



**Korešpondenčný seminár z programovania
XXIII. ročník, 2005/06**
Katedra základov a vyučovania informatiky FMFI UK,
Mlynská Dolina, 842 48 Bratislava

*KSP finančne podporujú: aSc – Applied Software Consultants spol. s r.o.
MICROSTEP-MIS spol. s r.o.*

Príklady 2. kola zimnej časti

*Stojí, stojí mohyla,
na mohyle zlá víla.
Na mohile chrastie, trnie,
a tie vrabce z toho tnia
čľup, žblnk do druhého tnia
(to ako tie Vtáky v tnni).
Rastie, kvety rozvija,
hlavou kameň rozbija.
(Fakt hlavou, tou ľavou!)*

Aj takéto veci môžete (ako súčasť jednej šifry) zažiť na našom sústreďení. Tak neváhajte a do **3. 1. 2006** nám posielajte svoje riešenia. S tými najšikovnejšími sa na najbližšom sústreďení stretneme už v marci!

Ak máš kladivo, všetky problémy časom začnú pripomínať klinec...

KSPáci

1. O nemocnici

15 bodov

Bolo raz jedno mesto. V tom meste bola nemocnica. V tej nemocnici boli pacienti a bolo ich dosť veľa. No prišiel Jurko Štatista a začal robiť štatistiku pacientov. Keď prišiel pacient do nemocnice, zapísal si jeho meno, rok narodenia, hmotnosť, výšku, veľkosť palca, lakťa a nechcete vedieť, čoho ešte všetkého. No nebol by to náš Jurko, keby nechcel všetky štatistické veci rátať a vyvodzovať z toho dôsledky.

I rozhodol sa on rátať medián výšok pacientov. Rozmýšľal a rozmýšľal, ale predsa len je to štatista a nie programátor.¹

Úloha: Na vstupe je číslo N a za ním N výšok pacientov v poradí, ako prichádzajú do nemocnice. Vašou úlohou je pre každého prichádzajúceho pacienta povedať, aký je medián výšok pacientov, ktorý do nemocnice prišli dovtedy (vrátane neho). Medián M prvkov je taký prvok, ktorý by bol po utriedení vzostupne na $\lceil M/2 \rceil$ -tom mieste.

Príklad:

Vstup:

$N = 10$

158 182 112 92 52 201 193 167 177 167

Výstup:

158 158 158 112 112 112 158 158 167 167

2. O problémoch s prehadzovaním

15 bodov

Prišli sme zo sústredka, zložili sme veci a spravili sme tým veľký neporiadok. Bolo by ho treba upratať. Také upratovanie ale vôbec nie je jednoduché. Spočíva v tom, že sa veci

¹A tobož nie je štatistik. Ak neviete, aký je v tom rozdiel, nalistujte si v slovníku. Zjavne to nevedel ani autor textu k tomuto príkladu :-).

poprehadzujú z miesta, na ktorom sú, na miesto, na ktoré patria. No a na to treba určitý manipulačný priestor, musí sa človeku chcieť, musí vedieť, kam čo patrí, a ešte kopu ďalších vecí.

Rozhodli sme sa teda, že upratovanie prenecháme stroju. Kúpili sme teda namakané zariadenie – Kombinačný Samočinný Poprehadzovávač (KSP). Pre tých, čo ešte KSP nevideli, stručne popíšem. Zariadenie predpokladá, že máme N miest, na ktorých sú veci.

Poprehadzovávaču zadáme program, ktorý pre každé miesto hovorí, kam (na ktoré miesto) chceme presunúť vec, ktorá na ňom je. Nesmieme pritom chcieť dať dve veci na to isté miesto (to by sa nezместilo). Potom už stačí KSP spustiť a on to všetko poprehadzuje (a ešte treba ujsť niekam preč, aby nepoprehadzoval aj nás).

Už by sme tu aj mali upratané, keby sa nám KSP nepokazil. Ono totiž cestou sem nám asi trikrát spadol na zem a asi kvôli tomu po spustení sa program vykoná niekoľkokrát (presnejšie K -krát). Teda aby sme úspešne upratali, potrebujeme KSP zadať taký program, ktorý keď sa zopakuje K -krát, tak nám prehádza veci tak, ako chceme. Ale nech sa snažíme ako chceme, nedarí sa nám a chceli by sme vás poprosiť o pomoc.

Úloha: Napíšte program, ktorý dostane na vstupe čísla N , K a naše želané poprehadzovanie vecí (teda na vstupe bude pre každé miesto určené, kam chceme prehodiť vec, ktorá na ňom je) a vypíše program pre Poprehadzovávač, ktorý keď sa K -krát zopakuje, prehádza veci tak, ako chceme. Ak sa to náhodou nedá, program by mal o tom podať vhodnú správu.

Príklad:

Vstup:

$N = 3$, $K = 2$

chceme prehodiť: $1 \rightarrow 2$, $2 \rightarrow 3$, $3 \rightarrow 1$

Výstup:

program: $1 \rightarrow 3$, $2 \rightarrow 1$, $3 \rightarrow 2$

(Vec, ktorá leží na prvom mieste, pri prvom prehadzovaní poputuje na miesto 3 a odtiaľ v druhom kole na miesto 2, kde aj mala skončiť. Podobne pre ostatné dve veci.)

Vstup:

$N = 4$, $K = 3$

chceme prehodiť: $1 \rightarrow 1$, $2 \rightarrow 3$, $3 \rightarrow 4$, $4 \rightarrow 2$

Výstup:

nedá sa

3. O Rômeovi a Juliäi

15 bodov

Bolo raz jedno mestečko. A v tom mestečku bol raz jeden Rômeo. A div sa svete bola aj Juliä. No a čo že by to už bol za príbeh, keby neboli spolu v jednom malom útulnom domčeku? A čo už by také mohli robiť, keď nie počítať integrály spojitých funkcií? A ako si tak pekne hrkútajú o existencii druhej derivácie, zrazu sa Rômeo udrie do čela a skríkne: „ABCDEFGH, veď sa už stmieva a matka ma čaká s večerou!“ Juliä sa naňho pozrie pohľadom plným pobavenia a hnevu a nežným hláskom na Rômea zvrieskne: „Ty papľuh, matka ti je prednejšia ako hyperbolické funkcie?“ „Ale...“, namietne Rômeo. „Neprerušuj ma! Máš šťastie, že mňa matka tiež čaká s večerou, inak by bol medzi nami koniec.“

Po chvíli búrlivej výmeny argumentov a návratových hodnôt sa dohodli, že pôjdu domov tak, aby išli čo najdlhší kus cesty spolu. Ale pretože sa tvária, že sa ponáhľajú, tak pôjdu tak, aby sa obaja stále približovali k svojmu domovu.² Nakoľko Rômeo a Juliä nemajú skúsenosti s hľadaním optimálnych ciest, tak si znova začali zúfať, lebo nevedia, ktorou uličkou sa vydať. Buďte tak milí a pomôžte im. Určite viete, čo je to nahnevaná mamina...

Úloha: Je zadané N – počet domčekov v mestečku a M – počet uličiek medzi nimi. Na druhom riadku sú čísla A, B, C – A je Juliäin domček, B Rômeov a C je domček, kde sa

²Teda aby sa najkratšia vzdialenosť od obidvoch ich domov stále znižovala.

nachádzajú. Na ďalších M riadkoch sú trojice čísel X, Y, Z . Tieto nám hovoria, že domček X je spojený s domčekom Y obojsmernou ulicou kladnej dĺžky Z . Nájdite dĺžku najdlhšej cesty, ktorú môžu Rômeo s Juliäou spolu prejsť, ak sa každou uličkou, ktorou prejdú, musia zároveň priblížiť ku svojim domčekom.

Príklad:

Vstup:

4 5
1 2 3
1 3 3.8
2 3 3.1
1 4 2.5
2 4 2.4
3 4 2.3

Výstup:

2.3

4. O klinco

15 bodov

Náš malý nezbedník Mirko bol cez leto na prázdninách u babky a dedka. Najviac sa mu páčilo v dedkovej dielni, kde trávil veľa času. Naučil sa pracovať s kladivom, skrutkovačom alebo kliešťami. Najviac sa mu však páčila píłka na železo. Našiel kúsok plechu a vyrezal z neho namakaný pliešok, z dialky pripomínajúci žabu. Keď už mal pliešok, tak sa šiel poobzerať do záhrady. Zrazu vidí, ako zo zeme trčí klinec. Skoro naňho stúpil!

Klinec sa mu veľmi páčil a tak skúsil položiť pliešok vodorovne na klinec tak, aby nespadol, teda zostal vo vodorovnej polohe. Skúšanie však veľmi rýchlo vzdal, lebo pliešok mu vždy spadol. Preto chce, aby ste mu pomohli. Pliešok má tvar mnohouholníka a je všade rovnako hrubý.

Úloha: Na vstupe je číslo N , udávajúce počet bodov plieška, za ním nasleduje N dvojíc (x_i, y_i) , ktoré určujú postupne po obvode súradnice N vrcholov mnohouholníka. Vašou úlohou je nájsť bod, v ktorom sa má pliešok dotýkať klinca tak, aby nespadol. Ak taký bod neexistuje, vypíšte o tom správu.

Príklad:

Vstup:

$N = 4$
0 0
1 0
1 1
0 1

Výstup:

0.5 0.5

5. Opäť dešifrovať?!

12 bodov

Zase raz tu pre vás máme úlohu, v ktorej dostanete zašifrovaný text a máte ho dešifrovať. Ale aby to nebolo také trápne jednoduché, povieme vám k tomu trochu tej matiky. Tentokrát totiž zadanú šifru pravdepodobne ručne dešifrovať nezvládnete.

Majme nejaký jav, ktorý nastáva s pravdepodobnosťou p . Hodnotu $\lg(1/p)$ (kde $\lg$ je logaritmus so základom 2) nazveme *prekvapením* z toho, že jav p nastal. (Čím je táto hodnota väčšia, tým je prekvapujúcejšie, že tento jav nastal.)

Napríklad keď hodím tromi mincami, šanca, že padnú samé znaky je $1/8$, prekvapenie z toho, že tento jav nastal, je $\lg(1/(1/8)) = \lg 8 = 3$.

Silným nástrojom kryptológov je štatistika. Prvé a najpriamočiarejšie, čo môžeme urobiť, je spočítať si frekvencie výskytov jednotlivých písmen. Zoberieme dosť veľký text a spočítame, ako často sa v ňom ktoré písmeno vyskytuje. Väčšinou zistíme, že najčastejšie sú samohlásky. (V slovenčine je to A, v češtine a anglosaských jazykoch je to E.)

Jednou z najjednoduchších šifier je substitučná šifra. Tej princíp je taký, že si zvolíme nejakú náhodnú permutáciu množiny písmen. Následne v otvorenom texte každé písmeno nahradíme jeho obrazom. Teda napríklad namiesto každého A napíšeme K, namiesto každého L napíšeme F, namiesto každého Z bude A, atď.

Keď sa snažíme dešifrovať substitučnú šifru, vieme na základe frekvencií písmen odhadnúť napríklad ktoré znaky sú zašifrované samohlásky, dokonca si podľa frekvencií jednotlivých znakov vieme pomerne spoľahlivo tipnúť jazyk, v ktorom je pôvodný text napísaný.

Ak by sme ale chceli počítač naučiť riešiť substitučné šifry, toto zďaleka nestačí. My vieme zvoliť konkrétne samohlásky a spoluhlásky tak, aby nám slová dávali zmysel, ale počítač nie. Potrebovali by sme mu nejako vysvetliť, ktorý výsledok vyzerá dobre a ktorý nie.

Jednou možnosťou je použiť wordlist, teda zoznam slov. Dobré budú také výsledky, v ktorých je veľa slov z nášho zoznamu. Ukážeme si ešte jednu, v praxi o dosť spoľahlivejšiu metódu, založenú na štatistike.

Zoberieme dostatočne veľkú vzorku textu písaného v nejakom jazyku a pre každú štvoricu po sebe idúcich písmen (odborne zvanú *tetragram*) si spočítame, koľkokrát sa v ňom vyskytuje. Na základe týchto údajov vieme pre každý tetragram odhadnúť pravdepodobnosť, s akou sa vyskytuje v texte.³ Teraz vieme povedať, že riešenie šifry je tým lepšie, čím menej je prekvapujúce, že je písané v danom jazyku. (Teda pre daný reťazec N písmen, ktorý dostaneme, sčítame prekvapenie pre všetkých $N - 3$ jeho tetragramov.)

No, dosť bolo návodu, tu je zadanie, dešifrujte ho. A ak si pri riešení nebodaj napíšete nejaký program, pošlite nám aj ten.

```
misof izntq ymios nvqvs cikdn rwpin lgvya ixsvr rsini kkitf icxai nicfr aitvx xfire pvxdz
ixucs inrec iligf mirwp ucinc linic xivyk lvaic rfsir fdrfv ntinq inoin nfrcw psciu vpxxi
pzyxl sizuv xsini nifuv inrwp icxfi cxoci guicf inixf kinxf dsini cpyl igrp nqcig rficg
inui xinic xixrw puini xnywt rvwtr wpgie eixzy rrkyn nicwp yxsvn zlcgf svrri gaiic xizyx
oiinr wpicx ficxi znicw pixri pnqci gtgic xinv ricxi zvnzi xkyna vriav ggrec iginl cgfv
rdaic icxin eiwpr fnvpx irfic linfr cwpsv rlixy pgrcw pzipn vxrfn ixlix oyzyr rixui rpvga
sinav ggrwp nyzek fscik nvlis civgg ixics inyzf nicaf agica fvggi nscxl rdkki xuvru vnoyi
nrfsv sinln drria vggds insin inkdg lsixx dasci fnikk rcwpi nixrd lyfrc xsuic gsina vggky
nrcir wpxc zzinl ndrri nuvnd sinin rfsin inkdg lsixa vgguv wprix gvrrf ucrr ixywp scier
hwpdg dlixx cwpf
```

(Hint: Nik nepovedal, že to bude po slovensky...)

³Jeden by čakal, že tento odhad spravíme tak, že počet výskytov daného tetragramu vydáme ich počtom. Nuž, nie celkom. Lepšie je ešte pred delením pridať každému tetragramu jeden výskyt, vyhneme sa tak nepríjemnostiam, ak sa nám v šifre vyskytne podľa našej štatistiky „nemožný“ tetragram.