Ukol 2: Kryptoanalyza sifry $|ap+b|_m$ (2)

```
In[200]:=
ST =
  "VMRBAVAVUPUVDBAVNKAVNRPRBVRJSKFVUKCNKZROBMPUCRONNSRBUZURJWDPUNVZFKXROBMZUPROCJ␣
    QFUVRNVMRXVKVMRNVOCJOFJKAVSAVUZCKZUPROFEAXRCVNOFRNSRBUZURJKFOZUPROFEAXRCV␣
    UNONUCEPRJONMBAVFROJNZFKXVMRNVOCJOFJUCSAVVMRUVRXNNSRBUZURJWDPUNVBOCWRUCVR␣
    FXNKZBKPAXCSKNUVUKCKFUCVRFXNKZZURPJNJRPUXUVRJWDONSRBUOPBMOFOBVRFBKPAXCCAX␣
    WRFUCENVOFVNZFKXVMRPUNVKSVUKCOFEAXRCVUNOBKXXOKFQMUVRNSOBRNRSOFOVRJNRVKZCA␣
    XWRFNOCJKFCAXWRFFOCERNCAXWRFFOCERNBKCNUNVKZOCAXWRFOJONMOCJONRBKCJCAXWRFOC␣
    JNRPRBVVMRZURPJNKFBKPAXCNZFKXVMRZUFNVCAXWRFVKVMRNRBKCJUCBPANUIRCAXWRFNKFC␣
    AXWRFFOCERNXODWRSFRBRJRJWDOJONMQMUBMNRPRBVNOPPZURPJNKFBKPAXCNZFKXVKVMRPON␣
    VCAXWRFCAXWRFNKFCAXWRFFOCERNXODWRZKPPKQRJWDOJONMQMUBMNRPRBVNOPPZURPJNKFBK␣
    PAXCNZFKXVMRPONVCAXWRFVKVMRRCJKZVMRPUCRCAXWRFNOCJCAXWRFFOCERNXODWRFRSROVR␣
    JKIRFPOSSUCEOCJUCOCDKFJRFUZOZURPJKFBKPAXCUNNSRBUZURJXAPVUSPRVUXRNUVQUPPOS␣
    SROFKCPDKCBRUCVMRKAVSAVUVUNCKVOCRFFKFVKNRPRBVZURPJNKFBKPAXCNCKVSFRNRCVUCV␣
    MRUCSAVPUCR";
```

2. Az obdrzite sifrovy text od souseda, priradte jeho hodnotu do promenne ST:

```
In[201]:=
NCharacters = 29;
```

Nyni provedte analyzu cetnosti:

```
In[202]:=
RelCetnosti[ST]
```

```
Out[202]//TableForm=
A       B       C       D       E       F       G
0.043   0.039   0.076   0.012   0.012   0.071   0
H       I       J       K       L       M       N
0       0.0022  0.041   0.065   0       0.030   0.077
O       P       Q       R       S       T       U
0.066   0.052   0.0067  0.12    0.025   0       0.070
V       W       X       Y       Z       [       \
0.080   0.027   0.048   0       0.033   0       0
]
0
```

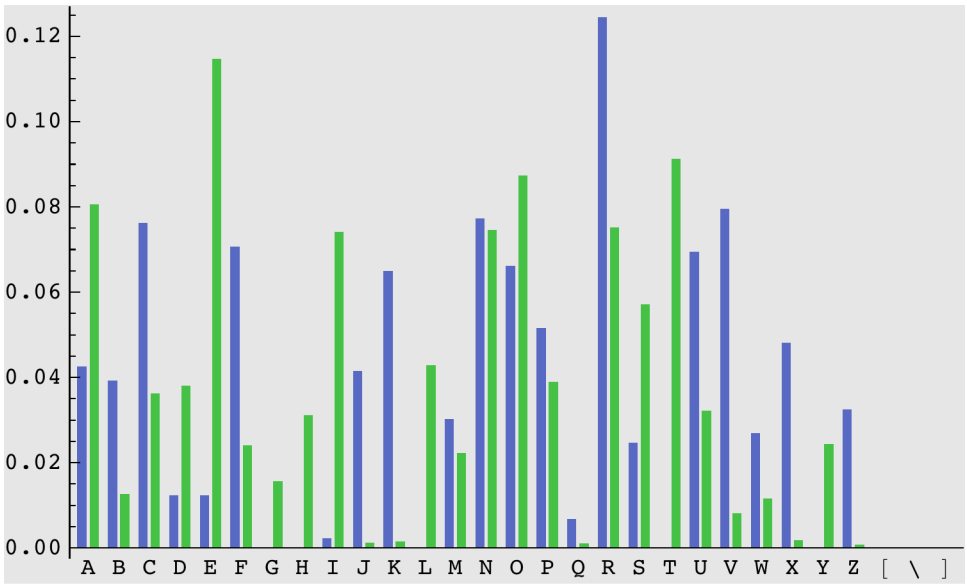
A srovnejte ji s cetnostmi pro anglictinu:

```
In[203]:=
RelCetnostiZBEZRelCetnosti[ENGLISH]
```

```
Out[203]//TableForm=
A       B       C       D       E       F       G
0.081   0.013   0.036   0.038   0.11    0.024   0.016
H       I       J       K       L       M       N
0.031   0.074   0.0013  0.0015  0.043   0.022   0.075
O       P       Q       R       S       T       U
0.087   0.039   0.0010  0.075   0.057   0.091   0.032
V       W       X       Y       Z
0.0082  0.012   0.0018  0.024   0.00074
```

```
In[204]:=
BEZGrafyRelCetnostiSAnglictinou[ST]
```

```
Out[204]=
```



Ukol 2: Kryptoanalyza sifry $|ap+b|_m$ (3)

Z analyzy relativnich cetnosti muzeme zjistit, ze nejcetni pismena pro anglictinu jsou T a E. Toho muzeme pouzit pro zjisteni desifrovaciho klice. Vybereme tedy 2 nejcetnejsi pismena z analyzy sifroveho textu a zkusime je namapovat na T a E. Resenim soustavy 2 rovnic o 2 neznamych vypocteme neznane koeficienty a a b.

Rekneme ze pro nas priklad vidime, ze nejcetnejsi jsou pismena U a B. Zkusme tedy predpokladat, ze:

$$U = |a\,T + b|_{29}$$

$$B = |a\,E + b|_{29}$$

Tedy, z T neznamou transformaci vznikne U a z E touz transformaci vznikne B. Abychom urcili a a b, musime uz jen vyresit tyto dve rovnice napriklad dosazovaci metodou:

$$b = |U - a\,T|_{29}$$

$$B = |a\,E + |U - a\,T|_{29}|_{29}$$

Protoze nezalezi, kdy redukci mod 29 provedeme, muzeme vztah prepsat jako:

$$B = |a\,(E - T) + U|_{29}$$

$$a = |(B - U)*(E - T)^{-1}|_{29}$$

$$b = |U - (B - U)*(E - T)^{-1}\,T|_{29}$$

Nyni muzeme predpis zkusit (pozn. pokud budete pocitat na papire, nezapomente ze A odpovida 0, B 1, atd.):

Ukol 2: Kryptoanalyza sifry $|ap+b|_m$ (4)

Pro jednoduchost jsou zde rovnice implementovany do systemu *Mathematica* a vypoctene konstanty se ulozi do promennych c a d.

```
In[207]:=
    c = Mod[(Pozice["R"] - Pozice["V"]) *
        BEZInverse[Pozice["E"] - Pozice["T"], NCharacters], NCharacters]
    d = Mod[Pozice["V"] - c * Pozice["T"], NCharacters]

Out[207]=
    8

Out[208]=
    14
```

Nyni se muzeme pokusit text desifrovat:

```
In[209]:=
    AXPBDecrypt[ST, c, d]

Out[209]=
    THECUTUTILITYCUTSOUTSELECTEDPORTIONSOFEACHLINEASSPECIFIEDBYLISTFROMEACHFILEANDWRI
       TESTHEMTOTHESTANDARDOUTPUTIFNOFILEARGUMENTSARESPECIFIEDORAFILEARGUMENTISASING
       LEDASHCUTREADSFROMTHESTANDARDINPUTTHEITEMSSPECIFIEDBYLISTCANBEINTERMSOFCOLUMN
       POSITIONORINTERMSOFFIELDSDELIMITEDBYASPECIALCHARACTERCOLUMNNUMBERINGSTARTSFRO
       MTHELISTOPTIONARGUMENTISACOMMAORWHITESPACESEPARATEDSETOFNUMBERSANDORNUMBERRAN
       GESNUMBERRANGESCONSISTOFANUMBERADASHANDASECONDNUMBERANDSELECTTHEFIELDSORCOLUM
       NSFROMTHEFIRSTNUMBERTOTHESECONDINCLUSIVENUMBERSORNUMBERRANGESMAYBEPRECEDEDBYA
       DASHWHICHSELECTSALLFIELDSORCOLUMNSFROMTOTHELASTNUMBERNUMBERSORNUMBERRANGESMAY
       BEFOLLOWEDBYADASHWHICHSELECTSALLFIELDSORCOLUMNSFROMTHELASTNUMBERTOTHEENDOFTHE
       LINENUMBERSANDNUMBERRANGESMAYBEREPEATEDOVERLAPPINGANDINANYORDERIFAFIELDORCOLU
       MNISSPECIFIEDMULTIPLETIMESITWILLAPPEARONLYONCEINTHEOUTPUTITISNOTANERRORTOSELE
       CTFIELDSORCOLUMNSNOTPRESENTINTHEINPUTLINE
```

Transpozice

Substituce zpusobuje konfuzi nahradou jednoho znaku znakem jinym a sifry zalozene na ni jsou zranitelne frekvencni analyzou. Proto obvykle substituci kombinujeme s transpozici, ktera preskupuje poradi pismen v textu (difuze). To se v praxi provadi zapsanim otevreho textu do matice po radcich a precteni po sloupcich. Ukazme si to na priklade textu "PLEASE SEND MONEY", ktery nejdrive doplnime vyplni (X) na delku, ktera obsadi celou matici. Tak ziskame matici:

$$\begin{pmatrix} P & L & E & A & S & E \\ S & E & N & D & M & O \\ N & E & Y & X & X & X \end{pmatrix}$$, kterou transponujeme $$\begin{pmatrix} P & S & N \\ L & E & E \\ E & N & Y \\ A & D & X \\ S & M & X \\ E & O & X \end{pmatrix}$$ a precteme text po radcich, cimz dostavame:

PSNLEEENYADXSMXEOX. V kombinaci se substituci napriklad pomoci afinni sifry je vysledna sifra posilena. Transpozici si muzete vyzkouset volanim funkce **Transpozice[retezec, pocet sloupcu]**:

```
In[63]:= NCharacters = 26;
         ST = Transpozice["THE GOLD IS BURIED IN ORONO", 6]
```

Pokud bychom chteli videt matici, muzete pouzit funkci **BEZGenerMatrix[retez, pocet sloupcu].** Tim zaroven uvidime mnozstvi vyplne, ktere se pridalo na zarovnani na potrebnou delku.