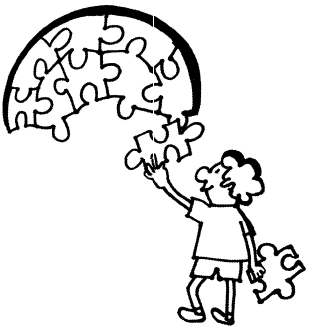
INFORMATIKA

Slovní úlohy o celku a částech

STANISLAV TRÁVNÍČEK

Přírodovědecká fakulta UP, Olomouc



Měla babka čtyři jabka
a dědoušek jen dvě,
dej mi babko jedno jabko,
budeme mít stejně

Slovní úlohy o celku a jeho částech patří k úlohám, s nimiž se žáci tu a tam mohou v učebnicích a sbírkách setkávat. Jedna taková úloha je řešena i v uvedené písničce. Základní typy spočívají v tom, že se z podmínek pro části má určit celek nebo naopak z podmínek pro některé části a pro celek se má určit stanovená část.

Z hlediska matematického nevidíme u slovních úloh o celku a jeho částech přílišnou pestrost, matematickými modely jsou zpravidla lineární rovnice nebo soustavy lineárních rovnic. Složitosti (vesměs uměle zkonstruované) tu najdeme nejspíše v zamotaných podmínkách pro části celku.

Základní úlohy

U těchto úloh je modelem zpravidla jen jedna lineární rovnice o jedné neznámé, jsou přístupné pro žáky ZŠ a jedinou komplikací mohou být jen „zamotané“ vztahy mezi počty prvků v částech celku.

Typ 1.1. Jsou dány relativní podmínky (a jedna absolutní) pro počet prvků částí celku, má se určit počet prvků celku.

Úloha 1.1.1

Pokladník hokejového klubu hlásil tržbu za poslední 4 utkání: „Nebylo to špatné – v 1. utkání jsme získali 1/6 této částky, za 2. utkání 1/4, za 3. pak 1/3 a konečně za čtvrté 24 000 Kč. Celkem to dělá nějak kolem 100 000 Kč.“ Tak nepřesně pokladníci nemají referovat, opravme ho.

Je-li tržba x Kč, máme $x = \frac{x}{6} + \frac{x}{4} + \frac{x}{3} + 24\,000 \Rightarrow x = 96\,000$.

Úloha 1.1.2

Při hodnocení testů bylo 10 % uchazečů hodnoceno známkou 1, 55 známkou 2, 37 % známkou 3 a zbylých 42 % neuspělo. Kolik bylo výborných?

Vypočteme, kolik bylo všech a z toho, kolik bylo výborných.

$$0{,}1x + 55 + 0{,}37x + 0{,}42x = x \Rightarrow 0{,}11x = 55, \quad x = 500,$$

výborných bylo 50.

Typ 1.2. Je dán počet prvků celku a počty nebo relativní počty prvků některých částí, má se určit počet prvků vybrané části.

Úloha 1.2.1

Vedoucí údržby silnic počítá: „Na údržbu silnic jsme si na podzim obstarali 21 tunovou zásobu posypového materiálu. Do konce roku jsme spotřebovali 1/3 zásoby, v lednu 1/4, v únoru 1/5 a v březnu 3t. Kolik nám vlastně ještě zbylo?“

Zbylo x tun.

$$21 \cdot \frac{1}{3} + 21 \cdot \frac{1}{4} + 21 \cdot \frac{1}{5} + 3 + x = 21 \Rightarrow 16{,}45 + 3 + x = 21, \quad x = 1{,}55;$$

zbylo 1,55 tun materiálu.

Úloha 1.2.2

Třída 8.A sebrala 20 kg kovového šrotu, aby získala příspěvek na výlet. Bylo tam 15 % zinku, 25 % mědi, 35 % mosazi; zbytek byl hliník. Kolik kg ho bylo?

Bylo ho x kg: $20 \cdot 0{,}15 + 20 \cdot 0{,}25 + 20 \cdot 0{,}35 + x = 20 \Rightarrow x = 20 \cdot 0{,}25 = 5$, hliníku bylo 5 kg.

Typ 1.3. Jako typ 1.1, ale v podmínkách jsou vazby mezi počty prvků jednotlivých částí, má se opět určit počet prvků celku.

Úloha 1.3.1

Pan ředitel ZŠ je matematik, ale zapomněl, kolik má ve škole žáků. Ví však, že 53 % z nich je ve třídách $1-5$, 14 % je v 6. třídě, 13 % je v 7. třídě, v 8. je o 3 méně než v 7. a v 9. je o 24 méně než v 8. Takže není problém počet žáků jeho ZŠ zjistit.

Žáků je x.

$$x \cdot 0{,}53 + x \cdot 0{,}14 + x \cdot 0{,}13 + (x \cdot 0{,}13 - 3) + (x \cdot 0{,}13 - 3 - 24) = x \Rightarrow$$

$$\Rightarrow x \cdot (1{,}06 - 1) = 30, \qquad x = 500,$$

škola má 500 žáků.

Úloha 1.3.2

Ke svému cíli jelo auto čtvrtinu cesty do kopce, cesta z kopce byla pak o 5 km delší a až zbylých 12 km jelo po rovině. Kolik km ujelo do cíle?

Ujelo x km.

$$\frac{x}{4} + \left(\frac{x}{4} + 5\right) + 12 = x \Rightarrow x = 34;$$

ujelo 34 km.

Typ 1.4. Jako typ 1.2, ale v podmínkách jsou vazby mezi počty prvků jednotlivých částí, má se opět určit počet prvků vybrané části.

Úloha 1.4.1

Vypočtěte velikosti úhlů v trojúhelníku, kde druhý úhel je o polovinu větší než první a třetí úhel o třetinu větší než druhý.

První úhel má velikost α. Součet úhlů v trojúhelníku (tj. „počet prvků“ v celku) je 180°.

$$\alpha + \frac{3}{2}\alpha + \frac{3}{2} \cdot \frac{4}{3}\alpha = 180 \Rightarrow \alpha = 40;$$

úhly v trojúhelníku mají velikost 40°, 60°, 80°

Úloha 1.4.2

Letěla husa a potkala hejno hus: „Ahoj sto husí!“ zvolala. Husa vedoucí hejno jí však odpověděla: „Kdepak sto, kdyby nás bylo ještě jednou tolik a ještě polovina našeho počtu a ještě čtvrtina z nás a ještě ty, huso, kdybys letěla s námi, to by nás bylo sto, ale takhle ne!“ Kolik hus bylo v hejnu?

Za celek považujme 100 hus, hledanou část (počet hus v hejnu) označíme x.

$$x + x + \frac{x}{2} + \frac{x}{4} + 1 = 100 \Rightarrow \frac{11}{4}x = 99, \quad x = 36;$$

v hejnu bylo 36 hus.

Jak početné jsou jednotlivé množiny

Tyto úlohy vedou zpravidla na řešení soustav lineárních rovnic, tj. modelem jsou soustavy rovnic o více neznámých.

Typ 2.1. Máme 2 druhy objektů, údaj o jejich celkovém počtu a o celkovém počtu jistých charakteristik těchto objektů.

Úloha 2.1.1

Na dvorku pobíhali králíci a slepice, bylo jich celkem 23 a měli dohromady 60 nohou. Kolik bylo kterých?

Označme x ... počet králíků, y ... počet slepic

$$\begin{aligned} x + y &= 23 \\ 4x + 2y &= 60. \end{aligned}$$

Řešení soustavy dává $[x; y] = [7; 16]$, bylo tak 7 králíků a 16 slepic. (Charakteristika – počet nohou jedince.)

Úloha 2.1.2

Na rodinnou oslavu bylo nakoupeno za 540 Kč celkem 5 kg masa, hovězího po 150 Kč/kg a vepřového po 90 Kč/kg. Kolik kterého bylo nakoupeno?

Koupilo se h kg hovězího a v kg vepřového;

$$\begin{aligned} h + v &= 5 \\ 150h + 90v &= 540 \quad (5h + 3v = 18) \end{aligned}$$

Řešení soustavy dává $[h; v] = [1,5; 3,5]$, bylo koupeno 1,5 kg masa hovězího a 3,5 kg vepřového. (Charakteristika – cena 1 kg masa.)

Typ 2.2. Máme 2 nebo více druhů objektů, údaj o celkovém počtu objektů a údaje svazující počty jednotlivých druhů objektů. Určit počty objektů jednotlivých druhů.

Úloha 2.2.1

Na besedu o volbě povolání pro rodiče a žáky přišlo 48 osob. Maminek bylo o 4 více než tatínků a žáků 9. tříd o 6 méně než polovina dospělých. Kolik bylo kterých?

Maminek bylo m, tatínků t a žáků z.

$$\begin{aligned} m + t + z &= 48 \\ m &= t + 4 \\ z + 6 &= (m + t) \end{aligned}$$

Řešení soustavy dává $[m; t; z] = [20; 16; 12]$; bylo přítomno 20 maminek, 16 tatínků a 12 žáků.

Úloha 2.2.2

Zahradník měl v sadu 60 stromů, jabloně, hrušně a třešně. Jabloní měl o 10 víc než hrušní a třešní dohromady, hrušní o 4 víc než je dvojnásobek třešní. Kolik kterých měl stromů?

Jabloní měl j, hrušní h a třešní t.

$$\begin{aligned} j + h + t &= 60 \\ j &= h + t + 10 \\ h &= 2t + 4 \end{aligned}$$

Řešení soustavy dává $[j; h; t] = [35; 18; 7]$; měl v sadu 35 jabloní, 18 hrušní a 7 třešní.

Počet prvků dvou množin zjišťovaný na základě dvojího porovnání

Modelem těchto úloh bývají lineární rovnice nebo soustavy.

Typ 3.1. Porovnáváme a zjišťujeme počty prvků dvou množin před změnami a po změnách.

Úloha 3.1.1

V tanečních bylo chlapců o 2 méně než dívek. Když však přišlo ještě 6 chlapců a počet dívek se zvětšil o jednu třetinu, bylo obojích stejně. Kolik párů vytvořili?

Původně chlapců x, dívek y.

$$x + 2 = y$$
$$x + 6 = \frac{4}{3}y$$

Řešení soustavy dává $[x; y] = [10; 12]$; pak přibylo 6 chlapců a 4 dívky, takže vytvořili 16 párů.

Úloha 3.1.2

Zemědělský závod sklidil ze dvou lánů 500 tun pšenice. V příštím roce byla úroda na 1. lánu o 30 % a na 2. lánu o 20 % vyšší, takže získali 650 t pšenice. Kolik tun sklidili na kterém lánu?

Na 1. lánu v 1. roce sklidili x tun, na 2. lánu y tun.

$$x + y = 500$$
$$1{,}3x + 1{,}2y = 650$$

Řešení soustavy dává $[x; y] = [300; 200]$; pak $[390; 240]$; na 1. lánu bylo sklizeno 300 resp. 390 tun pšenice, na 2. lánu 200, resp. 240 tun.

Typ 3.2. Zjišťujeme počty prvků dvou množin pomocí jejich různého uspořádání.

Úloha 3.2.1

Chlapci z 8.A se chtěli složit na kopací míč. Zjistili, že příspěvek 26 Kč na každého je malý, chybělo by jim 84 Kč, ale 32 Kč na žáka už stačí a ještě jim zbude 12 Kč. Kolik je žáků a kolik stojí míč?

Žáků je x, cena míče je y.

$$26x = y - 84$$
$$32x = y + 12$$

Řešení soustavy dává $[x; y] = [16; 500]$; na míč se skládá 16 žáků, míč stojí 500 Kč.

Úloha 3.2.2

V prvním sudu bylo o 2 litry benzínu méně než ve druhém. Když však z druhého sudu přelijeme do prvního 25 litrů, bude v prvním ještě o litr

více než je dvojnásobné množství toho, co zůstane ve druhém. Kolik máme benzínu?

V prvním sudu původně x litrů, ve druhém y litrů.

$$x + 2 = y$$
$$x + 25 = 2(y - 25) + 1$$

Řešení soustavy dává $[x; y] = [70; 72]$; máme 142 litrů benzínu.

Jiné

Náš výčet typů úloh je jen orientační, nedělá si ani nároky na úplnost. Svět matematických úloh je velmi pestrý, ale ukázali jsme, že přece jen některé skupiny úloh něco svazuje zejména princip řešení a jeho matematický model. Na závěr uveďme ještě jinou úlohu a můžeme – chceme-li – uvažovat, zda by se vešla do některého z výše uvedených typů, např. 2.1.

Úloha 4.1

V 9. třídách prospělo v pololetí 96 % žáků 9. tříd; dívky všechny, ale z 22 chlapců prospělo jen 20. Kolik dívek je v 9. třídách?

Dívek je x.

$$\frac{20 + x}{22 + x} = \frac{96}{100}$$

Řešením je číslo 28; v 9. třídách je 28 dívek.

Programové řešení

Naším cílem je nyní vytvoření krátkého a jednoduchého počítačového programu, s jehož pomocí lze řešit některé typy úloh o celku a částech. Jestliže si z tohoto hlediska projdeme jednotlivé typy úloh, vidíme, že se nabízejí první dva typy úloh, k nimž lze vstupy do značné míry standardizovat. Tuto standardizaci provedeme tak, že pro části bude vstupem *hodnota* této části nebo *kolik procent celku* má tato část. U úloh 2. typu pak lze zadávat *velikost celku*.

V programu zvolíme v proměnné *Pocet* počet částí, indexy částí jsou $K = 1, \ldots,$ *Pocet* a celek má index *Pocet* +1.

U každé zadávané části bude vstup tvořen dvěma údaji, *kódem druhu údaje* (pro K-tou část celku je dále označován `Co[K]` typu Char) a *hodnotou údaje* (dále označovanou `C[K]` typu Real). Budeme pracovat se třemi kódy:

„%“ udává, že následující hodnota `C[K]` je počet procent K-té části z celku,

„–“ udává, že následující hodnota `C[K]` znamená velikost části,
„?“ udává, že velikost této části je neznámá (úlohy 2. typu).

(Z důvodu jednoduchosti programu fungují všechny znaky kromě „%“ a „?“ stejně jako znak „–“.) U celku se v případě úloh 1. typu předpokládá implicitně „?“, u úloh 2. typu „–“. Při zadávání vstupů je tedy třeba informace typu „část tvoří 1/3 celku“ transformovat na procenta, např. na 33,33 %.

Při zadávání údajů o částech program akumuluje do proměnné SH hodnoty částí (jsouli zadány) a do SP počty procent. U úloh 1. typu, je-li X neznámá velikost celku, pak platí

$$X = SH + X \cdot \frac{SP}{100}$$

a z toho

$$X = \frac{100 \cdot SH}{100 - SP}.$$

U úloh 2. typu je X neznámá velikost části a je zadána ještě velikost celku, označme ji zde C, takže

$$C = X + SH + C\frac{SP}{100}$$

a z toho

$$X = C - SH - C\frac{SP}{100}.$$

Výsledek se tiskne na řádek (s indexem KK), na němž byl zadán otazník.

```
Ulohy o celku a castech

Pocet casti: 4

1. cast, zadej (%,-,?) % hodnota: 16.67
2. cast, zadej (%,-,?) % hodnota: 25
3. cast, zadej (%,-,?) % hodnota: 33.33
4. cast, zadej (%,-,?) - hodnota: 24000
celek                  ?          96000
```

Obr. 1. Řešení úlohy 1.1.1.

```
Ulohy o celku a castech

Pocet casti: 5

1. cast, zadej (%,-,?) % hodnota: 33.33
2. cast, zadej (%,-,?) % hodnota: 25
3. cast, zadej (%,-,?) % hodnota: 20
4. cast, zadej (%,-,?) - hodnota: 3
5. cast, zadej (%,-,?) ?          1.55
celek                  hodnota: 21
```

Obr. 2. Řešení úlohy 1.2.1.

```
program CCasti;
uses Crt;

const
  PocetCasti = 10;

var
  K, KK, Pocet, Radek: Integer;
  Co: array [1..PocetCasti] of Char;
  C: array [1..PocetCasti] of Real;
  X, SH, SP: Real;

begin {program}
  ClrScr; TextAttr := 15; WriteLn;
  WriteLn('  Ulohy o celku a castech');
  WriteLn; TextAttr := 7;
  Write('  Pocet casti: ');
  ReadLn(Pocet); WriteLn;
  K := 0; KK := 0; SP := 0; SH := 0;
  repeat                        {cyklus zadani casti a celku}
    Inc(K);
    GotoXY(3,K+5);
    if K <= Pocet then             {rozliseni casti a celku}
    begin
      Write(K,'. cast, zadej (\%,-,?) ');
      Co[K] := ReadKey                          {kod polozky}
    end
    else begin
```

```
      Write('celek');
      if (KK>0) then Co[K] := ''
      else begin
        Co[K] := '?'; KK := Pocet+1
      end
    end;
    GotoXY(26,K+5); Write(Co[K]);
    if not (Co[K] = '?') then       {podminka cteni hodnoty}
    begin
      GotoXY(28,K+5);
      Write('hodnota: ');
      ReadLn(C[K])                          {hodnota polozky}
    end;
    if K <= Pocet then
    case Co[K] of                         {akumulace polozek}
      '%': SP := SP + C[K];
      '?': KK := K;
      else  SH := SH + C[K]
    end;
  until K = Pocet+1;                            {konec cyklu}

  if (KK <= Pocet) then                    {vypocet nezname}
    X := C[K] - SH - C[K]*SP/100
  else
    X := SH*100/(100-SP);
  GotoXY(37,KK+5); TextAttr:=14;               {tisk nezname}
  if Abs(Int(X)X) < 0.005 then WriteLn(X:3:0)
  else WriteLn(X:5:2);
  TextAttr := 7; WriteLn; ReadLn
end. {program}
```

(Autorkou úvodní ilustrace je Mgr. Jaroslava Čermáková.)

Počítačová bezpečnost ve výuce informatiky

(1. část – Tvorba hesel a steganografie)

MICHAL MUSÍLEK – ŠTĚPÁN HUBÁLOVSKÝ.

Přírodovědecká fakulta Univerzity Hradec Králové

V této části článku se zaměříme na dvě oblasti – na metodiku tvorby vhodných přístupových hesel a na způsoby ukrývání zpráv – ve smyslu skrytí existence tajné zprávy (často v rámci jiné zprávy). *Kryptologie* jako součást učiva informatiky má obrovskou výhodu v tom, že přirozeně vybízí k budování mezipředmětových vztahů s mateřským jazykem, cizími jazyky, matematikou, dějepisem a výchovou občana demokratické společnosti.

Informační společnost

V současné době se bouřlivě mění význam pojmů používaných v rámci informatiky, ať jako vědní discipliny, či jako vyučovacího předmětu. Přestáváme používat pojem výpočetní technika zajisté i proto, že jen malá část uživatelů osobních počítačů je používá k výpočtům, a nahrazujeme jej pojmem informační a komunikační technologie, protože mnohem častěji lidé používají počítače k získávání, filtrování a uspořádání informací a ke vzájemné komunikaci.

Moderní způsoby komunikace mají proti klasickým způsobům řadu výhod. Nejvýraznější je určitě rychlost, protože e-mail putuje internetem nanejvýš několik sekund, zatímco klasický dopis pošta doručí za jeden až několik dní od jeho podání. Má však také své nevýhody. Zde se nám jako nejvýraznější nevýhoda jeví potenciální ztráta soukromí, protože odposlech elektronické komunikace (pokud není šifrována) je technicky mnohem jednodušší než zachycování klasické korespondence. Elektronický odposlech lze navíc snadno maskovat (originální zprávu odposlech nijak nenaruší), automatizovat a nasazovat v masovém měřítku.

Kontrola společnosti nad rozsahem a zaměřením odposlechů ať již ze strany organizovaného zločinu, přehnaně aktivních marketingových společností, konkurenčních firem, či vládou zřízených institucí (policie, rozvědka,

atd.) je nutnou podmínkou správného fungování demokratické společnosti. Proto by se již žáci druhého stupně základní školy měli vhodnou formou seznamovat s prvky počítačové bezpečnosti, a to včetně základů kryptologie.

Tvorba hesel

U mnoha lidí jsme se setkali s velmi rozšířenými nešvary při vytváření a používání hesel. Jedná se zejména o používání jednoho hesla pro řadu přístupů k programům s rozdílnou četností a důležitostí použití. Představme si například, že máme stejné heslo k e-mailovému účtu a k rozhraní internetového bankovnictví. K e-mailu přistupujeme poměrně často a naše heslo (zvlášť je-li snadno uhodnutelné) může útočník (člověk, který nám chce ublížit, okrást nás apod.) odpozorovat. Pak v okamžiku, kdy získal heslo k e-mailu, získal zároveň heslo i k našemu kontu.

Dalším rozšířeným nešvarem je používání snadno uhodnutelných hesel. Lidé často místo skutečného hesla použijí své křestní jméno, jeho zdrobnělinu, přezdívku. Zejména ženy často použijí křestní jména svých dětí, svého partnera, či domácího mazlíčka. Jména blízkých zkušený útočník vyzkouší jako první a snadno takové heslo – neheslo prolomí. Jinými častými nekvalitními hesly (nehesly) jsou sekvence po sobě jdoucích číslic (12345), písmen (ABC, efgh, xyz), sekvence písmen tak, jak jsou vedle sebe na klávesnici (qwertz, uiop), nebo jejich jednoduché kombinace (ABC123).

Pokud chceme tvořit skutečně silná hesla, která nám poskytnou dobrou ochranu, je lépe se úplně vyhnout slovům, která dávají smysl. Proč? Jedním z důvodů je např. výrazné snížení možnosti odpozorování hesla ve chvíli, kdy ho vyťukáváme na klávesnici. Jiným je obrana proti tzv. slovníkovému útoku. Zkušený útočník neodpozoroval celé naše heslo, ale všiml si např., že začíná písmenem „A“ a celková délka hesla je 7 znaků. Vezme připravený slovník českých slov a z něj vyfiltruje všechna slova začínající na „A“ s délkou 7 písmen. Pak už jen zkouší jedno po druhém, buď ručně, nebo automaticky pomocí připraveného software.

Ujasnili jsme si, jak by hesla neměla vypadat. Existuje ale nějaký jednoduchý návod, jak silná a přitom snadno zapamatovatelná hesla vytvářet? Naštěstí ano. Dokonce je takových možností několik. Jako základní doporučujeme žáky naučit obměnu systému, který popisuje jako jeden z možných (Pavel Vondruška [3]). Heslo můžeme vytvářet na základě textu oblíbené písničky, básně, přísloví, bonmotu apod. Jednodušší varianta vytvoří heslo pomocí prvních písmen každého ze slov textu. Ve složitější variantě bu-

deme rozlišovat slova podle slovního druhu, ke kterému patří, a pro některý slovní druh použijeme např. velká písmena namísto malých, nebo číslo označující pořadí písmene v abecedě namísto tohoto písmene apod. Pokud jde o pořadí písmene v abecedě, můžeme volit mezi anglickou abecedou (pouze písmena bez diakritiky) a českou abecedou, případně místo prostého pořadí v abecedě použít ASCII kód písmene.

Příklad tvorby hesla

Text pro zapamatování hesla:	Znám křišťálovou studánku, kde nejhlubší je les, tam roste tmavé kapradí a vůkol rudý vřes.
Heslo – jednodušší varianta:	zksknjltrtkavrv
Heslo – složitější varianta:	z11Sk14jLtr20Kav18V

U složitější varianty jsme použili pro podstatná jména velké písmeno a pro přídavná jména pořadí písmene v anglické abecedě. Žáky bychom ovšem upozornili, že volba slovních druhů, kterým „přidělili“ velká písmena, či pořadí v abecedě, závisí jen na nich. Stejně tak, zda pořadí budou psát s tečkou (jako řadovou číslovku), či bez tečky, zda pořadí menší než 10 budou psát jednou číslicí, nebo s nulou na začátku apod. Existuje celá řada obměn.

Při tvorbě hesel je ve výhodě člověk, který má koníčka, v němž je zvyklý pravidelně cvičit paměť. Ten, kdo rád zpívá či recituje, má zásobu textů pro vytváření hesel výše popsaným způsobem. Šachista může jako hesla využívat zásobu svých oblíbených zahájení, či problémů, opět v různých variantách (úplná notace, zkrácená notace). Ten, kdo se učí cizí jazyk, zvlášť jedná-li se o jazyk méně frekventovaný, může hesla sestavovat pomocí slovíček z tohoto jazyka, která vhodně doplní o čísla (např. španělské slovíčko doplní o čísla vyjadřující pořadí prvních dvou písmen českého překladu slovíčka). Žáci jistě dokážou sami vymyslet nějaký další systém. Cílem vzdělávání žáků v této oblasti počítačové bezpečnosti by mělo být vybudování zodpovědného a pečlivého postoje k tvorbě, ochraně a používání hesel. Žáci by si měli uvědomovat, že hesla představují klíče, které chrání jejich soukromí, jejich cenné informace a často i jejich pravomoci a peníze.

Steganografie

Steganografie je jednou ze tří součástí kryptologie. Kryptologie je věda o utajení obsahu zpráv. Lze ji rozdělit na kryptografii, kryptoanalýzu a ste-

ganografii. Kryptografie se zabývá matematickými metodami se vztahem k prvkům informační bezpečnosti, jako je zajištění důvěrnosti zprávy, integrity (neporušenosti) dat, autentizace subjektu (ověření totožnosti) a původu dat (autorství), a to včetně zkoumání silných a slabých stránek a odolnosti vůči různým typům útoků [3]. V dřívějším užším chápání šlo o vědní disciplinu, zabývající se návrhem a používáním šifrovacích systémů. Jejím úkolem tedy bylo učinit výslednou zašifrovanou zprávu nečitelnou pro nepovolané osoby i v situaci, kdy je zachycena a v plném rozsahu prozrazená. Opakem kryptografie je kryptoanalýza, která hledá metody proniknutí do šifrovacích systémů, umožňující jejich rozluštění i bez předchozí znalosti šifrovacího systému, hesla použitého k šifrování apod. Steganografie má blíže ke kryptografii, ale liší se od ní metodou ukrývání. Zatímco cílem kryptografie je skrytí obsahu zprávy, i v případě, že byla zachycena, úkolem steganografie je skrytí samotné existence zprávy (často jako součásti jiné zprávy s méně důležitými informacemi), tedy zjednodušeně řečeno její „zneviditelnění“. Při použití steganografických metod může být zpráva předávána ve srozumitelné podobě, ale útočník nesmí poznat, že je zpráva vůbec předávána.

Již staří Řekové ...

Mezi nejstarší zaznamenané metody patří dvě, které popsal Hérodotos ve svých Dějinách. Obě se udály v době válek s Peršany. První spočívala v tom, že zprávu napsal odesilatel, jménem Histiaeus, svému otroku na hlavu, kterou mu předtím pečlivě oholil. Když otroku dorostly vlasy, vydal se na cestu do Milétu, kde svými informacemi pomohl připravit povstání proti Peršanům [4]. Je vidět, že ve starověku na nějakém tom týdnu prodlení nezáleželo, protože čekání na dorůstání přiměřeně dlouhých vlasů jistě nějakou dobu trvalo.

Druhý případ se udál roku 480 př. n. l. zhruba takto: Řek Demaratus, který žil v perském městě Susy ve vyhnanství, ale přesto byl loajální vůči svým krajanům, zpozoroval válečné přípravy Peršanů a zjistil, kdy hodlá král Xerxes vytáhnout s armádou proto Spartě. Rozhodl se poslat zprávu, ale kdyby ji vyryl běžným způsobem do vosku na psacích destičkách, dopis by s největší pravděpodobností padl Peršanům do rukou, takže by nedorazil do cíle a stal by se důkazem proti němu. Demaratus proto seškrábal vosk ze dvou psacích destiček, sepsal Xerxovy záměry přímo na jejich dřevo a potom zprávu znovu zakryl voskem. Tabulky byly na první pohled prázdné a nevzbudily zájem stráží. Ve Spartě nejprve nevěděli co

s nimi, ale pak Gorgó, manželka krále Leónida, uhodla, oč jde a dala seškrábat vosk. Řekové se tak mohli na Xerxův útok dobře připravit a Peršané ztratili moment překvapení [2].

V českých dějinách se také objevují zmínky o utajené komunikaci. Mistr Jan Hus psal z vězení Kostnici dopisy svým věrným Čechům. Jejich existenci však nebylo možné utajit, takže steganografické metody nemohl použít a použil jednoduchou substituční šifru [1]. Šiframi se však budeme zabývat až příště, takže potom se k dopisům z Kostnice vrátíme podrobněji.

Ke klasickým steganografickým metodám patří také použití nejrůznějších neviditelných inkoustů, které lze zviditelnit zahřáním, chemickou reakcí, nebo UV zářením [3]. Rozšířenou steganografickou metodou bylo také označování písmen ukryté zprávy v otevřeném textu tečkami či nepatrnými vpichy jehlou, nebo tzv. agenturní systémy založené na dohodnuté pozici písmene ve větě (např. třetí písmeno každého prvního slova v jednotlivých větách). Všimli jste si slabých čárek pod některými písmeny v tomto odstavci?

Počítačová steganografie

Běžný aplikační software nám umožňuje vytváření poměrně rafinovaných steganografických dokumentů. Můžeme s nimi seznámit již žáky druhého stupně základní školy, podobně jako s tvorbou hesel.

Jedna z metod spočívá ve vepisování neviditelných řádků mezi běžný text. Běžně píšeme text písmem velikosti 12 pt s řádkováním 1,5 a za odstavce vynecháváme mezeru o výšce 6 pt, nebo 10 pt. Tuto mezeru můžeme snadno využít pro ukrytí tajné zprávy. Zmenšíme mezeru za odstavce na 0 pt a tajný text napíšeme za odstavec do samostatného řádku drobným písmem o velikosti 6 pt. Pokud se příjemci zprávy špatně čte drobný text, není problém, aby si jej pro čtení zprávy zvětšil. Takto napsaný text označíme a zvolíme barvu textu bílou. Bílé písmo na bílém papíře není vidět, zpráva je ukryta. Musíme si ovšem dát pozor, aby v textu nebyly pravopisné chyby. Nestandardně umístěná červená vlnovka označující slovo s chybou by mohla ukrytý text prozradit.

Jinou, technicky ještě jednodušší, ale také snáze odhalitelnou metodou je nastavení obtékání textu „Před textem“, které ukryje tajný text za obrázek. Tajný text je možné ukrýt i za konec běžného textu (opět napsaný bílým písmem na bílý papír), ale zde je snáze odhalitelný než v prvním případě. Microsoft Word 2007 obsahuje další zajímavý „steganografický

nástroj“. Tajnou zprávu napíšeme kamkoliv mezi otevřený text. Pak ji označíme jako blok a na záložce „Domů“ zvolíme dialog „Písmo“, ve kterém v nabídce „Styl“ zaškrtneme volbu „Skryté“. Příjemce potom označí celý text dokumentu (Ctrl + A) a vyvolá stejný dialog „Písmo“. Volba „Skrytý“ zde není ani zaškrtnutá ani prázdná, ale menší zelený čtverec uvnitř boxu značí, že část textu je skrytá. Klikneme-li do boxu myší, zaškrtne se a po druhém kliknutí se zaškrtnutí zruší. Potvrzením tohoto nastavení skrytý text zviditelníme.

Jiný typ počítačové steganografie spočívá v napsání otevřeného textu v poznámkovém bloku. Tajný text celý napíšeme a pak uložíme pomocí nabídky „Uložit jako ...“ z menu „Soubor“, kde parametr „Uložit jako typ:“ změníme na „Všechny soubory“. Souboru pak dáme název s příponou označující obrázek, např. „kopretina.jpg“. Takový soubor bude neoprávněná osoba považovat za poškozený soubor s bitmapovou grafikou, zatímco poučený příjemce jej snadno otevře v poznámkovém bloku. Seznámením s touto metodou navíc připomeneme žákům, že operační systém Windows důsledně posuzuje typ souboru podle přípony a na základě asociací jej automaticky otevírá ve zvoleném programu.

Závěr

Steganografické metody jsou poměrně jednoduché na použití. Protože jsou navíc zajímavým způsobem nakládání s informacemi, které chceme utajit před nepovolanýma očima, rozhodně doporučujeme je zařadit do osnov informatiky v rámci školního vzdělávacího programu každé základní školy. Jsme přesvědčeni, že těch několik vyučovacích hodin, které učitel informatiky věnuje steganografii, bude patřit k těm, jejichž učivo si žáci trvale zapamatují.

Slabou stránkou samotné steganografie je ovšem otevřená podoba skrytého textu. Jakmile je prozrazena existence zprávy, je prozrazen i celý její obsah. Proto se při komunikaci s tajným obsahem často používalo a používá šifrování (kryptografie), případně kombinace kryptografických a steganografických metod. Šifrováním se budeme zabývat příště.

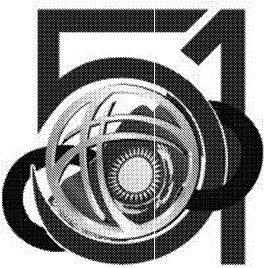
Literatura

[1] *Bíč, J.*: Jak mistr Jan Hus kódoval dopisy z kostnice? History revue, prosinec 2009, roč. 2, č. 12, s. 73–75. ISSN 1803–0440.

[2] *Singh, S.*: Kniha kódů a šifer . 2. vyd. Praha: Argo a Dokořán, 2009. 384 s. ISBN 978–80–7363–268–7 (Dokořán), ISBN 987–80–257–0144–7 (Argo).
[3] *Vondruška, P.*: Kryptologie, šifrování a tajná písma . 1. vyd. Praha: Albatros, 2006. 344 s. ISBN 80–00–01888–8.
[4] *Vondruška, P.*: Začínáme steganografií. Crypto–World, září 2000, roč. 2, č. 9, s. 3–5. ISSN 1801–2140.

ZPRÁVY

51. Mezinárodní matematická olympiáda



Jedenapadesátý ročník Mezinárodní matematické olympiády (IMO) se uskutečnil 2.–14. července 2010 v hlavním městě Republiky Kazachstán – v Astaně. Letos se této nejstarší mezinárodní předmětové soutěže zúčastnilo 517 studentů z 97 zemí pěti kontinentů. Žádní tradiční účastníci nechyběli, nově přibylo Pobřeží slonoviny.

České družstvo sestavené na základě výsledků celostátního kola 59. ročníku MO, krajského kola a přípravného soustředění tvořili tito soutěžící: *David Klaška* z G v Brně, tř. Kpt. Jaroše, *Radek Marciňa* a *Jáchym Sýkora*, oba z GChD v Praze 5, Zborovská, *Miroslav Olšák* z GB v Praze 5, Pod Žvahovem, *Petr Ryšavý* z GJH v Praze 5, Mezi Školami a *Tomáš Zeman* z GJK v Praze 6, Parléřova.

Vedoucím českého družstva a zástupcem České republiky v mezinárodní jury byl *Mgr. Martin Panák, Ph.D.*, z Přírodovědecké fakulty MU v Brně jeho zástupcem a pedagogickým vedoucím byl *RNDr. Pavel Calábek, Ph.D.*, z Přírodovědecké fakulty UP v Olomouci.

Vedoucí jednotlivých delegací a další členové jury se sjeli do bývalého hlavního města Kazachstánu Almaty 2. července, kde proběhly první tři zasedání jury. Na těchto zasedáních byla vybrána šestice soutěžních úloh. Soutěžící spolu s pedagogickými vedoucími přiletěli 5. července do Astany, kde se ubytovali v hotelu Duman.

Slavnostní zahájení 51. ročníku IMO se uskutečnilo den po příjezdu všech soutěžících v Paláci nezávislosti v Astaně. Aby se ho mohli zúčastnit i členové jury, pořadatelé je přepravili 1000 km letadly z Almaty do Astany. Na slavnostním zahájení přivítali účastníky místopředseda senátu *Muchambed Kopej* a ministr vzdělávání a vědy *Žanseit Tujmebajev*, který také přečetl dopis Prezidenta Republiky Kazachstán *Nursultana Nazarbajeva*. Dále účastníky přivítali představitelé společenského a politického života Kazachstánu. Po slavnostním zahájení byli účastníci a pedagogičtí vedoucí přepraveni do 240 km vzdáleného národního parku Burabaj, kde se soutěžící ubytovali v léčebně-vzdělávacím kom-