bigramy s nejvetsi cetnosti, coz jsou: TH, HE, AN, RE, ER, IN, ON, AT, ND, ST, ES, EN, OF, TE a ze vzdalenosti znaku bigramu se snazime stanovit parametry transpozice, ktere byly pouzity. Pro sifrovy textTDIRHIEOESDNG-BIOOUNXLROX vidime ihned bigramy TH a HE z cehoz usoudime, ze mela matice 4 radky:

```
In[215]:=
    Transpozice["TDIRHIEOESDNGBIOOUNXLROX", 4]

Out[215]=
    THEGOLDISBURIEDINORONOXX
```

Dalsi moznosti je faktorizovat delku textu a tim zjistit vsechny delitele delky textu a postupne je zkusit.

```
In[216]:=
    FactorInteger[StringLength["TDIRHIEOESDNGBIOOUNXLROX"]] /.
     {x_Integer, y_Integer} → HoldForm[x^y]

Out[216]=
    {2^3, 3^1}
```

Zde tento pripad vidime, ze delka textu je 24 znaku. Z toho muzeme usoudit, ze pro transpozice mohla byt: 2*12, 3*8, 4*6, 6*4, 8*3, 12*2. Jine kombinace neexistuji. Pro nas pripad byla pouzita transpozice 6*4.

Pokud text nebyl tak dlouhy, jak byl zadan predpis, musel byt doplnen vyplni (padding). Ze znalosti funkce, ktera transpozici provadi vime, ze tato funkce doplnuje na konec textu pismena X, dokud nezarovna text na potrebnou delku a to je skutecnost, kterou muzeme vyuzit k prolomeni transpozice, protoze vzdalenost teto vyplne (zvlaste v pripade, ze bylo doplneno vice znaku X) udava transpozicni konstantu, ktera byla pouzita pri sifrovani. Delka textu/tato konstanta udava detranspozicni konstantu.

Pro nas text vidime, ze vzdalenost paddingu X je 4 znaky, z cehoz rovnou plyne konstanta pro detranspozici.

Upozorneni: Pokud byla transpozice pouzita vicenosobne, je jeji kryptoanalyza znacne obtiznejsi!!

```
In[217]:=
    Transpozice[Transpozice["THEGOLDISBURIEDINORONO", 4], 3]

Out[217]=
    TIHEEDGIONLODRIOSNBOUXRX
```

Ukol 3: Kryptoanalyza transpozice

Napiste kus anglickeho textu o delce 30-50 znaku a nahodne zvolte transpozicni konstantu. Provedte nad timto textem transpozici s vami zvolenou konstantou a vysledny sifrovy text poslete sousedovi.

```
In[218]:=
    OT = "DEFEATTHETRANSPOSITIONCHALLENGE"

Out[218]=
    DEFEATTHETRANSPOSITIONCHALLENGE

In[219]:=
    Transpozice[OT, 9]

Out[219]=
    DTTEERINFAOGENNEASCXTPHXTOAXHSLXEILX
```

Az obdrzite text od souseda, priradte ho to teto promenne:

In[223]:=

```
ST =
 "TSSITUAOLLSSNOHSNTYEOWAARROCEAHDIMNTIATTUIINSETEAETTOHTDTPLCE[IESFNETISFEUEOATA
    HHSNTDOOOTEEUASIALOHSRLGVRDELOOIOHTSNEABRAICNHROTSIOLNYTTEOREASOSTOISNSEHCF
    SETRIRSSOHDEHSORIRVITEPLODHDTFWCSFTUTETAIEINGFAIDNDBTUAEETYPUAEIMEWRSMEAASO
    LAENCHAEIMUAERITOEIGFISUAUTISFUGSDETERDTAVHBTEEWLEEIEFEINYNROMHEAHAATPTTAIR
    HCTRNORASNFGEETTNDRHOTSGLNBEAKHPAFVTFALMDHOMRNEDUSKSHRAOIHCAGVSUSTIRSOWPIOE
    AENIOEOVPHIRRNTEASTOCIRIEFAAMSEROHLOBEOYNHRAUATOEREEHSEHEFOTEESEANPIAUEAIVR
    TAPIOEHHAIGNWTEKNNSIPSUAEDTSCVICIRVFNRADSMEROEEVEVTHATIHFONINRLRLEIDIDELNIR
    MCAEAPGVERRSNNOCRASSRAWAERNEUNNGLGTITIRUGLDOENOEEEENSDATSLTSGAIHIAITITOETOT
    CATENEKRNEAEEENIOEGVGDATOTLSNTNAAOOREMEMRBHUANYRHWBRHINTCASASPBDWBGYULEUSSM
    YBHIINRDIRWRDETNLETAHTENOEGNVEAHDLHWIHCHHRDEISDNSRRDVNCRESATORIOHDHGYCCFTIU
    NEHIYSGDOEARYARNDOUUASETYLYLCX"
```

Out[223]=

```
TSSITUAOLLSSNOHSNTYEOWAARROCEAHDIMNTIATTUIINSETEAETTOHTDTPLCE[IESFNETISFEUEOATAHH
   SNTDOOOTEEUASIALOHSRLGVRDELOOIOHTSNEABRAICNHROTSIOLNYTTEOREASOSTOISNSEHCFSETR
   IRSSOHDEHSORIRVITEPLODHDTFWCSFTUTETAIEINGFAIDNDBTUAEETYPUAEIMEWRSMEAASOLAENCH
   AEIMUAERITOEIGFISUAUTISFUGSDETERDTAVHBTEEWLEEIEFEINYNROMHEAHAATPTTAIRHCTRNORA
   SNFGEETTNDRHOTSGLNBEAKHPAFVTFALMDHOMRNEDUSKSHRAOIHCAGVSUSTIRSOWPIOEAENIOEOVPH
   IRRNTEASTOCIRIEFAAMSEROHLOBEOYNHRAUATOEREEHSEHEFOTEESEANPIAUEAIVRTAPIOEHHAIGN
   WTEKNNSIPSUAEDTSCVICIRVFNRADSMEROEEVEVTHATIHFONINRLRLEIDIDELNIRMCAEAPGVERRSNN
   OCRASSRAWAERNEUNNGLGTITIRUGLDOENOEEEENSDATSLTSGAIHIAITITOETOTCATENEKRNEAEEENI
   OEGVGDATOTLSNTNAAOOREMEMRBHUANYRHWBRHINTCASASPBDWBGYULEUSSMYBHIINRDIRWRDETNLE
   TAHTENOEGNVEAHDLHWIHCHHRDEISDNSRRDVNCRESATORIOHDHGYCCFTIUNEHIYSGDOEARYARNDOUU
   ASETYLYLCX
```

Nyni se snazte zjistit, jakou transpozici vas soused pouzil. Vyuzijte metod popsanych na minulem slajdu. Pro jednoduchost faktorizaci opakujeme nyni pro promennou sifroveho textu:

In[228]:=

```
FactorInteger[StringLength[ST]] /. {x_Integer, y_Integer} → HoldForm[x^y]
```

Out[228]=

$\{2^4, 7^2\}$

In[229]:=

```
Transpozice[ST, 112]
```

Out[229]=

```
THEAUGUSTAFELLSSAVAGEINSTITUTEOFVISUALARTSABALTIMOREMARYLANDPUBLICHIGHSCHOOLISNAM
   EDINHERHONORINHERHOMEANDSTUDIOINSAUGERTIESNEWYORKWERELISTEDONTHENEWYORKSTATEA
   NDNATIONALREGISTEROFHISTORICPLACESASTHEAUGUSTASAVAGEHOUSEANDSTUDIOITISTHEMOST
   SIGNIFICANTSURVIVINGSITEASSOCIATEDWITHTHEPRODUCTIVELIFEOFTHISRENOWNEDARTISTTE
   ACHERANDACTIVISTHERHOMEHASBEENRESTOREDTOEVOKETHEPERIODWHENSHELIVEDTHEREANDSER
   VESTOINTERPRETHERLIFEANDCREATIVEVISION[INTHECITYOFGREENCOVESPRINGSFLORIDANOMINA
   TEDHERTOTHEFLORIDAARTISTHALLOFFAMESHEWASINDUCTEDTHESPRINGOFTODAYATTHEACTUALLO
   CATIONOFHERBIRTHTHEREISACOMMUNITYCENTERNAMEDINHERHONORABIOGRAPHYOFAUGUSTASAVA
   GEINTENDEDFORYOUNGERREADERSHASBEENWRITTENBYAUTHORALANSCHROEDERINHERHANDSTHEST
   ORYOFSCULPTORAUGUSTASAVAGEWASRELEASEDINSEPTEMBERBYLEEANDLOWANEWYORKPUBLISHING
   COMPANYX
```