TMOU 5

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

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

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

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“.

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

> Úč N: Vyvarovat se překombinovaných konstrukcí, to je základ. A použít vždy vhodný nástroj. Jestli to dokážeme, tak určitě dokončíme. Jak vypadá další šifra?
>
> 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?
>
> Úč N : Já bych byl pro. Ale co s tou šifrou? Vypadá fakt složitě. To je drsný.
>
> 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 ...
>
> 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?
>
> 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:
>
> > 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.
> >
> > Org O: Vyvarovat se překombinovaných konstrukcí, to je základ. K sebereferenčním šifrám jsem nedůvěřivý. Když už, tak to musí být pořádně ořezané, aby tam zůstaly pouze důležité prvky. A vůbec, kdo je to meta-org?
>
> 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.
>
> > 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.
> >
> > Org R: Můžeme to povolení získat? Zkus tomu meta-orgovi zavolat.
> >
> > > 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.
> > >
> > > Meta-org U: Orgu, co zase potřebuješ?
> > >
> > > 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.
> > >
> > > Meta-org U: Chceš říct, že bych se v té šifře vyskytoval i já? To je drsný. Fakt drsný.
> > >
> > > Org S : Aspoň to ukáže, jak reálně fungují šifrovací hry.
> > >
> > > Meta-org U: Zní to dost šíleně. V tomto případě ovšem potřebujeme povolení od meta-meta-orga. Moment, zavolám mu.
> > >
> > > Meta-meta-org V: Meta-orgu, co potřebuješ? Zase nějaké problémy s tou pochybnou večerní hrou?
> > >
> > > 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.*
> > >
> > > Meta-meta-org V: Děkuji za povolení meta-meta-meta-orgu. Meta-orgu, potvrzuji, že povolení je přiděleno, identifikační kód šifry je `K28K528K28K55`.
> > >
> > > Meta-org U : Děkuji za povolení meta-meta-orgu. Orgu, potvrzuji, že povolení je přiděleno, identifikační kód šifry je `K28K5`.
> > >
> > > 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?
> > >
> > > Meta-org U: Vypadá to zajímavě. Akorát bys tam měl ještě přidat umyvadlo. To nesmí chybět v žádné pořádné meta-šifře.

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.

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.

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.

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?

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.

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.

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.

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?

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".

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?

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

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!

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.

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.

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?

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.

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.

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.

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.

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.