (GO 5)   (SI 3)   (KG 3)
(OI 3)   (US 3)   (SI 3)   (GL 3)   (FZ 4)   (ZC 7)   (CC 3)   (CN 5)   (GY 4)   (YS 5)   (SF 4)   (US 3)
(CN 5)   (XE 3)   (NC 5)   (CG 7)   (GY 4)   (XE 3)   (AC 5)   (CG 7)   (GL 3)   (AC 5)   (CI 3)   (GO 5)
(CK 5)   (XC 3)   (CJ 3)   (CI 3)   (ZC 7)   (FZ 4)   (ZC 7)   (CC 3)   (CN 5)   (GY 4)   (YS 5)   (SF 4)
(ZC 7)   (FZ 4)   (ZC 7)   (CC 3)   (CN 5)   (NC 5)   (CI 3)   (AC 5)   (ZE 3)   (NC 5)   (SH 3)   (FZ 4)
(ZE 3)   (XC 3)   (CY 4)   (CJ 3)   (MG 3)   (GK 4)   (KU 3)   (CY 4)

Tri:=table();

for i from 1 to length(Citxt)-2 do Tri[Citxt[i..i+2]]:=0 od:
for i from 1 to length(Citxt)-2 do Tri[Citxt[i..i+2]]:=Tri[Citxt[i..i+2]]+1 od:
for i from 1 to length(Citxt)-2 do
    if (Tri[Citxt[i..i+2]]>1) then
        printf("(%s %d)  ",Citxt[i..i+2],Tri[Citxt[i..i+2]]);
    end if
end do;
(YSF 3)  (CYK 2)  (JCK 2)  (GOL 2)  (ICG 2)  (CGI 2)  (NCG 2)  (GAC 2)  (CKS 2)  (SAC 2)  (CYK 2)
(CKX 2)  (JCK 2)  (CKS 2)  (KSH 2)  (GOI 3)  (ZCN 2)  (KSH 2)  (ICG 2)  (CGI 2)  (KGO 2)  (GOL 2)
(KGO 2)  (GOI 3)  (FZC 3)  (ZCC 3)  (CCN 3)  (CND 2)  (NDG 2)  (DGY 2)  (GYY 2)  (YYS 2)  (YSF 3)
(ZCN 2)  (JNC 2)  (NCG 2)  (GAC 2)  (SAC 2)  (GOI 3)  (CKX 2)  (CJU 2)  (UZC 2)  (CFZ 2)  (FZC 3)
(ZCC 3)  (CCN 3)  (CND 2)  (NDG 2)  (DGY 2)  (GYY 2)  (YYS 2)  (YSF 3)  (UZC 2)  (CFZ 2)  (FZC 3)
(ZCC 3)  (CCN 3)  (ZEJ 2)  (JNC 2)  (ZEJ 2)  (CJU 2)
```

(b) We first determine that there is a trigram that occurs 5 times in the cipher text with the spacing from the first occurrence to the other four being (respectively), $18, 156, 210$ and 222. The greatest common divisor of these four numbers is 6 so it is a good candidate for the length of the keyword.

Further analysis yields that when $m = 6$ the index of coincidences is $0.063, 0.0841, 0.049, 0.065, 0.043, 0.073$ which is the closest to the desired 0.065 of all the other index of coincidences for other m's.

Looking at the chart for the values of $M_g(y_i)$ we select the highest probability from each i which corresponds to the keyword "CRYPTO" or the numeric key $3 - 18 - 25 - 16 - 20 - 15$.

We then use this keyword to decrypt the message which is found on the last line of output.

```
Sigma:="ABCDEFGHIJKLMNOPQRSTUVWXYZ":

Citxt:="KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUDDKOTFMBPVGEGLTGCKQR
ACQCWDNAWCRXIZAKFTLEWRPTYCQKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAH
CTRLSVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMVGKMITZHFPDISPZLVLGWTFP
LKKEBDPGCEBSHCTJRWXBAFSPEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHIF
FSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIYCWHJVLNHIQIBTKHJVNPIST":

sTri:={seq(Citxt[i..i+2],i=1..length(Citxt)-2)}:
Tri:=table();

for i from 1 to length(Citxt)-2 do Tri[Citxt[i..i+2]]:=0 od:
for i from 1 to length(Citxt)-2 do Tri[Citxt[i..i+2]]:=Tri[Citxt[i..i+2]]+1 od:
M:=max(seq(Tri[Citxt[i..i+2]],i=1..length(Citxt)-2));

                                5
loc:=[];
                                []
for i from 1 to length(Citxt)-2 do
    if (Tri[Citxt[i..i+2]]=M) then
       loc:=[op(loc),i];
    end if
end do;

pos:=seq(loc[i]-loc[1],i=2..nops(loc));
                       18, 156, 210, 222
igcd(pos);
                                6
freq:=table();

for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:
for i from 1 to length(Citxt) do freq[Citxt[i]]:=freq[Citxt[i]]+1: od:

print(freq);
TABLE(["C" = 24, "A" = 14, "B" = 14, "F" = 16, "O" = 5, "D" = 16, "E" = 10,
  "Z" = 7, "X" = 7, "G" = 16, "Y" = 8, "J" = 11, "U" = 4, "W" = 14, "H" = 14,

  "V" = 18, "I" = 14, "K" = 20, "P" = 15, "T" = 19, "N" = 10, "Q" = 13,

  "R" = 16, "M" = 6, "L" = 11, "S" = 15])

Ic:=proc(X) local i::int, freq::table;
     freq:=table();
     for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:
     for i from 1 to length(X) do freq[X[i]]:=freq[X[i]]+1: od:
     return add(freq[Sigma[i]]*(freq[Sigma[i]]-1),i=1..26)/(length(X)*(length(X)-1));
end proc:

blCoIn:=proc(n)
    return seq(evalf[2](Ic(seq(cat(seq(Citxt[n*i+j],i=0..length(Citxt)/n-1)),j=1..n)[k])),k=1..n);
end proc;

for i from 1 to 10 do print(i); blCoIn(i); od;
                               1
                             0.041
                               2
                          0.038, 0.047
                               3
                      0.055, 0.048, 0.048
                               4
                   0.037, 0.043, 0.038, 0.049
                               5
               0.043, 0.043, 0.033, 0.035, 0.043
                               6
            0.063, 0.084, 0.049, 0.065, 0.043, 0.073
                               7
        0.031, 0.044, 0.043, 0.041, 0.044, 0.044, 0.041
                               8
     0.031, 0.041, 0.034, 0.041, 0.039, 0.045, 0.041, 0.055
                               9
 0.051, 0.041, 0.059, 0.071, 0.041, 0.035, 0.044, 0.048, 0.042
                               10
0.042, 0.045, 0.034, 0.040, 0.034, 0.044, 0.034, 0.028, 0.030, 0.049

n:=6:

Yi:=[seq(cat(seq(Citxt[n*i+j],i=0..length(Citxt)/n-1)),j=1..n)]:

Mgt:=proc(y,g) local freq::table, i::int;
     freq:=table();
     for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:
     for i from 1 to length(y) do freq[y[i]]:=freq[y[i]]+1: od:
     return evalf[2](add(((p[i+1]*freq[Sigma[(i+g) mod 26+1]])/(length(Citxt)/6)),i=0..25));
end proc:

seq(Mgt(Yi[1],i),i=0..25);
0.030, 0.035, 0.066, 0.040, 0.032, 0.042, 0.036, 0.031, 0.040, 0.046, 0.025,
0.034, 0.037, 0.042, 0.037, 0.044, 0.034, 0.040, 0.044, 0.033, 0.032, 0.038,
0.042, 0.034, 0.039, 0.032
```

```
seq(Mgt(Yi[2],i),i=0..25);
0.037, 0.036, 0.048, 0.041, 0.039, 0.033, 0.046, 0.029, 0.025, 0.035, 0.042,
0.029, 0.034, 0.044, 0.040, 0.032, 0.034, 0.067, 0.036, 0.029, 0.028, 0.033,
0.028, 0.036, 0.044, 0.036

seq(Mgt(Yi[3],i),i=0..25);
0.033, 0.035, 0.033, 0.038, 0.034, 0.039, 0.028, 0.037, 0.032, 0.040, 0.039,
0.045, 0.039, 0.041, 0.036, 0.030, 0.034, 0.039, 0.043, 0.031, 0.038, 0.032,
0.032, 0.043, 0.056, 0.045

seq(Mgt(Yi[4],i),i=0..25);
0.043, 0.038, 0.044, 0.034, 0.036, 0.037, 0.029, 0.032, 0.038, 0.037, 0.035,
0.050, 0.039, 0.029, 0.033, 0.065, 0.035, 0.029, 0.038, 0.040, 0.024, 0.033,
0.038, 0.033, 0.033, 0.042

seq(Mgt(Yi[5],i),i=0..25);
0.039, 0.032, 0.032, 0.038, 0.045, 0.032, 0.041, 0.046, 0.046, 0.032, 0.034,
0.034, 0.033, 0.034, 0.033, 0.045, 0.034, 0.035, 0.036, 0.054, 0.038, 0.034,
0.044, 0.043, 0.031, 0.030

seq(Mgt(Yi[6],i),i=0..25);
0.041, 0.035, 0.036, 0.040, 0.039, 0.026, 0.032, 0.037, 0.036, 0.034, 0.047,
0.033, 0.025, 0.037, 0.069, 0.041, 0.029, 0.031, 0.037, 0.031, 0.039, 0.040,
0.033, 0.035, 0.037, 0.045

chNum:=table(); numCh:=array(0..25):

for i from 1 to 26 do
     chNum[Sigma[i]]:=i;
     numCh[i-1]:=Sigma[i];
od:

key:=array(0..5,[3,18,25,16,20,15]);

for i from 0 to (length(Citxt)-1) do
    Plntxt:=cat(Plntxt,numCh[(chNum[Citxt[i+1]]-(key[(i mod 6)])) mod 26]);
od:
print(Plntxt);

"ILEARNEDHOWTOCALCULATETHEAMOUNTOFPAPERNEEDEDFORAROOMWHENIWASATSCHOO
LYOUMULTIPLYTHESQUAREFOOTAGEOFTHEWALLSBYTHECUBICCONTENTSOFTHEFLOORAND
CEILINGCOMBINEDANDDOUBLEITYOUTHENALLOWHALFTHETOTALFOROPENINGSSUCHASWIND
OWSANDDOORSTHENYOUALLOWTHEOTHERHALFFORMATCHINGTHEPATTERNTHENYOUDOUB
LETHEWHOLETHINGAGAINTOGIVEAMARGINOFERRORANDTHENYOUORDERTHEPAPER"
```

(c) Given that one of the messages is non-english and the last cipher text is known to be english (it is stated in the question that it is from an english book) this message is not english. Guessing that the message is probably one of the "math" languages (where now we can rule out Russian because of special characters) we will test to see if the text could be either French or German.

Taking the probabilities from (http://www.santacruzpl.org) we find that the expected $I(x)$'s are 0.07930850080 for French and 0.07365403820 for German. Given that $I_c(citxt)$ is actually 0.08458320580, French, in this case, would be the better guess (also its a Canadian book so French seems like a good candidate anyways).

Since the character 'C' occurs with the highest probability in the cipher-text it most likely the encryption of 'E' which is the actual highest occurring character in French. This gives $e_K(4) = 2$. The second most frequent letter in the cipher text is 'B' so it most likely mapped to by 'A', 'T', 'S', 'I', or 'N' (the second most likely french occurring characters).

Trying $e_k(`A') = `B' \rightarrow e_k(0) = 1$ is not a good choice because the system of equations

$$4a + b = 2$$

$$0a + b = 1$$

implies that $a = \frac{1}{4}$ which is impossible since 4 does not have inverse modulo 26.

The next choice of $e_k(`T') = `B' \rightarrow e_k(19) = 1$ which gives the system of equations

$$4a + b = 2$$

$$19a + b = 1$$

which has solution $a = 19$, $b = 4$. Trying these numbers as the key proves fruitful since it is the right choice. The code for the decryption and the plaintext follows.

```
restart();
Sigma:="ABCDEFGHIJKLMNOPQRSTUVWXYZ":

Citxt:="KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUPKRIOFKPAC
UZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKPBCPFEQPKAZBKRHAIBKAPCCIB
URCCDKDCCJCIDFUIXPAFFERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKB
COCPERKIVKSCPICBRKIJPKABI":

T:=table();

for i from 1 to length(Sigma) do T[Sigma[i]]:=0; od:
for i from 1 to length(Citxt) do T[Citxt[i]]:=T[Citxt[i]]+1: od:

seq(printf("%c    %d     %f\n",Sigma[i],T[Sigma[i]],T[Sigma[i]]/length(Citxt)),i=1..26);
A    13     0.065657
B    21     0.106061
C    32     0.161616
D    9     0.045455
E    13     0.065657
F    10     0.050505
G    0     0.000000
H    1     0.005051
I    16     0.080808
J    6     0.030303
K    20     0.101010
L    0     0.000000
M    0     0.000000
N    1     0.005051
O    2     0.010101
P    20     0.101010
Q    4     0.020202
R    12     0.060606
S    1     0.005051
T    0     0.000000
U    6     0.030303
V    4     0.020202
```

```
W    0     0.000000
X    2     0.010101
Y    1     0.005051
Z    4     0.020202
charPr:=table();

for i from 1 to length(Sigma) do charPr[Sigma[i]]:=T[Sigma[i]]/length(Citxt); od:
evalf(add(charPr[Sigma[i]]^2,i=1..length(Sigma)));
                         0.08458320580
frenchFreq:=[175.64,81.47,80.13,75.59,73.53,73.22,62.91,59.91,57.83,52.89,41.25,30.63
,29.90,29.80,15.57,13.61,10.51,9.59,8.76,7.21,5.98,3.50,1.16,.72,.41,.20];

add((frenchFreq[i]/1000)^2,i=1..26);
                         0.07930850080

germanFreq:=[166.93,99.05,78.12,67.65,67.42,65.39,65.06,54.14,40.64,37.03,36.47,30.05
,28.37,28.25,25.66,22.85,20.44,18.79,13.96,10.69,10.02,9.44,1.91,.55,.32,.22];

add((germanFreq[i]/1000)^2,i=1..26);
                         0.07365403820

chNum:=table(); numCh:=array(0..25);

for i from 1 to 26 do
     chNum[Sigma[i]]:=i-1;
     numCh[i-1]:=Sigma[i];
od:

a:=19; b:=4; A:=(1/a) mod 26:

plntxt:="";
for i from 1 to length(Citxt) do
    plntxt:=cat(plntxt,numCh[(chNum[Citxt[i]]-b)*A mod 26]);
od:
print(plntxt);

"OCANADATERREDENOSAIEUXTONFRONTESTCEINTDEFLEURONS
GLORIEUXCARTONBRASSAITPORTERLEPEEILSAITPORTERLACRO
IXTONHISTOIREESTUNEEPOPEEDESPLUSBRILLANTSEXPLOITSET
TAVALEURDEFOITREMPEEPROTEGERANOSFOYERSETNOSDROITS"
```

(d) Since the $I_c(citxt) = 0.04138199429$ and the text is english we can rule out every type of cipher but Vignère. Doing the same type of analysis as in (a) we discover that there are only trigrams at most length 2. Looking at the difference in positions of the trigram pairs we can observe that these spaces have a common divisor of 6, which may be the block size.

The index of coincidences at $m = 6$ give $0.0497, 0.0613, 0.0550, 0.0709, 0.0555, 0.0698$ which is promising. Investigating the $M_g(y_i)$ we take the highest probability letters which give the keyword "THEORY" or numeric key $20 - 8 - 5 - 15 - 18 - 25$. We use this keyword to decrypt the message which is on the last line of output.

```
Sigma:="ABCDEFGHIJKLMNOPQRSTUVWXYZ":
p:=[0.082,0.015,0.028,0.043,.127,0.022,.020,.061,.070,.002,.008,
.040,.024,0.067,0.075,0.019,0.001,0.060,0.063,0.091,0.028,0.010,0.023,0.001,0.020,.001]:
```

```
Citxt:="BNVSNSIHQCEELSSKKYERIFJKXUMBGYKAMQLJTYAVFBK
VTDVBPVVRJYYLAOKYMPQSCGDLFSRLLPROYGESEBUUALRWX
MMASAZLGLEDFJBZAVVPXWICGJXASCBYEHOSNMULKCEAHTQ
OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKCGJI
WEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBNLHJMBLRFFJ
ELHWEYLWISTFVVYFJCMHYUYRUFSFMGESIGRLWALSWMNUH
SIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAUMELCM
OEHVLTIPSUYILVGFLMVWDVYDBTHFRAYISYSGKVSUUHYHGGC
KTMBLRX":

sTri:={seq(Citxt[i..i+2],i=1..length(Citxt)-2)}:

Tri:=table();

for i from 1 to length(Citxt)-2 do Tri[Citxt[i..i+2]]:=0 od:

for i from 1 to length(Citxt)-2 do Tri[Citxt[i..i+2]]:=Tri[Citxt[i..i+2]]+1 od:

M:=max(seq(Tri[Citxt[i..i+2]],i=1..length(Citxt)-2));

                               2
sTri:=[];

for i from 1 to length(Citxt)-2 do
    if (Tri[Citxt[i..i+2]]=M) then
       sTri:=[op(sTri),(Citxt[i..i+2])];
    end if
end do;
                               []
loc:=[]:
for i from 1 to length(Citxt)-2 do
    if (Citxt[i..i+2]=sTri[8]) then
       loc:=[op(loc),i];
    end if
end do:
pos:=seq(loc[i]-loc[1],i=2..nops(loc));
                               54
ifactor(pos);
                                   3
                            (2) (3)
freq:=table();

for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:

for i from 1 to length(Citxt) do freq[Citxt[i]]:=freq[Citxt[i]]+1: od:

Ic:=proc(X) local i::int, freq::table;
     freq:=table();
     for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:
     for i from 1 to length(X) do freq[X[i]]:=freq[X[i]]+1: od:
     return add(freq[Sigma[i]]*(freq[Sigma[i]]-1),i=1..26)/(length(X)*(length(X)-1));
end proc:

blCoIn:=proc(n)
```

```
    return seq(evalf[2](Ic(seq(cat(seq(Citxt[n*i+j],i=0..length(Citxt)/n-1)),j=1..n)[k])),k=1..n);
end proc:

for i from 1 to 10 do print(i); blCoIn(i); od;

                               1
                             0.041
                               2
                          0.044, 0.046
                               3
                      0.044, 0.048, 0.048
                               4
                   0.043, 0.056, 0.047, 0.048
                               5
               0.044, 0.042, 0.040, 0.043, 0.037
                               6
            0.050, 0.061, 0.055, 0.071, 0.056, 0.070
                               7
        0.038, 0.046, 0.044, 0.038, 0.046, 0.033, 0.046
                               8
     0.058, 0.054, 0.049, 0.043, 0.038, 0.065, 0.046, 0.050
                               9
 0.044, 0.043, 0.040, 0.037, 0.040, 0.040, 0.043, 0.045, 0.062
                               10
0.069, 0.041, 0.024, 0.047, 0.041, 0.041, 0.054, 0.047, 0.053, 0.051

n:=6;
                               6

Yi:=[seq(cat(seq(Citxt[n*i+j],i=0..length(Citxt)/n-1)),j=1..n)]:

Mgt:=proc(y,g) local freq::table, i::int;
     freq:=table();
     for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:
     for i from 1 to length(y) do freq[y[i]]:=freq[y[i]]+1: od:
     return evalf[2](add(((p[i+1]*freq[Sigma[(i+g) mod 26+1]])/(length(Citxt)/6)),i=0..25));
end proc:

find:=proc(S) local i::int;
    for i from 1 to 26 do
        if (S[i]=max(op(S))) then
            print(i);
        end if;
    end do
end proc:

S1:=seq(Mgt(Yi[1],i),i=0..25);
0.040, 0.034, 0.034, 0.033, 0.044, 0.036, 0.040, 0.035, 0.046, 0.033, 0.037,
0.035, 0.044, 0.035, 0.028, 0.041, 0.040, 0.033, 0.034, 0.059, 0.042, 0.032,
0.035, 0.045, 0.034, 0.038

S2:=seq(Mgt(Yi[2],i),i=0..25);
0.041, 0.034, 0.032, 0.044, 0.036, 0.034, 0.037, 0.069, 0.036, 0.034, 0.028,
0.046, 0.029, 0.039, 0.035, 0.036, 0.036, 0.039, 0.049, 0.040, 0.046, 0.034,
0.041, 0.036, 0.035, 0.030

S3:=seq(Mgt(Yi[3],i),i=0..25);
0.053, 0.035, 0.032, 0.036, 0.062, 0.037, 0.028, 0.036, 0.042, 0.028, 0.033,
0.034, 0.038, 0.040, 0.045, 0.044, 0.038, 0.042, 0.034, 0.038, 0.037, 0.033,
0.034, 0.036, 0.034, 0.036

S4:=seq(Mgt(Yi[4],i),i=0..25);
0.041, 0.041, 0.038, 0.043, 0.035, 0.031, 0.030, 0.030, 0.028, 0.033, 0.052,
0.036, 0.030, 0.039, 0.068, 0.044, 0.033, 0.035, 0.042, 0.031, 0.032, 0.035,
0.030, 0.036, 0.043, 0.052

S5:=seq(Mgt(Yi[5],i),i=0..25);
0.037, 0.043, 0.048, 0.033, 0.042, 0.037, 0.040, 0.034, 0.034, 0.035, 0.034,
0.034, 0.033, 0.047, 0.035, 0.028, 0.039, 0.063, 0.041, 0.034, 0.040, 0.037,
0.029, 0.039, 0.041, 0.029

S6:=seq(Mgt(Yi[6],i),i=0..25);
0.031, 0.035, 0.035, 0.026, 0.035, 0.048, 0.033, 0.040, 0.043, 0.045, 0.037,
0.039, 0.033, 0.038, 0.032, 0.028, 0.039, 0.036, 0.040, 0.039, 0.053, 0.037,
0.033, 0.035, 0.065, 0.034

find([S1]); find([S2]); find([S3]); find([S4]); find([S5]); find([S6]);
                               20
                               8
                               5
                               15
                               18
                               25
Sigma[20];Sigma[8];Sigma[5];Sigma[15];Sigma[18];Sigma[25];
                              "T"
                              "H"
                              "E"
                              "O"
                              "R"
                              "Y"
chNum:=table(): numCh:=array(0..25):
for i from 1 to 26 do
     chNum[Sigma[i]]:=i;
     numCh[i-1]:=Sigma[i];
od:
key:=array(0..5,[20,8,5,15,18,25]);

Plntxt:="":
for i from 0 to (length(Citxt)-1) do
    Plntxt:=cat(Plntxt,numCh[(chNum[Citxt[i+1]]-(key[(i mod 6)])) mod 26]);
od:
print(Plntxt);
"IGREWUPAMONGSLOWTALKERSMENINPARTICULARWHODROPPED
WORDSAFEWATATIMELIKEBEANSINAHILLANDWHENIGOTTOMINNEA
POLISWHEREPEOPLETOOKALAKEWOBEGONCOMMATOMEANTHEEN
DOFASTORYICOULDNTSPEAKAWHOLESENTENCEINCOMPANYANDW
ASCONSIDEREDNOTTOOBRIGHTSOIENROLLEDINASPEECHCOURSE
TAUGHTBYORVILLESANDTHEFOUNDEROFREFLEXIVERELAXOLOGY
```

```
ASELFHYPNOTICTECHNIQUETHATENABLEDAPERSONTOSPEAKUPT
OTHREEHUNDREDWORDSPERMINUTE"
```

Question A1

See attached sheet at end.

Question A2

I just recycled code from the other two Vignère codes where I had to calculate the M_g table anyways. The small discrepancy in the third digit of the numbers is most likely caused by a combination of the rounding/truncation $n' = \frac{n}{m}$ and the way `evalf`[2] is outputting.

```
Sigma:="ABCDEFGHIJKLMNOPQRSTUVWXYZ":
p:=0.082,0.015,0.028,0.043,.127,0.022,.020,.061,.070,.002,.008,.040,
.024,0.067,0.075,0.019,0.001,0.060,0.063,0.091,0.028,0.010,0.023,0.001,0.020,.001]:

Citxt:="CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAKLXFP
SKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELXVRVPRTULH
DNQWTWDTYGBPHXTFALJHASVBFXNGLLCHRZBWELEKMSJIKNBH
WRJGNMGJSGLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLXRRIMG
NSNRWCHRQHAEYEVTAQEBBIPEEWEVKAKOEWADREMXMTBHHC
HRTKDNVRZCHRCLQOHPWQAIIWXNRMGWOIIFKEE":

freq:=table():

for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:

for i from 1 to length(Citxt) do freq[Citxt[i]]:=freq[Citxt[i]]+1: od:

Ic:=proc(X) local i::int, freq::table;
     freq:=table();
     for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:
     for i from 1 to length(X) do freq[X[i]]:=freq[X[i]]+1: od:
     return add(freq[Sigma[i]]*(freq[Sigma[i]]-1),i=1..26)/(length(X)*(length(X)-1));
end proc:

blCoIn:=proc(n)
    return seq(evalf[2](Ic(seq(cat(seq(Citxt[n*i+j],i=0..length(Citxt)/n-1)),j=1..n)[k])),k=1..n);
end proc:

Yi:=[seq(cat(seq(Citxt[n*i+j],i=0..length(Citxt)/n-1)),j=1..n)]:

Mgt:=proc(y,g)::float; local freq::table, i::int;
     freq:=table();
     for i from 1 to length(Sigma) do freq[Sigma[i]]:=0; od:
     for i from 1 to length(y) do freq[y[i]]:=freq[y[i]]+1: od:
     return evalf[3](add(((p[i+1]*freq[Sigma[((i+g) mod 26) +1]])/(length(Citxt)/n)),i=0..25));
end proc:


seq(Mgt(Yi[2],i),i=0..25);

0.0672, 0.0435, 0.0322, 0.0350, 0.0431, 0.0346, 0.0355, 0.0329, 0.0293,
0.0312, 0.0416, 0.0436, 0.0387, 0.0441, 0.0460, 0.0424, 0.0361, 0.0312,
0.0335, 0.0370, 0.0325, 0.0337, 0.0424, 0.0305, 0.0262, 0.0467
```

Question A3

See attached sheet at end.