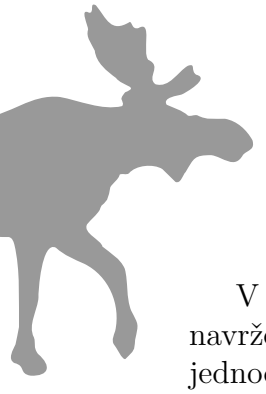
P4 ReMorse

InterLoS 2012

Naučte počítač morseovku! V externím souboru *dataMorse.zip* najdete kódovaný text, který je potřeba přeložit. Výstup se skládá pouze z velkých písmen anglické abecedy a interpunkčních znamének. Kódování je shodné s popisem Morseovy abecedy na wikipedii (http://cs.wikipedia.org/wiki/Morseova_abeceda). Tečka je kódována znakem ".", čárka "-", lomítko "/". Odkud pochází věta v řešení? Heslo je jedno slovo popisující původ této věty.

Externí soubor dataMorse.zip s konkrétním zadáním najdete mezi soubory k sadě.



P5 Losí komprese

InterLoS 2012

V této úloze si představíme jeden zbrusu nový kompresní algoritmus, který je speciálně navržen pro kompresi řetězců, které jsou tvořeny znaky L, O a S. Algoritmus je to velmi jednoduchý a efektivní, leč možná trochu ztrátový. Kdykoliv jsou vedle sebe dva různé znaky (kdekoliv v řetězci), nahradíme je tím třetím znakem. Komprese řetězce 'LOSS' tedy může vypadat následovně: $LOSS \to SSS$ nebo $LOSS \to LLS \to LO \to S$. Jak vidíte, záleží zde na výběru dvojice, kterou nahradíte, takže jeden řetězec může mít mnoho zkomprimovaných podob.

Vašim úkolem je najít délku té nejkratší. Stáhněte si soubor *los.txt*, ve kterém je 10 řetězců. Pro každý spočtěte délku nejkratšího řetězce, který lze dostat opakováním výše zmíněné operace. Jako odpověd na tuto úlohu napište tyto délky za sebou (např. pokud bychom měli jen 3 řetězce a délky by byly 5,2,11, odpověď je „5211“).

Externí soubor los.txt s konkrétním zadáním najdete mezi soubory k sadě.

P6 Prolomení hesla

InterLoS 2012

Kód této úlohy se dozvíte po přečtení následujícího textu:

vlswkfzsilbwdrkkozqcceyffjxuiztmkigvcnzrhyfdrmlpeigkysocbhoswlbuodkuyqqkpxzyhhdrvgjtks

Jak je asi vidět, text je potřeba napřed rozšifrovat :-) Bohužel, klíč se nám ztratil, tak to budete muset zkusit ručně. Vzpomínáme si jenom na to, že někde v textu je „hashovaci“.

Zbytek zadání popisuje použitý šifrovací algoritmus. Kromě tohoto popisu můžete využít i referenční implementaci v jazyce C na adrese http://www.fi.muni.cz/~xbouda2/interlos/crypt-ref.c

Vstupem algoritmu je klíč a text k zašifrování, výstupem je zašifrovaný text. Vstupní i výstupní text jsou tvořeny pouze malými písmeny anglické abecedy. Šifrování probíhá ve dvou základních fázích: v první fázi se vezme klíč a vytvoří se z něj 8bytový haš. V druhé fázi již probíhá samotné šifrování textu pomocí haše vytvořeného v první fázi.

Hašování

Vstupem pro hašování je klíč (libovolný řetězec znaků, označme je $s_1, s+2,' \ldots, s_n$), výstupem pole 8 bytů. Pro účely hašování používáme kódování znaků ASCII (např. pro 'a' je kód 97). Pokud při hašování pracujeme se znaky coby s čísly, myslíme tím implicitně příslušné kódy ASCII. S každým bytem pracujeme nezávisle na ostatních, aritmetické operace provádíme modulo 256 (tzn. pokud by se nějaký výsledek nevešel do rozsahu 0-255, vezme se jeho zbytek po dělení 256). Hašování probíhá ve třech fázích.

V první fázi se definují 4 základní byty, označme je $k0$, $k1$, $k2$, $k3$:

- Byte $k0$ je naplněn součtem všech znaků klíče:

$$k0 = s_1 + s_2 + \ldots + s_n$$

- Byte $k1$ je definován jako exklusivní součet osmých mocnin znaků klíče:

$$k1 = s_1^8 \oplus s_2^8 \oplus \ldots \oplus s_n^8$$

- Byte $k2$ je exklusivním součtem znaků klíče, přičemž ale u každého lichého znaku se vymění 1. a 2. čtveřice bitů (tj. provede se rotace vpravo o 4 bity, značíme $>>> 4$):

$$k2 = (s_1 >>> 4) \oplus s_2 \oplus (s_3 >>> 4) \oplus s_4 \oplus \ldots$$

- Byte $k3$ se zkonstruuje stejně jako $k2$, jen namísto každého lichého znaku se čtveřice bitů vyměňují u každého sudého znaku:

$$k3 = s_1 \oplus (s_2 >>> 4) \oplus s_3 \oplus (s_4 >>> 4) \oplus \ldots$$

POZNÁMKA: *úloha pokračuje na další straně*

P6 Prolomení hesla *(pokračování)*

InterLoS 2012

V druhé fázi se zkonstruované základní byty rotují vpravo dle znaků klíče:

$$r0 = k0 >>> (s_1 + s_5 + s_9 + \ldots)$$
$$r1 = k2 >>> (s_2 + s_6 + s_1 0 + \ldots)$$
$$r2 = k2 >>> (s_3 + s_7 + s_1 1 + \ldots)$$
$$r3 = k3 >>> (s_4 + s_8 + s_1 2 + \ldots)$$

V poslední fázi se z těchto bytů naplňuje osmice výsledných bytů následovně – r_d značí použití pouze dolní poloviny bytu r, a naopak r_h značí použití pouze horní poloviny bytu r (např. pokud $r0$ je 10010111, pak $r0_d$ je 00000111 a $r0_h$ je 10010000):

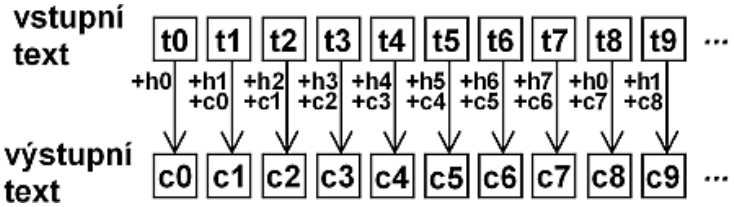
$$h0 = r0_d$$
$$h1 = r1_d >>> 1$$
$$h2 = r2_d >>> 2$$
$$h3 = r3_d >>> 3$$
$$h4 = r0_h$$
$$h5 = r1_h >>> 1$$
$$h6 = r2_h >>> 2$$
$$h7 = r3_h >>> 3$$

Výsledným hašem je osmice bytů $h0, h1, \ldots, h7$.

Šifrování

Šifrování textu pomocí vypočítaného haše již probíhá jednoduše. Bere se postupně znak po znaku vstupního textu a každý se posune o několik pozic. Pracujeme jen nad malými písmeny anglické abecedy, takže např. 'a' + 3 = 'a' + 29 = 'd'. První znak textu se posune o $h0$, výsledný znak označme $c0$. Další znak textu se posune o $h1 + p(c0)$ na $c1$, kde funkce p dává 0 pro 'a', 1 pro 'b', až 25 pro 'z'. Následující znak se posune o $h2 + p(c1)$ atd. Pro 9. znak se opět použije posun o $h0 + p(c7)$, pro 10. znak posun o $h1 + p(c8)$ atd.

Celé šifrování ilustruje následující diagram:

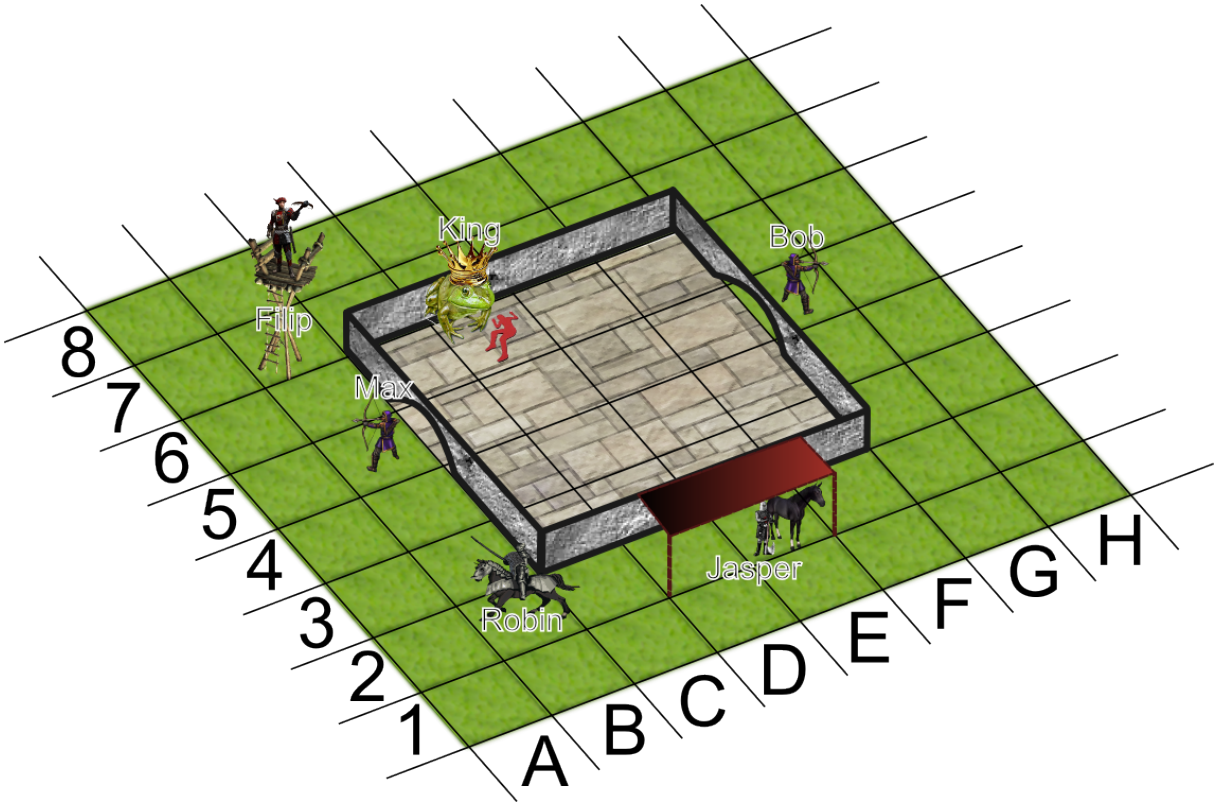


L4 Záhada v královském paláci

InterLoS 2012

Stala se hrozivá věc, vražda v královském paláci. Jen její důkladné vyšetření vás posune dál. Všichni obyvatelé hradu jsou čestní a jejich slova jsou pravdivá, až na jednoho. Kdo lže, ten i vraždí.

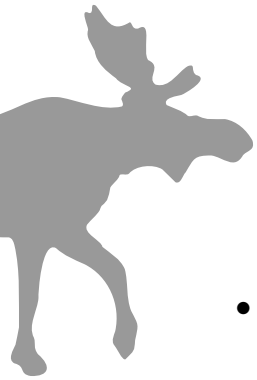
Čas v paláci tiká. Během každého tiku se každý obyvatel může, ale nemusí posunout. Jak? Tak, jak umí. Řešením úlohy jsou zakódované pozice všech přítomných v okamžiku, kdy k vraždě došlo, to jest před třemi tiky. Kódy pište abecedně dle jmen postav, každé pole je kódováno písmenem a číslem [Sloupec,Řada]. Např. Filip má kód B7 a Jasper E2. Nynější rozestavení je na obrázku a jeho kód je G5B7E2D6B5B2.



Výpovědi, co se stalo během posledních tří tiků:

- Bob: Stojím si na stráži na vnějším kraji zahrady, když vidím, jak někdo zapichuje královnu. No, rozběhnu se za ním. Pachatel je však krok napřed, takže když po prvním tiku dojdu na místo činu, on stojí už u brány. Vyrazím k bráně, ale když jsem vyběhl z paláce, nebylo po něm ani stopy.
- Filip: Tak si tu stojím na hlídce a žádného vraha jsem neviděl. Jen když jsem uslyšel křik, Bob hned vběhl do paláce a Max šel za ním, ale nijak nespěchal. Přestože stál na začátku vedle Boba a šel stále k místu činu, neprošel ani bránou. Ve třetím tiku se zpoza rohu vynořil Robin, kůň byl udýchaný, asi celé tři tiky běžel.

POZNÁMKA: *úloha pokračuje na další straně*



L4 Záhada v královském paláci *(pokračování)*

InterLoS 2012

- Jasper: Sedlám si tu svého koně ve stájích, když se zpoza rohu vynoří Robin a očividně spěchá. Normálně by mě to nezajímalo, ale když proběhne kůň, vždycky se za ním otočím. Já ty koně prostě miluji.
- King: V rohu paláce pracuji, kralování je pěkná dřina. Žena mě nijak neohrožovala a měl jsem i prostor, leč minimální, k pohybu. Mohl jsem chodit sem a tam. když najednou slyším, jak mi žena křičí. Zvednu oči, a co nevidím. Žena v kaluži krve a nad ní někdo stojí. Začal jsem se belhat k místu činu, ale zločinec se dal na útěk. Ještě jsem ani nedošel k mé, nyní již bývalé, choti a už byl zlosyn z paláce venku.
- Max: Stojím tu vedle Boba, sehnu se, abych si spravil tkaničky, a Bob najednou nikde. Tak jsem se šel podívat do paláce, co se děje, když nebyl nikdo blízko na povídání. Celou dobu, co jsem na hlídce, po mně koukal Filip z té své věže. Myslím si, že bychom měli mít nějaké právo na soukromí.
- Robin: Chtěl jsem se trochu po zahradách projet, zkusit si, za jak dlouho dojedu z jednoho rohu zahrady do druhého. Po třech ticích mě ale zastavili a začali vyslýchat, tak jsem dalšího rohu ani nedosáhl.

Pro lepší přehlednost je nynější rozestavení dostupné také ve větší velkosti jako pallace.png mezi soubory k sadě.

L5 Logická řada

InterLoS 2012

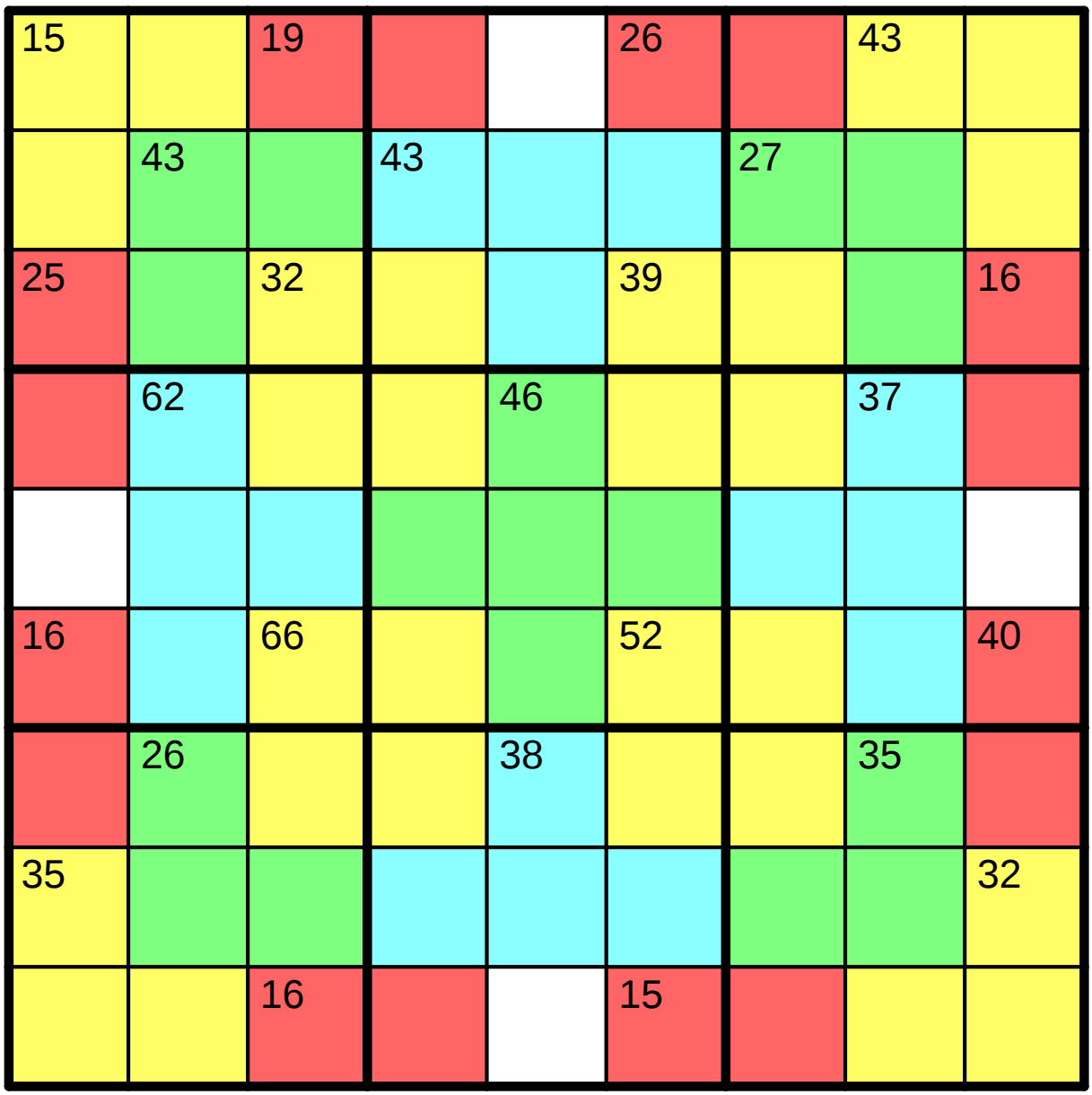
PAF REZ NIT TON ???

L6 Prvočíselné sudoku

InterLoS 2012

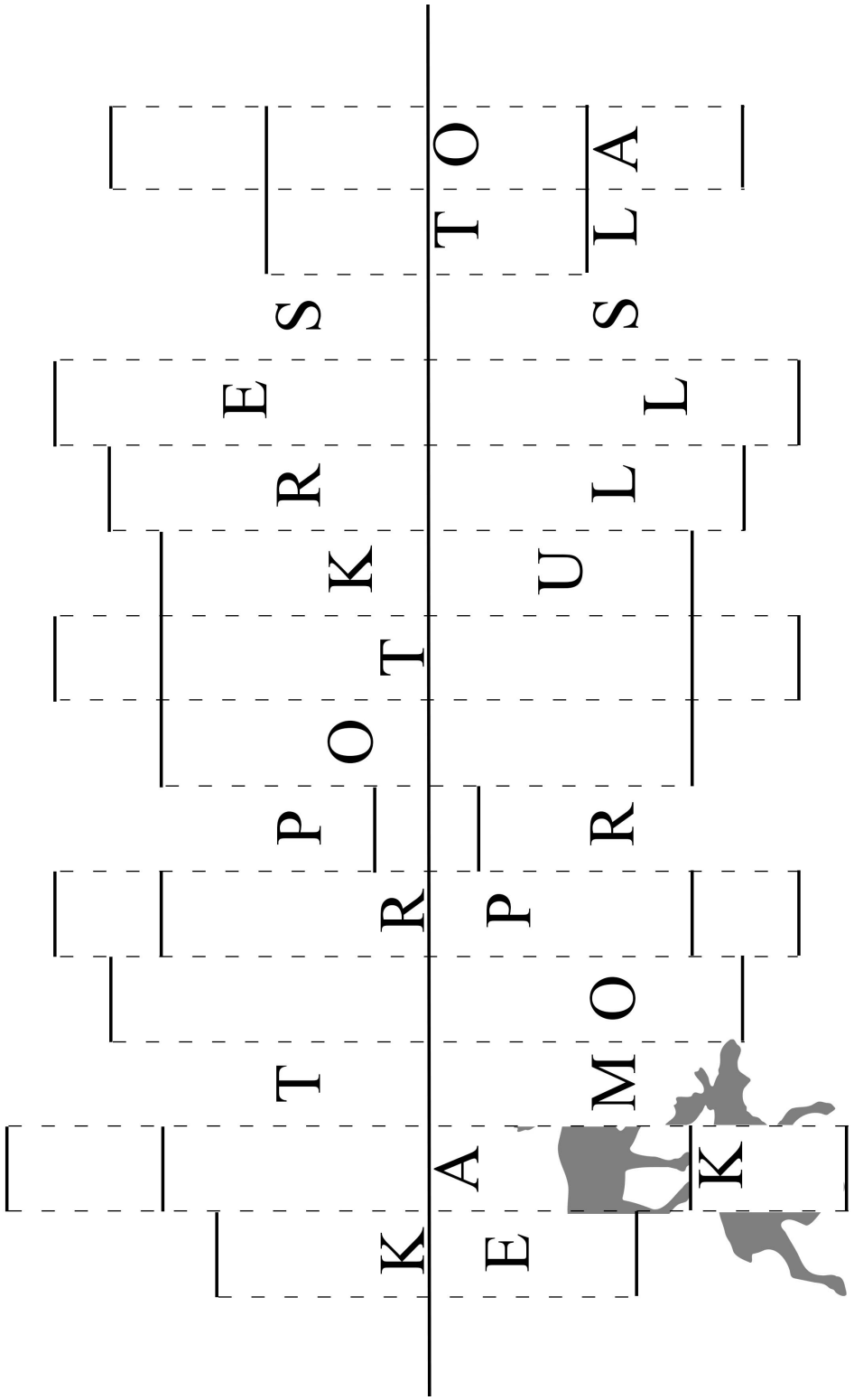
Vepište do každého políčka jedno prvočíslo menší než 25 tak, aby se stejná prvočísla neopakovala v žádném řádku, sloupci ani v devíti vyznačených menších čtvercích. Tabulka je rozdělena na dílky, každý dílek obsahuje navzájem různá prvočísla a vy znáte pouze jejich součet.

Kódem jsou bez mezer po řádcích zapsané čísla z modrých dílků.



S4 Použij nůžky!

InterLoS 2012



S5 Nie som, čo som

InterLoS 2012

Zadanie úlohy je v externom súbore 01.jpg, ktorý nájdete medzi súbormi k sade.

S6 Co chybí?

InterLoS 2012

JA	CILA	JMEN
DANE JMEN	L	CATICE
LCE	TATNE JMEN	CITLCE