TMOU 5 Řešení

1 Úvodní poznámky

Základní podoba šifry – rozhovor s rekurzivním zanořováním – je inspirována knihou *Gödel, Escher, Bach: an Eternal Golden Braid* (podobně jako rozhovor na TMOU 3). Originální rozhovor v uvedené knize v sobě neskrývá žádnou šifru, ale ilustruje některé z principů týkajících se logiky, rekurze, nerozhodnutelnosti. Narážka na „konzistenci šifrovacího prostoru“ je parodií na konzistenci logických axiomatických systémů. I když je to jeden z mála prvků v zadání šifry, který nenese informaci použitelnou pro šifrování, nechtěli jsme si jej odpustit. Znalost uvedené knihy nemá žádný vliv na luštění, pouze ti, co ji znají, si možná zadání užili více než ostatní.

Protože šifra vlastně popisuje sama sebe, většina textu řešení jsou pouze vhodně přeuspořádané citáty ze zadání (psané italikou) doplněné o vysvětlující komentář.

Poznámka ze zákulisí: Šifra má ještě víc sebe-referenční charakter než by se mohlo zdát. Některé z výroků uvedených v zadání totiž opravdu zazněly na schůzkách organizátorů…

2 Řešení

2.1 Hlavní princip

- *Ono tam těch informací bude hodně, protože téměř každá věta ponese důležitou informaci. Šifra bude tedy náročná na pozornost …*
- *Všechny šifry by však měly být v textu zmíněny a vysvětleny.*
- *… jasně tam uvedeme, že mají pracovat jen s tím, co je přímo napovězeno v textu …*
- *Šifra obsahuje několik nezávislých podčástí.*

2.2 Morseovka

- *… zmínit morseovku skrytou v samohláskách a souhláskách …*
- *… jména postav. Zatím je využíváš jen pro tu morseovku …*
- *… přebytečná mezera funguje jako oddělovač …* (jde o mezeru mezi jménem postavy a následnou dvoutečkou)
- vypsaná jména postav s přebytečnými mezerami:
  `BCBC B NIN KNK SOIS RS USUS UVU VU SUOI SR SRSR SINK NA CBCA BA`

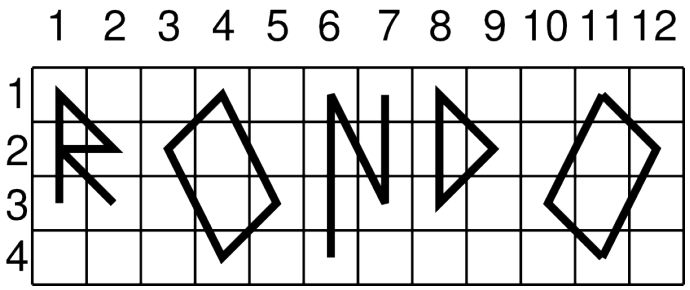
- tedy v morseovce: `herspickajihlava`
- *Ta drobná zkomolenost je důsledek systému. To ale myslím nevadí, je dost zřejmé, že se má vzít křižovatka těch dvou ulic.* (důsledek systému: kvůli grafické šifře je potřeba přesně 48 znaků (jmen postav), navíc pokud chceme, aby střídání postav bylo smysluplné, tak je systém věru hodně omezující)
- řešení: křižovatka ulic Heršpická a Jihlavská

2.3 Popis cesty

- *... mluví o ulici Kamenná a o tom, že jdou na zastávku.*
- *... nastupují do šaliny a jedou až na ... konečnou ...* (jde o konečnou osmičky)
- *... až vystoupíme, budeme šlapat po výpadovce na západ.* (ulice Pražská)
- *... směr našeho postupu se začíná podezřele podobat našemu zákysu na TMOU 3.* (narážka na Troubsko)
- *... jsme u kostela uprostřed náměstí v jakési okrajové díře a nikde nic. Jsem si docela jistý, že jsme na správném místě ...*
- *... zrovna na tomto místě přiběhl org a sebral mi boty ...*
- řešení: Bosonohy střed náměstí (kostel)

2.4 Grafická šifra

- *... když si to takhle správně očísluji, tak vyjde čtyřikrát dvanácka ...* (4 úrovně zanoření rozhovoru, v každé 12 replik)
- *A pak stačí sledovat podezřelé věci v textu. Třeba opakující se věty. Vidíš?* (v textu se vyskytují opakující se věty, například „Třeba opakující se věty.“ a „Vidíš?“)
- *Tak jsem si udělal tabulku. Podle [opakujích se vět] v tabulce udělám čáry a vykreslí se písmenka.*



- řešení: hala Rondo

2.5 Substituce dle nekonečného kódu

- *... na způsob rekurzivních akronymů. Něco na styl „TMOU = TMOU Musí Organizovat Úchyláci“.*
- *... kód šifry je `K28K528K28K55`... kód šifry je `K28K5` ... kód `K`*
- *Heslo je rekurzivní a během procesu odsouhlasení je postupně komprimováno ... Jsou používány rekurzivní identifikační kódy – ty můžeš expandovat na libovolnou délku, kterou potřebuješ do šifry.*
- Kód se expanduje podle pravidla „všechny výskyty `K` nahraď za `K28K5`“, postupným generováním tedy dostáváme:
  `K`
  `K28K5`
  `K28K528K28K55`
  `K28K528K28K5528K28K528K28K555`
  `K28K528K28K5528K28K528K28K55528K28K528K28K5528K28K528K28K5555`
  atd.
- *symbol `K` se používá jen pro generování, nikoliv jako součást vlastního hesla*
- *při expandování zachovává prefix, takže luštitel už z toho částečně expandovaného kódu, který má k dispozici, může dešifrovat ‘trista’, což mu potvrdí, že postupuje správně*
- *Identifikační kód ... použít ... jako kód pro posunutí*
- *tady s tím podivným řetězcem jsme ještě nepracovali:*
  `VZNUBCUADEPQLSGWFSWNEQAVWUQDKKJRQZCDFPGPMGTANFG`
- *Pojďte vyluštit tu sekvenci znaků... Co kdybychom na to použili kód z toho snu?*
- jde o běžný posun v abecedě:

```
 VZNUBCUEFRIFVJQLMZNETUBQXTXQEMRTTIXISAVGJTANIA
-2852828552828528285552828528285528285282855552
 ----------------------------------------------
 TRISTAMZAPADNEODKRIZOSTOPOVICEMORAVANYNEBOVIDY
```

- řešení: 300 metrů západně od křižovatky silnic mezi Ostopovicemi, Moravany a Nebovididy

2.6 Heslo z meta-indícií

- *... pětipísmenném hesle, které se získá skrze meta-indície.*
- *... každou indícii získám ze tří meta-indícií.*
- *Jména postav můžeme použít pro výběr slov z jejich replik – třeba přes první písmena. Z těch slov poskládáme heslo...*
- *S: ... když já řeknu 'strom', tak tomu mají věnovat náležitou pozornost...*
- V textu se vyskytuje právě 12 slov, která začínají stejným písmenem jako jméno postavy, která je říká. Tato slova můžeme roztřídit do 4 skupin po 3 podle úrovní, na kterých se vyskytují (čemuž mimo jiné odpovídají i blízká počáteční písmena v abecedě). Tyto trojice jsou vždy meta-indície na jednu indícii:
  - nástroj, kadeřnictví, nehty: nůžky
  - stůl, ořezané, strom: dřevo
  - sračky, večerní, umyvadlo: toaleta
  - aktuální, cenzuroval, bulvární: tisk
- Z těchto indícií (nůžky, dřevo, toaleta, tisk) dostáváme pětípísmenné heslo: papír.

2.7 Určení polohy stanoviště

- *... systému určení místa, ten uděláme rekurzivní ...*
- *... jednotlivá místa bude potřeba zkombinovat geometricky ...*
- *Vyjde čtyřúhelník. Pak najdou středy stran. Tím vzniknou čtyři nová místa, na která rekurzivně použijí stejnou proceduru. Po nekonečném počtu kroků ty čtyři body splynou, což určí polohu dalšího stanoviště.*
- Postup je jasně popsán, stačí ho tedy aplikovat. Není nutné provádět nekonečně mnoho kroků, stačí provést pár iterací a výsledek aproximovat – v doprovodném textu je napsáno, že další stanoviště se nachází ve velké šedé budově a tu už by neměl být problém dohledat.
- Poznámka (užitečná spíše pro konstrukci zadání než pro řešení): Místo lze určit v konečném počtu kroků dokonce i přesně. Po prvním kroku nám totiž vyjde kosodélník a pro kosodélník platí, že uvedená rekurzivní konstrukce vede do průsečíku uhlopříček. (Uvedené není zcela zřejmé, ale k důkazu lze vystačit se základními poznatky geometrie.)
- Výsledná poloha stanoviště: hala kousek východně od křižovatky Dlouhá a Neužilova.

3 Ladicí verze šifry

Poznámky ze zákulisí: Šifra je vygenerována sázecím systémem LaTeX. Ve zdrojovém kódu jsou použity makra, která umožňují přepínat mezi „ostrou“ sazbou šifry a „ladicím“ výpisem. Následuje ladicí výpis.

Poznámka ze zákulisí 2: Některé dílčí kroky byly konstruovány, resp. kontrolovány programem (např. posun v abecedě nebo kontrola prvních písmen slov). Ani sebelepší technické finty vám nepomůžou, když si systematicky pletete západ a východ. Živý tester je prostě nezbytný.

1 Org B: Já chci letos udělat meta-šifru. Zase nějaký rozhovor.

2 Org C: Šifru v šifře už jsme jednou měli. Jak by se to lišilo?

3 Org B: Tohle nebude ani tak šifra v šifře, jako spíš šifra o šifře. Nějaké zanořování a rekurzivní prvky se tam samozřejmě také hodí.

4 Org C : Já bych byl pro. Už jsem si dlouho říkal, že bychom mohli využít něco na způsob rekurzivních akronymů. Něco na styl „TMOU = TMOU Musí Organizovat Úchyláci“.

5 Org B : Představuji si to jako rozhovor imaginárních účastníků, kteří sedí na stanovišti, na němž reální účastníci šifru najdou. Třeba něco jako:

> 1 Úč N: Vyvarovat se překombinovaných konstrukcí, to je základ. A použít vždy vhodný **nástroj**. Jestli to dokážeme, tak určitě dokončíme. Jak vypadá další šifra?
>
> 2 Úč I: Jak vypadá další šifra? Zase nějaký rozhovor. Teda vlastně několik zanořených rozhovorů, mimo jiné také rozhovor účastníků, kteří jsou přesně na tomto místě. Sleduj, tady mluví o ulici Kamenná a o tom, že jdou na zastávku. Jdem taky?
>
> 3 Úč N : Já bych byl pro. Ale co s tou šifrou? Vypadá fakt složitě. To je drsný.
>
> 4 Úč K: Podívej, tady účastníci mluví o tom, jak postupují. Je tady informace o tom, že ignorují veškerá **kadeřnictví** po cestě. Nevím, proč to tam je, ale budiž. Důležitější bude asi informace, že nastupují do šaliny a jedou až na ...
>
> 5 Úč N: ... konečnou. Tak jedem taky. Ty jo, a tady se píše o pětipísmenném hesle, které se získá skrze meta-indície. A to je jako co?
>
> 6 Úč K : Zdá se, že až vystoupíme, budeme šlapat po výpadovce na západ. Tak to bych vám po cestě mohl povykládat sen, co se mi dneska zdál. Možná z toho pochopíš, co jsou meta-indície. Zdálo se mi totiž, že jsem na schůzce organizátorů TMOU a oni tam se vedli takový ujetý rozhovor:
>
> > 1 Org S: Pojďme vyložit karty na **stůl**. Já chci letos udělat meta-šifru. Nejenom šifru v šifře, ale šifru o šifře. To tu ještě nebylo. Ale není to jen tak, na to potřebujeme povolení meta-orga.
> >
> > 2 Org O: Vyvarovat se překombinovaných konstrukcí, to je základ. K sebe-referenčním šifrám jsem nedůvěřivý. Když už, tak to musí být pořádně **ořezané**, aby tam zůstaly pouze důležité prvky. A vůbec, kdo je to meta-org?

7 Úč I: Tvůj sen je jistě zajímavý, ale měli bychom se věnovat šifře. Nějak se mi to nezdá, mám pocit, že směr našeho postupu se začíná podezřele podobat našemu zákysu na TMOU 3. No ale dobře, dopovídej to, třeba nás to k něčemu nakopne.

3 Org S : Meta-org je organizátor, který organizuje organizátory. Normální šifry můžeš dělat dle libosti, ale šifra, která popisuje vlastní vznik, je meta-šifrou. Kdyby kdokoliv dle libosti dělal meta-šifry, mohla by být narušena konzistence šifrovacího prostoru. Proto musíš mít povolení meta-orga.

4 Org R: Můžeme to povolení získat? Zkus tomu meta-orgovi zavolat.

1 Org S : Zkusím to. Doufám, že zase nebude dělat, jako by TMOU byly **sračky** pod jeho úroveň. Jdu tedy na meta-organizátorskou úroveň a volám meta-orga.

2 Meta-org U: Orgu, co zase potřebuješ?

3 Org S: Chtěli bychom povolení na meta-šifru na TMOU. Šifra by popisovala vlastní vznik a asi by v ní byl uveden i tento rozhovor.

4 Meta-org U: Chceš říct, že bych se v té šifře vyskytoval i já? To je drsný. Fakt drsný.

5 Org S : Aspoň to ukáže, jak reálně fungují šifrovací hry.

6 Meta-org U: Zní to dost šíleně. V tomto případě ovšem potřebujeme povolení od meta-meta-orga. Moment, zavolám mu.

7 Meta-meta-org V: Meta-orgu, co potřebuješ? Zase nějaké problémy s tou pochybnou **večerní** hrou?

8 Meta-org U : Je to noční hra, ale jinak máš zcela pravdu. Potřeboval bych pro TMOU povolení na meta-meta-šifru.

Následuje stále se zrychlující nekonečný řetěz dotazů a odpovědí mezi meta^n-orgy a meta^{n+1}-orgy.

9 Meta-meta-org V: Děkuji za povolení meta-meta-meta-orgu. Meta-orgu, potvrzuji, že povolení je přiděleno, identifikační kód šifry je
`K28K528K28K55`.

10 Meta-org U : Děkuji za povolení meta-meta-orgu. Orgu, potvrzuji, že povolení je přiděleno, identifikační kód šifry je `K28K5`.

11 Org S: Děkuji za povolení meta-orgu. Takže máme povolení a identifikační kód `K`. Teď toho akorát musíme využít. Už mám pracovní návrh. Mělo by to být pořádně provázané. Vidíš?

12 Meta-org U: Vypadá to zajímavě. Akorát bys tam měl ještě přidat **umyvadlo**. To nesmí chybět v žádné pořádné meta-šifře.

5 Org O: Fakt drsný. Už jsem si dlouho říkal, že bychom mohli využít něco na způsob rekurzivních akronymů. A jestli tomu dobře rozumím, ten identifikační kód je něco na ten způsob.

8 Uč I : Že tě zase vyrušuji v tom vyprávění. Popis cesty ale za chvíli končí a třeba tady s tím podivným řetězcem jsme ještě nepracovali:
`VZNUBCUEFRIFVJQLMZNETUBQXTXQEMRTTIXISAVGJTANIA`
No dobře, tak pokračuj a rychle to dopovídej.

6 Org S: Přesně tak. Je to něco jako vodoznak. Identifikační kód, který jsi dostal přidělený, musíš v šifře použít, třeba jako kód pro posunutí. Tím prokazuješ, že jsi dostal k šifře povolení a že nebude narušena konzistence šifrovacího prostoru.

7 Org R : O konzistenci šifrovacího prostoru jsem teda ještě neslyšel. Ale budiž. Není mi ale jasné, proč meta-org říkal jiný kód než meta-meta-org. Jak to vlastně funguje?

8 Org S: Je to jednodušší, než to vypadá. Heslo je rekurzivní a během procesu odsouhlasení je postupně komprimováno. Protože v době žádosti o povolení není jasné, jak šifra bude vypadat, není vhodné přidělovat identifikační kód pevné délky. Jak to vyřešit? Jsou používány rekurzivní identifikační kódy – ty můžeš expandovat na libovolnou délku, kterou potřebuješ do šifry.

9 Org R: Aha, to je fikaný. Předpokládám, že symbol K se používá jen pro generování, nikoliv jako součást vlastního hesla. A teď se dívám, že to dokonce při expandování zachovává prefix, takže luštitel už z toho částečně expandovaného kódu, který má k dispozici, může dešifrovat 'trista', což mu potvrdí, že postupuje správně.

10 Org S: To je detail. Na to účastníci přijdou. Nicméně toto by rozhodně neměla být jediná šifra, která tam bude. Mělo by to být pořádně provázané. Všechny šifry by však měly být v textu zmíněny a vysvětleny. Třeba tam musí být uvedeno, že každou indícii získám ze tří meta-indícií.

11 Org R : Chápu to dobře? Chceš třeba nechat jednu postavu přímo zmínit morseovku skrytou v samohláskách a souhláskách a opravdu tam tu morseovku dát? Nebude to příliš laciné?

12 Org S: Ono tam těch informací bude hodně, protože téměř každá věta ponese důležitou informaci. Šifra bude tedy náročná na pozornost, takže tam klidně mohou být návodné věty typu „když já řeknu '**strom**', tak tomu mají věnovat náležitou pozornost".

9 Úč I: Tak jsme u kostela uprostřed náměstí v jakési okrajové díře a nikde nic. Jsem si docela jistý, že jsme na správném místě, ale klidně jsme to mohli vyčíst z mapy a nemuseli sem chodit. Těch míst je totiž v šifře nejspíš víc. Šifra obsahuje několik nezávislých podčástí. Pojďte vyluštit tu sekvenci znaků. Jak to vyřešit? Co kdybychom na to použili kód z toho snu?

10 Úč N: Myslíš, že organizátoři mohou počítat s tím, jaké se účastníkům zdají sny?

11 Úč K : Pokud mohou oblepit celé město plakáty, proč by nemohli propašovat vhodné halucinogeny do mého obědu? Taky bych se vůbec nedivil, pokud by zrovna na tomto místě přiběhl org a sebral mi boty. Jsou schopní čehokoliv!

12 Úč N: Zatímco vy kecáte, já jsem si všiml pár věcí. Koukejte, když si to takhle správně očísluji, tak vyjde čtyřikrát dvanáctka. Tak jsem si udělal tabulku. A pak stačí sledovat podezřelé věci v textu. Třeba opakující se věty. Vidíš? Podle toho v tabulce udělám čáry a vykreslí se písmenka. Mám pocit, že bych měl zdůraznit, že oproti vyrývání čar do papíru **nehty** je lepší použít tužku. Ale to je přece jasné, tak proč to říkám? To budou asi ty halucinogeny od orgů.

6 Org A : Zní to dost šíleně. O konzistenci šifrovacího prostoru jsem teda

JEŠTĚ NESLYŠEL. No budiž, určitě je to **aktuální** téma. Bude to však dlouhá šifra, čímž hrozí, že v ní najdou spoustu nezamýšlených věcí.

7 Org C: Jasně, oni jsou schopní někde najít číslo 26, i když tys to vůbec nezamýšlel a žádná šifra v tom není. Navíc já se pořád přesně nechytám. JAK TO VLASTNĚ FUNGUJE?

8 Org B: JE TO JEDNODUŠŠÍ, NEŽ TO VYPADÁ. ŠIFRA OBSAHUJE NĚKOLIK NEZÁVISLÝCH PODČÁSTÍ. Každá z těchto podčástí určí jedno místo. Tyto místa se zkombinují a tím vyjde poloha dalšího stanoviště. Aby to bylo jednoznačné, jasně tam uvedeme, že mají pracovat jen s tím, co je přímo napovězeno v textu. Třeba že přebytečná mezera funguje jako oddělovač.

9 Org C: Ještě bychom měli dotáhnout ta jména postav. Zatím je využíváš jen pro tu morseovku, to je nedostatečné využití potenciálu. Navíc ten výsledek morseovky je nějaký zkomolený. To bych ještě **cenzuroval**.

10 Org A : Ta drobná zkomolenost je důsledek systému. To ale myslím nevadí, je dost zřejmé, že se má vzít křižovatka těch dvou ulic. Jména postav můžeme použít pro výběr slov z jejich replik – třeba přes první písmena. Z těch slov poskládáme heslo, které zkontrolujeme na dalším stanovišti. Kontrola je stejně potřeba, protože ta jednotlivá místa bude potřeba zkombinovat geometricky. To by samo o sobě mělo nevýhodu, že by mohli haluzit.

11 Org B: TO JE DETAIL. Haluzení je **bulvární**, to už dneska žádný pořádný tým nedělá. Každopádně musí zvládnout vyřešit všechno. Dáme jim jak nenápadné hinty, tak jasné věci. TŘEBA OPAKUJÍCÍ SE VĚTY. A co se týče systému určení místa, ten uděláme rekurzivní, ať je to v duchu šifry.

12 Org A: Jasně! Vyjde čtyřúhelník. Pak najdou středy stran. Tím vzniknou čtyři nová místa, na která rekurzivně použijí stejnou proceduru. Po nekonečném počtu kroků ty čtyři body splynou, což určí polohu dalšího stanoviště. To bychom mohli použít jako slogan: Kdo chce projít TMOU, musí zvládat nekonečně mnoho kroků v konečném čase.