Studentský matematicko-fyzikální časopis

Ročník XX / Číslo 4

Časopis M&M a stejnojmenný korespondenční seminář je určen pro studenty středních škol, kteří se zajímají o matematiku, fyziku či informatiku. Během školního roku dostávají řešitelé zdarma čísla se zadáním úloh a témat k přemýšlení. Svá řešení odesílají k nám do redakce. My jejich příspěvky opravíme, obodujeme a pošleme zpět. Nejzajímavější řešení otiskujeme.

Milý řešiteli,
blíží se pololetí a společně s ním se i náš korespondenční seminář dostává do druhé poloviny. Opět ti přinášíme nové úlohy i několik příspěvků k tématům. Stále můžeš ale přispívat i k tématům uveřejněným v některém z předchozích čísel. Rádi bychom připomněli, že autor nejpovedenějšího příspěvku k tématu od nás dostane na konci školního roku dort.

Přibližně 20 nejúspěšnějších řešitelů pozveme jako obvykle na jaře na soustředění (konkrétně se bude konat 29. 3.–6. 4.). Při pohledu do výsledkové listiny zjistíš, že na 20. pozici v semináři zatím není potřeba až tak moc bodů, na soustředění se tedy může dostat skutečně každý. Nenech se o tuto možnost připravit!

Ještě před soustředěním bychom tě ale rádi pozvali i na další akce, které Matfyz v Praze pořádá. Ve čtvrtek 6. února se koná Jeden den s fyzikou (den plný přednášek a exkurzí pro veřejnost), 14. února je pak tradiční fyzikální týmová soutěž Fykosí Fyziklání. Více informací najdeš v přiložených letáčcích.

Pokud bys chtěl strávit zábavou s matematikou a fyzikou i část letních prázdnin, můžeme ti doporučit Letní školu matematiky a fyziky, která probíhá podobně jako naše soustředění a o jejímž termínu tě budeme ještě informovat. Jestli upřednostňuješ více odborného programu, jsou tu pro tebe odborné tábory, jejichž nabídku přikládáme už nyní.

Přejeme ti hodně úspěchů nejen při potýkání se s problémy našeho semináře.

organizátoři M&M

Zadání úloh

Termín odeslání třetí série: 3. 3. 2014

Zde úhlopříčky
rovné a nespoutané
obsáhnou nebe.

Úloha 4.1 – Mnohoúhelník (3b)

Sestrojte pravidelný mnohoúhelník, když znáte délku nejdelší a druhé nejdelší úhlopříčky. Aby to nebylo moc jednoduché, tak ale neznáte počet stran mnohoúhelníku.

Jarní nálada
zahalí přetlakovou
komůrku ticha.

Úloha 4.2 – Poissonova (3b)

Uvažujme uzavřenou nádobu se vzduchem. Nádobu přetlakujeme na tlak p_1 při pokojové teplotě. Poté na krátký čas otočíme ventilem, než se vyrovná tlak v nádobě s okolím. Jaký tlak bude v nádobě po vyrovnání teplot plynu s okolím?

Uvažujte tlaky blízké atmosferickému tlaku. Mohla by se hodit aproximace $(1+x)^n \approx 1+xn$ pro $x \ll 1$.

Vlahá je rosa
cestou pak po zelené
kácíme stromy.

Úloha 4.3 – Barvení grafu (4b)

Máme acyklický orientovaný graf[1] s nejdelší orientovanou cestou délky[2] maximálně k. Ukažte, že lze vrcholy grafu obarvit nejvýše k barvami tak, aby žádná hrana nespojovala dva vrcholy se stejnou barvou.

Mlhavý opar
kulatou sklenkou napůl
rozléván ránem.

Úloha 4.4 – Kruhy (2b)

Ukažte, že kruh s průměrem 2 lze pokrýt sedmi kruhy s průměrem 1.

Řešení úloh

Úloha 2.1 – Kříž (3b)

Zadání:
Papír ve tvaru čtverce tužkou rozdělíme na 9 menších stejně velkých čtverců. Po odstřihnutí 4 rohových čtverců dostaneme kříž. Jak ho lze rozdělit dvěma řezy tak, aby ze vzniklých částí bylo možné opět poskládat čtverec?

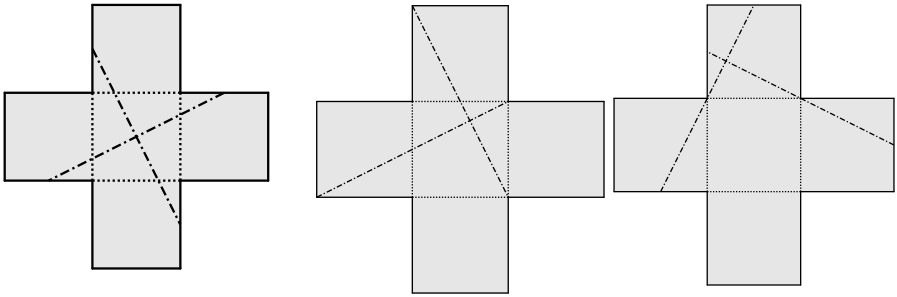
Řešení:
Protože máme čtverec rozdělit na 9 stejných čtverců, jediné řešení je rozdělit

[1] *Graf* si můžete představit jako nějaké body, například města, (těm se říká *vrcholy*) pospojované cestami (těm se říká *hrany*), pokud se cesty kříží tak vždy mimoúrovňově (tj. přejet na jinou cestu se dá jen ve městě). *Orientovaný* znamená, že všechny cesty jsou jednosměrky. *Acyklický* znamená, že když vyrazíte z libovolného města, tak už do něj nikdy nemůžete dojet zpět.

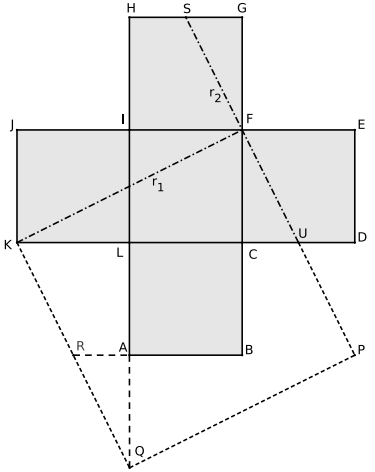
[2] Cesta délky k je cesta, během které navštívím k měst, včetně počátečního a koncového.

každou stranu na třetiny. Zvolme, že délka strany původního čtverce je 3. Potom má vzniklý kříž délky stran 1 a obsah 5. Pokud ho chceme jakkoli rozdělit a vytvořit čtverec, musí mít čtverec také obsah 5 a tedy délku strany $\sqrt{5}$.

Musíme tedy v kříži najít dva řezy délky $\sqrt{5}$, protože $\sqrt{5}$ nelze vyjádřit jako součet přirozených čísel (déka strany kříže) a nějakých jiných druhých odmocnin (jiné řezy). Způsobů, jak tento řez umístit je několik, příklady vidíte na obrázcích. Druhý řez musí být na první kolmý, protože řezy budou tvořit obvod čtverce a strany čtverce jsou na sebe kolmé. Opět máme několik způsobů, jak tento řez umístit. Poté už stačí ukázat, že do sebe díly zapadnou, což je většinou vidět přes jednoduché shodnosti.



Jedno z možných řešení detailněji: Kříž $ABCDEFGHIJKL$, řezy r_1, r_2. Řezy $|KF| = |SU| = \sqrt{2^2 + 1^2} = \sqrt{5}$. U je střed CD, protože r_2 půlí obdélník $BPEF$. Pokud tento obdélník posuneme po r_2 tak, že $P' = F$, tak získáme, že S je středem GH. Proto pokud posuneme $KFSHIJ$ tak, že $K'F' = QP$, tak na sebe budou části navazovat.



SGF je shodné s RAQ, protože $|AQ| = |GF|$, oba jsou pravoúhlé a KQ je

rovnoběžná s PS, tedy mají shodné všechny úhly a stranu. Obdobně $UDEF$ je shodný s $RALK$, protože má 2 úhly pravé, $|UD| = |SG| = |RA|$ a $1 = |FE| = |ED| = |KL| = |LA|$.

Tímto jsme dokázali, že díly na sebe navazují a tvoří čtverec. *Jethro*

Úloha 2.2 – Knihovna (2b)

Zadání:
Regál obsahuje N knih seřazených podle svého názvu, přičemž žádné dvě knihy se nejmenují stejně. Chtěli bychom je přeuspořádat tak, aby každá byla na pozici právě o K větší nebo menší. Pro jaká K v závislosti na N to můžeme provést?

Řešení:
Knihy si po řadě očíslujeme $1, 2, \ldots, N$. Všimněme si nejdřív, že $K < N$. V opačném případě bychom nemohli žádnou knihu přesunout. Pokud by byla kniha na pozici $1 \leq p \leq N$, pak ji musíme přesunout buď na pozici $p+K \geq p+N \geq N+1$, nebo na pozici $p-K \leq p-N \leq 0$, ale takové pozice v knihovně nejsou.

Teď si všimněme, že knihy na pozicích $1, \ldots, K$ musíme přesunout doprava, nalevo bychom narazili na okraj knihovny. Knihy tedy přesuneme na pozice $K+1, \ldots, 2K$. Naopak na pozice $1, \ldots, K$ můžeme přesunout pouze knihy z pozic $K+1, \ldots, 2K$. A vida, N musí být alespoň $2K$, jinak prvních K knih nepřesuneme.

Tím jsme vyřešili prvních $2K$ knih a už s nimi nemůžeme hýbat. Pokud $N = 2K$, tak jsme vyhráli a knihy jsou správně přeskládané. V opačném případě jsme se ale dostali do situace, kdy máme přesunout knihy v knihovně o $N-2K$ knihách. Pro prvních $2K$ knih (tj. knihy na pozicích $2K+1$ až $4K$) máme opět jednoznačně určeno, jak je přesunout. Postupně tedy musíme přeskládávat bloky o $2K$ knihách, dokud nepřeskládáme celou knihovnu, nebo neskončíme s blokem menším než $2K$, který přeskládat nelze.

Došli jsme tedy k tomu, že knihy lze přeskládat pouze tehdy, když můžeme knihovnu rozdělit na bloky o velikost $2K$, tedy $N = 2Ka$ pro nějaké přirozené číslo a. Číslo K tudíž musí být nějaký dělitel $N/2$ (což má samozřejmě smysl jen, je-li $N/2$ celé). Navíc jsme předtím ukázali, že pokud toto platí, tak knihovnu přeskládat můžeme, tedy opravdu vyhovují všechna taková K. Leč, zapomněli jsme (stejně jako spousta z vás) na jeden triviální případ – $K = 0$. Tehdy knihy můžeme přeskládat vždy – prostě je necháme na původních místech.

Asi nejčastější chybou bylo, že jste usoudili, že knihovna je cyklická. Bohužel nás nenapadlo, že by si někdo mohl zadání takto vykládat, přece jen, poličky v knihovně prostě do kruhu nejsou. Navíc, takové přesunutí knih většinou zadanou podmínku nesplní. Vezměme si třeba $N = 5$, $K = 3$ a knihu na pozici $p = 4$. Podle zadání máme tuto knihu přesunout na pozici $p+K = 7$ nebo $p-K = 1$. Tím, že ji cyklicky přesuneme dozadu, ji ale přesuneme na pozici 2, což zadání nevyhovuje.
$\mathcal{O}(N)$dra

Úloha 2.3 – Sušárna (4b)

Zadání:
Venku je 0° C a prší. V malé nevětrané sušárně vytopené na 25° C se snažíme usušit velké množství mokrého prádla. Po několika dnech je prádlo stále mokré. Pomůže sušení rychlé vyvětrání? Kolik vody zkondenzuje v místnosti nebo kolik vody se odpaří z prádla po jednom rychlém vyvětrání?

Řešení:
Shrňme si napřed, co vlastně víme – to je vždycky dobrý začátek... Máme malou místnost se spoustou mokrého prádla, které nám nechce schnout. Z toho lze vyvodit, že vzduch v místnosti je už vodou zcela nasycen. V místnosti je stoprocentní vlhkost.

Venku prší. Déšť nastává, když už vzduch není schopen udržet vodu, a začne ji uvolňovat. Můžeme tedy říci, že venku je také stoprocentní vlhkost. (Vlastně v sobě vzduch tu vlhkost už nemohl udržet déle, proto se vytvořila ta soustava mikrokapiček, které říkáme mrak.)

Vyvětráním vyměníme vzduch z místnosti za vzduch z venku.

Mluvíme ale o relativní vlhkosti. Ta je definována jako poměr množství vody reálně přítomné v daném objemu vzduchu, ϱ [g/m^3], vůči množství vody, které daný objem vzduchu maximálně pojme při dané teplotě t, ϱ_t [g/m^3]. Pokud chceme zjistit absolutní vlhkost vzduchu venku a vevnitř, musíme v tabulkách dohledat tyto maximální hodnoty pro dané teploty. Moje tabulky maximální množství vody ve vzduchu dané teploty uvádějí jako dva různé parametry: hustotu a tlak nasycené vodní páry.

Hustota nasycené páry je naše ϱ_t. Pokud jste našli tyto údaje, byl výpočet triviální:

Při teplotě 0 °C je hustota nasycených par 4.85 g/m^3, při teplotě 25 °C je to 23.04 g/m^3. Pokud naplníme místnost studeným vzduchem zvenku a zavřeme okno, vzduch se ohřeje opět na teplotu 25 °C. Při teplotě 25 °C se nám do kubíku vzduchu vejde 23.04 g vody, ale máme v něm jenom 4.85 g, takže se ještě dalších 18.19 g vody na každý kubík vzduchu v místnosti může vypařit z prádla.

Pokud jste našli jen tlak nasycených par, bylo potřeba trochu počítat.

Budeme předpokládat, že vodní pára je ideální plyn. Při takto nízkých tlacích to, jak uvidíte, sedí. Stavová rovnice ideálního plynu je

$$pV = nRT\,,$$

kde p je tlak vodních par, V objem, my budeme uvažovat jednotkový objem (1 m^3), n molární množství plynu, $R = 8.31$ J/(K · mol) univerzální plynová konstanta a T absolutní teplota. Molární množství plynu si můžeme vyjádřit jako

$$n = \frac{m}{M}\,,$$

kde m je jeho hmotnost a M molární hmotnost vody. Molární hmotnost vody je 18 g/mol. Dosadíme do stavové rovnice a dostaneme

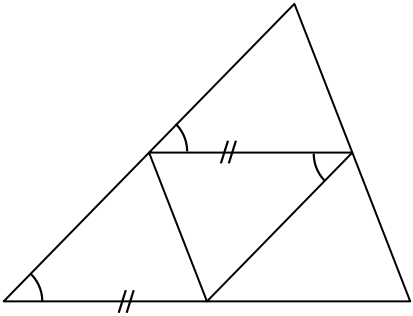
$$p = RT\frac{m}{VM} = \frac{RT\varrho}{M}.$$

Tím jsme získali přepočet tlaku vodních par na jejich hustotu a převedli tak situaci na předchozí případ. Tabulky tvrdí, že tlak nasycených vodních par při teplotě 0 °C je 611 Pa a při teplotě 25 °C 3168 Pa. Pokud tyto hodnoty dosadíme do odvozeného vzorce, dostaneme skutečně dříve zmíněné hustoty nasycených vodních par, a je tak vidět, že aproximace ideálním plynem je v pořádku.

Zuzka

Úloha 2.4 – Čtyřstěn (2b)

Zadání:
Součet úhlů kolem každého vrcholu čtyřstěnu je roven 180 °. *Ukažte, že všechny stěny čtyřstěnu si jsou podobné.*



Řešení:
Rozložme si čtyřstěn na jeho trojúhelníkovou síť tak, jak je vidět na obrázku – vrcholy prostředního trojúhelníka označme A, B, C, zbývající vrcholy krajních trojúhelníků označme postupně D, E, F. Z podmínky ze zadání plyne, že úhly EAF, FBD a DCE mají hodnotu 180 ° – jsou přímé. Trojúhelníky tvořící síť tedy tvoří jeden velký trojúhelník s vrcholy D, E, F. Body A, B, C jsou středy stran velkého trojúhelníka DEF (úsečky AE a AF mají stejnou délku, protože obě odpovídají stejné hraně původního čtyřstěnu, obdobně postupujeme pro další strany). To znamená, že AB, BC a CA jsou střední příčky trojúhelníka DEF. Střední příčka je rovnoběžná se svou odpovídající stranou, takže $AB \parallel ED$, $BC \parallel FE$, $CA \parallel DF$. S využitím souhlasných a střídavých úhlů již snadno ověříme, že jsou všechny čtyři trojúhelníky podobné. Platí $\angle FAB = \angle FEC = \angle AEC = \angle BCD$, $\angle FBA = \angle FDC = \angle BDC = \angle ACE$, takže trojúhelníky ABF, BCD a CAE si jsou navzájem podobné podle věty *uu*. Navíc $\angle CAB = \angle ABF$ a $\angle CBA = \angle BAF$ (střídavé úhly), takže i prostřední trojúhelník ABC je podobný ostatním. Ve skutečnosti jsou strany čtyřstěnu dokonce shodné, neboť mají stejné délky.

Pepa

Řešení témat

Téma 3 – FlatFox

Od Mgr.MM Dominika Krasuly jsme dostali několik krátkých příspěvků řešících některé běžnější matematické problémy a úkony s důrazem na efektivitu. Mezi nimi odmocňování, rozkládání na čtverce, některé kombinatorické funkce (binomický koeficient a Catalanova čísla), největší společný dělitel a pak několik operací, které berou číslo v registru jako řetězec cifer[3], konkrétně ciferný součet v dané soustavě a pak převod mezi soustavami (opět vnímáme-li číslo jako řetězec). Všechny programy jsou pro původní FlatFox.

Stále je velmi otevřené téma novinek v FF++, ať už síla a rychlost ve srovnání s FF, teoretické koncepty volání podporgramů a jejich struktura, nebo konkrétní programy řešící zajímavé úlohy.

Tomáš

Hrátky se čtverci (8b)

Mgr.MM Dominik Krasula

Pozn. red.: Uvádíme jen jeden ze série článků Mgr.MM Krasuly. Programy a několik dalších textů najdete na stránce tématu.

Jak vytvořit čtverec[4]

Můžeme číslo prostě umocnit na druhou. Jedná se o základní funkci FlatFoxu (hodnotu zkopírujeme a poté kopii a původní číslo vynásobíme). Není to však jediná možnost:

Tvrzení. Pro každé $n \in \mathbb{N}$ platí $n^2 = \sum_{k=0}^{n-1} 2k + 1$

Důkaz. Dokážeme to indukcí, pro $n = 1$ to platí triviálně. Předpokládáme tedy, že pro n vzorec platí. Ukážeme, že musí platit i pro $n+1$: $(n+1)^2 = n^2 + 2n + 1 \rightarrow (n+1)^2 - n^2 = 2n + 1$. □

Odmocnění

S využitím vztahu výše můžeme přesně odmocnit čtverec. V případě odmocňování nečtverce získáme horní celou část odmocniny.

1. Máme nějaký odečetní registr, v něm je na začátku jednička.
2. Tento registr vždy odečteme od hodnoty odmocňovaného čísla
3. Přičteme jedna k registru pro výsledek.
4. Zkontrolujeme, zda-li je v odmocňovaném registru ještě kladná hodnota, pokud ano, přičteme k odečetnímu registru 2 a vracíme se ke kroku 2.
5. Pokud se odmocňovaný registr již vynuloval, program končí.

[3] I když jsou čísla zobrazena desítkově, interpretr je vidí jen jako hodnoty bez konkrétní soustavy.

[4] Čtverec je označení pro druhou mocninu přirozeného čísla.

Prvočísla a čtverce

Tvrzení. Pro $k \in \mathbb{N}$:

1. Každé prvočíslo, které lze zapsat ve tvaru $4k+1$, lze zapsat jsko součet dvou čtverců.
2. Každé liché prvočíslo, které nelze zapsat ve tvaru $4k+1$, nelze zapsat jako součet dvou čtverců.

Dokážeme si pouze část 2, důkaz části 1 je velmi dlouhý a je v něm použitá složitá matematika.

Lemma. Každý čtverec lze zapsat ve tvaru $4k$, jedná-li se o sudý čtverec. Pokud je lichý, lze ho zapsat pouze ve tvaru $4k+1$.

Důkaz lemmatu. Jakékoliv číslo můžeme zapsat jako $4k+l$, kde l je jedno z čísel $0, 1, 2, 3$. Když takové číslo mocníme, získáme: $(4k+0)^2 \equiv 0 \pmod 4$, $(4k+1)^2 \equiv 1 \pmod 4$, $(4k+2)^2 \equiv 4 \pmod 4 \equiv 0 \pmod 4$ nebo $(4k+3)^2 \equiv 9 \pmod 4 \equiv 1 \pmod 4$. □

Důkaz tvrzení. Prvočíslo lze zapsat buď ve tvaru $4k+1$ nebo $4k+3$, jinak by se jednalo o sudé číslo. Hodnotu $4k+3$ součtem dvou čtverců získat dle lemmatu nemůžeme, jedná se o liché číslo, musí tedy být součtem lichého a sudého čísla, tedy $4k+(4l+1) = 4(k+l)+1$. Z lemmatu dále vyplývá, že prvočíslo ve tvaru $4k+1$ bude součtem lichého a sudého čtverce. □

Program

Následující program zjistí, zda-li je číslo ve tvaru $4k+1$ a pokud ano, rozdělí jej na dva čtverce. Jestli se jedná o prvočíslo můžeme ověřit tak, že přidáme na začátek program Prime, nicméně primární účel programu je rozdělit prvočíslo na čtverce, takže bude předpokládat, že mu jako vstup budeme dávat prvočísla.

Princip programu je jednoduchý, bude od původního čísla odečítat liché čtverce a výsledek vždy zkusí odmocnit, pokud odmocnění nevyjde, tak použitý lichý čtverec nebyl správný. Kdybychom číslo neustále obnovovali, byla by časová složitost programu vysoká. Proto by bylo dobré odečítat rozdíl mezi lichým čtvercem, který jsme již odečetli, a následujícím lichým čtvercem, nemuseli bychom pak číslo obnovovat.

Rozdíl mezi lichými čtverci je

$$(2n+3)^2 - (2n+1)^2 = (4n^2 - 4n^2) + (12n - 4n) + (9-1) = 8n + 8,$$

můžeme tedy vyvodit vztah $(2n+1)^2 = 1 + \sum_{k=0}^{n} 8k$.

Z toho lze napsat program pro odmocnění lichého čísla. Odmocňované číslo je v registru R, používáme pomocný registr B, do registru G ukládáme výsledek.

1. Odečteme 1 od R.
2. $B := B + 8; R := R - B; G := G + 8$

3. Zkouška, zda-li je R čtvercem.
   Pokud ano, program končí, našli jsme výsledek.
   Pokud ne, vrať se k 2.

Zjednodušit můžeme i odmocňování sudých čtverců:

$$(2n+2)^2 - (2n)^2 = (4n^2 - 4n^2) + (8n) + (4) = 8n + 4,$$

vztah pak bude $(2n)^2 = \sum_{k=0}^{n}(8k+4)$ a program obdobný jako výše.

Celkový program tedy bude vypadat následovně:
Odečte 1 od vstupu (nejnižší lichý čtverec), zkusí odmocnit.
Odečte 8 od vstupu (už odečetl 9, druhý nejnižší lichý čtverec), zkusí odmocnit.
Odečte 16 od vstupu (už odečetl 25, třetí nejnižší lichý čtverec), zkusí odmocnit.
...

Téma 4 – Do hlubin

K tématu přišly pouze dva příspěvky, které přinášejí mnohem více otázek než odpovědí. Objevuje se několik zajímavých myšlenek, bohužel všechny končí jejich pouhým konstatováním. Doufáme, že se někdo další chopí příležitosti a některý z aspektů mise vyřeší podrobněji. Články otiskujeme jen s dotazy a poznámkami redakce.

Projekt Lindenbaum (2b)

Bc.^{MM} Aneta K. Lesná

Představuji vám projekt „Lindenbaum“, projekt české ponorky navržené primárně pro účel průzkumu Marianského příkopu.

Ponorka „Linde“ vypadá i z dálky na první pohled jako ponorka. To znamená, že má tvar, který si lidé obvykle asociují s ponorkami. Vztlak zajišťuje benzín. (Jako vztlaková kapalina je použit benzín zejména pro svou nízkou hustotu a téměř nulovou stlačitelnost.) (Místo benzínu by mohla být použita pěna typu Isofloat, ta byla ale po konsultaci s odborníkem zavrhnuta.) Délka je přibližně dvacet metrů.

Posádku tvoří tři lidé. V souvislosti s tím je třeba zajistit základní potřeby, ponorka tedy má jednoduchý záchod a prostory pro skladování menšího množství jídla a vody. Tlaková sfera, ve které bude umístěna posádka, poskytuje plně funkční systém podpory života. Přítomen je CCR (closed-circuit rebreather) systém podobný tomu v moderních vesmírných lodích a skafandrech. Stěny sfery jsou více než patnáct centimetrů silné, tlak by proto měly vydržet. Posádka má možnost pozorovat své okolí díky malému okénku z akrylického skla. (Akrylické sklo je jediná dostupná průhledná látka schopná přestát extremní tlak.) Vnější osvětlení zajišťují křemenné obloukové lampy, které prokazatelně vydrží tlak více než tisíc atmosfér.

V případě nedostatku jiných možností může být komunikace realizována pomocí zařízení na bazi sonaru či hydrofonu. Sběr vzorků bude realizován pomocí robotických paží s napojením nezbytných zařízení. Díky důmyslné konstrukci jim práce pod velikým tlakem nedělá problém. Ponorka má dostatek úložného prostoru. Energii dodávají baterie. Velké elektromagnety udržují na místě zátěž v podobě deseti tun magnetických železných částí. V případě selhání baterií se tedy ponorka automaticky vynoří na povrch.

Předpokládaná délka jedné mise je asi deset hodin. Průběh mise řídí kapitán, který se řídí instrukcemi, které mu zadala pověřená osoba. Posádka bude vybrána na základě předem stanovených kriterií ze skupiny uchazečů soustředěné v Praze. Přesný termín prvního sestupu ponorky zatím nebyl specifikován.

Poznámky redakce:

1. *Zajímalo by nás, jaký přesně tvar si lidé asociují s ponorkami a proč? Je tento tvar skutečně pro ponorku nejvhodnější? Jaké parametry musí splňovat?*
2. *Jak by fungovalo užití vztlakové kapaliny? V jaké části ponorky by byla umístěna? A kolik by jí bylo potřeba? Pokud by tedy bylo použito toto řešení odlehčení ponorky...*
3. *Je 20 m skutečně vhodný rozměr pro naši ponorku? Proveďte odhad, co všechno se do ní musí vejít, kolik prostoru zabere samotná konstrukce, ...*
4. *Pokud bychom přijali tříčlennou posádku, co bude mít kdo na starosti? Budou opravdu všichni přiměřeně vytíženi?*
5. *Jak vypadá záchod v ponorce?*
6. *Kolik jídla a pití bude posádka na misi potřebovat?*
7. *Co všechno zahrnuje podpora života a jak je to zajištěno?*
8. *Je 15 cm síla stěn opravdu adekvátní? Jaký je na dně Mariánského příkopu tlak? Neplýtváme materiálem?*
9. *Jak byste provedli zapojení křemenných obloukových lamp do pláště ponorky? Jak budou chráněny před vlhkem? Jak bude vyřešen přívod energie?*
10. *Jaký komunikační protokol je vhodný při použití sonaru či hydrofonu? Je to vůbec na takovou vzdálenost (dno–hladina) možné?*
11. *Jak má vypadat robotická paže, aby byla schopná sbírat vzorky? Jaká to důmyslná konstrukce jim umožní pracovat v obrovských tlacích?*
12. *Kolik úložného prostoru ponorka potřebuje (a na co)?*
13. *Jaké baterie jsou nejvhodnější pro takovou misi a proč? Kolik jich bude potřeba?*
14. *Jaké parametry musí mít elektromagnety, aby udržely požadovaný objem kovu? Proč zrovna deset tun (autorka neuvádí hmotnost ponorky)? Kolik energie z baterií by tyto elektromagnety spotřebovávaly na udržení onoho závaží?*
15. *Co vše se musí během mise stihnout a jak dlouho to bude trvat? Stačí*

opravdu 10 hodin? Jak dlouho vůbec trvá klesání a stoupání rozumnou rychlostí?

16. *Jaká rychlost je rozumná?*
17. *Podle jakých kritérií je vhodné vybírat posádku?*

Plán mise (3b)

Dominika Tanglová

Pro misi na dno Mariánského příkopu je potřeba ponorka, která bude čelit obrovskému tlaku. Nejvhodnější materiál pro ponorku by byla slitina skla a polymeru – něco jako neprůstřelné sklo. Sklo by bylo uspořádané do dvou vrstev, přičemž vnitřní vrstva by byla vyztužena nejméně 7 vzpěrami uspořádanými do hvězdy. Veškeré zařízení by bylo ukryto ve vnitřní části ponorky, prostor mezi plášti by byl použit k načerpání vody a tím zatížení ponorky a vyrovnání vnitřního tlaku. Ve vnitřní části by bylo zařízení pro přetlak, kdy postupně bude zvyšovat tlak uvnitř ponorky aby nedošlo k implozi. Pro pohon by byly použity elektromotory umístěné opět ve vnitřní části. Turbíny by byly umístěny na vrchní části pláště. Všechny komponenty umístěné vně ponorky by byly vyrobeny z odolné kalené oceli. Turbíny by se používaly pouze až po sestupu a následně by dopomohly k vyzvednutí ponorky. Pro sestup by byla použita koule z betonu, která by se na dně oddělila a ponechala by se na dně. Pro vzestup by byl použit zabudovaný přetlakový ventil s nepropustnou vrstvou. Když by byl vnitřní tlak vyšší než vnější, držel by ventil pevně na svém místě, v případě, že by venku byl tlak větší, ventil by se uvolnil a tlaky by se vyrovnaly.[5] Ponorka by byla plně robotická, ovládaná na dálkové ovládání. Pro zesílení signálu by byly v rozestupech umístěné zesilovače, které by přeposílaly signály. Pro sledování okolí by byly použity kamery umístěné v trupu ponorky, jejich obraz by nebyl kvůli vodě příliš ostrý, avšak pro pozorování dějů a orientaci by to stačilo. Sběr vzorků by zajišťovaly robotické paže, vzorky se budou ukládat do vaků přidělaných na povrchu ponorky. Doba trvání mise záleží na výkonnosti akumulátorů. Při dobré výkonnosti by doba pobytu ponorky na dně mohla být i okolo 2 dnů. Cesta zpátky by měla trvat nejméně den, aby se postupně vyrovnávaly tlaky a nedošlo k poškození ponorky, to stejné platí i pro cestu dolů. Ponorka bude vybavena GPS pro pozdější nalezení a vytažení z vody. Velikost vnitřního pláště by se mohla pohybovat okolo 2–3 metrů v průměru a vnější průměr kolem 2,5–3,5 metru.

Průběh mise:

1. Spuštění zesilovačů a vysílačů.
2. Spuštění závaží a ponorky do vody.
3. Pomalé tlakování ponorky. Sestup na dno.
4. Odpojení závaží.

[5] To bylo předpokládáme myšleno opačně.

5. Zkoumání dna, odebírání vzorků.
6. Odlehčení ponorky, pomalý vzestup.
7. Vyrovnávání tlaku pomocí ventilu.
8. Navedení ponorky na souřadnice vyzvednutí.
9. Vyzvednutí ponorky.
10. Zajištění vzorků.
11. Konec mise.

Poznámky redakce:

1. *Jaký konkrétně kompozit skla a polymeru je vhodný pro stavbu ponorky, nebo aspoň okýnek? (Slitina se tomu neříká.)*
2. *Je skutečně vhodná topologie výztuh čtrnácticípá hvězda? Vymyslíte lepší?*
3. *Zjevně má mít ponorka více plášťů... Jak musí být jednotlivé pláště silné? Jak velká má být mezera mezi nimi, aby měla dostatečnou zátěž, pokud je mezi ně načerpána voda? Jak silná čerpadla potřebujeme?*
4. *Jak funguje přetlakové zařízení?*
5. *Proč je vhodné použít na vnější komponenty kalenou ocel? Proč ne třeba dural, karbon, litinu...*
6. *Jaký výkon turbín motorů potřebujeme k vyzdvižení ponorky ze dna?*
7. *Jak velkou betonovou kouli je třeba užít jako zátěž, aby klesání probíhalo rozumnou rychlostí? Kdy přesně je vhodné ji oddělit?*
8. *Zdá se, že v článku byla myšlena rádiová komunikace. Jak daleko od sebe musí být zesilovače, aby byl signál dostatečný? Jaká bude prodleva způsobená takovýmto přenosem signálu?*
9. *Proč je (anebo není?) obraz kamer ve vodě neostrý?*
10. *Z jakého materiálu by měly být vaky na vzorky? Jak by měly být přichyceny k ponorce? Budeme všechno sbírat do několika vaků, nebo budeme vzorky separovat?*
11. *Jak dlouho vydrží ponorka v provozu a kolik jakých zdrojů je na to potřeba? Je odhad 2 dny reálný?*
12. *Použití GPS je dobrý nápad, jako pojistka... Je ale pravděpodobné, že ji budeme potřebovat?*

Zuzka

Téma 5 – Sdílení tajemství

K tématu přišly hned čtyři zajímavé příspěvky. Každý z autorů ke sdílení tajemství přistoupil trochu jinak. Doc.[MM] Markéta Calábková pracuje s virtuálními zámky a neřeší jejich přesnou implementaci. Naopak Dr.[MM] Matej Lieskovský a Mgr.[MM] Dominik Krasula navrhují detailně popsaná schémata. První se rozhodl využít Čínskou zbytkovou větu, druhý rozklady na prvočísla. Ač by se tyto

přístupy mohly zdát podobné, mnoho společného v jejich případě nemají. Poslední přispívající Bc.^{MM} Aneta Lesná navrhuje využít velká prvočísla, svůj návrh ale pořádně nespecifikuje.

Doc.^{MM} Markéta Calábková a Bc.^{MM} Aneta Lesná se zabývají také dalšími aplikacemi pro sdílení tajemství. Aplikace navrhované Markétou si můžete přečíst v jejím článku, který níže otiskujeme. Aneta navrhuje: „Další možností využití takového tajemství by mohlo být společenství, kde ke spuštění jistého zařízení stačí určitý počet hlasů. Pokud své číslo poskytne dostatečný počet lidí, měly by stačit ke spuštění zařízení. Pokud rozvinu příklad s bankou, dokážu si dobře představit trezor, který vlastní skupina lidí a který se otevře, pouze pokud dostatek z nich (případně všichni) číslo poskytne.“

Vzhledem k rozdílným přístupům přispěvatelů otiskuje níže hned tři články. Některé z nich pro úsporu místa jen ve zkrácené podobě. Jejich plnou verzi najdete na našem webu.

A co dále?

Ještě než dojde na příspěvky, mám několik tipů, čím se v rámci tématu nadále zabývat. Určitě lze vymýšlet další a dokonalejší schémata, než ta navrhovaná. Navíc i samotné příspěvky ještě nechávají trochu volného prostoru na vylepšení, podívejte se na poznámky redakce pod každým z nich.

Zkusme si ale představit úplně novou situaci pro sdílení tajemství. Chtěli bychom si zahrát po telefonu hru kámen, nůžky, papír. Jak to udělat? Potřebovali bychom kamarádovi na druhé straně nejdřív sdělit nějaký náš závazek, ze kterého by on nepoznal, jaký symbol chceme dát. Pak ho nechat, ať on nám svou volbu prozradí a následně mu poslat nějaký „klíč“, pomocí kterého rozšifruje náš závazek. Přitom musí být zajištěno, abychom nemohli podvádět. Tedy k závazku nesmíme umět najít „klíč“ vedoucí k různým symbolům.

Na první pohled to možná vypadá neřešitelně, ale řešení existuje a kupodivu není až tak složité. Mimochodem, pro schémata založená na podobném principu existují i všelijaká reálná uplatnění. Napadnou vás nějaká?

O klíčích teoreticky (9b)

Doc.^{MM} Markéta Calábková

Nejdříve vyřeším úlohu pro n osob, z nichž má tajemství znát libovolných $n-1$, ale už ne $n-2$. Radši si to budu představovat, že ty osoby mají určitý počet různých typů klíčů a jedná se o dveře s určitým počtem zámků. Tedy vezmeme si nějakou skupinu o $n-2$ členech. Ta určitě tajemství nezná, tedy nemá všechny druhy klíčů. Potom z původních n lidí po odebrání těchto $n-2$ osob zbudou 2 osoby, z nichž když kteroukoliv přidáme do naší skupiny o $n-2$ členech, vytvoříme autorizovanou skupinu. Tedy tyto dvě osoby musí mít aspoň jeden společný klíč, který nikdo z vybraných $n-2$ osob nemá a který je potřeba k otevření dveří. Ke stejnému závěru se dostaneme, když si vybereme jakoukoliv jinou $(n-2)$-tici lidí,

přičemž pro každou zbylou dvojici bude daný klíč unikátní. Takže máme nejméně $\binom{n}{n-2} = \binom{n}{2} = \frac{n(n-1)}{2}$ zámků, tedy celkem nejméně $n(n-1)$ klíčů, tedy každá osoba má $n-1$ klíčů u sebe, aby tento systém fungoval. Takže pro zadaných 7 osob by Korunní komora měla mít 21 různých zámků a každá z pověřených osob by měla mít 6 klíčů. Funguje to, protože když si teď vyberu $n-1$ lidí, mají všechny klíče (protože zbyl jeden a ten má každý svůj klíč společný s nějakou jinou osobou), ale pro $n-2$ lidí mi zbude skupina o dvou lidech, která má podle schématu svůj unikátní klíč.

Když už vím, jak se to počítá, můžu najít schéma pro obecné k. Vyberu si skupinu o $k-1$ lidech, která podle zadání neumí dveře otevřít, takže mi z původních n zbude $n-k+1$ lidí. Stejnou úvahou jako předtím zjistím, že tyto osoby mají svůj společný unikátní klíč, tedy typů klíčů (čili zámků) bude $\binom{n}{k-1} = \binom{n}{n-k+1}$, tedy celkem klíčů bude $\binom{n}{n-k+1} \cdot (n-k+1)$, takže každá osoba bude vlastnit $\frac{\binom{n}{n-k+1}\cdot(n-k+1)}{n} = \binom{n-1}{n-k}$ klíčů. Zase si můžeme zkusit, že to bude fungovat.

Prozatím jsem řešila situaci pro zcela rovnocenné osoby, což neplatí pro uvedeného krále se třemi vojevůdci. Tak… vyberu si jediného krále, který neumí dveře sám otevřít, a zbudou tři vojevůdci, z nichž když jakéhokoliv přidáme ke králi, otevřou to. Tedy všichni tři vojevůdci musí mít stejný unikátní typ klíče. Dále si vyberu dva vojevůdce. K nim když přidám zbývajícího vojevůdce, otevřou dveře, ale bez něj ne. Tedy každý vojevůdce musí mít aspoň jeden klíč, který ostatní vojevůdci nemají, ale král mít může. Aby ale dveře mohli otevřít král s jedním vojevůdcem, musí mít král všechny klíče, které vojevůdci chybějí, tedy klíče všech ostatních vojevůdců bez toho, který mají jenom vojevůdci. Takže král má klíče všech vojevůdců kromě toho, který je všem třem vojevůdcům společný. Bude lepší si to nějak označit. Takže si vojevůdce označím V_1, V_2 a V_3, krále K. Klíč, který má V_1 a ostatní vojevůdci ne, bude v_1. Obdobně zadefinuji v_2 a v_3. Klíč, který je všem vojevůdcům společný, ale král ho nemá, označím v. Takže V_1 bude mít klíče v_1 a v, V_2 klíče v_2 a v, V_3 klíče v_3 a v a konečně K bude mít klíče v_1, v_2 a v_3. Máme čtyři zámky: v_1, v_2, v_3 a v. Tohle schéma funguje.

Praktické aplikace už byly popsány v zadání, tak třeba ještě: kdyby mělo několik lidí sdílený počítač, aby heslo nemohl změnit jen jeden, ale víc – „zaheslované heslo“ – dost šílený nápad. Ale to je zase situace peer-to-peer, ta není tak zajímavá a ta je tu navíc popsaná. A nebo když máme firmu, která je z různých částí vlastněna akcionáři, abychom v tom neměli nepořádek (když má firma akcie na burze), tak jim firmu poměrově přerozdělíme až od určitého počtu vlastněných akcií (třeba jako volby do poslanecké sněmovny, tam taky nepostoupí strany, co mají méně jak 5 % hlasů a zbylé si křesla přerozdělí podle poměru získaných hlasů). Tak by třeba mohlo jít zaheslovat účet té firmy tak, aby s ním mohli manipulovat pouze akcionáři, co vlastní v součtu víc jak 50 % firmy. Předpokládám, že každý investor vlastní celočíselný počet akcií. Tohle schéma jsem už popsala u krále a tří vojevůdců, kde si to taky můžu představit tak, že král má tři akcie a vojevůdci dvě. Mohl tam být třeba ještě princ, který jakoby vlastnil jen jednu

akcii, ale nic tam neměnil, takže se s ním nemuselo počítat. Takže podobně. Čím víc akcií vlastník má, tím víc klíčů dostane. Každá skupina, která má v součtu více než polovinu počtu akcií pověřených akcionářů, ale nemá žádnou takovou podskupinu, má svůj unikátní klíč. Přičemž akcionáři, kteří nic nemohou ovlivnit (respektive nepřehoupnou žádnou skupinu z podpoloviční do nadpoloviční) budou z rozdělování klíčů vyloučeni. Takhle by to mělo být funkční.

Poznámka redakce: Článek se zabývá teoretickým rozborem problému, což není vůbec na škodu. Jak by se ale takový zámek dal realizovat prakticky například v počítači?

O využití prvočísel pro sdílení tajemství (9b)

Mgr.^{MM} Dominik Krasula

Zvolit jako klíč konkrétní číslo není dobrý nápad. Lepší by bylo nastavit zámek tak, aby se otevřel, pokud mu zadané číslo splňuje nějakou vlastnost/soubor vlastností nebo právě naopak se jej daná vlastnost netýká. Když se to vymyslí chytře, nemusejí ani vlastníci klíčů znát vlastnosti, jenž zámek zkoumá.

Pro začátek je tedy dobré zvolit, jaké vlastnosti u čísla budeme zkoumat. Jaké podmínky musí splňovat. Tento článek se bude zabývat myšlenkou výběru čísla podle toho, zda-li má dané prvočinitele, hodnoty získané z klíčů se násobí. Možností je určitě více.

Máme-li n osob, tak každá bude mít ve svém čísle $n-1$ různých prvočísel krát nějaké matoucí bezpečnostní hodnoty (ty nebudu pro jednoduchost výkladu brát v potaz, prostě osoba, co má klíč $5 \cdot 3$, nebude mít číslo 15, ale třeba 345). Každá osoba bude tedy mít všechna čísla z n-číselného bloku, vyjma jednoho, u každého to bude jiné.

Pokud zámek nastavíme tak, že každé prvočíslo musí být ve výsledném čísle $(n-1)$-krát, musejí se sejít všichni, když $(n-2)$, stačí, když se sejde libovolných $n-2$ osob a tak dále.

Příklad: Máme tři osoby, první má klíč $2 \cdot 3$, druhá $3 \cdot 5$, třetí $2 \cdot 5$, klíč se otevře, jen když dostane násobek $2 \cdot 3 \cdot 5$ – musejí se sejít alespoň dva, je jedno jací.

Tento princip umožňuje zámek nastavit tak, aby otevřel libovolnému, předem danému počtu zasvěcených lidí. Jsou ale situace, kdy si nejsou všichni rovni. Někdo má větší pravomoc, takže by mu mělo stačit méně dalších pomocníků k otevření zámku.

„Nadklíč“ by tedy měl lepší číslo. Řešme třeba případ ze zadání. Máme tři osoby a krále. Na tuto situaci se může nahlížet jako na situaci, kdy máme pět osob a otevřít zámek mohou libovolné tři, přičemž král jsou právě dvě běžné osoby (má dvě čísla – třeba $3 \cdot 2$ a $5 \cdot 2$, kdežto generál má pouze $3 \cdot 2$). Jdou tím řešit i překvapivě složité poměry, se složitým systémem, kdy postavy mají nejrůznější hodnosti:

Postačující klíč mají buď čtyři vojíni, tři plukovníci, dva generálové nebo posloupnost vojín, plukovník, generál. Zprvu to vypadá neřešitelně, ale co kdybychom za nad-osobu prohlásili i vojína? Kdyby měl vojín dvě čísla, mohli bychom plukovníkovi dát tři, generálovi čtyři, a požadovat osm čísel k otevření. Potom systém opět funguje. A je celkem odolný. Dá se zocelovat – prostě jen bude nejnižší osoba mít více čísel a pak si můžeme pěkně hrát s poměry.

Co když se ale král obává svých generálů. Může potom říci, že nechce, aby spojí-li se jeho generálové, otevřeli zámek. Generálovi s deseti plukovníky už může věřit – buď je skutečně s ním anebo už má tolik lidí na své straně, že je to stejně jedno. Nabízí se použít prostě systém, kdy dva generálové nemají dostatečnou hodnotu, aby zámek otevřeli. Ovšem tento systém nemusí být funkční, dvěma generálům prostě stačí překecat dva/tři plukovníky a můžou zámek v pohodě otevřít. Jak tedy řešit situaci, kdy nějaká podmnožina konkrétních lidí zámek prostě nemůže otevřít?

Můžeme si tu třeba hrát s dělitelností. Třeba dát generálům do součinu čísla $n \cdot m$, a nastavit zámek tak, že dostane-li číslo dělitelné $n^2 \cdot m^2$ tak se neotevře, ale dělitelnost číslem $n \cdot m$ mu nevadí. Tato metoda se dá šikovně využít i při ochraně před špiony. Vypustit několik čísel se zakázanou hodnotou (třeba právě hodnotou $n^2 \cdot m^2$), takže je-li ve skupině byť jen jediný špión, zámek se neotevře.

Poznámka redakce: Zbytek článku rozebírající další speciální případy rozdělení moci mezi různé skupiny naleznete na našem webu.

Poznámka redakce: Nevýhodou zde nabízeného systému je snadná možnost podvádění. Zakládat bezpečnost na neznámém principu ověřování se za vhodné obvykle nepovažuje. Stačilo by ale místo malých prvočísel volit prvočísla velká a systém by mohl fungovat docela obstojně. Faktorizovat velká čísla je totiž složitý problém, na jehož neřešitelnosti v reálném čase je založen například velmi populární algoritmus RSA.

Přesto i při použití velkých prvočísel má nabízený systém jednu potenciální slabinu. Napadne vás?

Sdílení tajemství na čínský způsob (10b)

Dr.^{MM} Matej Lieskovský

Klíč je pro potřeby tohoto článku definován jako nějaké přirozené číslo (včetně nuly), které je potřeba znát k získání přístupu. Cílem je nějak distribuovat klíč nebo jeho části mezi n lidí tak, aby libovolných k z nich umělo relativně rychle klíč určit, ale aby libovolných $k-1$ toho o klíči vědělo co nejméně. Bude nám stačit, aby určení klíče pro $k-1$ lidí bylo mnohem složitější než pro k, absolutní složitost umíme snadno navýšit, způsob uvedu. Ve všech případech je bezpečnost proti útoku z vnějšku určena počtem možných klíčů. Bezpečnost pro $k-1$ budu určovat jako počet klíčů, ze kterých budou muset tipovat.

Tady bych rád upozornil na něco, co vnímám jako chybu v zadání témátka. Požadavek na to, aby libovolných $k-1$ lidí nevědělo o klíči vůbec nic, je podle mě zbytečný. Úplně stačí, aby mělo $k-1$ lidí potřebu vybírat z alespoň dvou možností, načež umíme bezpečnost exponenciálně zvyšovat použitím několika klíčů. Skupina $k-1$ lidí na tom bude výrazně lépe než vnější útočník, ale pokud na tom i tak budou zoufale špatně, tak nám to zrovna moc nevadí.

Nejdříve uvádím několik specifických řešení pro daná k. Jsou implementačně jednodušší, než obecné řešení, které uvádím na konci této práce.

Poznámka redakce: Řešení pro $k = 1$, n, 2 a $n-1$ z prostorových důvodů vynecháváme. Najdete je na webu. Následuje obecné řešení pro libovolné k a n.

Čínská věta o zbytcích říká, že známe-li zbytky po dělení nějakého čísla n několika vzájemně nesoudělnými čísly $p_1, p_2, p_3, \ldots, p_n$, dokážeme číslo n jednoznačně určit právě, když je menší než součin $p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n$.

Každý z n lidí bude mít přiděleno jedno z n vzájemně nesoudělných čísel a následně se dozví zbytek po vydělení klíče tímto číslem. Klíč se dá určit jako nejmenší číslo, které bude splňovat libovolných k zbytků.

Jelikož chceme, aby klíč bylo možné určit z libovolných k zbytků, musí klíč být menší, než součin k nejmenších přidělených čísel. Současně ale nesmí být klíč určitelný z $k-1$ zbytků, musí tedy být větší než součin $k-1$ největších přidělených čísel. Obě podmínky dohromady s požadavkem na vzájemnou nesoudělnost přidělených čísel nám výrazně komplikuje výběr přidělených čísel. Dá se ukázat, že nejtěžší je toto přidělování zvládnout pro $k = \lceil n/2 \rceil$. Méně přesná, ale jednodušší postačující podmínka je, že největší přidělené číslo musí být menší, než to nejmenší na $k/(k-1)$. Pokud budeme přidělovat prvočísla, tak podle Bertrandova postulátu nám budou „stačit“ čísla řádově 2^{n^2}. Je to sice opravdu hodně, ale pro menší množství lidí to bude fungovat. Lepší nalézání vzájemně nesoudělných čísel je rozhodně otevřený problém k dalšímu výzkumu.

Touto metodou lze řešit i úlohu s králem a vojevůdci. Snadno nahlédneme, že král se chová jako dva vojevůdci. Tudíž vygenerujeme zbytky pro $(n, k) = (5, 3)$, každý vojevůdce dostane jeden zbytek a král dva. Obdobně umíme vyřešit libovolný případ, který umíme převést na problém s lidmi, jejichž „váha“ při otevírání je racionálním číslem.

Domnívám se, že implementace sdílení tajemství pomocí čínské zbytkové věty je dostatečně silná na to, aby bylo možné opět zobecnit zadání. Máme n lidí a seznam všech minimálních autorizovaných skupin, kdy přístup má dostat (pouze) libovolná skupina, která obsahuje alespoň jednu celou minimální autorizovanou skupinu. Zatím nevím, jak přesně tento algoritmus implementovat, ale bude postaven na principu používání čísel, která jsou vzájemně dle potřeby soudělná.

Poznámka redakce: Jestli fakt, že neautorizovaná skupina držitelů klíče o tomto klíči může získat nějakou alespoň kusou informaci, je na závadu, je spíše filosofickou otázkou. Pochopitelně i pokud část informace získá, může být schéma ještě pořád dostatečně bezpečné. Takže tímto směrem má smysl zadání rozšířit. Na druhou stranu takové schéma už alespoň podle mě není tak hezké.

Článek docela složitě rozebírá problematiku možné velikosti hledaného klíče. Toto téma by určitě stálo za to ještě prozkoumat. Čím více možností pro klíč budeme mít, tím bude schéma bezpečnější. Nehrozí, že bude možností na klíč třeba tak málo, že by bylo možné je vyzkoušet hrubou silou jednu po druhé?

Na zaslaném příspěvku oceňuji, že jako jediný z došlých měl skutečně podobu článku včetně nadpisu. I toto se promítlo do jeho bodového hodnocení.

Kuba

Výsledková listina 2. čísla

				Úlohy								
Poř.	**Jméno**	**R.**	$\sum_{-1}$	**r1**	**r2**	**r3**	**r4**	**t3**	**t4**	**t5**	$\sum_0$	$\sum_1$
1.	Mgr.[MM] D. Krasula	1.	44					8		9	17	44
2.	Doc.[MM] M. Calábková	3.	119	3	2		2			9	16	36
3.	Dr.[MM] M. Lieskovský	4.	93							10	10	26
4.	Mgr.[MM] P. Souček	2.	36	3	2		2				7	25
5.	Mgr.[MM] L. Studená	4.	24	3	2	1	2				8	24
6.	Doc.[MM] A. Šťastná	4.	111	3	2	3					8	22
7.–8.	Mgr.[MM] O. Hollmann	4.	21	3	1						4	21
	Mgr.[MM] V. Rozhoň	3.	21								0	21
9.	Dr.[MM] P. Nácovský	3.	57	2	1	4					7	20
10.	Bc.[MM] A. K. Lesna	1.	17	2	0	0	2		2	3	9	17
11.–12.	Bc.[MM] V. Bartovic	2.	12	0	0	1					1	12
	Dr.[MM] J. Kušnír	3.	53	0	0	4	0				4	12
13.	Bc.[MM] J. Havelka	1.	11	3	2						5	11
14.	Bc.[MM] J. Václavek	2.	10	3	1						4	10
15.–18.	V. Končický	3.	9	3	2	2	2				9	9
	T. Paliesek	2.	9	2	0						2	9
	D. Tanglová	1.	9	0	0		0		3		3	9
	Bc.[MM] A. Teichmann	4.	18								0	9
19.–20.	Dr.[MM] F. Homza	4.	95	3			2				5	8
	J. Liška	2.	8	0	1	1	1				3	8
21.	Mgr.[MM] L. Langerová	3.	42								0	6
22.–25.	J. Nosková	4.	5								0	5
	A. Šedová	2.	5								0	5
	Bc.[MM] V. Václavík	4.	13	3				1			4	5
	Dr.[MM] P. Vincena	3.	63				2				2	5
26.–29.	R. Hlavinka	2.	4	0	0	0	0				0	4
	E. Klimentová	4.	4	2			2				4	4

Poř.	Jméno	R.	$\sum_{-1}$	Úlohy r1	r2	r3	r4	t3	t4	t5	$\sum_0$	$\sum_1$
	Mgr.[MM] M. Poljak	2.	38								0	4
	J. Stanovský	2.	4								0	4
30.–33.	D. Dimitrov	3.	3								0	3
	Dr.[MM] A. Hrušková	4.	59								0	3
	K. Kolář	2.	6								0	3
	J. Škvára	3.	6								0	3
34.–38.	Bc.[MM] J. Dittrich	2.	14								0	2
	Bc.[MM] Z. Garčic	3.	12				2				2	2
	Doc.[MM] J. Kadlec	3.	100								0	2
	Mgr.[MM] V. Skoupý	4.	44								0	2
	Bc.[MM] M. Šafek	3.	14								0	2
39.–40.	Bc.[MM] K. Ilievová	3.	12								0	1
	F. Zajíc	1.	1								0	1
41.–43.	Mgr.[MM] J. Cerman	2.	33				0				0	0
	Bc.[MM] D. Macháčová	4.	16								0	0
	M. Müller	4.	0								0	0

Sloupeček $\sum_{-1}$ je součet všech bodů získaných v našem semináři, $\sum_0$ je součet bodů v aktuální sérii a $\sum_1$ součet všech bodů v tomto ročníku. Tituly uvedené v předchozím textu slouží pouze pro účely M&M

Adresa redakce:

M&M, OVVP, UK MFF
Ke Karlovu 3
121 16 Praha 2

E-mail: mam@matfyz.cz
WWW: http://mam.mff.cuni.cz

Časopis M&M je zastřešen Oddělením pro vnější vztahy a propagaci Univerzity Karlovy, Matematicko-fyzikální fakulty a vydáván za podpory středočeské pobočky Jednoty českých matematiků a fyziků.