Šifrování v oddíle

2017

František Fladung (Frfla)

TK Draci Roztoky

Úvod

V této práci se chci zabývat tím, jak vytvářet šifry pro děti a jak je učit je luštit. Toto téma jsem si zvolil, protože šifrování je mi velmi blízké. Myslím si, že šifrování je v oddíle důležité a zároveň bývá opomíjeno vedoucími a ne příliš oblíbené mezi dětmi.

Práce je psaná jako úvaha, neuvádím v ní fakta, která bych měl podložená odborným výzkumem, ale vlastní dojmy a zkušenosti z našeho oddílu. Práci tedy neberte doslova, ale jako podnět k zamyšlení a jiný na vašem oddíle nezávislý názor.

Co myslím šifrou?

Pro jistotu, abych předešel zmatení. Šifrou myslím, hru, matematickou, logickou, grafickou nebo jinou hříčku. Nějaký způsob jak před dětmi něco ukrýt tak, aby to našly, budou-li se snažit. Může to schovávat slovo, věta, ale i předmět, místo nebo osoba.

Pod pojmem šifra si určitě nepředstavujte nějaký složitý matematický algoritmus, na který potřebujete vysokou školu. Šifry o kterých mluvím já jsou jednoduché a pokud možno nezávislé na nějakých znalostech. K řešení musí být možné dojít jenom za pomoci logiky a indícií.

Význam šifer

Význam šifer vidím především v rozvoji myšlení dětí. Mají možnost si při nich nacvičit několik různých postupů řešení problému. Některé šifry se mohou zaměřovat přímo na konkrétní oblast, ale většina šifer vyžaduje zapojení více technik.

Analytické myšlení

Analytické myšlení je při řešení šifer velmi důležité, skoro by se dalo říci nejdůležitější. Abyste se dostali k řešení jakékoliv šifry potřebujete vymyslet možný způsob řešení a vyzkoušet ho.

Takové přímočaré řešení ale není příliš efektivní. Čím je šifra složitější, tím déle trvá vyzkoušet postup řešení a především velmi rychle roste počet řešení, které luštitel musí zkusit. Správné zhodnocení zadání může velmi omezit množství postupů, které vůbec vyzkoušíte.

Když jsem takhle obecně popsal co myslím analytickým myšlením, určitě jste si všimli že to vlastně vůbec nesouvisí s šiframi, vždyť to je přece potřeba pro řešení problémů i ("problémů"), kterých řešíme každý den stovky. Většinu jich vyřešíme jednoduše, a se složitými se setkáváme jenom výjimečně. Proto si myslím že řešení umělých problémů jako jsou šifry a na jejichž vyřešení vlastně moc nezáleží, si děti toto analytické myšlení trénují.

Kreativita

Může se zdát, a podle mých osobní zkušeností si to hodně lidí myslí, že kreativní činnosti jsou kreslení, zpívání, hraní na hudební nastroj, atd. a že matematika, logika, šifrování jsou nějaká svoje speciální kategorie, která s kreativitou vůbec nesouvisí. Podle mě to vůbec není pravda a myslím si, že dítě, které kreslí na výtvarné výchově stejný domeček jako všechny ostatní není o nic víc kreativní než to, které zrovna v matematice počítá násobilku. Dokonce bych tvrdil, že dítě, které luští hádanku je kreativnější než to, které se učí hrát na flétnu. Podle mě kreativita znamená kolik a jak moc originálních řešení jste schopni vymyslet a je jedno, jestli malujete a nebo počítáte.

Především kreativita se dá trénovat a právě na to jsou šifry skvělé, a to nejen luštění. Takže si můžete procvičit svůj mozek při vymýšlení nejoriginálnější šifry pro děti.

Týmová spolupráce

Další důležitou oblastí, kterou šifry rozvíjejí je spolupráce v týmu. Ta se samozřejmě v oddílu učí při téměř všech aktivitách a šifrování není žádnou výjimkou. Oproti většině ostatních činností se nejvíc zaměřuje na jeden konkrétní aspekt spolupráce, a tím je brainstorming. Tento pojem tu neuvádím proto že je zrovna v módě, ale proto že je to slovo opravdu výstižné. Brainstormingem se myslí sdílení všech nápadů které dostanete hned jak je dostanete. Nepřemýšlíte tedy sami nad tím, jestli je to skvělý nápad, nebo nesmysl sami, ale rozdělíte práci mezi všechny ostatní. Tato metoda má spoustu výhod. Nemusíte nic vymýšlet dvakrát, jednou se něco řekne a už o tom všichni vědí. Hodnocení kvality návrhu se rozloží mezi více lidí a tím se jak urychlí tak i zpřesní. K takovému způsobu týmového přemýšlení se děti mohou dostat poprvé právě u šifer a může jim to přinést velkou výhodu, až budou potřebovat řešit nějaký skutečný problém.

Jak vytvářet šifry pro děti

Píši jak vytvářet šifry pro děti, ale vlastně vůbec nezáleží na tom, pro koho šifru vymýšlíte. Pokud vymýšlíte šifru pro pobavení, dodržováním těchto doporučení nic nezkazíte. Znovu zde ale upozorňuji, že nevycházím z žádných skutečných dat, ale jenom z vlastní zkušenosti takže mě berte trochu s rezervou.

Motivace

Motivace hodně souvisí s jakoukoliv prací v oddíle. Pokud chcete, aby si děti jakoukoliv hru užili musíte je přimět k tomu, aby si jí chtěli užít. K tomu se vyžívá nepřeberného množství triků. I když se to nemusí zdát, velké množství z nich jde aplikovat i na šifry.

Hojně používanou motivací (alespoň v našem oddíle) je příběh. Libovolný, krátký nesmysl (musí ale upoutat), kterým svou šifru opředete jí dodá úplně jiný rozměr. Například před schůzkou v zimě řeknete, že nějaký zámečnický naschválníček schoval klíče od klubovny a zanechal zprávu kam, ta se ale zdá býti poněkud nečitelnou, protože zámečníkovi byla zima a klepal se tak, že to po něm nejde přečíst.

Skvělým nástrojem pro zvýšení zájmu je autentičnost. Pokud všichni přítomní vedoucí budou přesvědčiví, že ho viděli a jeden dokonce ukáže roztrženou kalhotu, když se se skřítkem popral, příběhu to hodně přidá. Důležitý tu je smysl pro detail, když šifra bude vytištěná na počítači, moc to nepomůže. To je ale snad hodně obecně známý fakt mezi vedoucími.

Jak nastavit obtížnost

Toto téma je asi nejnáročnější co se týče šifer pro děti. Často jsou pak šifry velmi jednoduché a děti se pak u jejich luštění moc nezapotí. Podle mého názoru není naškodu udělat šifru trochu těžší, pokud toho dosáhnete správným způsobem.

Je několik způsobů, jakými můžeme udělat šifru těžkou. Nejjednodušším způsobem je zkombinovat několik šifer, či šifřiček dohromady. Například mohu napsat text do morseovky a pak ještě písmena posunout v abecedě. Tohle je asi nejhorší možný způsob zvyšování obtížnosti šifer, protože si když si luštitel všimne toho, že se jedná o morseovku a začne rozklíčovávat, brzy mu začnou vycházet nesmysly a to ho většinou přesvědčí, že se nejedná o morseovku a už to znovu nezkusí. Takové šifry vedou k frustraci dětí, že už vyzkoušely všechno a ony pořád vycházejí nesmysly. To je asi nejhorší pocit, který může šifra v dětech vyvolat.

Dalším už zajímavějším způsobem je změna formy šifry. Morseovka se skádá z čárek a teček. Ty se dají najít téměř všude, obrázek, na kterém jsou různě dlouhá stébla trávy, provázek s různými uzlíky, střídání dvou barev, levé a pravé stopy v hlíně, atd. Morseovka samozřejmě není jediná šifra, jakákoliv z šifer které v oddíle běžně používáte půjde předělat do nějaké alternativní formy.

K těm nejlepším ale i nejnáročnejším způsobům patří úplně originální šifrovací postup. Tady můžete popustit uzdu své fantazii, protože šifrou může být naprosto cokoliv. Matematická úloha, hraní písničky, chození po louce, mapování, poslouchání rozhovoru, modelování z papíru. Tady nemohu dát dostatek příkladů, protože každá šifra může být úplně nová. Takové šifry nejlépe rozvíjí kreativní myšlení a přináší největší potěšení z vyluštění.

Poslední změnou, kterou dokážu vymyslet jsou hádanky. Částečně se kryjí se změnou šifrovacího postupu, ale ne úplně. Hádanka je výrok, věta, nebo i celý odstavec textu, který na první pohled dává smysl, ale skrývá se v něm něco jiného. Ne že by stačilo přečíst každé třetí písmeno. Hádanku je třeba pochopit. Vymýšlení hádanek je těžké, hádanky nejsou šifry v pravém slova smyslu, není možné je vyřešit jen za pomoci indícií, které dostanete během hry, něco už musíte znát. Hádanky se dají kombinovat i s jinými šifrovacími postupy, protože poznáte, že jste první krok udělali správně.

Šifrování pro začátečníky

Na závěr bych chtěl uvést jednoduchou teorii k šifrování, která by mohla sloužit pro inspiraci k vytváření šifer a jeden z možných postupů, jak mohou děti postupovat při luštění. Uvedu zde základní typy šifer které se používají u nás v oddíle (a předpokládám i ve spoustě jiných). Rozdělení do třech kategorií je moje pomůcka, když řeším šifry, nebo když vymýšlím více šifer a chci, aby byly co nejméně podobné. Profesionální kryptografové určitě rozlišují mnohem více druhů šifer, já jsem kryptograf-amatér a toto rozdělení jsem si zavedl sám pro sebe.

Substituční šifry

Pod tímto mysteriózním slovem se skrývá obrovské množství šifer, nejspíš většina šifer, které jste kdy použili. Princip substitučních šifer je, jak název napovídá, v nahrazení znaku nebo skupiny znaků v šifrovaném jiným znakem nebo skupinou znaků. Můžete si vymyslet vlastní znakovou řeč, nebo použít nějakou z už zaběhlých šifer. Mezi zaběhlé šifry patří morseovka, brailovo písmo, Cézarova šifra (posunutí všech písmen v abecedě o stejný počet), Vernamova šifra (posunutí písmen v abecedě podle klíče), polský kříž, telefon, atd. Patří sem také každe *n*-té písmeno, první písmeno v řádku, apod.

Substituční šifry poznáte podle toho, že zadání budou nějaké znaky, ať už písmena nebo obrázky, u nichž půjde určit jejich počet a počet druhů. Pokud tušíte, jak by mohlo vypadat řešení (slovo, věta, souřadnice, příběh) využijte toho k rozlišení, zda se jedná o substituci jednoho znaku za jiný, nebo jednoho znaku za více znaků. Pokud je šifra dlouhá, hledejte znaky, které se často opakují, mohou to být samohlásky.

Transpoziční šifry

Transpozičních šifer se používá méně často než substitučních, občas jsou se substitučními šiframi kombinovány. Jde o změnu pozice částí zprávy, tedy o přesmyčky. Můžou se přemisťovat písmena, slova i věty. Transpoziční šifry mohou být luštitelné pomocí klíče (např. nějké známé slovo/věta jsou přeházené stejným způsobem jako zašifrovaná zpráva) nebo bez klíče (slova/věty lze seřadit podle abecedy, počtu písmen, barvy, počtu čárek v morseovce, atd.).

Na čistě transpoziční šifru často nenarazíte, nejspíš bude součástí nějaké jiné šifry, ale pokud ano, poznáte ji podle toho, že počet znaků bude odpovídat počtu znaků očekávané odpovědi a hlavně bude normálné frekvence různých písmen.

Grafické šifry

Do grafických šifer můžete s trochou snahy zařadit téměř jakoukoliv šifru, já sem řadí všechný šifry, které se nehodí do předešlých dvou kategorii a nejsou zároveň super exotické nebo jenom hádanky.

Když dostanete šifru, která na první pohled jako grafická, nejdříve se ujistěte, že nejde o nějakou změněou forum substituční šifry. Teprve potom se snažte najít grafické řešení. Zkuste si spočítat vše co můžete, dokreslit co by mohlo jít dokreslit, zakrýt některé části, podívat se na šifru zdálky, vzhůru nohama, přes zrcátko. Přemýšlejte, jestli nemáte k dispozici jiné nástroje: pravítko, buzolu, lupu, nerezovou lžíci. U grafických šifer vám nezbývá nic jiného než zapojit tu představivost.