Manuál Tmou

2004

Zadání některých cvičení byla převzata z her Bedna, Exit a Sendvič.
Připomínky a náměty k tomuto textu zasílejte na adresu *tmou-manual@instruktori.cz*.
Děkujeme.

Obsah

Kapitola 1

Úvod

Zabít tebe (žes to spáchal) nebo sebe (že jsem tak tupá)...

Protože účastníci Tmou jsou stále zkušenější a vytrénovanější, organizátoři musí neustále vymýšlet stále rafinovanější šifry a úkoly. Chceme, aby hra zůstala zajímavá i pro zkušené týmy, a přitom aby i ti, co hrají poprvé, měli šanci se někam dostat. Proto jsme se rozhodli vydat tento manuál, který by měl nováčkům předat alespoň něco z potřebných zkušeností. Primárně je tedy tento text určen těm, co hrají poprvé. Ale věříme, že i zkušení hráči zde najdou něco užitečného[1].

V této první motivační kapitole se podíváme na historii Tmou. Také se zmíníme o dalších podobných hrách, u kterých by se vám mohly načerpané znalosti hodit.

1.1 Historie

Tmou I (podzim 2000)

- Počet týmů: 50
- Vítěz: –
- Celkem dorazilo týmů: 0

Hra začala hlášením na hlavním nádraží. Městská část probíhala v centru (cigareta, inzerát, jízdní řády trolejbusů), asi v 11 hodin byl hromadný odjezd vlakem do Bílovic, kde byla asi nejtěžší šifra (substituční xyz). Odtud se pokračovalo přes Mariánské údolí na Stránskou skálu. První tým dorazil 20 minut po limitu, který byl stanoven východem slunce.

[1] Jestli tedy víte, co tím myslíme...

Tmou II (jaro 2001)

- Počet týmů: 132
- Vítěz: Antracit (11:25)
- Celkem dorazilo týmů: 3

Hra začala na Kraví hoře zvoněním budíku a během k odpadkovým košům. Trasa vedla přes centrum (krokodýl, noty, CD s Partyzánskou písní), Královo pole (”turistická žlutá značka”, kterou většina týmů přeskočila), Soběšice, lesy kolem řeky Svitavy (písmenka s tečkami), až do Bílovic. Konec hry byl tentokrát poprvé určen na 12:00.

Tmou III (podzim 2001)

- Počet týmů: 198
- Vítěz: Žlutý bagr (8:26)
- Celkem dorazilo týmů: 20

Start byl za Lužánkami. Jeden člen z každého týmu byl se zavázanýma očima odvezen autobusem směrem k Soběšicím. Poté, co se týmy sešly, pokračovaly přes Sady národního odboje (které asi třetina týmů z neznámých důvodů hledala v Troubsku). Dále trasa vedla přes centrum (disketa), kde se týmy opět na chvíli rozdělily (Lužánky, výstaviště), a pak již přes Bystrc (spermie), do lesů okolo Říšovy studánky (šifra v šifře) a zpět směrem k Bystrci.

Tmou IV (podzim 2002)

- Počet týmů: 205
- Vítěz: FIMAN++ (7:40)
- Celkem dorazilo týmů: 28

Tentokrát se začínalo v přednáškových místnostech, odkud se šlo přes kopce a vyhlídky (fotka, šifra s klávesnicí) do památné podzemní stoky. Dále pak přes Medlánecký kopec do terénu (nejtěžší šifra s doplňováním písmen), kolem dvou studánek až do Útěchova.

Tmou V (podzim 2003)

- Počet týmů: 250
- Vítěz: –
- Celkem dorazilo týmů: 0

Tentokrát se poprvé šifrovalo ještě před začátkem: při registraci. Vlastní hra pak začala nenápadně v Lužánkách (tři chodci v červených tričkách). Již na třetím stanovišti byla záludná kazeta s prohlídkou Brna, která si vyžádala neplánovanou nápovědu v 0:15 na Zelňáku. Dál se pokračovalo směrem na Stránskou skálu (hliněná destička), do Líšně (šifra se špendlíkem) a dál až do Babic, kam však nikdo regulérně nedošel.

Tmou VI (podzim 2004)

Tož to se teprve uvidí.

1.2 Podobné hry

Inspirací Tmou byla hra Open Blood, která se konala na Vysočině na konci 90. let. Oproti Tmou se odehrávala pouze v terénu a trvala celých 24 hodin. Dalších podobných her se za poslední roky vynořila celá řada, viz. Tabulka 1.1. Většina těchto her má velmi podobný princip, pravidla i dobu trvání jako Tmou (s výjimkou Dnem, které jak již název napovídá, probíhá ve dne). Hry Exit a Sendvič jsou kratší, využívají Internet a nejsou terénní. Hra 66 hodin je naopak výrazně delší a probíhá na rozsáhlejším území. Všechno jsou to však týmové hry využívající šifrovací a logické úkoly. Doufáme, že tento text pomůže i účastníkům těchto her.

Název	**Kde**	**2002**	**2003**	**2004**
Bedna *http://bedna.obluda.cz*	Praha	•	•	•
Dnem *http://www.dnem.zde.cz*	Brno	•	•	•
Exit *http://exit.gdi.cz*	Brno	•	•	•
Lampa *http://lampa.webz.cz*	Česká Třebová	•		•
Libereckou tmou	Liberec	•		
Nachtschicht *http://nachtschicht.redingo.net*	Dortmund (Německo)		•	•
OSUD *http://www.zas.cz/osud*	Zlín			•
Sendvič *http://sendvic.gdi.cz*	web			•
Svíčky *http://www.svicky.wz.cz*			•	
66 hodin *http://velkyvuz.adam.cz/66hodin*	ČR	•	•	•

Tabulka 1.1: Přehled her

Kapitola 2

Základní šifry

Luštění šifer je podle mého názoru tou nejvíce fascinující ze všech dovedností.

Charles Babbage

Tato kapitola poskytuje přehled klasických šifer. Při vlastní hře se setkáte spíše s různými nadstavbami a kombinacemi. Je tedy důležité, abyste tyto základy dobře ovládali. Vzhledem k tomu, že čtenář, potenciální účastník Tmou, má IQ větší než 150, jsou šifry popsány poměrně stručně. Detaily si již jistě domyslíte či dohledáte v dostupné literatuře [7, 1, 8]. Pro ilustraci uvádíme ke každému typu šifer několik cvičení. Protože toto je trénink na Tmou, řešení *není* uvedeno na konci textu. Fakt ne.

Na tomto místě je potřeba podotknout, že použití šifer při hrách je poněkud odlišné od klasického použití v kryptografii. Za normálních okolností máme dvě strany (odesílatel a příjemce, kryptografové), které se snaží využít šifru k tomu, aby si vyměnily soukromé sdělení. Třetí strana (odposlouchávající kryptoanalytik) se snaží toto sdělení odhalit. Naproti tomu u her máme pouze dvě strany (odesílatel = kryptograf, příjemce = kryptoanalytik). Smysl šifrování je "pouze" udělat příjemci zprávy život těžší (respektive zajímavější). Důsledkem toho je, že při hrách se používají některé šifry, které v klasické kryptografii nemají obdoby (např. grafické šifry), a naopak mnohé šifry z moderní kryptografie jsou nepoužitelné při hrách.[1]

2.1 Substituční šifry

Substituční šifry jsou, zjednodušeně řečeno, založeny na přepisu do jiné abecedy (sady znaků). Jako základ se většinou využívá anglická abeceda o 26 písmenech – český text je tedy nejprve odháčkován a odčárkován a pak teprve substituován.

[1] Ani lidé s IQ $>$ 150 většinou nezvládají rychle faktorizovat stociferná čísla.

Kódování

Primární účel kódování je nikoli utajení, ale usnadnění a umožnění přenosu zprávy. Příklady různých kódování jsou (některá z nich jsou uvedena v příloze):

- morseova abeceda (vizuální a zvukový přenos)
- brailovo písmo (přenos hmatem)
- vlajková abeceda (vizuální přenos)
- semafor (vizuální přenos)
- čísla (reprezentace pro počítače)
- národní abecedy, runy, hieroglyfy,...

Tato kódování lze využít pro šifrování tak, že je různě maskujeme či znetvoříme. Nejčastěji se k tomuto účelu používá morseovka, příklady maskování mohou být:

- převrácené pořadí, zaměněné tečky a čárky
- morseovka v obrázku (kytičky, noty, čínské znaky)
- morseovka v textu (velká/malá písmena, sudá/lichá čísla)

Základem řešení je samozřejmě poznat, co kóduje čárku, co tečku a co oddělovač znaků. V drtivé většině případů se vyplatí nemachrovat, přepsat si to nejdřív do teček a čárek a pak teprve číst.

Cvičení:

1. · · – – |· |· – · |– · |· – – ·
2. – · · – · · · · · – · – – – – · – · · · – · · · · · – – · · – · – · –
3. · – · |· · · |· · |– – |· –
4. 075111077105110
5. Ale les asi se hrne v otep.

Základní substituce

Písmena jsou nahrazena jinými znaky, většinou jde o zobrazení 1:1 (monoalfabetická šifra). Jedno písmeno však může být kódováno i více znaky (viz. šifra xyz na Tmou I) nebo naopak více znaků se může zakódovat na stejný znak. Ono to pak sice není úplně jednoznačné, ale o to zajímavější.

Postup dešifrování je většinou založen na uhádnutí klíčových písmen – substituce zachovává četnosti znaků. Četnosti písmen jsou ve smysluplném textu pro jednotlivá písmena značně rozdílné. Následující tabulka udává nejčastější výskyty pro češtinu:[2]

Nejčastější písmena:	e, a, o, i, n, t, s, v, l, k
Nejčastější bigramy:	st, ní, po, ov, ro, en, na, je, pr, te
Nejčastější trigramy:	pro, ost, sta, pře, ter, ení, ova, pod, kte, pra

Podle četnosti se tedy pokusíme uhádnout nejfrekventovanější písmena a ostatní doplníme dle slov, která nám postupně vycházejí. Alternativou je přímé uhádnutí nějakého slova (oslovení, podpis,...). Obecně platí, že k dešifrování tohoto typu šifer potřebujeme buď rozumně dlouhý text, rámcovou znalost obsahu textu nebo velkou haluz (většinou stačí jedno z toho).

Cvičení:

1. OMUTMOTUTMOU OUMTTOUM
   TMUOTOMUOTUMTMOUOUMT MTOUTOMUUTMO
   TMOUOTUMUOMTUMTOMOTUUMOTTOMUTMOUMOTUOTUM?
   Pokud ano, pak jistě víš, že heslo je UMTOMOTUTMOUOTUMTMUO-OUMTMTOUMOTU

2. $\varepsilon\ \varpi\xi\zeta\varpi\xi\ \iota\varepsilon\pi\varpi\pi,\ \varepsilon\pi\ \mu\varpi\pi\nu\pi\zeta\ \omega\pi\ \varpi\xi\sigma\alpha\mu\ \lambda\varpi\nu\delta\pi\eta\alpha\ \gamma\ \theta\alpha\vartheta\varphi,\ \delta\nu\alpha\nu\xi\vartheta\eta\alpha\ \alpha\ \sigma\alpha\vartheta\iota\mu\pi,\ \iota\pi\ \eta\pi\tau\chi\tau\alpha\ \nu\xi\varepsilon\gamma\sigma\xi\varepsilon\gamma\varpi\ \varepsilon\pi\ \varepsilon\alpha\sigma\pi\ \tau\alpha\ \nu\alpha\varpi\alpha\varpi\ \iota\pi\ \iota\varpi\xi\mu\alpha\sigma\xi\zeta\pi\varpi\nu\xi\varepsilon\xi\lambda\ \nu\varphi\tau\chi\sigma\xi\iota\varpi\alpha\ \delta\xi\ \theta\pi\varpi\xi\eta\xi\varepsilon\pi\ \omega\alpha\varepsilon\pi\ \eta\gamma\ \mu\nu\gamma\omega\alpha\eta\pi,\ \varepsilon\varphi\delta\xi\lambda\iota\varpi\pi\varpi$

   $\iota\varepsilon\varphi\zeta\ \theta\sigma\alpha\eta\alpha\zeta\ \vartheta\xi\ \delta\sigma\alpha\tau\ \varpi\xi\kappa\alpha\tau\mu\pi\ \pi\kappa\chi\gamma\sigma\gamma\varpi\varphi,\ \delta\nu\pi\omega\alpha\vartheta\pi\varpi\ \omega\pi\mu\varphi\ \gamma\ \delta\nu\pi\chi\sigma\alpha\pi\varpi\ \delta\nu\alpha\nu\xi\vartheta\lambda.\ \delta\nu\alpha\delta\gamma\vartheta\gamma\sigma\ \theta\varphi\tau\chi\ \iota\alpha\ \varepsilon\lambda\sigma\varphi\gamma\nu\eta\alpha\ldots\ \pi.\ \mu\xi\chi\gamma\mu$

Systematické substituce

Šifra je zobrazením z abecedy zpět do stejné abecedy. Oproti základním substitučním šifrám je však navíc nějakým způsobem systematická. Základní dva typy jsou "konstantní" a "proměnné" zobrazení.

Při konstantním zobrazení se dané písmeno zobrazuje na stále stejné písmeno, např. posuny v abecedě, jednoduché permutace (otočená abeceda, posun v rámci samohlásek/souhlásek); toto lze dešifrovat i pro poměrně krátký text (nejlépe tak, že uhádneme konkrétní princip).

Při proměnném zobrazení záleží to, na co se dané písmeno zobrazí, nejen na tomto písmenu, ale i na jeho poloze v textu. Příklady proměnného posunu:

[2] Zdroj *http://nlp.fi.muni.cz/nlp*

- První písmeno posunuto o jedna, druhé o dva, atd.
- Šifrování dle hesla: dochází k posunu dle písmen hesla, které periodicky opakujeme. Příklad:

zpráva	M	A	M		V	B	O	T	E		K	A	M	I	N	E	K
heslo		A	H	O		J	A	H	O	J		A	H	O	J	A	H	O
šifra	M	H	A		E	B	V	H	N		K	H	A	R	N	L	Y

  Pro dešifrování se poměrně dost hodí znát heslo. Existují metody jak z delšího textu dešifrovat i bez znalosti hesla: nejdříve se na základě určitých kouzel odhadne délka klíče, a jakmile jednou známe délku klíče, tak to již zvládneme pomocí frekvenční analýzy. Ale to je (zatím) nad rámec Tmou.
- Šifrování dle nekonečného hesla: bezpečná varianta předchozího (leč trochu nepraktická).
- Šifrování dle sebe sama: každé písmeno posunujeme dle předcházejícího, první písmeno zůstává stejné.

Více informací o metodách řešení substitučních šifer lze najít v [4].

Cvičení:

1. PECPKF
2. CCKM JMRLII KDTGEIBHT RX DSJTVBGFS HXXRGJXWQIN PXPLZAQXGE Y HCBRFOM G. Z. RBYEOCRX… (heslo je PEXESO)
3. RRDHNR AW SDDHKVFPJVT GRD YQVHDZX

Substituce dle speciálního textu či předmětu

Šifrování dle hesla je již relativně bezpečné, avšak v případě, že heslo je krátké a text dlouhý, je stále napadnutelné (vyluštitelné). Proto se občas v kryptografii využíval určitý dlouhý text, který byl znám oběma stranám. Může se jednat buď o dopředu domluvený text, nebo o nějaký všeobecně rozšířený text (např. bible, prohlášení o nezávislosti). V případě her takovým textem může být například text pravidel či text na pomníku, u kterého ležela zpráva. Kódový text pak můžeme využít například následovně:

- Jako heslo, dle kterého děláme posuny (viz. předchozí část).
- Každé písmeno kódujeme pomocí čísla, které udává pořadí slova v kódovém textu, které začíná na toto písmeno.

Kromě textů můžeme podobným způsobem využívat ke kódování i jiné předměty (např. rozložení písmen na mobilním telefonu či klávesnici, jízdní řády).

Cvičení:

1. 14/1, 9/1, 11/3, 19/4, 7/1, 24/1, 4/3
   (nápověda: hymna)
2. RY9LCBQZ5DBM8KOM

Číselné šifry

Při převodu písmen na čísla se většinou používá číslování 0–25 či 1–26. Případně je možné pracovat s většími čísly, pak to bereme "modulo" 26 (zbytek po dělení 26). Dále je možno použít různé jiné číselné soustavy (binární, šestnáckovou, římskou,...).

Moderní šifry pracují právě na principu převodu na čísla a intenzivního šolichání s těmito čísly. Musí šolichat opravdu intenzivně, protože na rozdíl od šifer na Tmou je jejich princip všeobecně znám, a přesto nejsou vyluštitelné v rozumném čase.

Jako příklad si uveďme šifru RSA. Jedná se o šifru s asymetrickým klíčem. Ten se skládá ze soukromé a veřejné části. Šifrujeme pomocí veřejného klíče. Dešifrujeme pomocí soukromého klíče. Za rozumných předpokladů nelze dešifraci provést bez znalosti soukromého klíče. Základní postup je následující (operace mod je "zbytek po dělení"):

- Zvolte dvě tajná prvočísla p, q.
- Spočítejte $n = p \cdot q$ a $r = (p-1) \cdot (q-1)$.
- Zvolte číslo k nesoudělné s r a najděte g tak, aby $g \cdot k \ mod \ r = 1$
- Dvojice (k, n) je veřejný klíč, g je soukromý klíč.
- Zprávu $M \leq n-1$ nyní zašifrujeme jako $e(M) = M^k \ mod \ n = H$.
- Zašifrovanou zprávu H dešifrujeme jako $d(H) = H^g \ mod \ n = M$.

Korektnost šifry ($d(e(M)) = M$) je založena na Fermatově větě[3]. Bezpečnost šifry je založena na tom, že pokud p, q jsou dostatečně velká, nikomu se nepodaří je zpětně vypočítat z veřejně dostupného čísla n (kdyby se to někomu podařilo, už by si snadno dopočítal soukromý klíč g). Fakt, že se to nikomu nepodaří, je založen na tom, že to nikdo neumí dost rychle, nikoliv na tom, že by to v principu nešlo.

Pro ilustraci si uveďme příklad s malými čísly:

- Zvolme $p = 47, q = 71$.

[3] Platí totiž $\varphi(p \cdot q) = (p-1)(q-1)$ a odtud tedy $d(e(M)) = d(M^k \ mod \ n) = (M^k \ mod \ n)^g \ mod \ n = M^{kg} \ mod \ n = M^{c(p-1)(q-1)+1} \ mod \ n = M \cdot M^{c(p-1)(q-1)} \ mod \ n = M \cdot 1 \ mod \ n = M$.

- Pak tedy $n = 3337, r = 3220$.
- Zvolme $k = 79$, dopočítáme $g = 1019$.
- Veřejný klíč je tedy $(3337, 79)$, soukromý klíč je 1019.
- Požadovanou zprávu převedeme na číslo, nechť je to třeba 688.
- Zašifrování: $e(688) = 688^{79}\ mod\ 3337 = 1570$.
- Dešifrování: $d(1570) = 1570^{1019}\ mod\ 3337 = 688$.

Cvičení:

1. 1111 10110 10011 101 11 1000 1110 1111 10011 101 10010 1111 11010 100 101 1100
2. YIO-YOI-YYII-IO-YIY-I–YIO-YOI-IY–YYIII-Y–YII-IYIO–YII-YIY-I-III-Y–YYIII-O-YIII-II-YIII-YOI-YYII-IO
3. (Exit) 13, 15, 7, 5, 17, 18, 6, 21, 22, 24, 18, 16, 11, 14, 27, 7, 20, 22, 10, 12, 11, 6, 23, 8 - PI
4. RSA: Veřejný klíč je $(3233, 17)$, soukromý klíč je 2753. Dešifrujte zprávu 855.
5. 

Tabulky

Tabulky jsou dalším způsobem systematické substituce. Klasický je zejména ”polský kříž” uvedený na Obrázku 2.1. Existuje několik dalších variant tohoto kříže, viz. [7, 8]. Můžeme si též vyrobit vlastní tabulku. V tom případě je však vhodné mít ji při dešifrování.

A	B	C	D	E	F	G	H	Ch
I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z

Obrázek 2.1: Polský kříž

Cvičení:

1. 12 51 14 55 51 14 23 24

	1	2	3	4	5
1	S	E	Q	H	O
2	K	F	B	I	G
3	X	A	L	P	V
4	R	N	T	C	Z
5	J	Y	D	U	M

2. 

2.2 Transpoziční šifry

Transpoziční šifry, narozdíl od substitučních šifer, nemění "vzhled" písmen (maximální úpravou je odháčkování a odčárkování), ale mění jejich pořadí. Základními principy, se kterými se můžeme setkat, jsou:

- vynechání mezer, udělání mezer na jiných místech
- psaní pozpátku
- přesmyčky = přeházení písmen v rámci jednoho slova
- přidání redundantních písmen
- psaní zprávy ob dva znaky, ob tři,...
- psaní cik-cak mezi dvěma řádky, případně dle jiných pravidelných vzorů (např. hradby)
- psaní zprávy do tabulky, dle určitého pravidla (např. šnek, skákání koněm)

Dobrou metodou řešení je pořádně se podívat a uvidět nějaké slovo. Ještě lepší metodou[4] je nejdříve uhádnout, jaké slovo by se asi v textu mohlo vyskytovat a pak se ho tam snažit najít. Jakmile uvidíte jedno slovo, tak už snadno odhalíte princip a máte vyhráno.

Trochu složitějším principem je pak *šifrovací mřížka*. Ta umožňuje přeházet text do tabulky $N \times N$ a to tak, že pro $N \geq 8$ je text prakticky nedešifrovatelný bez toho, aby luštitel měl k dispozici šifrovací mřížku[5]. Základní princip je jednoduchý – písmena čteme po řádcích, tabulku otáčíme po směru hodinových ručiček. Text "Má Ema má malou mísu" bychom tedy mohli zašifrovat třeba následovně:

[4] No dobře. Jak kdy.

[5] Pokud tedy dostanete do ruky tabulku 10×10 polí a nemáte k dispozici žádnou mřížku, pak (A) jste někde něco zapomněli, (B) je to jiná šifra, (C) organizátoři jsou fakt drsní.

Mřížka

X			
		X	
X			
	X		

Zpráva

M	A	U	A
M	I	A	O
E	L	M	U
M	M	S	A

Cvičení:

1. kmybmvuliat
   edyzalovssv
   lnbctmevszn
   iaeylleptie
2. tep lekol a ckyastu de nemle kotiu de lajido bre.
3. eeeededaaceeeaeagaaae
   ijhmohonpokjkkolhonkiho
   vttvrtuzrurutstusvtuustrvr

2.3 Steganografie

Steganografické metody se nesnaží zprávu znečitelnit, ale *skrýt* ji. Pro větší účinnost je samozřejmě možné tento přístup kombinovat s dalšími metodami. Příklady skrývání jsou následující:

- Neviditelné inkousty (aby se zpráva objevila, je potřeba papír nejdříve nahřát, případně přetřít speciálním roztokem).
- Zpráva je skryta v jídle či v určitém předmětu (např. uvnitř diskety).
- Zpráva je skryta v hudební nahrávce (např. jako morseovka v bubnech), v obrázku (např. výběr určité barvy) či fotografii (např. rozdíl oproti realitě).
- Celá zpráva je zmenšena tak, že vypadá jako tečka na konci věty.
- Zpráva je napsána psacím strojem bez inkoustu (pouze průklepy) a poté přepsána nějakým irelevantním textem.
- Oholíme poslovi hlavu, zprávu napíšeme na vyholenou lebku, počkáme až poslovi dorostou vlasy a teprve pak ho pošleme.[6]

Nejvíce používanou metodou je skrývání v rámci nějakého zdánlivě smysluplném textu. Zprávu je potřeba určitým způsobem "vybrat", vybíráme například:

[6] Slibujeme, že tento princip nebude na Tmou nikdy použit. Proto, prosím, neholte náhodným kolemjdoucím během hry jejich hlavy. Děkujeme.

- pouze první písmena/slova
- písmena následující po něčem význačném (často se opakující hláska, chyba)
- vhodně vybrané písmeno (zadané číslem)
- označená písmena (jiný font, velká písmena, písmena označená tečkou)

Zvláště pokud vybíráme písmena dle určitých čísel, máme mnoho možností výběru: počítat od začátku věty, řádku, slova nebo od předchozího vybraného písmene, atd. Složitější šifry pak samy v sobě obsahují indicie k vyluštění. Například číslo vyskytující se ve větě může udávat pořadí písmena, které je potřeba vzít od začátku věty.

Cvičení:

1. Dana má modré tkaničky a nebydlí vedle Evžena. Standa je vlastníkem želvy, která ujde 3 metry za hodinu. Ema má maso, máma má mísu. Tomáš slaví narozeniny. Kolik je mu let?
2. Mluvit přímo, směle a upřímě je veliké umění. Mezi zkřivenými větvemi stařičké lípy nad námi, nad rozkvetlými snítkami se shlukly celé roje včel. Nad pustým polem se rozléhal havranní křik. Uvědomyli jsme si svou povinnost. A sovětští lidé, usměvaví Ukrajinci nebo vysocí Rusové ze severu, nám vykládali, jak krásné jsou jihomoravské vinice zjara, jak půvabná je krajina za Břeclaví, a nejednou se stalo, že ji znali líp než tamější člověk, protože oni jí nejen prošli, oni v ní bojovaly. Encyklopedycký slovník je nezbytnou příručkou každého vzdělance. Ve výhni se tyč rozžhavyla do běla. O prázdninách jsme podnikli obtížnou tůru po Vysokých Tatrách. Stali se klasiky barbarského světa, který spojili s Antickou kulturou. Byl čas jiter čím dále temnějších.

2.4 Grafické šifry

Grafické šifry udávají návod, jak vykreslit písmena, číslice, mapovou značku, či něco jiného, co určí následující stanoviště. Vykreslování může být založeno například na následujících principech:

- Vybraná písmena/čísla z textu vytvoří obrázek. Je vhodné si text přepsat do mřížky a pak zvýraznit podezřelé entity.
- Pospojováním vhodných bodů v zadání vznikne obrázek.
- Zadání určuje, jak kreslit (šipečky, souřadnice bodů).

- Zadaní popisuje určitý děj a když jej sledujeme, se nám tak vykreslí obrázek, například šachová partie (rozestavení figurek na konci hry) či popis sportovního utkání (pohyb míče po ploše vykresluje písmeno).
- Materiály, které jsme obdrželi, na sebe vhodně přiložíme, prosvítíme,... a ono se něco objeví.

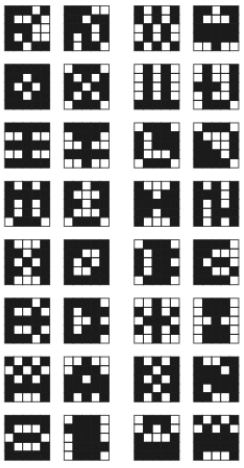
Případně se může stát, že šifra je již přímo výsledným obrázkem a je "jen" potřeba ji správně interpretovat. Příkladem může být situace, kdy je zadáním nějaký útvar nacházející se na mapě (vrstevnice, železnice, elektrické vedení) nebo v realitě (socha, výstavní štít). Pokud je takový útvar vytržený z kontextu a trochu upravený a abstrahovaný, může být k nepoznání.

Cvičení:

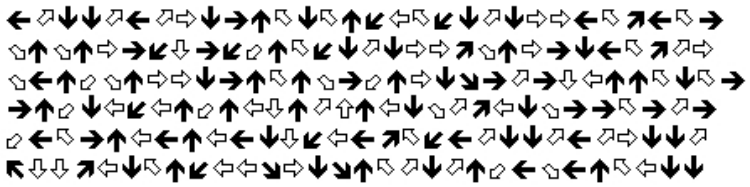
1. 3,0.5 - 5,0.5 - 5,1.5 - 1,1.5 - 1,2.5 - 1.5,2.5 - 1.5,2 - 2,2 - 2.5,2.5 - 2.5,2 - 3.5,2 - 3.5,3 - 3,3 - 3,2.5 - 2.5,2.5 - 2.5,3 - 2,3 - 2,2.5 - 1.5,2.5 - 1.5,3 - 1,3 - 1,2.5 - 0,2.5 - 0,4 - 1,4 - 1,3.5 - 3,3.5 - 3,5 - 4,5 - 4,4.5 - 5.5,4.5 - 10,4 - 18,3 - 10,1.5 - 10,0 - 7,0 - 7,0.5 - 9,0.5 - 9,1.5 - 6,1.5 - 6,0 - 3,0

2. (Sendvič)
   Samoobsluho,komustovkou?kdoprodákiloočí?
   PaníMarnáaHladkáiAdamHadraautadodaj
   Béé́é,aovceznělyzčerného sv ětaejajbéé́é,bůů
   AtyIvo,jdikIvějdiIvěuzmibiča2tyčky.
   Tybludedržhubutvébububujeúnavnéužumři!hu

3. (Bedna)



4. (Bedna)



2.5 Hádanky, úkoly a spol.

Dále můžeme narazit také na různé hádanky a úkoly. Většinou jsou vysvětleny, takže princip je jasný a jde "jen" o to je vyřešit. Občas můžou být ale i součástí šifry bez vysvětlení. Uveďme si několik příkladů:

- logické hádanky
- hádanky lidové
- slovní hříčky, asociace
- křížovky, osmisměrky,...
- rébusy

Zvláště oblíbené je doplňování řad známé z IQ testů. Nejčastější principy jsou následující:

- číselné řady
  - aritmetické (rozdíly konstantní)
  - geometrické (podíly konstantní)
  - kombinace aritmetických a geometrických, posloupnosti vyšších řádů (rozdíly/podíly tvoří aritmetickou/geometrickou posloupnost)
  - posloupnosti založené na pravidelných vzorech
  - prvočísla, sudost, dělitelnost,...
- poloha písmen v abecedě (napsat si čísla a převést na předchozí bod)
- gramatický význam písmen (např. samohlásky, bflmpsvz)
- první písmena známých posloupností (měsíce, dny v týdnu, planety) či známých vět (např. slova písniček)
- známé věci z různých oblastí (např. chemické prvky, historické roky,...)

Některé z těchto úkolů mohou být založeny na specifických znalostech. Většinou by člověk měl vystačit s běžnými středoškolskými znalostmi. Ale i pokud by vám znalosti chyběly, neměl by pro vás být problém si je sehnat: na internetu, u přítele na telefonu, ve zlatých stránkách, od kolemjdoucích.

Cvičení:

1. (Sendvič) Řešením je pětipísmenné slovo:

```
E, b, B, F, C, G, _
D, A, P, O, D, O, _
W, =, S, X, M, X, _
P, N, K, I, F, D, _
N,CH, R, T, H, K, _
M, J, U, 7, Y, G, _
F, C, L, B, R, I, _
```

2. J, D, T, Č, P, ?
3. 11 21 23 12 34 12 34 51 23 ??
4. 18, 35, 38, 45, 48, 53, 57, 68, 75, ??
5. (Bedna) 5,h,s,i,?
6. 1000EDD
7. $(S + 50)_r K$
8. (Bedna) Nerušit Z=RU.

2.6 Rozpoznávání šifer

Cvičení v předchozích kapitolách jsou velmi ulehčená tím, že víte, jaký princip hledat. To nejtěžší na šifrování je většinou právě přijít na to, jaký princip je třeba použít. Několik hrubých rad:

- tvoří to skupinky o 1 až 4 znacích ⇒ morseovka
- je tam určitých objektů zhruba 26 ⇒ písmena abecedy
- rozličná četnost symbolů ⇒ písmena abecedy
- frekvence písmen odpovídají češtině ⇒ transpozice
- věty jsou smysluplné avšak dosti kostrbaté ⇒ steganografie (výběr písmen)

- text vypadá úplně normálně a plynule ⇒ steganografie (nějaká finta)
- nic z předchozího ⇒ grafická

Zkuste se též zamyslet, co nese informaci a co je jen šum. Dávejte pozor na "trojské koně" (vypadají jako jedna šifra, ale jsou úplně jinou).

Cvičení:

1. (Bedna) 7-5/2.5 4.0 8.0 7.5/1.5 9.5-6/2-4.5/3-1 8-6 7-5/2.5 3.0 8.8-7/2.5 9.0 8.8/2-1.4-3/1.5 9-3/1.5 9.0-3-1-6/4-1-1.5 6.0 5.0/2.5-1 9-4.5/3-1-1-3/1.5-1-05 5/2.5 8/2.5-2.2 8.8/2-3.6/1.5 9.6/2-1.8 7-7.5/2.5

2. Slohová práce: Jak jsem umřel
   Potom, co jsem si přečetl Alchymistu, jsem se rozhodl, že nebudu dbát na své dvě křečové žíly a půjdu také hledat poklad. Protože jsem se bál, že ho bude hlídat drak, vzal jsem ještě Honzu (on je sice trochu hloupý, ale zato má tři koloběžky). Avšak potom, co spadl do první jámy, uplavala mu jeho oblíbená černá ponožka a nadýchal se ozónu, ho to přestalo bavit a zakalil. Naštěstí jsem se brzy spřátelil s orlem a odletěli jsme do Švédska, kde se mě ujaly čtyři krásné panny, které mě uvedly za panem králem (nevím proč, ale seděl pod stromem). Ani jsem se nestihl zeptat, proč je jediné královské jablko modré, a přišel policajt a zatkl mě za pašování slivovice. Zavřel mě na místním zámku Boyard a jediné, co mi nechal, byly čtvery housle. Protože na ně neumím hrát, tak jsem je alespoň vyměnil s hostinským za dvě bečky kofoly. Bylo to tam otravnější než ve škole, a tak jsem napsal dva pohledy a poslal je po psovi na poštu. Pak přišla strašná bouře, která mě odnesla z toho hroznýho města přes jednu (ale za to velkou) poušť až na romantickou pláž. Moře bylo fakt úžasný, ale rádio hlásilo, že už jsou čtyři, a tak jsem si oblékl svetr a vydal se lovit ovce. Jenže Karlovi, kterýmu patřily, to vadilo, přivázal mě provazem k jednomu velkýmu kameni a hodil do řeky. A tam jsem se utopil.

Kapitola 3

Pohyb v terénu

Jedinou cestou kolem propasti je často cesta kolem propasti.

Tato kapitola uvádí přehled toho, co byste měli umět, aby váš terénní postup dopadl bez problémů. Pokud si nejste příliš jistí, radši si své znalosti a dovednosti doplňte. Text kapitoly je inspirován knihou [3], která je dobrým zdrojem detailnějších informací.

3.1 Mapy

Základní znalosti:

- mapové značky
- měřítko, odhad vzdáleností v mapě
- vrstevnice, ekvidistance
- určování toho, kde je nahoře a kde dole

U terénních her se můžete setkat i s mapami na orientační běh. Ty se liší nejen měřítkem a podrobností (která výrazně převyšuje normální mapy), ale i barevností. Na orienťáckých mapách se barvy používají následovně:

- bílá – les, bez obtíží průběžný
- zelená – les hustý, špatně průchodný nebo křoví (čím sytější zelená, tím hůře prostupný les)
- žlutá – otevřený terén bez stromů (pole, louky, paseky)
- modrá – vodstvo (potoky, rybníky, prameny, bažiny aj.)

- hnědá – výškopis (především vrstevnice) a netrvalé terénní útvary (vývraty, jámy, kupky)
- černá – objekty trvalého charakteru umělé (cesty, ploty, budovy, atd.) a přírodní (skály a kameny)

Zejména v noci a za deště se hodí mít mapu zalaminovanou, používat mapník nebo alespoň eurofólii. Je velmi vhodné mít s sebou přesně to vydání mapy, které doporučují organizátoři (různá vydání se mohou lišit v detailech, jako je například výška kóty, které jsou však během hry zásadní). Občas se vyplatí mapu otočit. Informace se nachází i na druhé straně. Také je dobré mít kvalitní a aktuální mapu města, nejlépe s rejstříkem ulic a mapu MHD.

3.2 Azimuty

Základní znalosti:

- určování světových stran, dle slunce, měsíce, hvězd, mraveniš́... a také buzoly
- určení azimutu, čtení azimutu z mapy
- chůze dle azimutu (s pomocí orientačních bodů), v noci či v terénu bez výrazných bodů (tři lidé za sebou)

Detailnější rady k práci s buzolou najdete třeba v [5]. Zde jen připomeneme, abyste si při odměřování azimutu dávali pozor na obligátní závory, elektrická vedení, ale i mobilní telefony.

3.3 Volba postupu

Jak zvolit postup na další stanoviště? Existuje několik univerzálních, zaručených, jednoduchých, mnohokrát vyzkoušených *nevhodných* metod:

- zkratka (”já to tady znám”, ”je to sice dál, ale o to horší cesta”)
- hurá postup (zdánlivě jasná cesta, která pak není tak jasná, ale když už se tudy jde, tak se přece nebudeme vracet)
- postup opatrných obcházečů (nepřemýšlet, neremcat, obcházet)
- postup po spojnici (dle azimutu, nebo lépe, moderně, dle GPS)
- postup nerozhodných (pravidelné střídání předchozích)

Žádná univerzální vhodná metoda asi neexistuje. Snad několik obecných rad:

- Nejdřív najít výrazný záchytný bod (soutok, křižovatka, objekt) a od něj dohledávat cílové místo.

- Určovat si zarážky (když dojdu k zarážce, tak už jsem moc daleko; zarážkou může být potok, křižovatka, klesání).
- Po cestách je postup výrazně rychlejší a méně fyzicky namáhavý (zejména v noci).
- Při plánování cesty brát v úvahu kopce.
- Nestydět se uznat chybu a vrátit se.
- Nespoléhat se slepě na mapu, zejména cesty se docela rychle mění.
- Neignorovat mapu, zejména vrstevnice se většinou moc rychle nemění.

3.4 Rychlost postupu terénem

Při tradičním orientačním běhu – tj. běh terénem, kvalitní mapa, přímý průstup terénem od bodu k bodu (ne obcházení obtížných úseků) – se počítá průměrně 1 minuta na 100 metrů horizontální vzdálenosti.

Pro dlouhodobější chůzi po upravené cestě můžeme použít následující metodu odhadu. Jednotlivec, případně malá skupinka, ujde za 1 hodinu:

- 5 km horizontální vzdálenosti
- 400 výškových metrů ve výstupu
- 800 výškových metrů při sestupu

Údaje platí pro trénované jednotlivce s lehkým batohem (do 12 kg). Při chůzi "na pohodu" údaje opravte na 300/600 výškových metrů a 4,5 km vzdálenosti. Samotný výpočet doby probíhá tak, že se vypočte čas vyplývající z převýšení a čas vyplývající z délky trasy, menší se vydělí dvěma a přičte k většímu. Příklad:

- profil trasy:
  - 0. km, 450 m.n.m
  - 2. km, 300 m.n.m.
  - 7. km, 500 m.n.m.
  - 8. km, 400 m.n.m.
- z toho vychází údaje:
  - délka trasy 8 km
  - výstup 200 m
  - sestup 250 m
- čas na trasu:

- délka: (8 km/5 km) · 60 min = 96 min
- výstupy a sestupy: ((250m/800m)+(200m/400m)) · 60 min = 49 min
- výsledek: 96 min + (49 min/2) = 2 hod

V případě "pohodovějšího postupu" 2 hod 18 min.

Otestujte si, jakou vzdálenost ujdete za 1 hodinu vy a jaká převýšení jste schopni zdolat, pomůcka pak funguje velmi pěkně.

3.5 Chování v přírodě

Připomínáme, že i při hře je nutno dodržovat následující ustanovení zákona o lesích. V lesích je zakázáno:

- rušit klid a ticho
- sbírat lesní plody způsobem, který poškozuje les
- vstupovat do míst oplocených nebo označených zákazem vstupu
- umožnit volný pohyb psům
- kouřit, rozdělávat nebo udržovat otevřené ohně (a to i tehdy, když je vám zima!)
- odhazovat hořící nebo doutnající předměty
- narušovat vodní režim a hrabat stelivo
- znečišťovat les odpady a odpadky
- a hlavně… pást dobytek či umožňovat výběh hospodářským zvířatům a průhon dobytka lesními porosty.

3.6 Vybavení

Jídlo, pití – Dostatek energetických věcí (čokoláda, hroznový cukr). Termoska s teplým čajem. Dostatek pití (alespoň 2l na osobu, půjdete možná 18 hodin, s dočerpáním se nedá počítat). Alkohol výrazně nedoporučujeme (kdo zrmzne, umře).

Oblečení, boty – Teplé oblečení (doporučujeme více vrstev oblečení, které budete přidělávat a ubírat dle potřeby), pláštěnka (na chůzi), deštník (na luštění), boty (ne nové, namazané). Spacák a karimatka dle vlastního zvážení.

Turistické vybavení – Mapy, buzola, KPZ či základní lékárnička, tužky, papíry, podložka na psaní, pravítko.

Technika – Čelovka (náhradní baterie), nabitý mobil, kalkulačka. Složitější technika jako GPS či notebook je dle našeho názoru naprosto zbytečná.

Cvičení:

1. Organizátoři vás omámili, všechno vám sebrali a převezli na neznámé místo. Jak zjistíte na kterém bodě Země se nacházíte? Jaké minimální (co do technologií, ne do počtu) pomůcky byste potřebovali, abyste dosáhli slušné přesnosti?

2. Zvolte si dvě místa vzdálená zhruba 1 km v terénu. Změřte si, jak dlouho vám bude trvat přesun: A) přímo azimutem (maximální odchylka 10m od směru), B) relativně přímo, po malých cestách, C) obcházením po cestách, D) v noci, E) během. Zkuste si dopředu udělat časové odhady.

3. Vyberte v mapě dvě náhodná místa. Diskutujte o různých možnostech přesunu a odhadněte časovou náročnost. Ověřte svůj odhad.

4. Zkuste odhadnout hmotnosti jednotlivých věcí, které s sebou nesete. Zvažte, co byste si vzali, kdybyste měli váhový limit 0,1 kg; 0,5 kg; 1 kg; 2 kg; 5 kg.

Kapitola 4

Tipy

Máš IQ > 150? Tak to ti stačit nebude...

Úvodem této kapitoly musíme připomenout, že ji sepsali organizátoři, kteří mají s účastí minimální zkušenosti. Ale něco jsme občas zaslechli...

4.1 Složení týmu

- Víc hlav víc ví. Rozhodně se vyplatí jít v "plném počtu".
- Různorodé složení týmu je výhodou. Ani ne tak kvůli specifickým znalostem, jako spíš kvůli specifickým způsobům uvažování. Každopádně by v týmu měl být někdo, kdo dokáže logicky myslet, někdo, kdo se trochu vyzná v Brně a někdo, kdo se umí orientovat v noci. A samozřejmě taky někdo, kdo má pevnou vůli a dobré motivační schopnosti.
- Určitě je lepší, když je tým složen z lidí, kteří se vzájemně znají a ví, co od sebe mohou očekávat. Je to náročná hra s náročnými situacemi. Tým domluvený po internetu může být začátkem dobrého přátelství, ale i přesto bychom ho nedoporučovali.
- Nejlepší je samozřejmě tradiční tým, s tradičním názvem a tradičními soupeři...

4.2 Příprava na hru

- Před hrou si pořádně přečtěte aktuální pravidla a veškeré další užitečné informace, které organizátoři poskytují. Raději si to vytiskněte.
- Noc před hrou se pořádně vyspěte.

- I když Tmou není nijak extrémně fyzicky namáhavé, můžete zkusit následující "maratónovou dietu": od soboty do úterka nebudete jíst téměř nic sladkého, od středy do pátku pak naopak budete jíst hodně sladkého. Tento ověřený postup zajistí, že se vám cukr lépe naváže a tato energie při hře jistě přijde vhod.

4.3 Šifrování

Pointa šifrování je v tom, že na to neexistuje žádný mechanický recept. Proto není divu, že některé z následujících rad k šifrování si trochu protiřečí...

- Užitečnou technikou je *brainstorming*. Má dvě fáze. V první fázi všichni chrlí nápady a ty se zapisují. Důležité je, že v této fázi cizí nápady nehodnotíme. Naopak, cizí absurdní nápady využíváme k vymýšlení ještě absurdnějších. V druhé fázi projdeme seznam vygenerovaných nápadů, kriticky proškrtáme všechny nesmysly a pokud nám něco zbude, tak se nad tím více zamyslíme.
- Zkoušejte nejdříve jednodušší principy.
- Zkuste zpětné inženýrství. Pokud máte před sebou nějakou obskurní změť znaků a nevíte co s tím, zkuste se zamyslet, jak byste *vy* převedli smysluplný text na něco takového. Nejlépe zkuste i uhádnout, jaký text by to zhruba mohl být[1]. Koukejte do mapy, zkuste otipovat, co z toho by mohlo být řešením (číslo kóty, mapová značka) a zkuste to napasovat na zadání.
- Řekněte si jasně, co chcete vyzkoušet (který nápad, jakou metodu) a vydržte s tím pracovat nějakou dobu. Často se stane, že člověk má správný nápad, jenom to nedotáhne do konce nebo to vzdá, když mu prvních pár písmen vychází zdánlivě nesmyslně.
- Neupínejte se na jednu myšlenku. Dejte si časový limit a poté zkuste vymyslet nějakou jinou metodu.
- Pracujte paralelně. Zkoušejte víc možností řešení současně.
- Pracujte společně. Jeden člověk snadno udělá chybu, která způsobí, že správné řešení vypadá jako nesmysl.
- Buďte podezíraví. Podivné náhody často nejsou náhody. Všímejte si pravidelností (např. počet znaků na všech řádcích je stejný, součet určitých čísel je konstantní). Jakákoli pravidelnost či "náhoda" v zadání může být začátkem úspěšného řešení.
- Nebuďte paranoidní. Podivné náhody jsou často jenom náhody. Jakákoli "náhoda" v zadání může být začátkem několikahodinové neúspěšné procházky.

[1] Má první slovo 4 písmena a druhé slovo 9 písmen? Sázím boty, že to je "Milí účastníci"

- Nevymýšlejte překombinované konstrukce. Organizátoři v podstatě chtějí, aby většina týmů šifru vyluštila. Nápad na řešení, který je založen na počtu slečen v růžovém tričku, které jste po cestě potkali, obvodu kanálu který byl opodál předchozího stanoviště a ceně pizzy v obchůdku naproti, asi nebude úplně správný.
- Nikdy si nebuďte ničím jistí[2]. Organizátoři jsou v podstatě svině.
- Využíváte všechny informace, které máte k dispozici? Opravdu všechny? I tuto větu?

A několik rad pro případ nouze:

- Zkus morseovku.
- Vezmi první písmena.
- Rozbij to.

4.4 Ostatní

- Chladná hlava je důležitější než rychlé nohy. Minuty většinou nerozhodují. Běhat nemá příliš smysl. Tedy pokud nechcete ve dvanáct odpadnout a jít spát.
- Pokud vyjde správné řešení, je si člověk (většinou) jistý, že je to ono. Každopádně, dřív než půjdete 5 km daleko, tak se radši ještě jednou pořádně zamyslete. Zvláště pokud doposud byla všechna stanoviště po zhruba jednom kilometru a v zadání je doslova napsáno, že je to maximálně 3 km.
- Často se vyplatí obětovat trochu času a najít si útulné místo na luštění. Dle našeho odhadu lze v teplé tiché suché kavárně dosáhnout nejméně $7,42\times$ vyšší efektivity šifrování než za deště, pod lampou a vedle hlučné silnice.
- V terénu, kde se nevyskytují tiché suché kavárny, může být dobrou strategií proti promrznutí náhodné popojití očekávaným směrem dalšího stanoviště. Ono teda nakonec bude úplně na druhou stranu, ale alespoň vám nebude zima.
- Když nad ránem přijde krize, může být výhodné nechat nejunavenější členy týmu během luštění prospat. Stejně by moc nepomohli a alespoň budou mít víc sil na další šifru.
- Zprávu na stanovišti nehledejte déle než 20 minut. Pokud ji v této době nenajdete, pak jste na špatném místě.

[2] *Do přůšvihu nás nikdy nedostane to, co nevíme. Dostane nás tam to, co víme příliš jistě a ono to tak prostě není.* (Y. Berry)

- Pokud někde po cestě najdete v popelnici knížku, kterou jste tam konkrétně hledat neměli nebo pokud tato knížka nemá na první stránce logo Tmou, pak najít v ní polohu následujícího stanoviště je prakticky nemožné.
- Nepoškozujte prosím betonové roury v blízkosti trasy hry (např. chůzí, dotykem). Organizátorům takové počínání může působit jisté problémy.

Literatura

[1] S. Chromčák. *Šifrování pro děti*.
http://www.gjar-po.sk/import/sifry.
Další stránka s klasickými táborovými šiframi.

[2] E. Friedman. *Erich's Puzzle Palace*.
http://www.stetson.edu/ efriedma/puzzle.html.
Výborné stránky s logickými hádankami. Některé z nich se objevily v předchozích ročnících Tmou.

[3] J. Neuman. *Turistika a sporty v přírodě*. Portál, Praha, 2000.
Kniha obsahuje mimo jiné kapitolu o orientaci v terénu.

[4] R. Nichols. *Classical Cryptography Course*.
http://www.fortunecity.com/skyscraper/coding/379/lesson1.htm.
Anglicky psaný text o šifrách s podrobně vysvětlenou metodologií luštění substitučních šifer.

[5] Horolezecký oddíl Šakal. *Orientace s buzolou*.
http://sweb.cz/ho.sakal/orient/buzola.htm.
Základy práce s buzolou.

[6] S. Singh. *Kniha kódů a šifer*. Argo, Praha, 2003.
Kniha se zabývá zejména historií šifrování, ale jsou v ní popsány i principy některých klasických šifer. Na doprovodných webových stránkách (*http://www.simonsingh.net/Cipher_Challenge.html*) najdete několik zajímavých příkladů (vhodných třeba jako rozcvička na Tmou).

[7] *Stránky o šifrování oddílu Wakan*.
http://www.wakan.cz/sifry/list.php.
Podrobně vysvětlené základní šifry.

[8] V. Zoubek. *Šifry*.
http://home.tiscali.cz:8080/ cz077482/sifry.
A ještě jedna podobná.

[9] *Stránky Tmou a podobných her*.
Mnoho inspirace a zajímavých příkladů můžete najít na webových stránkách Tmou a podobných her. Odkazy viz. úvodní kapitola.

Kapitola A

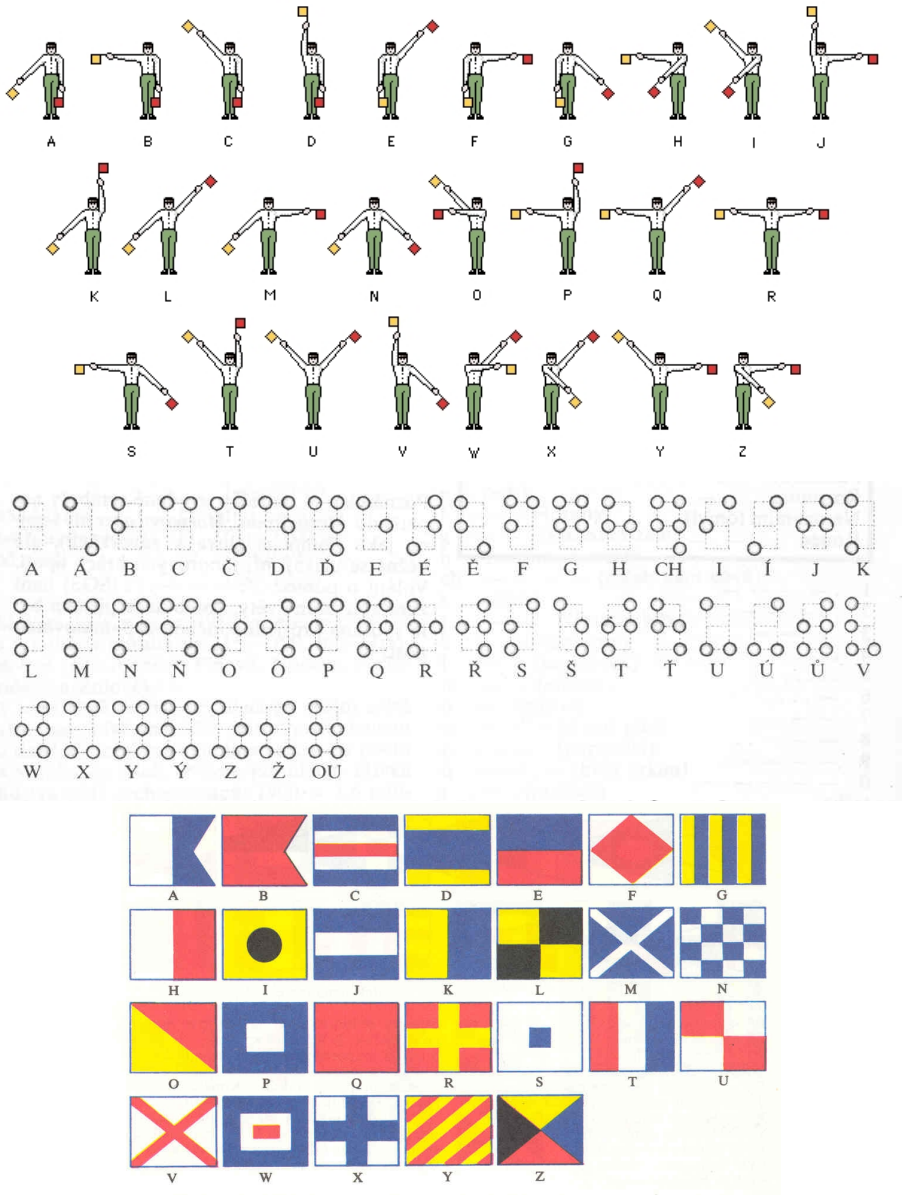
Šifrovací pomůcky

A	· –	Akát	N	– ·	Nástup
B	– · · ·	Blýskavice	O	– – –	Ó náš pán
C	– · – ·	Cílovníci	P	· – – ·	Papírníci
D	– · ·	Dálava	Q	– – · –	Kvílí orkán
E	·	Erb	R	· – ·	Rarášek
F	· · – ·	Filipíny	S	· · ·	Sobota
G	– – ·	Grónská zem	T	–	Trám
H	· · · ·	Hrachovina	U	· · –	Učený
Ch	– – – –	Chvátá k nám sám	V	· · · –	Vyučený
I	· ·	Ibis	W	· – –	Vagón klád
J	· – – –	Jasmín bílý	X	– · · –	Xénokratés
K	– · –	Krákorá	Y	– · – –	Ýgar mává
L	· – · ·	Lupíneček	Z	– – · ·	Známá žena
M	– –	Mává			

1	· – – – –	6	– · · · ·
2	· · – – –	7	– – · · ·
3	· · · – –	8	– – – · ·
4	· · · · –	9	– – – – ·
5	· · · · ·	0	– – – – –

otazník	· · – – · ·	pomlčka	– · · · · –
čárka, vykřičník	– – · · – –	odsuvník, tabelátor	· – – – – ·
tečka	· – · – · –	závorka	– · – – · –
středník	– · – · – ·	uvozovky	· – · · –
zlomková čára	– · · – ·	dvojtečka	– – – · · ·

Tabulka A.1: Morseovka



Obrázek A.1: Semafor, Braillovo písmo a vlajková abeceda

000	(nul)	016 ▶	(dle)	032 sp	048 0	064 @	080 P	096 `	112 p
001 ☺	(soh)	017 ◀	(dc1)	033 !	049 1	065 A	081 Q	097 a	113 q
002 ☻	(stx)	018 ↕	(dc2)	034 "	050 2	066 B	082 R	098 b	114 r
003 ♥	(etx)	019 ‼	(dc3)	035 #	051 3	067 C	083 S	099 c	115 s
004 ♦	(eot)	020 ¶	(dc4)	036 $	052 4	068 D	084 T	100 d	116 t
005 ♣	(enq)	021 §	(nak)	037 %	053 5	069 E	085 U	101 e	117 u
006 ♠	(ack)	022 ▬	(syn)	038 &	054 6	070 F	086 V	102 f	118 v
007 •	(bel)	023 ↨	(etb)	039 '	055 7	071 G	087 W	103 g	119 w
008 ◘	(bs)	024 ↑	(can)	040 (	056 8	072 H	088 X	104 h	120 x
009	(tab)	025 ↓	(em)	041)	057 9	073 I	089 Y	105 i	121 y
010	(lf)	026	(eof)	042 *	058 :	074 J	090 Z	106 j	122 z
011 ♂	(vt)	027 →	(esc)	043 +	059 ;	075 K	091 [	107 k	123 {
012 ♀	(np)	028 └	(fs)	044 ,	060 <	076 L	092 \	108 l	124 |
013	(cr)	029 ↔	(gs)	045 -	061 =	077 M	093]	109 m	125 }
014 ♫	(so)	030 ▲	(rs)	046 .	062 >	078 N	094 ^	110 n	126 ~
015 ☼	(si)	031 ▼	(us)	047 /	063 ?	079 O	095 _	111 o	127 ⌂

Obrázek A.2: ASCII tabulka

	0	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
	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	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
B	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
C	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	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Tabulka A.2: Převáděcí tabulka pro posuny v abecedě (číslování od nuly)

	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
	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	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Tabulka A.3: Převáděcí tabulka pro posuny v abecedě (číslování od jedničky)