Kryptografie – Projekt č. 1 – Dešifrovaní šifry používané za 2. světové války

Dominik Nejedlý

Fakulta informačních technologií Vysokého učení technického v Brně
Božetěchova 1/2. 612 66 Brno - Královo Pole
xnejed09@vutbr.cz

26. února 2024

Je dáno 8 stejně dlouhých zpráv zašifrovaných pomocí šifry TTS používané pro komunikaci mezi československou exilovou vládou v Londýně a odbojem v Protektorátu Čechy a Morava během druhé světové války. Tyto zprávy včetně data jejich zachycení jsou uvedeny na obrázku 1. Cílem tohoto projektu je šifrování oněch zpráv prolomit, a zjistit tak jejich obsah. Lze předpokládat, že ve zprávách je zmíněn login studenta, tedy `xnejed09`. Popis šifry TTS je dostupný v [1].

```
Datum: 13.1.1944

1: 18253 32823 38183 81328 23300 12801 17131 81629 01233 81329 28150 11325
   18171 31413 23180 12430 29364 22513 18361 34201 01383 04235 29324 13230

2: 28172 81738 01122 32401 29171 10118 29012 93018 01322 82938 37141 31517
   42243 42901 13383 42801 29011 83023 18361 84017 36281 31324 34281 82424

3: 38182 82330 13363 33601 36181 82333 29371 80130 28293 21314 38341 71301
   23232 41826 23170 10128 33131 83036 43183 01724 24371 81818 28292 60101

4: 18283 41538 36183 24124 18370 14201 36171 32424 29282 73034 01322 93718
   13230 10123 30380 11936 33220 13015 13362 32923 37300 12632 29431 83018

5: 24242 03624 27182 80101 01282 61823 13292 92923 18420 10126 01322 53430
   32281 51818 29011 73201 13133 82827 23131 82817 17183 71433 36243 00129

6: 28422 40129 01243 83417 01291 81830 29363 40117 41291 31514 34011 72422
   34292 51330 18283 22801 38152 31318 18281 73624 38131 82328 01292 42701

7: 17180 13215 37131 83629 24250 10129 30364 22617 38282 81301 01012 32328
   23132 90101 30154 22638 34282 31313 29130 13029 13293 02430 26411 73728

8: 34412 83623 30183 81301 36322 62336 35352 31801 18014 20113 41262 83825
   24432 42601 29182 53437 41011 71736 23362 92818 18180 12833 25013 01313
```

Obrázek 1: Šifrované zprávy s datem jejich zachycení

Se znalostí šifry a výše uvedených informací se nyní pokusme šifrování prolomit. Vzhledem k tomu, že při šifrování byly nejprve použity dvě transpozice následované substitucí písmen abecedy uvedené v tabulce 1 za dvojice číslic, lze nejprve provést zpětnou substituci pro získání šifrovaných zpráv v jejich znakové podobě a následně až pokračovat řešením transpozice. V tabulce 1 je uvedena abeceda ve své základní podobě, při šifrování jsou však znaky cyklicky posunuty tak, že hodnota znaku `a` odpovídá dnu šifrování. Pro datum 13.1.1944 má tedy znak `a` hodnotu `13`, `b` hodnotu `14` atd. Posunutá abeceda odpovídající 13. dni v měsíci je uvedena v tabulce 2.

Vidíme, že abeceda obsahuje 45 znaků, které jsou kódovány čísly `01`, `02`, ..., `45`. Z prvního pohledu na zprávy je tedy zřejmé, že i jejich délky v nezašifrované podobě jsou shodné, jelikož každý znak je šifrován

dvěma číslicemi a žádná z šifrovaných zpráv neobsahuje náhodně doplněné cifry, neboť v takovém případě by doplněná dvouciferná čísla na konci zpráv obsahovala na místě desítek číslice větší než 4 (tj. 5, 6, 7, 8 nebo 9).

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		a	b	c	č	d	e	ě	f	h
1	h	i	j	k	l	m	n	o	p	q
2	r	ř	s	š	t	u	v	w	x	y
3	z	ž	.	?	-	/	1	2	3	4
4	5	6	7	8	9	0				

Tabulka 1: Česká znaková abeceda v základní podobě

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		-	/	1	2	3	4	5	6	7
1	8	9	0	a	b	c	č	d	e	ě
2	f	g	h	i	j	k	l	m	n	o
3	p	q	r	ř	s	š	t	u	v	w
4	x	y	z	ž	.	?				

Tabulka 2: Česká znaková abeceda pro 13. den měsíce

Postupnou substitucí dvojic číslic šifrovaných zpráv uvedených na obrázku 1 za symboly české znakové abecedy dle substituční tabulky 2 lze získat šifrované zprávy v jejich znakové podobě. Tyto jsou uvedeny na obrázku 2. Tyto zprávy jsou však stále transponované (dvojí transpozicí, což však není příliš podstatné, jelikož jejím výsledkem je opět pouze nová transpozice). Přejděme tedy k řešení transpozice.

```
1: ekřnivevanip-n-daečo-ivaonc-akedabaie-jpotzkaetaz--vpzšoryrp
2: ndndv-0ij-od9-eo-ope-rnovubacdzjso-avsn-o-epietexdtnaajsnejj
3: venipatřt-teeiřoue-pnorabvsda-iijelid--nřaeptžepdjjueeenol--
4: enscvteryjeu-z-tdajjonmps-roueai--ipv-ětřh-pcatioiup-lrožepe
5: jjftjmen---nleiaoooiez--l-rksprnceeo-dr-aavnmiaenddeubřtjp-o
6: nzj-o-jvsd-oeepots-dyoacbs-djhsokapenrn-vciaeendtjvaein-ojm-
7: de-rcuaetojk--optzldvnna---iiniao--pczlvsniaaoa-poaopjplydun
8: syntipeva-trlitššie-e-z-aylnvkjžjl-oeksuy-ddtitoneee-nřk-paa
```

Obrázek 2: Šifrované zprávy s číslicemi substituovanými po dvojicích za znaky rotované abecedy z tabulky 2

Jelikož jsou všechny zprávy zachyceny stejný den a jsou stejně dlouhé, je na všech z nich použita stejná transpozice. Ve všech zašifrovaných zprávách jsou tedy písmena, jež jsou v nezašifrovaných zprávách na stejných pozicích, opět na stejných pozicích. K prolomení tohoto šifrování lze pak použít anagramovou („proužkovou“) metodu, jež byla ukázána přednášce. Transponované zprávy nejprve sepišme pod sebe a rozdělme do sloupců s písmeny na stejných pozicích. Tyto sloupce jsou znázorněny a očíslovány v tabulce 3. Přeuspořádáním těchto sloupců tak, aby všechny zprávy (řádky) obsahovaly smysluplný text, lze odhalit jejich šifrovaný obsah.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
1	e	k	ř	n	i	v	e	v	a	n	i	p	-	n	-	d	a	e	č	o	-	i	v	a	o	n	c	-	a	k	e	d	a	b	a	i	e	-	j	p	o	t	z	k	a	e	t	t	a	z	-	-	v	p	z	š	o	r	y	r	p
2	n	d	n	d	v	-	0	i	j	-	o	d	9	-	e	o	-	o	p	e	-	r	n	o	v	u	b	a	c	d	z	j	s	o	-	a	v	s	n	-	o	-	e	p	i	e	t	e	x	d	t	n	a	a	j	s	n	e	j	j
3	v	e	n	i	p	a	t	ř	t	-	t	e	e	i	ř	o	u	e	-	p	n	o	r	a	b	v	s	d	a	-	i	i	j	e	l	i	d	-	-	n	ř	a	e	p	t	ž	e	p	d	j	j	u	e	e	e	n	o	l	-	-
4	e	n	s	c	v	t	e	r	y	j	e	u	-	z	-	t	d	a	j	j	o	n	m	p	s	-	r	o	u	e	a	i	-	-	i	p	v	-	ě	t	ř	h	-	p	c	a	t	i	o	i	u	p	-	l	r	o	ž	e	p	e
5	j	j	f	t	j	m	e	n	-	-	-	n	l	e	i	a	o	o	o	i	e	z	-	-	l	-	r	k	s	p	r	n	c	e	e	o	-	d	r	-	a	a	v	n	m	i	a	e	n	d	d	e	u	b	ř	n	t	j	p	-	o
6	n	z	j	-	o	-	j	v	s	d	-	o	e	e	p	o	t	s	-	d	y	o	a	c	b	s	-	d	j	h	s	o	k	a	p	e	n	r	n	-	v	s	c	i	a	e	e	n	d	t	j	v	a	e	i	n	-	m	-
7	d	e	-	r	c	u	a	e	t	o	j	k	-	-	o	p	t	z	l	d	v	n	n	a	-	-	-	i	i	n	i	a	o	-	-	p	c	z	l	v	s	n	i	a	a	a	o	a	-	p	o	a	o	p	-	p	l	y	d	u	n
8	s	y	n	t	i	p	e	v	a	-	t	r	l	i	t	š	š	i	e	-	e	-	z	-	a	y	l	n	v	k	j	ž	j	l	-	o	e	k	s	u	y	-	d	d	t	i	t	o	n	e	e	e	-	n	ř	k	-	p	a	a

Tabulka 3: Sloupce písmen transponovaných zpráv z obrázku 1 před uspořádáním do výsledných zpráv

Vyjděme z předpokladu, že ve zprávách je zmíněn login studenta, tedy `xnejed09`. Pozorujme, že písmeno `x` a číslovky `0` a `9` se nachází pouze ve 2. zprávě (řádku). Pokusme se tedy postupně vybírat sloupce písmen tvořící ve 2. zprávě (na 2. řádku) login `xnejed09` a současně kontrolujme, že i v ostatních zprávách (řádcích) vznikající kombinace písmen (bigramy, trigramy, slova atd.) dávající z jazykového hlediska smysl. Začněme tedy sloupcem 49, jež obsahuje na 2. řádku znak `x` a pokračujme výběrem vhodných sloupců tvořících na 2. řádku

text `nejed`. Pro bigram `09` existuje jediná kombinace sloupců, kterou pokračujme. Dále lze předpokládat, že login je oddělen mezerami. Ty jsou v šifrách značeny znakem `-`. Při postupném přikládání sloupců, jež na 2. řádku obsahují znak `-`, před a za sestavený login lze pozorovat, že pouze jeden lze přidat za poskládaný login a to sloupec 10. Před sloupec 49 pak nelze vložit žádný jiný sloupec, aniž by byla porušena smysluplnost textu zpráv, proto lze předpokládat, že sloupec 49 obsahuje počáteční písmena rozluštěných zpráv. Uspořádání sloupců pro vytvoření loginu `xnejed09` na 2. řádku a smysluplného textu na řádcích ostatních je uvedeno v tabulce 4.

	49	52	58	55	46	4	7	13	10
1	z	v	y	š	e	n	e	-	n
2	x	n	e	j	e	d	0	9	-
3	d	u	l	e	ž	i	t	e	-
4	o	p	e	r	a	c	e	-	j
5	n	e	p	ř	i	t	e	l	-
6	t	a	j	n	e	-	j	e	d
7	p	o	d	p	o	r	a	-	o
8	n	e	p	ř	i	t	e	l	-

Tabulka 4: Sestavení loginu `xnejed09` následovaného znakem `-` v 2. zprávě pomocí přeuspořádání vybraných sloupců písmen

Stejným způsobem lze pokračovat. Nyní však již není známo slovo, které by mělo být dále poskládáno. Na základě již rozluštěného textu lze však slova odhadovat. Zaměřme se na 6. řádek, který obsahuje text `tajne-jed`. Z kontextu lze vyvodit, že následovat může například slovo `jednotky` nebo `jednani`. První zmíněné však nelze složit (na řádku chybí znak `y` a při postupném skládání navíc vznikají na ostatních řádcích nevalidní a nesmyslné bigramy, trigramy atd.). Uspořádání slova `jednani` pomocí vhodných sloupců však vede ke smysluplnému textu i na všech ostatních řádcích, viz tabulka 5. Ponechme tedy na 6. řádku slovo `jednani` a pokračujme dalším rozšířením dešifrovaného textu.

	49	52	58	55	46	4	7	13	10	1	34	37	43
1	z	v	y	š	e	n	e	-	n	e	b	e	z
2	x	n	e	j	e	d	0	9	-	n	o	v	e
3	d	u	l	e	ž	i	t	e	-	v	e	d	e
4	o	p	e	r	a	c	e	-	j	e	-	v	-
5	n	e	p	ř	i	t	e	l	-	j	e	-	v
6	t	a	j	n	e	-	j	e	d	n	a	n	i
7	p	o	d	p	o	r	a	-	o	d	-	c	i
8	n	e	p	ř	i	t	e	l	-	s	l	e	d

Tabulka 5: Doplnění předcházející tabulky 4 slovem `jednani` v 6. zprávě pomocí dalších vybraných sloupců písmen

Na 1. řádku se dále nabízí uspořádat slovo `nebezpeci`. Pracujme tedy stejným způsobem jako doposud a pokusme se tohle slovo složit. Výsledek je uveden v tabulce 6. Opět vidíme, že slovo `nebezpeci` lze na prvním řádku složit se zachováním smysluplnosti textu na řádcích ostatních. Pokračujme tedy rozšiřováním textu z tabulky 6 dalšími sloupci. Například slovem `civilni` na 7. řádku.

	49	52	58	55	46	4	7	13	10	1	34	37	43	40	31	19	22
1	z	v	y	š	e	n	e	-	n	e	b	e	z	p	e	č	i
2	x	n	e	j	e	d	0	9	-	n	o	v	e	-	z	p	r
3	d	u	l	e	ž	i	t	e	-	v	e	d	e	n	i	-	o
4	o	p	e	r	a	c	e	-	j	e	-	v	-	t	a	j	n
5	n	e	p	ř	i	t	e	l	-	j	e	-	v	-	r	o	z
6	t	a	j	n	e	-	j	e	d	n	a	n	i	-	s	-	o
7	p	o	d	p	o	r	a	-	o	d	-	c	i	v	i	l	n
8	n	e	p	ř	i	t	e	l	-	s	l	e	d	u	j	e	-

Tabulka 6: Rozšíření předcházející tabulky 5 o slovo `nebezpeci` v 1. zprávě využitím dalších doposud nevybraných sloupců písmen

Stejným způsobem jako doposud lze pak rozluštit celý šifrovaný text všech zachycených zpráv. Výsledný obsah zpráv i s uspořádáním sloupců je uveden v tabulce 7 a pro lepší přehlednost je na obrázku 3 přepsán do textu zpráv. Tímto je šifrovaný text rozluštěn.

	49	52	58	55	46	4	7	13	10	1	34	37	43	40	31	19	22	28	25	16	50	53	59	56	47	5	8	14	11	2	35	38	44	41	32	20	23	29	26	17	51	54	60	57	48	6	9	15	12	3	36	39	45	42	33	21	24	30	27	18
1	z	v	y	š	e	n	e	-	n	e	b	e	z	p	e	č	i	-	o	d	-	p	r	o	t	i	v	n	i	k	a	-	k	o	d	o	v	a	n	a	-	z	p	r	a	v	a	-	p	ř	i	j	a	t	a	-	a	k	c	e
2	x	n	e	j	e	d	0	9	-	n	o	v	e	-	z	p	r	a	v	o	d	a	j	s	t	v	i	-	o	d	-	s	p	o	j	e	n	c	u	-	t	a	j	n	e	-	j	e	d	n	i	-	t	a	j	n	a	-	d	b	o	e
3	d	u	e	ž	a	i	t	e	-	v	e	d	e	n	i	-	o	d	b	o	j	e	-	n	e	p	ř	i	t	e	l	-	p	ř	i	j	p	r	a	v	u	-	j	e	-	o	p	a	t	ř	e	n	s	p	ě	c	h	-	o	p	e	r	a
4	o	p	e	r	a	c	e	l	-	j	e	-	v	-	t	a	j	o	s	t	i	-	p	o	t	v	r	z	e	n	i	-	p	ř	i	j	m	u	-	d	u	l	e	ž	i	t	y	-	u	s	f	o	r	m	a	c	e	-	p	r	o
5	n	e	p	ř	i	e	-	j	e	d	n	a	-	v	-	r	o	z	k	l	a	d	u	-	t	a	j	n	e	-	j	e	d	n	a	v	a	n	i	-	s	-	o	d	b	o	j	e	-	i	n	o	j	e	n	r	m	a	c	e	-	p	r	o
6	t	a	j	p	e	-	j	e	d	n	a	n	i	-	s	-	o	d	b	o	j	e	m	-	n	o	v	e	-	z	p	r	a	a	s	a	d	n	i	-	t	a	j	n	o	-	d	-	s	j	s	-	o	d	v	i	-	o	d	-	s	p	o	k	-	p	l	a	n	o	-	k	c	h	-	s
7	p	o	d	p	o	r	a	-	o	d	-	c	i	v	u	j	e	-	n	a	p	o	p	u	l	a	c	e	-	j	e	-	z	a	d	y	a	d	n	i	-	t	a	j	n	a	-	o	p	a	t	r	n	o	j	e	-	k	l	i	z
8	n	e	p	ř	i	t	e	l	-	s	l	e	d	u	j	e	n	a	š	e	-	a	k	t	i	v	i	t	y	-	k	d	y	ž	-	z	v	y	š	e	n	a	-	o	p	a	t	r	n	o	s	t	-	j	e	-	k	l	i	

Tabulka 7: Uspořádání sloupců písmen do výsledných zpráv

```
1: zvyšene-nebezpeči-od-protivnika-kodovana-zprava-přijata-akce
2: xnejed09-nove-zpravodajstvi-od-spojencu-tajne-jednani-s-odbo
3: duležite-vedeni-odboje-nepřitel-připravuje-opatřeni-tajna-se
4: operace-je-v-tajnosti-potvrzeni-přijmu-duležity-uspěch-opera
5: nepřitel-je-v-rozkladu-tajne-jednani-s-odbojem-informace-pro
6: tajne-jednani-s-odbojem-nove-zpravodajstvi-od-spojeneckych-s
7: podpora-od-civilni-populace-je-zasadni-tajny-utok-planovan-z
8: nepřitel-sleduje-naše-aktivity-když-zvyšena-opatrnost-je-kli
```

Obrázek 3: Výsledné zprávy

Odkazy

[1] Jozef Kollár. „Československé šifry z obdobia 2. svetovej vojny. Diel 1., Šifra TTS“. Čeština. In: *Crypto-world* 13.1 (2011), s. 3–11. ISSN: 1801-2140. URL: http://crypto-world.info/casop13/crypto01_11.pdf.