Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 13, číslo 2/2011 **20. únor 2011**

2/2011

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1360 registrovaných odběratelů)

Obsah :

A. Československé šifry z obdobia 2. svetovej vojny Diel 2., Šifra „Rímska dva“

Jozef Kollár, jmkollar@math.sk
KMaDG, SvF STU v Bratislave

Mnohé informácie o československých šifrách z obdobia 2. svetovej vojny mi stále chýbajú. Preto ak niekto viete doplniť, prípadne opraviť mnou uvádzané popisy šifier (TTS, Rímska 2, 8, 9, 10, 13, Eva, Marta, Růžena, Utility a Palacký), alebo máte akékoľvek informácie o ďalších československých šifrách z obdobia 2. svetovej vojny, tak všetky tieto informácie s radosťou uvítam.

2 Šifra „Rímska dva“

Popis tejto šifry je uvedený v [2] (str. 115–116) a v [5] (str. 269–303). V druhom uvedenom zdroji je aj podrobná ukážka lúštenia tejto šifry na príklade autentických depeší z 2. svetovej vojny. Šifra „Rímska dva“ je šifra typu STT. Pri šifrovaní sa najskôr robí substitúcia znakov za dvojciferné čísla a následne dvojitá tabuľková transpozícia. Táto šifra bola zavedená ako zdokonalenie predtým používanej šifry TTS. Plukovník Moravec[1], ktorý bol prednostom vojenskej spravodajskej služby a pracoval pre exilovú vládu v Londýne, pokladal túto šifru za veľmi bezpečnú, pravdepodobne na veľké potešenie nemeckých lúštiteľov.

2.1 Všeobecný popis a príklad šifrovania depeší

Postup šifrovania je podobne jednoduchý ako pri šifre TTS. Rozdiel je len v poradí jednotlivých operácii, ktoré vykonávame pri šifrovaní. Pri šifre STT sa najskôr spravila substitúcia znakov za čísla a až potom sa robila dvojitá tabuľková transpozícia. Táto dvojitá transpozícia „roztrhala“ číselné dvojice predstavujúce jednotlivé znaky a to trocha skomplikovalo lúštenie, pretože

[1] Svoj nedostatok kompetentnosti bohato kompenzoval nadbytkom intrigánstva pred aj počas celej 2. svetovej vojny. Veľmi rád a aktívne sa zapájal do rôznych politických hier, intríg a podrazov. Svojou neschopnosťou a intrigami má priamo, či nepriamo, na svedomí stovky, možno tisíce, životov v domácom odboji.
(Zdroje: wikipedia http://cs.wikipedia.org/wiki/František_Moravec_(generál) a čiastočne aj knihy uvedené v použitej literatúre.)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		A	B	C	Č	D	Ď	E	Ě	F
1	G	H	I	J	K	L	M	N	Ň	O
2	P	Q	R	Ř	S	Š	T	Ť	U	V
3	W	X	Y	Z	Ž	.	?	-	/	,
4	:	1	2	3	4	5	6	7	8	9
5	0									

Tabuľka 1: Česká 50 znaková abeceda v základnej podobe

na desiatkových miestach mohla byť ľubovoľná z cifier 0 až 9. Preto sa niektorí používatelia tejto šifry domnievali, že je „nerozlúštiteľná“, resp. dostatočne bezpečná. Ďalší drobný rozdiel medzi šiframi TTS a STT spočíval v tom, že kým pri šifre TTS sa počet cifier v depeši dopĺňal na násobok 5 až celkom na záver šifrovania, pri šifre STT sa tento počet dopĺňal na začiatku, ihneď po substitúcii znakov za čísla.

Na substitúciu znakov sa najskôr používala, už z TTS známa, 45 znaková česká abeceda, modifikovaná pre príslušný deň šifrovania rovnako ako pri šifre TTS. Táto abeceda vo svojej základnej podobe je uvedená v tabuľke 1 na strane 4, v prvom diely tohto seriálu (Crypto-World 1/2011). Neskôr sa pre šifru STT používala rozšírená, 50 znaková česká abeceda vo svojej základnej podobe, t.j. znak `A` mal vždy hodnotu 01[2]. Táto 50 znaková abeceda je uvedená v tabuľke 1. Nie je vylúčené, že sa pre šifru STT používali ešte aj iné substitučné tabuľky.

Pokiaľ ide o transpozičné heslá pre prvú a druhú transpozičnú tabuľku, tak mi nie je známe akým spôsobom sa tieto heslá vyberali, prípadne tvorili. Podľa dostupných zdrojov (najmä kníh pána Janečka) sa dá predpokladať, že heslá boli vyberané z dohodnutých kníh, rovnako ako pri šifre TTS. Heslá mali mať dĺžku 10–25 znakov[3]. Pán Hanák vo svojom popise šifry STT v [2] na str. 115 uvádza, že heslá nemali byť kratšie než 15 znakov. Avšak príklady autentických depeší z 18. 7. 1942 uvedených v [5] na str. 269 majú dĺžku prvého transpozičného hesla 12, čo tvrdeniu pána Hanáka odporuje. Zrejme existovalo len doporučenie, že heslá by mali mať dĺžku aspoň 15 znakov, ale toto doporučenie sa asi nie vždy v praxi dodržiavalo.

Dlhšie texty sa, rovnako ako pri šifre TTS, rozdeľovali na časti. Podľa už spomenutých ukážok autentických depeší z 18. 7. 1942, uvedených v [5]

[2]Podľa [5], str. 301.
[3]Podľa [5], str. 277.

na str. 269, mali tieto časti dĺžku približne 100 znakov. Nadväznosť jednotlivých dielov seriálu sa zabezpečovala pridávaním znaku / a rovnakého písmena abecedy na koniec a začiatok nadväzujúcich častí. Čiže postup rozdeľovania a označovania častí bol rovnaký ako pri šifre TTS.

Pre ilustráciu si teraz zašifrujeme nejaký text šifrou STT. Na substitúciu použijeme 50 znakovú abecedu uvedenú v tabuľke 1. Predpokladajme, že šifrujeme 21. deň v mesiaci a na tento deň máme stanovené dĺžky hesiel `21-13-17`, čiže heslá prvej a druhej transpozičnej tabuľky budú mať dĺžku 13, resp. 17 znakov. Na tvorbu hesiel použijeme knihu Simona Singha: *Kniha kódů a šifer*, (Dokořán, 2003). Na 21. strane, na začiatku 21. riadku, vyberieme prvých 12 znakov ako základ hesla prvej transpozičnej tabuľky. Sú to znaky: `JE MOŽNÉ JE PRO`. Potom ďalších 12 znakov ako základ hesla druhej transpozičnej tabuľky. To budú znaky: `VĚTŠÍ BEZPEČN`. Medzery sa do počtu znakov nerátajú. Vybraných 12 znakov predĺžime na potrebnú dĺžku tak, že zopakujeme potrebný počet znakov zo začiatku vybraného úseku. Potom zapíšeme tieto znaky bez medzier a len pomocou znakov použitej substitučnej abecedy. Napokon obe transpozičné heslá vyčíslime obvyklým spôsobom, opäť podľa poradia znakov použitej substitučnej abecedy. V našom príklade dostaneme:

J	E	M	O	Ž	N	E	J	E	P	R	O	J
4	1	7	9	13	8	2	5	3	11	12	10	6

Tabuľka 2: Heslo prvej transpozičnej tabuľky a jeho vyčíslenie

V	Ě	T	Š	I	B	E	Z	P	E	Č	N	V	Ě	T	Š	I
15	5	13	11	7	1	3	17	10	4	2	9	16	6	14	12	8

Tabuľka 3: Heslo druhej transpozičnej tabuľky a jeho vyčíslenie

Máme teda obe transpozičné heslá a ich vyčíslenie a môžme pristúpiť k šifrovaniu textu. Ako príklad použijeme opäť citát od Senecu:

> *Cokoliv se přihodí řádnému muži, to ponese s vyrovnanou myslí; bude si vědom, že to přišlo z božského ustanovení, podle něhož se vše řídí.*
>
> *Seneca*[4]

[4]Pôvodná verzia v latinčine: *Quidquid illi (bono viro) accidit, aequo animo sustinebit; sciet enim id accidisse lege divina, qua universa procedunt. Seneca (Ep.76,23)*

Tento text prepíšeme len pomocou znakov zo substitučnej tabuľky, vynecháme znaky, ktoré v tejto tabuľke nie sú a medzery nahradíme pomlčkami. Všetky úpravy textu robíme rovnako ako to bolo popísané pri šifre TTS, akurát použitá substitučná tabuľka je mierne odlišná. Po týchto úpravách bude dĺžka textu 140 znakov. Podľa ukážok depeší z [5] sa bežne zvykli takto dlhé texty šifrovať aj do jednej depeše, ale mi si text rozdelíme na dve časti. Rozdeľujeme ho tak, aby každá časť končila celým slovom a dbáme na to aby žiadne dve (v prípade väčšieho počtu častí) časti nemali rovnakú dĺžku. Označíme ešte nadväznosť dielov a dostávame texty:

```
COKOLIV-SE-PŘIHODI-ŘADNEMU-MUŽI,TO-
PONESE-S-VYROVNANOU-MYSLI-BUDE-SI/A

A/VEDOM,ŽE-TO-PŘIŠLO-Z-BOŽSKEHO-
USTANOVENI,PODLE-NĚHOŽ-SE-VŠE-ŘIDI.SENECA
```

Teraz spravíme substitúciu písmen za čísla podľa substitučnej tabuľky a dostávame:

```
03 19 14 19 15 12 29 37 24 07 37 20 23 12 11 19 05 12 37 23
01 05 17 07 16 28 37 16 28 34 12 39 26 19 37 20 19 17 07 24
07 37 24 37 29 32 22 19 29 17 01 17 19 28 37 16 32 24 15 12
37 02 28 05 07 37 24 12 38 01

01 38 29 07 05 19 16 39 34 07 37 26 19 37 20 23 12 25 15 19
37 33 37 02 19 34 24 14 07 11 19 37 28 24 26 01 17 19 29 07
17 12 39 20 19 05 15 07 37 17 08 11 19 34 37 24 07 37 29 25
07 37 23 12 05 12 35 24 07 17 07 03 01
```

V uvedených depešiach sú cifry zatiaľ rozdelené po dvojiciach a zodpovedajú znakom podľa substitučnej tabuľky. Prvá depeša má 140 cifier, takže nemusíme nič doplňať do násobku 5. Druhá depeša má dĺžku 146 cifier, takže musíme na jej koniec doplniť náhodné 4 cifry. Doplníme ich tak, aby na mieste desiatok bola cifra, ktorá tam podľa substitučnej tabuľky nemôže figurovať, t.j. 6, 7, 8, alebo 9. Doplníme tam napríklad cifry `78 63`. Teraz zapíšeme depeše v číselnom tvare do prvej transpozičnej tabuľky. Zapisujeme ich po riadkoch zľava doprava a zhora nadol. Vyplnené prvé transpozičné tabuľky máme uvedené na strane 6. V druhej depeši (tabuľke) sú na konci tučným písmom zvýraznené štyri cifry, ktoré boli náhodne pridané, aby počet cifier depeše bol násobkom 5.

Ďalej z prvých transpozičných tabuliek vypisujeme cifry po stĺpcoch zhora nadol, pričom poradie stĺpcov je dané vyčíslením prvého transpozičného

4	1	7	9	13	8	2	5	3	11	12	10	6
0	3	1	9	1	4	1	9	1	5	1	2	2
9	3	7	2	4	0	7	3	7	2	0	2	3
1	2	1	1	1	9	0	5	1	2	3	7	2
3	0	1	0	5	1	7	0	7	1	6	2	8
3	7	1	6	2	8	3	4	1	2	3	9	2
6	1	9	3	7	2	0	1	9	1	7	0	7
2	4	0	7	3	7	2	4	3	7	2	9	3
2	2	2	1	9	2	9	1	7	0	1	1	7
1	9	2	8	3	7	1	6	3	2	2	4	1
5	1	2	3	7	0	2	2	8	0	5	0	7
3	7	2	4	1	2	3	8	0	1			

COKOLIV-SE-PŘIHODI-ŘADNEMU-MUŽI,TO-
PONESE-S-VYROVNANOU-MYSLI-BUDE-SI/A

4	1	7	9	13	8	2	5	3	11	12	10	6
0	1	3	8	2	9	0	7	0	5	1	9	1
6	3	9	3	4	0	7	3	7	2	6	1	9
3	7	2	0	2	3	1	2	2	5	1	5	1
9	3	7	3	3	3	7	0	2	1	9	3	4
2	4	1	4	0	7	1	1	1	9	3	7	2
8	2	4	2	6	0	1	1	7	1	9	2	9
0	7	1	7	1	2	3	9	2	0	1	9	0
5	1	5	0	7	3	7	1	7	0	8	1	1
1	9	3	4	3	7	2	4	0	7	3	7	2
9	2	5	0	7	3	7	2	3	1	2	0	5
1	2	3	5	2	4	0	7	1	7	0	7	0
3	0	1	**7**	**8**	**6**	**3**						

A/VEDOM,ŽE-TO-PŘIŠLO-Z-BOŽSKEHO-
USTANOVENI,PODLE-NĚHOŽ-SE-VŠE-ŘIDI.SENECA

Tabuľka 4: Prvé transpozičné tabuľky pre príklad šifry STT

hesla. Cifry budeme zapisovať do druhých transpozičných tabuliek bežným spôsobom po riadkoch zľava doprava a zhora nadol. Tým dostaneme druhé transpozičné tabuľky:

15	5	13	11	7	1	3	17	10	4	2	9	16	6	14	12	8
3	3	2	0	7	1	4	2	9	1	7	1	7	0	7	3	0
2	9	1	2	3	1	7	1	7	1	9	3	7	3	8	0	0
9	1	3	3	6	2	2	1	5	3	9	3	5	0	4	1	4
1	6	2	8	2	3	2	8	2	7	3	7	1	7	1	7	1
1	1	9	0	2	2	2	2	4	0	9	1	8	2	7	2	7
0	2	9	2	1	0	6	3	7	1	8	3	4	2	2	7	2
9	0	9	1	4	0	5	2	2	1	2	1	7	0	2	0	1
1	0	3	6	3	7	2	1	2	5	1	4	1	5	2	7	3
9	3	7	1													

`COKOLIV-SE-PŘIHODI-ŘADNEMU-MUŽI,TO-`
`PONESE-S-VYROVNANOU-MYSLI-BUDE-SI/A`

15	5	13	11	7	1	3	17	10	4	2	9	16	6	14	12	8
1	3	7	3	4	2	7	1	9	2	2	0	0	7	1	7	1
1	3	7	2	7	0	3	0	7	2	2	1	7	2	7	0	3
1	0	6	3	9	2	8	0	5	1	9	1	3	7	3	2	0
1	1	9	1	4	2	7	1	9	1	4	2	9	0	1	2	5
0	3	9	2	7	1	4	1	5	3	5	3	1	9	0	3	3
7	0	2	3	7	3	4	6	8	3	0	3	4	2	7	0	4
0	5	7	9	1	5	3	7	2	9	1	7	0	7	5	2	5
1	9	1	0	0	7	1	7	1	6	1	9	3	9	1	8	3
2	0	2	4	2	3	0	6	1	7	3	7	2	8			

`A/VEDOM,ŽE-TO-PŘIŠLO-Z-BOŽSKEHO-`
`USTANOVENI,PODLE-NĚHOŽ-SE-VŠE-ŘIDI.SENECA`

Tabuľka 5: Druhé transpozičné tabuľky pre príklad šifry STT

Z druhých transpozičných tabuliek vypíšeme cifry opäť po stĺpcoch zhora nadol, pričom poradie stĺpcov je dané vyčísleným druhého transpozičného hesla a cifry zapisujeme v päťčlenných skupinách. Napokon už len na začiatok pridáme návestie depeše v tvare `xxx-yyy-zz`, kde `xxx` je poradové číslo

depeše, `yyy` je počet cifier depeše a `zz` je deň šifrovania depeše. V našom príklade dostaneme dve, na odoslanie pripravené, depeše v tvare:

```
037-140-21
11232 00779 93982 14722 26521 13701 15391 61200 30307 22057
36221 43004 17213 13371 31497 52472 20238 02161 30172 70721
32999 37784 17222 32911 09197 75184 71211 82321

038-150-21
20221 35732 29450 11373 87443 10221 13396 73301 30590 72709
27984 79477 10213 05345 30112 33797 97595 82113 23123 90470
22302 87769 92712 17310 75111 11070 12073 91403 21001 16776
```

2.2 Postup pri šifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii text na šifrovanie.

b. Je daný dátum šifrovania. Pomocou neho boli v praxi dané dĺžky transpozičných hesiel pre prvú a druhú transpozičnú tabuľku a prípadne sa podľa dátumu aj vyberali heslá z dohodnutej knihy.

c. Sú dané heslá potrebnej dĺžky pre prvú aj druhú transpozičnú tabuľku. Nebudeme sa zaoberať tým ako sme tieto heslá dostali, proste sú dané.

Potom šifrovanie depeše bude prebiehať podľa nasledovných krokov:

1. Text, ktorý ideme šifrovať, prepíšeme len pomocou znakov obsiahnutých v substitučnej tabuľke, čiže nahradíme písmená a vynecháme špeciálne znaky, ktoré sa v substitučnej tabuľke nevyskytujú. Pri šifre STT budeme vždy používať substitučnú tabuľku s 50 znakovou abecedou. Je to tabuľka 1 na strane 3.

2. Medzery medzi slovami nahradíme pomlčkou. Pokiaľ sa medzi slovami textu nachádza niektorý zo špeciálnych znakov obsiahnutých v substitučnej tabuľke, tak sa za týmto znakom medzera vynecháva.

3. Text rozdelíme na časti približne 100 znakov dlhé tak, aby každá časť vždy končila kompletným slovom. Dávame pritom pozor, aby rôzne časti textu nemali rovnakú dĺžku, pričom zohľadníme aj znaky pridané k textu kvôli nadväznosti dielov (podľa ďalšieho bodu).

4. Na koniec prvej časti pridáme, kvôli nadväznosti dielov `/A`. Na začiatok druhej časti pridáme `A/`, na koniec druhej časti pridáme `/B` atď. Každá časť textu (okrem prvej a poslednej) bude mať na začiatku písmeno identické s koncovým písmenom predošlej časti a znak `/` a na konci textu znak `/` a písmeno identické s písmenom označujúcim nasledovnú časť textu. Písmena na označovanie častí berieme podľa abecedy. Prvá časť má označenie len na konci a posledná časť len na začiatku.

5. Každú časť textu šifrujeme zvlášť a každá časť textu tvorí samostatnú depešu s vlastným návestím.

6. Všetky znaky substituujeme za čísla podľa tabuľky 1.

7. Skontrolujeme dĺžky jednotlivých častí. Žiadne dve časti nesmú mať rovnaký počet cifier (znakov). Na toto treba dávať pozor už pri rozdelovaní textu na časti.

8. Potom skontrolujeme počet cifier jednotlivých častí. Počet cifier každej časti musí byť násobok 5. Pokiaľ nie je, tak náhodne doplníme potrebný počet cifier tak, aby na mieste desiatok boli len cifry 6, 7, 8, alebo 9, ktoré sa tam podľa substitučnej tabuľky nemôžu vyskytovať.

9. Pri šifrovaní cifry najskôr zapisujeme do prvej transpozičnej tabuľky po riadkoch zľava doprava a zhora nadol.

10. Z prvej transpozičnej tabuľky cifry čítame po stĺpcoch zhora nadol, pričom poradie stĺpcov určuje vyčíslenie transpozičného hesla pre prvú tabuľku. Tieto cifry zapisujeme do druhej transpozičnej tabuľky po riadkoch zľava doprava a zhora nadol.

11. Z druhej transpozičnej tabuľky cifry čítame po stĺpcoch zhora nadol, pričom poradie stĺpcov určuje vyčíslenie transpozičného hesla pre druhú tabuľku.

12. Postupnosť čísel, ktorú sme dostali rozdelíme na skupiny po 5 cifier.

13. Na začiatok depeše pridáme ešte návestie v tvare `xxx-yyy-zz`, kde `xxx` je poradové číslo depeše, `yyy` je počet cifier depeše (aj s náhodne pridanými ciframi, t.j. toto číslo musí byť násobkom 5) a `zz` je deň šifrovania depeše. Týmto je šifrovanie depeše ukončené a depeša je pripravená na odoslanie.

2.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše aj s návestím.

b. Sú dané heslá potrebnej dĺžky pre prvú aj druhú transpozičnú tabuľku.

Potom dešifrovanie depeše bude prebiehať podľa nasledovných krokov:

1. Na základe návestia si overíme kompletnosť depeše (počet cifier).

2. Vynecháme návestie depeše, ktoré už nebudeme potrebovať.

3. Posledný riadok oboch transpozičných tabuliek nemusí byť úplný. Poznáme ale počet cifier samotnej depeše, poznáme šírku prvej aj druhej transpozičnej tabuľky, a teda vieme, koľko posledných stĺpcov v oboch tabuľkách bude kratších. Označíme si v oboch tabuľkách tieto kratšie stĺpce.

4. Cifry depeše zapíšeme do druhej transpozičnej tabuľky po stĺpcoch zhora nadol, pričom poradie stĺpcov bude dané vyčíslením druhého transpozičného hesla a niekoľko posledných stĺpcov tabuľky môže byť kratších.

5. Cifry depeše čítame z druhej transpozičnej tabuľky po riadkoch zhora nadol a zľava doprava a zapisujeme do prvej transpozičnej tabuľky po stĺpcoch zhora nadol, pričom poradie stĺpcov bude dané vyčíslením prvého transpozičného hesla a niekoľko posledných stĺpcov tabuľky môže byť kratších.

6. Cifry depeše čítame z prvej transpozičnej tabuľky po riadkoch zhora nadol a zľava doprava a zapíšeme. Rozdeľujeme ich na dvojice a podľa substitučnej tabuľky ich nahradíme príslušnými znakmi. Pokiaľ boli na koniec depeše pridané náhodné čísla, tak ich vynecháme. Spoznáme ich tak, že na mieste desiatok môžu mať len cifry 6, 7, 8, alebo 9.

7. Pomlčky nahradíme medzerami a rovnako doplníme medzery za špeciálne znaky v texte. Týmto sme dostali pôvodný text depeše.

8. Pokiaľ sa jedná o seriál, tak text zostavíme v správnom poradí podľa označenia na začiatku a konci jednotlivých častí seriálu.

2.4 Lúštenie

V prípade šifry STT si plk. Moravec myslel že je bezpečná preto, že dvojitá transpozícia robená až po substitúcii, roztrhne desiatkové a jednotkové cifry jednotlivých znakov. Táto okolnosť síce trochu skomplikuje lúštenie, ale určite nespraví šifru STT bezpečnou. Pri lúštení sa rozlišujú dva prípady. Ak je dĺžka prvého transpozičného hesla párna, tak v druhej transpozičnej tabuľke sa budú striedať úseky desiatkových cifier s úsekmi jednotkových cifier. V prípade nepárnej dĺžky prvého transpozičného hesla sa budú v druhej transpozičnej tabuľke striedať desiatkové cifry s jednotkovými. Tento fakt sa pri lúštení využíva pri odhadovaní správnej veľkosti transpozičných tabuliek. Pokiaľ ide o substitúciu, tak použitá tabuľka sa len nepatrne líšila od tabuľky použitej pri šifre TTS. Nemeckí lúštitelia ju poznali a vedeli, ktoré cifry sa môžu, resp. nemôžu vyskytovať na desiatkových miestach znakov.

Postup lúštenia popísal veľmi dobre pán Janeček v knihe [5] (str. 269–303). Uvádza tam postup lúštenia na príklade autentických depeší z 2. svetovej vojny. Jedná sa o seriál obežníkových depeší zaslaných 18. júla 1942 z Londýna pre Jeruzalem, Moskvu a Istanbul. K tomuto už niet viac čo dodať a záujemcov možno len odporučiť na uvedený zdroj. Lúštenie sa zakladalo na anagramovej metóde a využívalo časté chyby šifrantov a predovšetkým to, že šifrovali rovnakými heslami veľké množstvo depeší rovnakej dĺžky. Nemeckí lúštitelia depeše šifrované pomocou STT lúštili počas celej doby ich používania.

Literatúra

[1] Grošek Otokar, Vojvoda Milan, Zajac Pavol: Klasické šifry
STU v Bratislave, 2007

[2] Hanák Vítězslav: Muži a radiostanice tajné války
Elli Print, 2002

[3] Janeček Jiří: Gentlemani (ne)čtou cizí dopisy
Books Bonus A, 1998

[4] Janeček Jiří: Odhalená tajemství šifrovacích klíčů minulosti
Naše vojsko, 1994

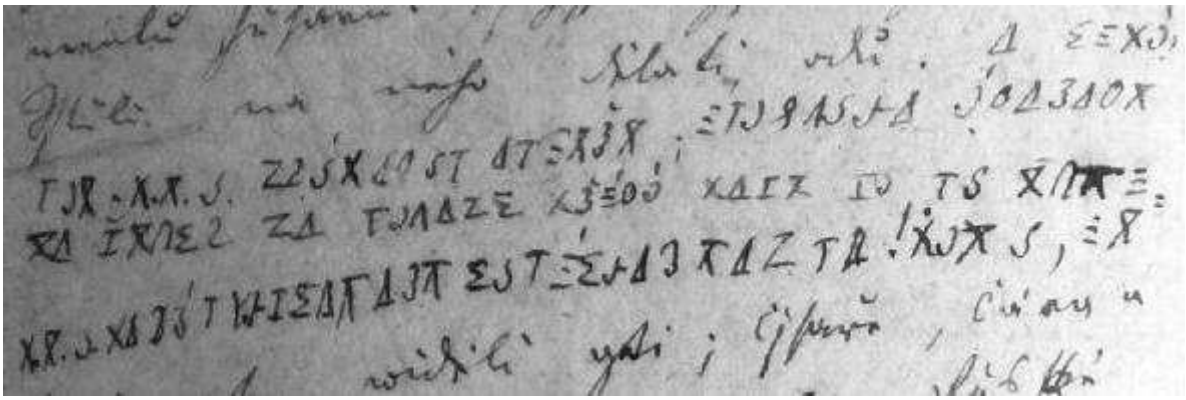
[5] Janeček Jiří: Válka šifer – výhry a prohry československé vojenské rozvědky (1939–1945)
Votobia, 2001

B. Pár poznámek k šifře použité v deníku Karla Hynka Máchy

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Deník K.H.Máchy

Na podzim roku 2010 mne kontaktoval Dr. Marek Přibil s velmi zajímavou nabídkou. Požádal mne, zda bych se podíval na šifrované poznámky v deníku básníka Karla Hynka Máchy (16.11.1810 - 6.11.1836) a poskytl mu na ně svůj názor a to zejména s ohledem na složitost dešifrace použité šifrové metody. PhDr. Marek Přibil je odborný pracovník Ústavu pro českou literaturu AV ČR a v poslední době se zabývá právě dílem K.H.Máchy. V souvislosti s dvousetletým výročím Máchova narození, které bylo slaveno právě v loňském roce, stoupl zájem o vše máchovské a znovu se tak dostal na přetřes i intimní obsah Máchova zašifrovaného deníku z podzimu roku 1835, který je částečně psaný v šifrách a který právě v těchto pasážích popisuje Máchův vztah se snoubenkou Lori Šomkovou. Jakub Arbes rozluštil část deníku, kterou měl k dispozici, již koncem 19. století. Na základě textu, který takto získal, nedoporučoval jeho zveřejnění. Deník pak rozluštil na základě úplného textu ve 20. letech 20. století Karel Janský a ani on, s ohledem na pověst Máchy, dešifraci nedával k dispozici.



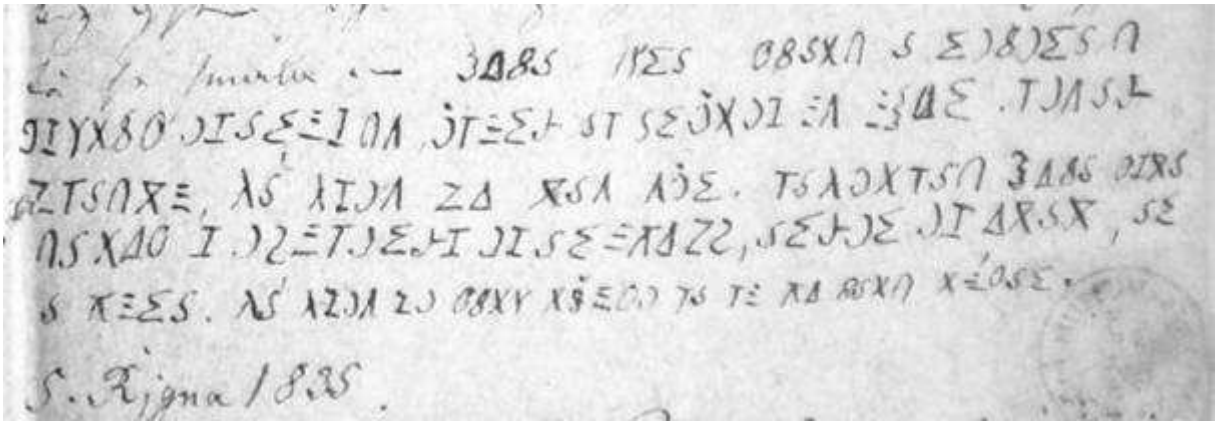
Nešlo však o to deník „rozluštit“, neboť Máchův *Deník z roku 1835 vyšel* kompletně i se šifrovanými pasážemi již celkem šestkrát (pokud nepočítáme mystifikační vydání ve 4. č. Analogonu z 1991, kde byl autentický Máchův text doplněn o „nové“ pasáže) a to konkrétně:
1) Neoficiální bibliofilie Oldřicha Hamery s ilustracemi Jiřího Koláře a s lapidárním titulem *K. H. Mácha*, Praha 1976.
2) Alena Wildová Tosi: *Un poeta romantico ceco*,Benátky 1976.
3) Toronto, Sixty-Eight Publischers, pravděpodobně z počátku 80. letech pod titulem *Byl lásky čas.*
4) Mnichov, v edici Poezie mimo domov, nakl. Obrys/Kontur 1986.
5) Miloš Pohorský: *Intimní Karel Hynek Mácha*, Praha 1993.
6) Pavel Vašák: *Šifrovaný deník K. H. Máchy,* nakl. Akropolis; 1. vyd. z 2007, 2. mírně rozšíř. vyd. z 2009;

Dr. Přibilovi šlo o posouzení, nakolik je vyluštění použité šifry skutečně obtížné a to zejména v kontextu toho, co je uváděno právě v poslední zmíněné knize věnované Máchově šifře.

V úvodu ke knize P.Vašáka se píše:
… přináší poprvé původní symboly Máchových šifer, frekvenci jejich výskytu a též podrobný popis dešifrace za pomoci ***metod matematické lingvistiky****.*

I na dalších stránkách tohoto zpracování se opakuje názor, že dešifrace (přesněji však luštění) nebyla jednoduchá. Opět cituji z uvedeného díla:
… dešifrace záznamů není nijak snadná. Jak se později ukáže, jednoduchý princip je narušován faktory, které dešifraci velmi ztěžují. Jak jsme se již zmínili, plynule se střídá čeština s němčinou, i když čeština převládá – ovšem tím je užití zákonů češtiny při dešifraci velmi ztíženo. … Pak je tu šifra komplikována polohou, protože první řádek se čte normálně, zleva doprava, další zprava doleva (řečeno jednoduše cik-cak), i když tento princip není ve dvou případech dodržen …

Účelem rozboru tedy bylo zjistit, jak skutečně složité je vyluštit deník Karla Hynka Máchy a to za pomocí běžné standardní analýzy četností, případně zkusit na jeho prolomení použít volně dostupný SW pro luštění jednoduché záměny na základě frekvencí. Za tímto účelem mi byly poskytnuty fotokopie všech šifrových pasáží, které jsou v deníku uvedeny.



Ukázka širy K.H.Máchy, zápis ze 4.října 1835

Rozbor

Následující odstavce jsou části volně vytržené z mého rozboru a poznámek k Máchově šifře, které jsem si v rámci této práce zaznamenal.

Z kryptografického hlediska se jedná o velmi slabou šifru, která vychází z klasické jednoduché záměny a to navíc s dělbou na slova a bez vlastních znaků pro písmena s diakritikou (diakritika je vyznačena u šifrových znaků jakoby to byly znaky otevřeného textu). Oba tyto faktory šifru významně zeslabují a umožňují její snadné vyluštění na základě odhadu hodnot jednotlivých písmen a předpokládaného slova. Nic na tom nemění ani to, že část textu je psána německy nebo obsahuje chyby. Luštitel při této metodě nepracuje s celým textem, ale vždy jen s vybranou částí (třeba jen jeden řádek) a pokud je neúspěšný, přechází k další části, která se zdá svojí strukturou zajímavá a dává větší naději na úspěch. Z tohoto důvodu není velkým problémem ani zajímavé posílení tohoto systému, který K. H. Mácha použil, a

to je změna směru psaní textu, které je vždy provedena (až na drobné výjimky) na konci řádku. Jakmile luštitel získá správné hodnoty pro jednotlivá písmena šifrového textu, tak je dosazuje do dalších částí šifrového textu, jednak aby text dešifroval a tím si potvrdil správnost přiřazení, ale také proto, aby získal převod pro šifrové znaky, které dosud nerozluštil. Při tomto postupu systém bez problému odhalí i to, že část textu je psána pozpátku.

Druhá metoda, která přichází při luštění této šifry do úvahy, byla známá již v 9. století a vychází ze statistického rozboru textu. Pro zajímavost uvádím, že metodu popsal roku 850 arabský vědec Abū-Yūsuf Ya'qūb ibn Ishāq al-Kindī (801–873). Jeho práce (zachovaná pouze v opise) je věnována luštění šifrových textů. V textu je použita metoda statistického rozboru šifrového textu a využití typických bigramů pro použitý jazyk (uvedeny jsou příklady z arabštiny).

Kombinace obou výše uvedených metod vedla k tomu, že ve 14. století i v Evropě již bylo všeobecně známo, že metoda jednoduché záměny je velmi slabá a byla i přes různé zesložitění (např. pomocí homofonů pro četná písmena, použití klamačů znaků, které nemají ekvivalent v otevřeném textu, šifrování mezer apod.) běžně luštěna.

Uvedený systém K.H.Máchy tedy patří mezi nejjednodušší verze jednoduché záměny (substituce) a zejména díky ponechané diakritice u šifrových znaků a dělbě na slova je systémem velmi slabým a řešení na základě kombinace předpokládaných písmen (odvozena z frekvence, diakritiky, spojek, předložek) a předpokládaných slov vede k velmi rychlému výsledku vyluštění a následné dešifraci celého textu. Dešifrace je proces zcela nenáročný, protože šifrové znaky jsou relativně dobře v jeho deníku čitelné.

Rozhodli jsme se podrobit šifrový text v deníku K.H.Máchy ještě zkoušce automatického luštění. Zde totiž metoda střídavého psaní vede k tomu, že četnost bigramů a trigramů, které se při automatickém luštění s výhodou používají, je narušena (příklad PR je četný bigram, ale RP se téměř nevyskytuje, při psaní oběma směry toho nelze využít, obdobně selže využití četnosti bigramu CH (četné)/ HC (nevyskytuje)).

Při délce šifrového textu je však možné, že automatické luštění zcela vystačí s charakteristikami, které prozrazuje frekvence jednotlivých písmen v češtině. Zde je možné na druhou stranu kalkulovat s tím, že dalším problémem by mohlo být, že čeština roku 1835 je odlišná od současné a navíc víme, že jsou v textu i části psané němčinou a že text je příliš monotématický ☺.

Pro automatické luštění jsme se navíc rozhodli použít zcela běžný nijak nespecializovaný na internetu dostupný software. Vhodným softwarem je aplikace Cipher-solver využívající Jakobsenův algoritmus, který kombinuje využití četností písmen a hlavních bigramů (http://thanzak.sweb.cz/Download.htm). Autorem je Mgr. Tomáš Hanzák, program vyhotovil roku 2004 během svého studia na MFF UK a program je nyní volně dostupný pro zájemce na jeho stránce. Výhodou je, že program řeší jednoduchou záměnu zcela automaticky. Stačí zadat na vstupu šifrový text (přepsaný do mezinárodní abecedy) a během několika vteřin program nabídne pravděpodobné řešení a převodovou tabulku jednoduché záměny. Pro texty mnohem kratší než je délka Máchova deníku dává správné výsledky. Je tedy otázka, zda

problém s nestandardním psaním šifrového textu bude mít takový vliv, aby program (algoritmus) selhal.

Postup

V prvé fázi bylo pro účely statistického rozboru a následného automatického luštění potřeba převést šifrové pasáže do abecedy, která je vhodná k takovému rozboru. Použili jsme standardní přepis do mezinárodní abecedy (skládá se z 26 písmen, využito jen 23).

Použitá převodová tabulka šifrových znaků pro přepis do mezinárodní abecedy

Při tomto převodu jsme nahradili šifrový znak opatřený diakritikou a bez diakritiky za jeden znak mezinárodní abecedy a to na základě hypotézy (kterou může luštitel přijmout jako skoro jistou), že mezi nimi je obdobný vztah i v otevřeném textu.

Text přepsaný dle naší transkripce začíná takto (zachováno řádkování v deníku):

XYHFHU MVPH
EBOL GRPD RWHF D PDWND VOL QD NDIH VOHFHQD OHKOD VL QD
NDQDSH MD QD QL WULNUDWH MVPH EBOL YBWUCHQL DC SULVOD
PDWND V RWFHP SDN EBOR SR YVRP EUCR VHO MVHP SRWRP GRPX
RQDQLH
X YHFHU SRCDGX
RGSROHGQH MVHP FKWHO QD CHPL RQD QHFKWHOD MXC REOLNOD VDWB
EDOD YVDN VH XVWDYLFQH CH EXGX PUCXWB SRWRP VH SUHGFH VYOLNOD D OH
KOL VPH VL X NDPHQ DEB QD QDV CDGQB QHSULVHO VWDKO MVHP NOLF

Následně jsme podrobili šifrový text v naší transkripci klasickým základním statistickým testům na četnost použitých znaků.

Relativní četnost šifrových znaků

A ...	0	N ...	3.5
B ...	2.1	O ...	7.4
C ...	2.8	P ...	4.9
D ...	11	Q ...	4.9
E ...	1.5	R ...	6.9
F ...	2.3	S ...	3.6
G ...	4.3	T ...	0
H ...	10.9	U ...	3.2
I ...	0.3	V ...	6.6
J ...	0.1	W ...	5
K ...	1.9	X ...	3.1
L ...	6.9	Y ...	3.2
M ...	3.8	Z ...	0

Absolutní četnost šifrových znaků

A ...	0	N ...	157
B ...	95	O ...	328
C ...	122	P ...	215
D ...	485	Q ...	215
E ...	65	R ...	305
F ...	103	S ...	160
G ...	191	T ...	0
H ...	484	U ...	141
I ...	13	V ...	290
J ...	5	W ...	220
K ...	83	X ...	137
L ...	304	Y ...	141
M ...	167	Z ...	0

Pro následný test se zcela automatizovaným výpočtem nebylo potřeba tyto statistiky provést, ale byly provedeny spíše pro úplnost a také pro následnou interpretaci výsledků.

Z prvního seznámení (za předpokladu, že neznáme hodnotu šifrových znaků) lze pouze konstatovat, že frekvence znaků dobře odpovídají rozložení frekvencí v češtině. Jasně zde je vidět pravděpodobná skupina četných znaků (v ní bývají obsaženy zejména samohlásky), skupina méně četných znaků a skupina málo četných znaků (pro češtinu j,b,g,f,x,w,q). Jak se ukáže po vyluštění šifry, rozdělení do skupin a i vlastní hodnoty šifrových znaků jsou v dobré shodě s rozdělením používaným pro charakteristiku českého jazyka. Pouze písmeno L má vyšší četnost než je běžná hodnota. Toto, jak se ukáže dále, se pak projeví i v automatické dešifraci.

v češtině		jiný zdroj	
A …	10,52%	E …	10,58%
O …	9,77%	A …	9,91%
E …	9,66%	O …	7,76%
N …	6,88%	I …	7,53%
I …	6,07%	N …	6,26%
L …	5,72%	S …	5,67%
.			
.			
J …	1,79%	J …	2,49%
Y …	1,44%	H …	2,48%
B …	1,1%	B …	1,64%
F …	0,17%	G …	0,17%
G …	0,17%	F …	0,16%

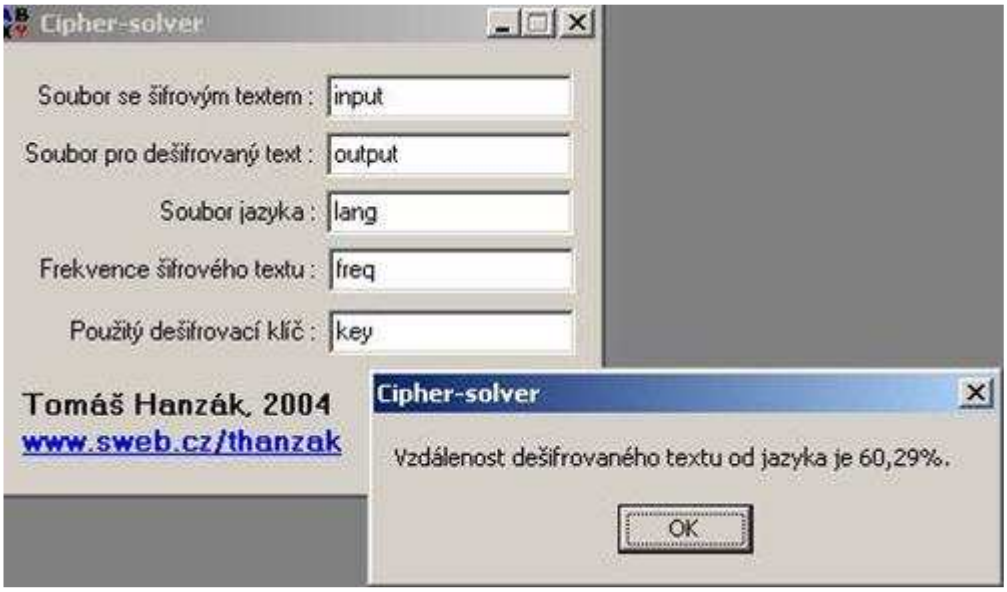
Pro kryptologa je dále zajímavý výsledek bigramové a trigramové analýzy. Tyto statistiky neodpovídají charakteristice českého jazyka. Je otázkou, zda z tohoto poznatku a předchozího poznatku (frekvence znaků) lze dovodit nepravidelnost ve způsobu psaní, ale určitě lze dovodit, že se jedná o jednoduchou záměnu s nějakou možnou velmi jednoduchou transpozicí (přeházení výsledného textu, zde dáno psaním pozpátku).

Frekvence bigramů absolutní

*	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	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
B	0	0	14	5	3	8	2	0	0	0	1	0	1	1	26	3	6	2	5	0	0	10	7	0	1	0
C	0	3	0	32	1	0	11	37	0	0	1	3	7	1	2	1	1	7	5	0	2	1	0	3	4	0
D	0	0	24	7	10	10	36	1	3	1	4	1	18	41	77	33	39	12	27	0	11	31	43	26	30	0
E	0	33	0	4	0	0	0	9	0	0	0	4	0	0	1	1	0	5	0	0	1	0	2	5	0	0
F	0	0	0	11	0	1	2	24	0	0	36	8	2	7	1	0	6	4	0	0	0	0	1	0	0	0
G	0	18	1	16	0	3	4	30	0	0	1	15	1	3	9	0	9	39	5	0	11	1	1	17	7	0
H	0	1	16	7	13	23	32	0	4	0	13	4	25	20	65	98	43	8	20	0	18	42	14	7	10	0
I	0	0	0	0	0	0	0	2	0	0	0	9	0	1	0	1	0	0	0	0	0	0	0	0	0	0
J	0	0	0	0	0	0	0	2	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0
K	0	1	0	9	1	3	0	4	0	0	2	3	1	2	8	2	5	15	4	0	2	4	10	5	2	0
L	0	0	7	9	7	39	12	11	5	0	3	2	11	39	30	11	27	5	20	0	2	20	18	8	27	0
M	0	0	0	11	0	0	1	19	0	0	0	47	0	0	0	0	0	0	0	0	0	68	0	1	0	0
N	0	4	1	41	1	0	18	2	0	0	0	0	10	0	18	0	13	23	1	0	14	3	1	5	2	0
O	0	2	9	90	2	3	14	35	0	0	3	60	33	3	2	2	9	22	13	0	1	10	1	10	4	0
P	0	1	6	16	8	2	3	44	1	0	2	12	29	3	3	5	13	8	11	0	4	24	4	13	3	0
Q	0	5	2	92	2	1	5	50	0	2	1	25	1	1	1	1	1	8	2	0	0	3	5	5	2	0
R	0	0	19	3	14	6	33	0	0	1	5	0	12	12	39	36	20	0	18	0	11	16	27	4	29	0
S	0	1	0	15	0	0	1	12	0	0	0	20	0	0	2	0	0	50	0	0	42	0	5	6	0	0
T	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
U	0	2	7	32	0	0	3	17	0	1	1	32	3	0	2	0	3	21	4	0	0	2	4	5	2	0
V	0	1	1	5	0	0	0	128	0	0	0	20	2	8	25	15	5	8	5	0	1	2	56	4	4	0
W	0	9	0	43	1	1	5	31	0	0	2	19	6	7	5	2	2	44	5	0	15	4	7	7	5	0
X	0	0	5	7	1	2	9	0	0	0	8	1	4	15	8	4	10	8	11	0	3	18	12	2	9	0
Y	0	14	10	30	1	1	0	26	0	0	0	19	1	2	3	0	3	9	3	0	3	11	2	3	0	0
Z	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

Automatické luštění

K pokusu o zcela automatické luštění byl použit již uvedený volně dostupný jednoduchý program Cipher-solver.



Vstupní soubor (input.txt) obsahoval námi připravenou transkripci celého šifrového textu K.H.Máchy přepsanou do mezinárodní abecedy. Po spuštění programu byl již za necelou vteřinu výpočtů výsledek automaticky dešifrovaného textu uložen do souboru output.txt a předpokládaný klíč, který byl programem nalezen do souboru key.txt.

Získaný výsledek je velmi dobrý a ukázalo se, že ani uvedený způsob střídání psaní zleva doprava a opačně a kombinace češtiny a němčiny neměl podstatný vliv na výsledek luštění a získání správného výsledku.

Ukázka získaného výstupu

automaticky dešifrovaný text
uvecer jsme
byni doma otec a matka sni la kafe **snecela nehna** si la
kalape ja la li trikrate jsme byni vytrzeli az prisna
matka s otcem pak byno po vsom brzo sen jsem potom domu
olalie
u vecer pozadu
odponedle jsem chten la zemi ola lechtena juz obnikna saty
bana vsak se ustavicle ze budu mrzuty potom se predce svnikna a ne
hni sme si u kamel aby la las zadly leprisen stahn jsem knic
doma jsem ji svnikn ze satu vyzvedn ji sukle a divan
se la li popredu po strale i po zadu niban stehla a tak dane po

Je vidět, že došlo k přiřazení šifrovým znakům jejich otevřených ekvivalentům při použití uvedeného softwaru jen k velmi málo chybám.

Porovnání automaticky získané převodové tabulky pomocí aplikace Cipher-solver se správným převodem:

Automatická dešifrace správné hodnoty

nalezený klíč			**správný klíč**
h=e	a=x		A=X
d=a	b=y		B=Y
r=o	c=z		C=Z
l=i	d=a		D=A
o=n	e=b		E=B
w=t	f=c		F=C
v=s	g=d		G=D
u=r	h=e		H=E
y=v	i=f		I=F
q=l	j=g		J=G
x=u	k=h		K=H
f=c	l=i		L=I
n=k	m=j		M=J
g=d	n=k		N=K
c=z	o=n		O=L
s=p	p=m		P=M
p=m	q=l		Q=N
b=y	r=o		R=O
k=h	s=p		S=P
m=j	t=w		T=Q
e=b	u=r		U=R
i=f	v=s		V=S
j=g	w=t		W=T
a=x	x=u		X=U
t=w	y=v		Y=V
z=q	z=q		Z=W

Při automatickém výpočtu tedy došlo pouze k záměně dvou písmen a to N/L a Q/W. Výsledek považuji za vynikající a přiznávám, že jsem jej vzhledem ke specifickým vlastnostem této jednoduché záměny nepředpokládal.

Poznámka
Pohorský ve svém díle *Intimní Karel Hynek Mácha se dopustil chyby a* v uvedené ukázce, kterou jsme zde použili jako ilustraci výstupu z automatického řešení, chybně uvádí *slečna lehla* místo správného *slečena lehla*.

Správná převodová dešifrovací tabulky „Máchovy šifry“.

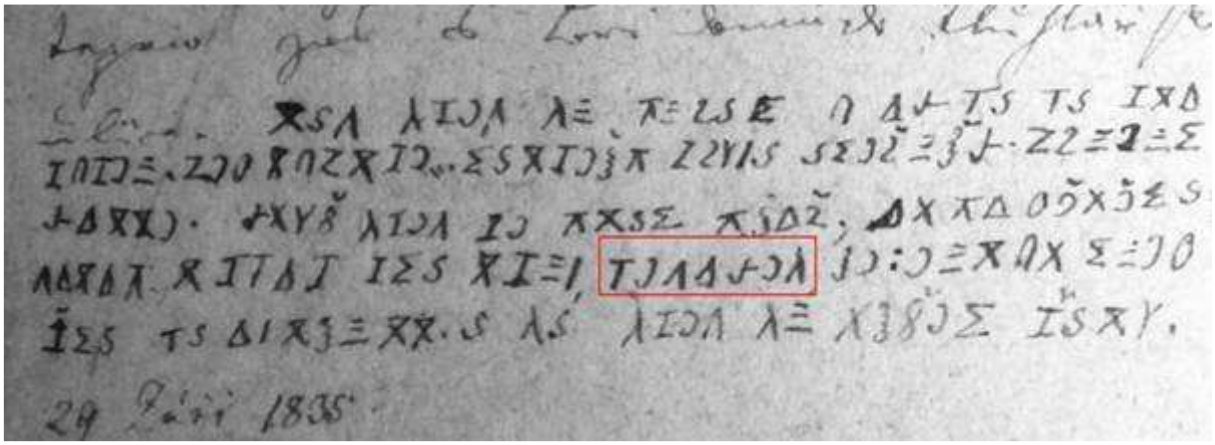
Symbol, kterému by odpovídalo písmeno *j*, se v Máchově šifrové abecedě vůbec nevyskytuje; hláska *j* je v souladu s dobovými pravopisnými zvyklostmi zapisována jako *g*. Dobře to ukazují právě německé pasáže, kde pro hlásku *g* Mácha používá stejný symbol jako pro hlásku *j* v českých textech. Obdobně se to týká použití jednoduchého a dvojitého *v/w*.

Závěr

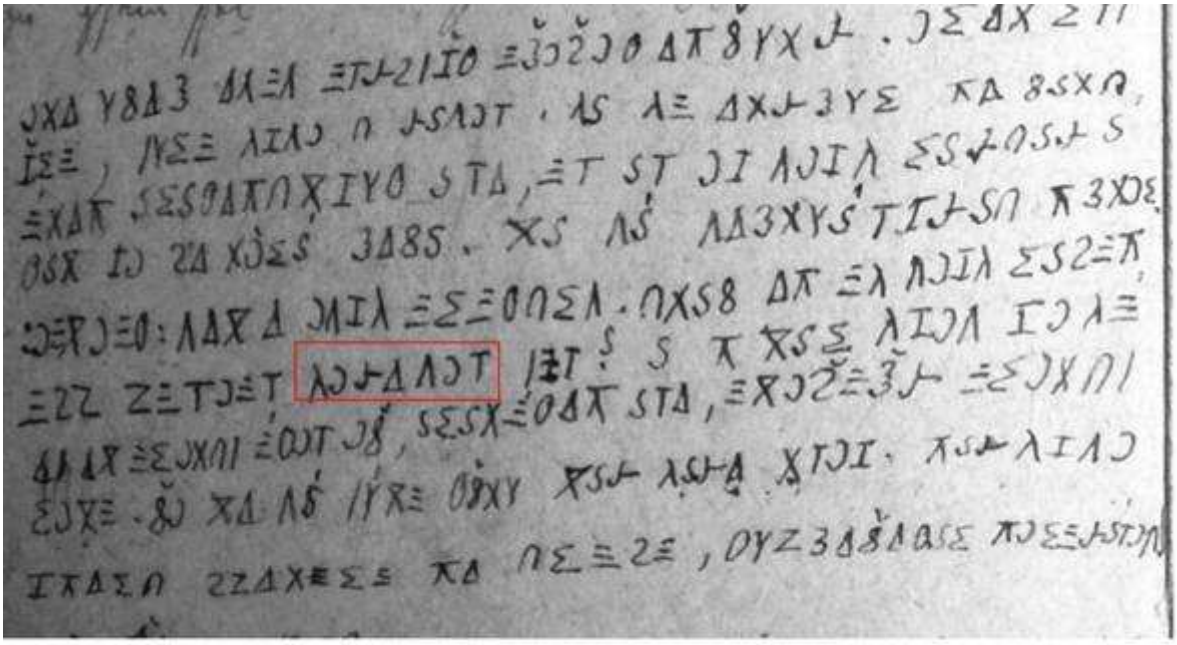
Šifrový text K.H.Máchy je lehce luštitelný manuálně s využitím markantů, které jsou lehce odhalitelné (dělba na slova, diakritika, předpokládaná slova, spojky, předložky) a lze získat kompletní převodovou tabulku pro zběhlého luštitele v řádu minut.
V případě kombinace manuálního luštění s přístupem k statistické frekvenci všech šifrových znaků, by byla práce při manuálním luštění významně ulehčena, ale pro samotný výsledke není nutná.

V případě, že luštitel má přepis šifrového textu k dispozici, může ke zcela automatické dešifraci použít zcela běžně dostupný nekomerční volně šiřitelný software, který mu během 1 vteřiny dá prakticky správný výsledek - dešifraci, která je téměř správná. Chyba se objevila pouze v záměně dvou písmen, jedné skupiny v textu poměrně frekventní (N/L) a jedné v textu zcela minoritní (W/Q). Z dešifrace plyne způsob zápisu a luštiteli tak stačí pouze prohodit výše uvedené záměny (N/L) a je s automatickou dešifrací hotov. Není k tomu potřeba žádný speciální software nebo metody matematické lingvistiky. Stačí opsat šifrový text a spustit příslušnou aplikaci ….

Ukázky na závěr



28. ZARI 1835
TAM JSEM JI PICAL U OKNA NA STO
LICICH. KRICELA ABYCH PRESTAL. "ES THUT VEH. IESUS — Obráceně
KOTTE. KDYZ JSEM SE PTAL PROC; ODPOVEDELA:
VEIL DU TIEFER **GEKOMEN** BIST ALS SONST. POTOM — Obráceně
SLA NA OBTRITT. A JA JSEM JI DRZEL SATY.



30. ZARI 1835

POTOM JSEM	
BYL DOLE. KDYZ PO VECERI VSICKNI MIMO ROZY ODE	obráceně
SLI, BYLI JSME U KAMEN. JA JI ODKRYL PO ZADU	
A KAUKAL JSEM SE NA NI, ONA VYSTUPOVALA PODI	obráceně
VAT SE CO DELA ROZA. TA MA MORDYANSKAU PRDEL.	
PICAL JSEM JI PO ZADU. MLUVILI JSME O TOM: VIE TIEF	Obráceně
ICH HINEIN **GEKOMEN** BIN? A PTAL JSEM SE JI	
BUDELI KRICETI, ONA POVIDALA, ZE NEVI BUDELI TO BO	obráceně
LETI. ZE TO MA BYTI VZDY TAK JAKO DNES. PAK JSME	
SPOLU CHODILI PO ULICI, VYHROZOVAL PELIKANEM.	

K uvedeným vybraným ukázkem PhDr. Marek Přibil ve svém příspěvku *Poznámky k Vašákově edici Máchova deníku z roku 1835*, který přednesel na II. textologickém kolokviu (k otázkám vydávání Máchova díla), 16. 12. 2010, ÚČL AV ČR, Praha poznamenává toto:

V autografu se vyskytují dvě podobné věty, které Vašák a Pohorský tisknou následovně: „Weil du tiefer je komen bist als sonst“ (28. září); „Wie tief ich hinein je komen bin“ (30. září)
V ostatních vydáních s *gekommen (přesněji gekomen poznámka PV)*.
Druhé/dřívější řešení se mi zdá vhodnější z několika důvodů:
a) Problematický úsek je psán zejména v druhém případě zřetelně dohromady, což v případě částice *je* není možné.
b) Vašákovo a Pohorského řešení vytváří nemožné gramatické monstrum, zatímco varianta s *gekomme* je gramaticky úplně korektní.

Děkuji touto cestou panu PhDr. M. Přibilovi za oslovení a za možnost se podílet na tak zajímavé práci jakou je rozbor šifry K.H.Máchy a dále za poskytnutí poznámek k jeho přednášce, které jsem v tomto článku použil.

C. O čem jsme psali v únoru 2000 – 2010

D. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: http://crypto-world.info

Všechna práva vyhrazena. Tato publikace ani žádná její část nesmí být reprodukována nebo šířena v žádné formě, elektronické nebo mechanické, včetně fotokopií, bez písemného souhlasu vydavatele.

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Vlastimil Klíma
	Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info