# ÚLOHA B

## Jednoduchá transpozice, úplná tabulka, délka transpozičního hesla menší než 9.

```
ULEPK HLOMI DOLUJ OKAAT EZNEL PENUE SIDNA ALYEL TPJKU SEMAJ DPLIP ZNLDE ECEEN
UKUJN EIMHL ILNCA NUPTD ONILI PTERK HUMEK ADPOS DENOU SIDSE LESIM HTMSA OJNES
YDONB UTODV NHLOS NOSBE SEAMA PNBKU ETLUT KDYAA DUTOD EUJEM AEAUE LTENV ASUDD
SLSAE OMDEY PEOOS
```

**Otázka (6 bodů)**

- Jako důkaz, že jste úlohu správně vyřešili, zadejte čtvrté slovo vyluštěného textu (otevřeného textu). Slovo zadejte velkými písmeny.

## Řešení:

```
ULEPKHLOMIDOLUJOKAATEZNELPENUESIDNAALYELTPJKUSEMAJDPLIPZNLDEECEENUKUJNEIMHLILNC
ANUPTDONILIPTERKHUMEKADPOSDENOUSIDSELESIMHTMSAOJNESYDONBUTODVNHLOSNOSBESEAMAPNB
KUETLUTKDYAADUTODEUJEMAEAUELTENVASUDDSLSAEOMDEYPEOOS
```

1) ZJIŠTĚNÍ SPRÁVNÉHO ROZMĚRU TABULKY
(POMĚR SMAOHLÁSEK A SOUHLÁSEK **2 : 3**)

**210**
2x105, 3x70, 5x48, 6x35, 7x30, 10x21, …

3x70 (1,2 : 1,8), 0,3 = 18 ze 70 = 25,7%

```
ULEPKHLOMIDOLUJOKAATEZNELPENUESIDNAALYELTPJKUSEMAJDPLIPZNLDEECEENUKUJN
EIMHLILNCANUPTDONILIPTERKHUMEKADPOSDENOUSIDSELESIMHTMSAOJNESYDONBUTODV
NHLOSNOSBESEAMAPNBKUETLUTKDYAADUTODEUJEMAEAUELTENVASUDDSLSAEOMDEYPEOOS
21110111030311120212201200213112021221311211202120101111002230221213 13
```

5x48 (2 : 3), 01345=11 z 48 =22,9%

```
ULEPKHLOMIDOLUJOKAATEZNELPENUESIDNAALYELTP
JKUSEMAJDPLIPZNLDEECEENUKUJNEIMHLILNCANUPT
DONILIPTERKHUMEKADPOSDENOUSIDSELESIMHTMSAO
JNESYDONBUTODVNHLOSNOSBESEAMAPNBKUETLUTKDY
AADUTODEUJEMAEAUELTENVASUDDSLSAEOMDEYPEOOS
22322222221322222322312323213222223223222 2
```

```
6x35 (2,4 : 3,6), 01456=14  z 35 =  40%
ULEPKHLOMIDOLUJOKAATEZNELPENUESIDNA
ALYELTPJKUSEMAJDPLIPZNLDEECEENUKUJN
EIMHLILNCANUPTDONILIPTERKHUMEKADPOS
DENOUSIDSELESIMHTMSAOJNESYDONBUTODV
NHLOSNOSBESEAMAPNBKUETLUTKDYAADUTOD
EUJEMAEAUELTENVASUDDSLSAEOMDEYPEOOS
432412321605231303233014232353333331

7x30 (2,8:4,2), 0145=13 Z 30 = 43%
ULEPKHLOMIDOLUJOKAATEZNELPENUE
SIDNAALYELTPJKUSEMAJDPLIPZNLDE
ECEENUKUJNEIMHLILNCANUPTDONILI
PTERKHUMEKADPOSDENOUSIDSELESIM
HTMSAOJNESYDONBUTODVNHLOSNOSBE
SEAMAPNBKUETLUTKDYAADUTODEUJEM
AEAUELTENVASUDDSLSAEOMDEYPEOOS
335243143252231323542305225244
```

10x21 (4 : 6)

```
ULEPKHLOMIDOLUJOKAATE
ZNELPENUESIDNAALYELTP
JKUSEMAJDPLIPZNLDEECE
ENUKUJNEIMHLILNCANUPT
DONILIPTERKHUMEKADPOS
DENOUSIDSELESIMHTMSAO
JNESYDONBUTODVNHLOSNO
SBESEAMAPNBKUETLUTKDY
AADUTODEUJEMAEAUELTEN
VASUDDSLSAEOMDEYPEOOS
346444353435454355455
```

## 2) Luštění (😊 – lištovka)

5X24 (2 : 3)

```
1    ULEPKHLOMIDOLUJOKAATEZNELPENUESIDNAALYELTP
2    JKUSEMAJDPLIPZNLDEECEENUKUJNEIMHLILNCANUPT
3    DONILIPTERKHUMEKADPOSDENOUSIDSELESIMHTMSAO
4    JNESYDONBUTODVNHLOSNOSBESEAMAPNBKUETLUTKDY
5    AADUTODEUJEMAEAUELTENVASUDDSLSAEOMDEYPEOOS

JDU JÁ ?

2    JKUSEMAJDPLIPZNLDEECEENUKUJNEIMHLILNCANUPT
3    DONILIPTERKHUMEKADPOSDENOUSIDSELESIMHTMSAO
1    ULEPKHLOMIDOLUJOKAATEZNELPENUESIDNAALYELTP
4    JNESYDONBUTODVNHLOSNOSBESEAMAPNBKUETLUTKDY
5    AADUTODEUJEMAEAUELTENVASUDDSLSAEOMDEYPEOOS
```

```
Já JDU ?

4     JNESYDONBUTODVNHLOSNOSBESEAMAPNBKUETLUTKDY
5     AADUTODEUJEMAEAUELTENVASUDDSLSAEOMDEYPEOOS
2     JKUSEMAJDPLIPZNLDEECEENUKUJNEIMHLILNCANUPT
3     DONILIPTERKHUMEKADPOSDENOUSIDSELESIMHTMSAO
1     ULEPKHLOMIDOLUJOKAATEZNELPENUESIDNAALYELTP
```

## 3) Řešení:

```
JNESYDONBUTODVNHLOSNOSBESEAMAPNBKUETLUTKDY
AADUTODEUJEMAEAUELTENVASUDDSLSAEOMDEYPEOOS
JKUSEMAJDPLIPZNLDEECEENUKUJNEIMHLILNCANUPT
DONILIPTERKHUMEKADPOSDENOUSIDSELESIMHTMSAO
ULEPKHLOMIDOLUJOKAATEZNELPENUESIDNAALYELTP
```

```
JA JDU NA KOLEDU NESU SI PYTEL KDO MI HO DA PLNEJ TO BUDE MUJ PRITEL KDO MI HO
DA PUL VEZMU NA NEJ HUL KOLEDA KOLEDA STEPANE CO TO NESES VE DZBANE NESU NESU
KOLEDU UPAD JSEM S NI NA LEDU PSI SE NA ME SBEHLI KOLEDU MI SNEDLI A TEN MALY
CHLUPATY TEN ME KOUSL DO PATY STOP
```

Použitý otevřený text je:

Já jdu na koledu, nesu si pytel, kdo mi ho dá plnej, to bude můj přítel. Kdo mi ho dá půl, vezmu na něj hůl. Koleda, koleda, Štěpáne, co to neseš ve džbáně? Nesu, nesu koledu, upad jsem s ní na ledu. Psi se na mě sběhli, koledu mi snědli a ten malý chlupatý, ten mě kousl do paty. Stop.

- Jako důkaz, že jste úlohu správně vyřešili, zadejte čtvrté slovo vyluštěného textu (otevřeného textu). Slovo zadejte velkými písmeny.

**správná odpověď**: ***KOLEDU***

```
4) Závěrečné informace

(AOPST - STOPA)
```

Pro šifrování a kontrolu dešifrování (nikoliv však luštění) lze použít např. tento software
https://asecuritysite.com/encryption/col

https://asecuritysite.com/encryption/col?phrase=defendtheeastwallofthecastle&key=GERMAN

## Columnar Transposition Cipher

Back A columnar transposition does a row-column transpose (see below).

**Parameters**

Message:

```
CANUPTDONILIPTERKHUMEKADPOSDENOUSIDSELE
SIMHTMSAOJNESYDONBUTODVNHLOSNOSBESEAMAP
NBKUETLUTKDYAADUTODEUJEMAEAUELTENVASUDD
SLSAEOMDEYPEOOS
```

Key:

STOPA

**Mode:** Encrypt:○ Decrypt:◉

```
JAJDUNAKOLEDUNESUSIPYTELKDOMIHODAPLNEJTOBUDEMUJPRITELKDOMIHODAPULVEZM
UNANEJHULKOLEDAKOLEDASTEPANECOTONESESVEDZBANENESUNESUKOLEDUUPADJSEMSN
INALEDUPSISENAMESBEHLIKOLEDUMISNEDLIATENMALYCHLUPATYTENMEKOUSLDOPATYS
TOP
```