

Milý řešiteli,

vítáme Tě u 3. série úloh 4. ročníku korespondenčního semináře MoRoUS. Doufáme, že se ti budou další úlohy líbit a také se něco nového naučíš.

## 3. série 2017/2018

Termín odeslání 3. série: 5. 3. 2018

*Planeta Mu byla poklidné místo k životu. Nekonalý se tu žádné vzpoury, žádné převraty, media nešířila žádné poplašné zprávy. Do větru se občas přimíchával jemný kovový zvuk, to jak se místní robotické obyvatelstvo přemisťovalo po planetě. Přeci jen, i tak bezproblémoví obyvatelé, jako jsou roboti, potřebují starostlivého vládcu, který se postará o jejich základní potřeby – například olej. To si pan profesor Morous, jediný lidský obyvatel planet, velmi dobře uvědomoval a tak si z jedné ze sousedních planet objednal velkou dodávku oleje, který plánoval svým obyvatelům rozdat. Avšak jakkoli byl život na planetě poklidný, jakmile jste se rozhodli vyrazit za obchodem k sousedním planetám, museli jste si dát pozor na pirátské flotily. Pojďte s námi poradit panu profesorovi jak spravedlivě rozdělit olej mezi potřebné tak, aby nikdo nepřišel zkrátka, a take pomoci našim obchodním lodím správně zakódovat zprávy, aby je piráti neměli šanci rozluštit.*

### Kam posílat řešení?

Až budeš mít řešení hotové, pošli nám prosím celá svá řešení, včetně všech nákresů, programků, prostě vše, co by nám usnadnilo opravování Tvé úlohy. Stačí, když pošleš řešení jen některých úloh nebo jejich částí.

Řešení posílej nejlépe e-mailem na adresu [seminar@morous.fel.cvut.cz](mailto:seminar@morous.fel.cvut.cz), nebo poštou (řešení každé úlohy v tomto případě napiš na samostatný papír A4) na adresu

Korespondenční seminář Morous,  
Katedra kybernetiky FEL ČVUT,  
Karlovo náměstí 13,  
121 35 Praha

*Aleš, Honza, Kája, Klárka, Martin, Mirek, Ondra a Terka*

## Úloha č. 1: Dělení oleje (20 bodů)

*Profesor Morous se po vítězství v Super Elite Robot rozhodl v dobrém rozmaru odměnit všechny robotické pracovníky na planetě (a navíc si všiml, že by jim nějaká ta údržba již prospěla). Rozhodl se proto, že jim daruje exkluzivní nový mazací olej, díky kterému budou voděodolní a jak se psalo na obalu, jejich součástky již nikdy nezrezaví a budou se třpytivě lesknout.*

### Otázka 1.1

Rozhodl se ale také, že by rád, kdyby se roboti byli schopni o dárek podělit (a stejně bylo oleje v láhvi více než na jednoho robota). Proto vyhlásil: „Roboti, odvedli jste na planetě spoustu práce. Vytvořili jste například skvělý zavlažovací systém a mimo jiné jste také dokázali vyhrát v nelehkých soutěžích. Proto jsem se rozhodl vás odměnit. Rozdělte se do trojic, ať vám mohu odměnu dát.“

Roboti se velmi organizovaně začali uspořádat a za chvíli před profesorem stály samé trojice až na jednu osamělou dvojici.

To profesora velmi zaujalo. Podrbal se na hlavě a řekl: „Nyní se pokuste rozdělit do pětic.“ Roboti se velmi rychle přeskládali. Nyní před profesorem stály samé pětičky a jedna osamělá trojice.

Pan profesor se podrbal na hlavě. Chtěl dát všem stejně. Zkusil to ještě jednou: „Nyní se rozdělte do sedmic.“ Roboti bez jediné námitky začali znovu popocházet a za chvíli tu byly samé sedmičky a dva osamělí roboti.

Pan profesor se dlouze zamyslel, poté si došel pro papír a začal nadšeně počítat, přičemž nechal na nádvoří nešťastné roboty stát. Až po dlouhé době se ozvalo vítězné zvolání: „Už konečně vím, kolik vás je.“ Poté je rozdělil tak, aby všechny skupinky byly stejně velké a rozdál jim sady olejů.

Víte i vy, kolik bylo na planetě robotů?

### Otázka 1.2

Uběhlo několik dalších měsíců, někteří roboti byli sešrotováni a jiní znovu vytvořeni a profesor Morous se rozhodl, že by rád znovu zjistil, kolik má na planetě robotů. Po minulé zkušenosti se rozhodl, že vyzkouší jiný, systematictější systém. Postupně žádal roboty, aby se rozdělili do dvojic, trojic, čtveřic, pětic a šestic, ale vždy zbyl jeden osamocený robot. Až když je požádal aby se rozdělili po sedmi, žádný robot nezbyl. Dokážete zjistit, jaký je nejmenší počet robotů, kteří mohli být na planetě?

### Otázka 1.3

Počítání lidí, věcí a robotů rozdělováním do skupin se od té doby stalo profesorem novou zábavou. Když uspořádal malé neformální setkání s přáteli, vymyslel dokonce hru, kdy si zavázal oči a řekl: „Povím vám, kolik vás je. Rozdělte se do dvojic, do trojic a do pětic a řekněte mi, kolik vás zbylo.“

Při zavázaných očích poslouchal posouvání nohou a poté slyšel odpověď: „1, 2 a 4.“

Chvíli se zamyslel a za chvíli odpověděl: „No, nejméně vás tu může být...“

Dokážete přijít na to, kolik návštěvníků dorazilo?

### Otázka 1.4

Profesor se tak vytrénoval, že nakonec jezdil na podobné soutěže po celé galaxii. Při jedné takové soutěži zjistil, že když se malí multi-agentní robůtci sdruží po pěticích, zbude 1 osamocený, když po sedmicích, zbudou 2, když po devíticích, zbudou 3 a když po 11, zbudou 4. Tentokrát ale nestačilo určit, jaký je nejmenší možný počet robotů, ale jaké jsou všechny možné počty robotů, které mohou toto uspořádání vytvořit.

## Úloha č. 2: Komunikace (20 bodů)

*Prof. Morous udržoval s většinou sousedních planet velmi dobré vztahy. Mezi planetami panoval čilý obchodní ruch, kdy si vyměňovali nejrůznější suroviny a informace. Vesmírem ale létaly i nepřátelské pirátské flotily, které se snažily mírumilovné obchodní loď oloupit a celou robotickou posádku na nich odstavit z provozu. Z toho důvodu se roboti naučili komunikovat výhradně pomocí šifrovaných zpráv, v kterých si vyměňovali informace o potřebném zboží a čase dalších dodávek, ale i o pozicích nepřátelských flotil.*

### Otázka 2.1

Z počátku jim stačilo pro komunikaci používat jen velmi jednoduchého kódování, kdy písmena zprávy nahradili písmeny nacházejícími se o zvolené číslo dále.

Každé písmeno ve zprávě je posunuto o  $n$  písmen v abecedě, kdy hodnota posunu  $n$  je známa. Za 26 základních písmen abecedy je přiřazeno i 10 číslic (abeceda tedy vypadá následovně: ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789). Jestliže se při posunu dostaneme za konec abecedy, budeme pokračovat znovu od začátku. Např. při posunu o 3 se Z transformuje na 2 a 8 na B.

Protože kapacita robotického mozku je mnohem větší než kapacita mozku lidského, nepotřebovali si roboti ani posílat hodnotu posunu. Pirátská flotila tak získala zprávu

«PV8XBNRYRX641ZNTOR6BCV64NI1Q21YRQORNY2UNZN74V6N».

Pokuste se nalézt původní zprávu a zjistit v kolik, kam a s jakým nákladem bude vypravena obchodní loď. Pokud se vám povede vytvořit na rozklíčování zprávy i nějaký malý prográmeček, přiložte k řešení i jeho zdrojové kódy.

### Otázka 2.2

První šifru piráti za několik týdnů prokoukli a tak museli roboti přijít s lepším šifrováním. Rozhodli se vždy text zapsat po řádkách do tabulky s daným počtem sloupců, přeházet sloupce a poté poslat postupně text po sloupcích. K tomu, aby mohli zprávu rozluštit, jednou za čas si vyměnili tajné heslo. Jeho délka určovala počet sloupců v tabulce a sloupce se přeskládaly podle pořadí jeho písmen v abecedě.

Například zpráva: «ZITRA SE UVIDIME V DESET» s heslem OSEL by se zapsala do tabulky takto:

O	S	E	L
Z	I	T	R
A	S	E	U
V	I	D	I
M	E	V	D
E	S	E	T

Slovo OSEL určuje 4 sloupce tabulky a pořadí jeho písmen v abecedě je 3-4-1-2. Po přeházení tedy bude vypadat tabulka následovně:

E	L	O	S
T	R	Z	I
E	U	A	S
D	I	V	I
V	D	M	E
E	T	E	S

Nyní se zpráva přečte po sloupcích a odešle jako «TEDVERUIDTZAVMEISIES».

Představte si, že piráti dostali do rukou zprávu

«SKPEEESIAATDTTAEUETRZBTONAUAEVOARLLVPLBIDSDKPNU».

Podarilo se jim ulovit i tabulku s klíčem, který byl ZLODEJI. Dokážete pirátům poradit na jakou hvězdu a kdy se bude doručovat další zásilka?

### Otázka 2.3

U další zprávy

«ISODRRSOCDZVPOUTELI IATVEA»

neměli sice piráti žádný klíč, ale dokázali ji rozluštit i tak. Jak je to možné? Dokážete i vy přijít na to, kam, kdy a co se bude doručovat?

### Otázka 2.4

Aby roboti zamezili takovémuto jednoduchému rozšifrování svých zpráv, rozhodli se zavést ještě druhý klíč, který bude tentokrát promíchávat ještě po promíchání sloupců i řádky. Piráti byli

dlouho bezradní až na chvíle, kdy se jim podařilo ulovit oba klíče. Jednoho dne dostali do rukou zprávu

«ILESIVNLERIOAASOTLREAZDKDYDRAPUATNI»

a klíče OSLICE a MAGNETY a nadšeně se vydali na lup. Přijdete na to, jaká byla původní zpráva?

## Otázka 2.5

Postupně roboti své šifry více a více zlepšovali a měnili. Piráti z předchozích zpráv věděli, že se chystá obří transport důležitých surovin. Nevěděli ale den v měsíci, kdy se akce uskuteční a jméno planety, na kterou se mají vydat. Zpráva, kterou tentokrát pirátská flotila objevila, byla následující

«IHGFEDC BAJIJ KIL CUAHMBI NI OKDKFCBIBD I OFLFPABUNCD GNAKYJD  
LFGNFK CEIHM OKFOEANI UCA NAJOAKIJABNBD KAHD VZBICIJ ZA BI NFJ  
BIZFKBAJ OKDGEILV U GICKBFV HEFCAGAJ I JDUFV GFPEDM BAHF SA EZA BI  
BAJ IUOFB OKDPEDZBA VGIZIN SIGYJ HEFCAGAJ SA UINVKBDB LFGNFK CEIHM  
UD NFNDZ KFZLAEDE EDLD OFLEA NFMF SIG UA HMFICISD C OFEFOKIZLBA  
GICKBA JISDED OKAL UAPFV JDUV GFPEDM OKALUNICNA UD EVXVUBD GICKBV  
ZI BALAEEDMF FLOFEALBA CABGV SA GKIUBY LAB I MFUNV C GICKBA  
SA JIEF VZ SUNA UA BIUBDLIED OKAHANED SUNA CUAHMBY BFCDBY I NAL  
SUNA UA OFMFLEBA FOKAED C JAGGAJ PFXV I ZIJYUEABA UA LDCINA BI JDUV  
GFPEDM BVLI UA OFJIEV KFZEAZI LF CUAHM GFVNV GICKBY I NV UA NALY  
JI VGIZIN LF GNAKA UGVODBY EDLD OFLEA NAFKDA LFGNFKI CEIHMI OINKDNA  
SUNAED OKY HEFCAGAJ PAZ QIBNIZDA PAZ NFMVY OF LYBIJDHA I PAZ UJYUEV  
OKF MVJFK PVLANA UA BI NY GFPEDMY LDCIN NVOA I PAZJYUEABGFCDNA  
NKAPI IZ LF OFEALBA I OIG UA ZCALBANA I OVSLANA G FPALV JIJ LVCFLBA  
OFLAZKABD ZA LF NANF OKCA UGVODBY ZIKIZVSA LFGNFK CEIHM NIGA JBA  
JYUEDJ ZA BABD C OKICV F MVJFKV I F NA LYBIJDHA BAPVLAJA JEVCDN IEA  
NF ZA JD VODKI QIBNIZDD GLYZ CD ZA UA JD OFCALEF UOKICBA»

Vyzkoušeli všechna možná šifrování a dekodování, která je jen napadla, ale stejně nebyli schopni šifru rozluštit. Se šifrou se jim podařilo zadržet i jednoho z robotů, který zprávu předával a poté co mu posílali do obvodů přesně odměřené dávky elektrického proudu a tekutin, dostali ho do téměř zkratovaného stavu, kdy jediné co vydával, byla stále se opakující dvě slova: „čeština“ a „kniha“. Prohledali archivy a jediné, co našli byla následující tabulka frekvencí výskytu jednotlivých písmen v češtině.

Tabulka frekvenčního výskytu písmen v češtině: číslo u každého písmene udává jeho procentuální výskyt v abecedě. Např. Číslo 9.6 u písmene A nám říká, že 9.6% všech písmen v abecedě bude písmeno A.

A	B	C	D	E	F	G	H	I	J	K	L	M
9.6	1.8	2.9	3.8	10.9	0.2	0.2	2.5	6.7	2.3	3.5	5.7	3.6
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5.9	8.1	3.1	0.0	4.4	5.6	5.4	3.6	3.9	0.1	0.0	2.9	3.3

Pustili se do analýzy textu s nesmyslnými slovy, který dostali, a po dlouhém snažení dostali záhadný text. Vzpomněli si na druhé slovo, který ten ubožák říkal a pátrali dál, až objevili, že ten kus textu skutečně patří do jedné z českých knih.

Pomůžete pirátům rozlišit tuto tajnou zprávu a zjistit, z jaké z knih je daný úryvek a jaký by tedy mohl být název planety, na kterou se výprava bude vydávat? Možná se vám podaří zjistit i v jaké kapitole úryvek je, abyste určili den v měsíci, kdy se výprava uskuteční.