Milé týmy,

protože nevíme, jaké šifry máte nebo nemáte rádi, ani jaké šifry vám jdou nebo nejdou, rozhodli jsme se na začátek letošní Tmou provést malý experiment. Pro jeho účely jsme identifikovali pět kategorií šifrovacích principů (vychází z Manuálu Tmou), do kterých obvykle šifry spadávají. Občas nemusí být určení kategorie zcela jasné, ale to pro náš experiment není důležité, protože šifry umíme vytvořit tak, aby to jasné bylo. Před hrou dostáváte na výběr z těchto pěti kategorií šifrovacích principů, zvolíte si z nich jeden a na startu pak obdržíte příslušnou obálku podle vaší volby. Ať už zvolíte jakkoli, bude vaším úkolem po doznění hymny vyluštit informace o tom odkud, jakým směrem a jak daleko se vydat. Typy šifer, včetně příkladů z minulých Tmou, uvádíme níže, všechny ukázkové šifry naleznete v přiloženém pdf. Vybírejte pečlivě!

Vaši organizátoři

Substituční šifry

Substituce = nahrazení. Tyto šifry nahrazují znaky tajenky jinými znaky. Nejběžněji se můžete setkat s těmito formami substitucí:

- Nahrazení písmen čísly. Nejčastěji se používá standardní anglická abeceda, znaky A-Z jsou očíslovány od 1 do 26. Ukázková šifra: **Tmou 18, šifra č. 8 „Rozhledna“**
- Použití známéno kódování. Běžně se můžete setkat s morseovou nebo vlajkovou abecedou, braillovým písmem, doporučujeme nahlédnout do pomůcek od Chlýftýmu, kde jsou snad všechna, co kdy můžete potřebovat. Ukázková šifra: **Tmou 17, šifra č. 9 „Morse“**
- Definování vlastního kódování. Šifra samotná může nějakým způsobem definovat zástupné znaky pro písmena abecedy. Způsobů je požehnaně, typickým jevem je existence nějakých šestadvaceti prvků. Ukázková šifra: **Tmou 16, šifra č. 2 „Divná povídka“**

Transpoziční šifry

Transpozice = přeskládání. V transpozičních šifrách nejsou písmena tajenky ukrytá, ale jsou nějak zpřeházená a cílem hráčů je odhalit, podle jakého klíče.

- Jednoduchou variantou transpozice je situace, kdy je možné prvky seřadit podle nějakého klíče, např. hory podle výšky nebo osobnosti podle data narození. Jednoduché vzestupné nebo sestupné řazení pak odkryje tajenku. Ukázková šifra: **Tmou 12, šifra č. 5 „Vrcholová“**
- Pokud nejsme schopní nalézt jasné řadící kritérium, můžeme zkusit řadit lokálně, tj. každá část tajenky zároveň ukazuje, kterou část máme číst v dalším kroku a postupně se tak odkryje celé řešení. Ukázková šifra: **Tmou X, šifra č. 7 „Bludiště s písmeny“**
- Samostatnou kapitolou transpozičních šifer jsou šifrovací mřížky. Typicky jsou v nějakém symetrickém obrazci (např. čtverci) určena místa, která po otočení padnou na část tajenky, která se čte se po řádcích. Ukázková šifra: **Tmou 18, šifra č. 1a „Aktivizační křížovka“**

Grafické šifry

Grafické šifry nějakým způsobem něco zakreslují. Tato kresba pak může napsat písmena nebo vytvořit obrázek, který je třeba interpretovat.

- Vybarvování rastru. Části šifry – pixely – je třeba vybarvit podle nějakého klíče. Po obarvení lze přečíst řešení podobně jako na digitální fotce. Časté je užití rastrového písma, kde každý znak odpovídá mřížce 3×5. Ukázková šifra: **Tmou 7, šifra č. 6**
- Tahy tužkou po papíře. Na rozdíl od vybarvování rastru připomíná spíše vektorovou grafiku. Často se tahem tužkou spojují části šifry (čára přes celý papír) nebo zaznamenává trajektorie pohybu. Opět může kreslit buď písmena nebo obrázek. Ukázková šifra: **Tmou 17 šifra č. 3 „Postavičky“**
- Přečtu a vidím. Některé grafické šifry ukazují řešení celkem přímočaře, stačí se správně podívat, vyfiltrovat nepotřebný balast případně provést nějakou grafickou operaci a můžeme číst tajenku. Ukázková šifra: **Tmou 13, šifra č. 8 „Plechovky“**

Steganografické šifry
Problémem ve steganografických šifrách nebývá ani tak šifru vyluštit, jako spíš ji odhalit. Často je třeba všimnout si zdánlivě nepodstatných detailů, které indikují přítomnost šifry.

- Přehlédli jsme to. Princip šifry je založen na nepodstatných detailech. Nepatrné změny velikosti, fontu, překlepy nebo drobné díry v papíru. Je třeba šifru důkladně prozkoumat a všímat si i zdánlivě nedůležitých drobností. Ukázková šifra: **Tmou X, šifra č. 4 „Alternativní hymna“**
- Nenašli jsme to. Tým má šifru, ale neví, že ji má a tak nemá co luštit. Pokud se do takové situace dostanete, zkuste se znovu podívat do startovní obálky a zamyslet se, jestli vám organizátoři nedali něco, co by vám mohlo pomoci. Divnou mapu, zvláštní předmět, netypickou formulaci v předstartovních informacích, cokoli. Ukázková šifra: **Tmou X, šifra č. 8**
- Nebylo to tam. Nejlepe ukryté šifry jsou takové, které objevit nejdou – protože vůbec neexistují. Informace totiž není skrytá v tom, co tým má ale tím, co nemá, co mu chybí. Hráči si tak nejdříve musí domyslet chybějící části a teprve poté se může pokoušet luštit dál. Ukázková šifra: **Tmou 13, šifra č. 9 „Slohovka“**

Šifry založené na znalostech
Jisté šifry vyžadují od hráčů určité znalosti. Použití různých typů znalostí závisí na charakteru hry a na uvážení organizátorů. Na terénních šifrovačkách se můžete setkat s těmito druhy:

- U *základních znalostí* se dá očekávat, že je bude mít každý nebo skoro každý člen týmu, úroveň zhruba žáka základní školy Patří sem dny v týdnu, měsíce v roce, autor Pána Prstenů, vzorec pro obsah kruhu, první československý prezident, správná identifikace světadílů, pravidla pro pexeso nebo pohyb šachových figur. Ukázková šifra: **Tmou 15, šifra č. 4 „Změť čar“**
- Dá se očekávat, že *obecnou znalost* bude mít alespoň jeden člen týmu. Zpravidla nejde o nic příliš odborného, spíše o neobvyklejší okruhy, které sice lze celkem bez problémů ignorovat, současně jsou ale poměrně rozšířené. Jde například o pravé jméno Batmana, autora Ferdy Mravence, délku jedné SMS zprávy, rok dobytí Konstantinopole nebo hlavní město Albánie. Ukázková šifra: **Tmou 16, šifra č. 1d „Výstava“**
- *Dohledatelné znalosti* jsou znalosti, o kterých člověk dokáže shledat, že je nemá a umí si je v takovém případě dohledat. V éře mobilního internetu skutečně není nutné pamatovat si všechna jména maršála Radeckého, seznam osmitisícovek, kalendář svátků, text listiny práv a svobod nebo periodickou soustavu prvků. **Ukázková šifra: Tmou 13, šifra č. 6 „Slova a tabulka“**

Toto dělení je individuální, co je pro jednoho triviální fakt může být pro jiného překvapivým zjištěním. Většina znalostí tak bude „někde mezi“. Nenechte se tím však odradit, znalostem, které člověk nemá a o nichž se z šifry nedozví, že je potřebuje, se organizátoři zpravidla vyhýbají.