INFORMATIKA

Úlohy o směsích

STANISLAV TRÁVNÍČEK

Přírodovědecká fakulta UP, Olomouc

Úlohy o směsích (slitinách a roztocích) jsou klasickým druhem slovních úloh. Zaveďme toto označení: 1. složka směsi má hmotnost m_1 a cenu c_1 Kč za kilogram, 2. složka směsi má hmotnost m_2 a cenu c_2 Kč za kilogram a výsledná směs má hmotnost m_3 a cenu c_3 za kilogram, do níž jsou zahrnuty ceny obou složek. Modelem úloh o směsích je tedy soustava

$$\begin{aligned} m_1 + m_2 &= m_3 \\ m_1c_1 + m_2c_2 &= m_3c_3. \end{aligned} \tag{1}$$

Z toho, že v soustavě (1) jsou dvě rovnice, nám plyne, že v úlohách jsou vždy čtyři z uvedených šesti proměnných zadány a dvě (neznámé) se počítají. Přitom však zadáváme nejvýše dvě z proměnných m_i, protože hodnota třetí plyne již přímo z 1. rovnice (1). Podle toho můžeme u těchto úloh rozlišit tyto typy:

T1: Zadáno: c_1, c_2, m_3, c_3, neznámé: m_1, m_2;
T2: Zadáno: c_1, m_2, c_2, c_3, neznámé: m_1, m_3;
Zadáno: m_1, c_1, c_2, c_3, neznámé: m_2, m_3;
T3: Zadáno: m_2, c_2, m_3, c_3, neznámé: m_1, c_1;
Zadáno: m_1, c_1, m_3, c_3, neznámé: m_2, c_2;

T4: Zadáno: c_1, m_2, m_3, c_3, neznámé: m_1, c_2;
Zadáno: m_1, c_2, m_3, c_3, neznámé: m_2, c_1;
T5: Zadáno: c_1, m_2, c_2, m_3, neznámé: m_1, c_3;
Zadáno: m_1, c_1, c_2, m_3, neznámé: m_2, c_3;
T6: Zadáno: m_1, m_2, c_2, c_3, neznámé: m_3, c_1;
Zadáno: m_1, c_1, m_2, c_3, neznámé: m_3, c_2;
T7: Zadáno: m_1, c_1, m_2, c_2, neznámé: m_3, c_3.

Soustava (1) může být modelem nejrůznějších reálných situací. Uveďme si příklady typických úloh, jak je najdeme v [1].

Úloha 1

Ze dvou druhů čaje v ceně 160 Kč a 220 Kč za 1 kilogram se má připravit 20 kg směsi v ceně 205 Kč za 1 kilogram.Kolik kilogramů každého druhu je třeba smíchat?
Zde $c_1 = 160$, $c_2 = 220$, $m_3 = 20$, $c_3 = 205$; neznámé jsou m_1, m_2, úloha je typu T1.
(Tato úloha se s jinými čísly a s kávou opakuje ve více učebnicích a sbírkách jako typická úloha o směsích.)

Úloha 2

Ze dvou kovů s hustotami 7,4 g/cm^3 a 8,2 g/cm^3 máme připravit 0,5 kg slitiny s hustotou 7,6 g/cm^3. Kolik gramů každého kovu je k tomu zapotřebí?
Zde c_i jsou hustoty; $c_1 = 7{,}4$, $c_2 = 8{,}2$, $m_3 = 500$, $c_3 = 7{,}6$; neznámé jsou m_1, m_2 a výsledek je v gramech. Úloha je rovněž typu T1.

Úloha 3

Kolik gramů 60%ního roztoku a kolik gramů 35%ního roztoku je třeba k vytvoření 100 gramů 40%ního roztoku?

Zde bychom měli brát $c_1 = 0{,}6$, $c_2 = 0{,}35$ a $c_3 = 0{,}4$. Když se však podíváme na druhou rovnici (1), vidíme, že po jejím vynásobení stem se význam rovnice nezmění, takže lze brát přímo $c_1 = 60$, $c_2 = 35$ a $c_3 = 40$; $m_3 = 100$, neznámé jsou m_1, m_2 a opět jde o úlohu typu T_1.

Úloha 4

Ředitelství školy na konci školního roku oznámilo, že z 250 dětí, které navštěvují školu, získalo 20 % vyznamenání. Přitom vyznamenání dosáhlo 18 % chlapců a 23 % dívek. Určete, kolik chlapců a kolik dívek navštěvuje tuto školu.

Zde $c_1 = 18$, $c_2 = 23$, $m_3 = 250$, $c_3 = 20$; neznámé jsou m_1, m_2, úloha je typu T1.

(V namátkou prohlédnutých učebnicích a sbírkách jsem jiné typy úloh nenašel). Typu T2 je např.

Úloha 5

Kolik vody je třeba přilít do patnácti litrů 60%ního lihu, abychom dostali líh 40%?
Zde $m_1 = 15$, $c_1 = 60$, $c_2 = 0$, $c_3 = 40$; neznámé jsou m_2 (kolik litrů vody je třeba přilít) m_3 (výsledný počet litrů 40%ního lihu).

Úloha 6

Přidáme-li do 0,6 litru 40%ního roztoku druhý roztok, dostaneme 1 litr roztoku 50%ního. Jaký byl druhý roztok?
Zde $m_1 = 0{,}6$, $c_1 = 40$, $m_3 = 1$, $c_3 = 50$; neznámé jsou m_2, c_2, úloha je typu T3.

Obměnou uvedených úloh je čtenář jistě schopen vytvořit si úlohy zbývajících typů. Na závěr přidejme ještě typ T7.

Úloha 7

Co vznikne, smícháme-li 5 litrů 40%ního lihu a 3 litry lihu 60%ního.
Zde $m_1 = 5$, $c_1 = 40$, $m_2 = 3$, $c_2 = 60$; neznámé jsou m_3, c_3.

Řešení všech typů úloh o směsích

V typech T3 až T7 jsou neznámé m_i a c_j, tedy o množství jsou dány dva údaje. Odsud a z 1. rovnice (1) plyne výpočet třetího množství, a to v typech T6 a T7

$$m_3 = m_1 + m_2$$

a v typech T3, T4 a T5

$$m_i = m_3 - m_{3-i}$$

pro $i = 1$ a 2. V typech T5 a T7 je pak podle 2. rovnice (1)

$$c_3 = \frac{m_1 c_1 + m_2 c_2}{m_3}$$

a pro typy T3, T4, T6 je

$$c_i = \frac{m_3 c_3 - m_{3-i} c_{3-i}}{m_i}$$

pro $i = 1$ a 2. Nyní se věnujeme typům T1 a T2. Položme v (1) $m_3 = 1$ a vypočtěme z této soustavy rovnic m_1 a m_2 jako neznámé. Protože však jde o zvláštní případ, zvolme pro tyto „neznámé“ označení r_1 a r_2. dostaneme

$$r_1 = \frac{c_2 - c_3}{c_2 - c_1}, \quad r_2 = \frac{c_3 - c_1}{c_2 - c_1}.$$

Ježto $r_1 + r_2 = 1$, vyjadřují tyto koeficienty relativní velikost hodnot m_1 a m_2, tj. též $m_1 : m_2 = r_1 : r_2$. Proto řešením typu T1 jsou hodnoty

$$m_1 = r_1 \cdot m_3, \quad m_2 = r_2 \cdot m_3.$$

U typu T2 neznáme m_3 a proto si je zjistíme pomocí množství, které známe, tj. pomocí m_i (tj. m_1 nebo m_2):

$$m_3 = \frac{m_i}{r_i}, \quad m_{3-i} = r_{3-i} \cdot m_3$$

pro $i = 1$ nebo 2.

Zadání a vytvoření programu

Má se sestavit jednoduchý program, který na základě zadání vstupních dat dovede řešit všechny typy úloh o směsích.

Doplníme k tomu: Zadání i výpočet m_i typu Real volíme s možností na 3 desetinná místa, zadání a výpočet c_i rovněž typu Real na dvě desetinná místa; nebudou se provádět žádné kontroly korektnosti zadání; bude umožněno provádění série výpočtů; vzhled obrazovky bude pro všechny typy úloh jednotný. Dále již popisujeme předložený program *Smesi*.

Obrazovka. Nejprve naplánujeme vzhled obrazovky v jednotlivých fázích chodu programu. Na obr. 1 je úvodní obrazovka s legendou a kurzorem. Na obr. 2 je obrazovka před koncem zadávání vstupů (na příkladu úlohy T7), přičemž do rubrik pro neznámé, které jsou cílem výpočtu, se vkládají pomlky nebo otazníky (zde v posledním řádku). Na navazujícím obr. 3 je obrazovka po stisku klávesy *Enter*, po němž proběhne výpočet a zobrazení výsledku (v barvě žluté pro rozlišení od vstupů). Z tiskových důvodů časopisu uvádíme naše ukázky v barevné inverzi, tj. pozadí je ve skutečnosti černé a písmo v obvyklé barvě světle šedé.

```
Ulohy o smesich

          mnozstvi    %  Kc
1.slozka:
2.slozka:
S m e s :
```

Obr. 1

```
Ulohy o smesich

          mnozstvi    %  Kc
1.slozka:    5.000    40.00
2.slozka:    3.000    60.00
S m e s :    -        -
```

Obr. 2

```
Ulohy o smesich

          mnozstvi    %  Kc
1.slozka:    5.000    40.00
2.slozka:    3.000    60.00
S m e s :    8.000    47.50

Konec prace (A/N):
```

Obr. 3

Po výpočtu umístí program na místa, kde byla pomlka nebo otazník, vypočtené hodnoty.

Označení proměnných a konstant. Hodnoty m_1, m_2, m_3 jsou v programu označeny $X[1]$, $X[2]$, $X[3]$, hodnoty c_1, c_2, c_3 pak $X[4]$, $X[5]$, $X[6]$. Konstanty PX, PY jsou adresami tisku na obrazovce, $V[1]$, $V[2]$ jsou indexy těch hodnot $X[I]$, které jsou cílem výpočtu, S je řetězec znaků při zadávání vstupů.

Úvod programu:

```
program Smesi;
uses Crt;

const
  D: array [1..3] of Real = (10,100,1000);
  PX: array [1..6] of Integer
      = (13,13,13,22,22,22);
  PY: array [1..6] of Integer
      = (5,6,7,5,6,7);
  Mez = '            ';

type
  str10 = string[10];
```

```
var
  K, L, M: Integer;
  V: array [1..2] of Integer;
  X: array [1..6] of Real;
  R: array [1..2] of Real;
  Ch: Char;
  S: str10;
```

Procedura *ZadejCislo* přečte číslice zadané řetězcem S a vytvoří z nich číslo, eviduje též desetinnou čárku nebo tečku, ostatní znaky ignoruje.

```
procedure ZadejCislo(var Z: Real);
var I, N: Integer;
Pred: Boolean;
begin
  ReadLn(S);
  Pred := true; Z := 0; N:=1;
  for I := 1 to Length(S) do
  begin
    if S[I] in ['0','1','2','3','4','5',
       '6','7','8','9'] then
      if Pred then Z := 10*Z + Ord(S[I])-48
      else begin
        Z := Z + (Ord(S[I])-48)/D[N]; Inc(N)
      end;
    if S[I] in [',','.'] then Pred := false
  end
end; {ZadejCislo}
```

Procedura *PripravVstupy* převezme vstupní údaje a nastaví indexy těch údajů, které jsou předmětem výpočtu, a vše vytiskne na obrazovku ve standardním formátu.

```
procedure PripravVstupy(A:Integer);
begin
  GotoXY(PX[A]+3,PY[A]);
  ZadejCislo(X[A]);
```

```
  if S[1] in ['?','-'] then
  begin
    Inc(L); V[L] := A
  end
  else begin
    GotoXY(PX[A],PY[A]); Write(Mez);
    GotoXY(PX[A],PY[A]); WriteLn(XY[A]:8:3-(A div 4));
  end
end; {PripravVstupy}
```

Vlastní program nejprve vytiskne na obrazovce standardní schéma úlohy a prostřednictvím procedur zjistí a vytiskne vstupní údaje (viz obr. 1). Pak porovná indexy neznámých tak, aby $V[1] < V[2]$; tím je připraveno provádění výpočtů.

```
begin {program}
  repeat
    ClrScr; TextAttr := 15; WriteLn;
    WriteLn('  Ulohy o smesich');
    WriteLn; TextAttr := 7;
    WriteLn(' mnozstvi    %  Kc');
    WriteLn('  1.slozka:       ');
    WriteLn('  2.slozka:       ');
    WriteLn('  S m e s :       ');
    L := 0;             {vstupy}
    for K := 1 to 3 do
    begin
      PripravVstupy(K);
      PripravVstupy(K+3);
    end;
    if V[2] < V[1] then
    begin
      M := V[1]; V[1] := V[2]; V[2] := M
    end;
```

Organizace výpočtů odpovídá členění výpočtu, jak jsme je uvedli výše v textu.

```
if V[2] > 3 then {vypocty}
begin
  if (V[1] = 3) then
    X[3] := X[1] + X[2]
  else
    X[V[1]] := X[3] - X[3-V[1]];
  if V[2] = 6 then
    X[6] := (X[1]*X[4] + X[2]*X[5])/X[3]
  else
    X[V[2]] := (X[3]*X[6]
    - X[6-V[2]]*X[9-V[2]])/X[V[2]-3]
end
else begin
  R[1] := (X[5]-X[6])/(X[5]-X[4]);
  R[2] := (X[6]-X[4])/(X[5]-X[4]);
  if V[2] = 2 then
  begin
    X[1] := R[1]*X[3];
    X[2] := R[2]*X[3]
  end
  else begin
    X[3] := X[3-V[1]]/R[3-V[1]];
    X[V[1]] := X[3]*R[V[1]]
  end
end;
```

Tisk výsledků je proveden na ta místa schématu, kam logicky patří. Nakonec se program ještě zeptá, zda se má práce ukončit; pokud ne, pokračuje se zadáním dalšího příkladu.

```
TextAttr := 14;   {tisk vysledku}
for K := 1 to 2 do
begin
  GotoXY(PX[V[K]],PY[V[K]]);
  Write(X[V[K]]:8:3-(V[K] div 4))
end;
WriteLn; WriteLn;
TextAttr := 7; GotoXY(3,9);
```

```
    Write('Konec prace (A/N): ');
    Ch := ReadKey;
  until (Ch = 'A') or (Ch = 'a')
end. {program}
```

Tento program lze využít více způsoby:

- Může sloužit jako jednoúčelový prográmek pro učitele, který připravuje tuto látku do výuky. K tomu poskytuje jednoduché a příjemné uživatelské prostředí.
- Zadání programu může být tématem pro samostatnou práci žáků při výuce programování. Při analýze jednotlivých typů úloh se žáci hlouběji seznámí s úlohami o směsích.
- Samotný předložený program může být objektem, na kterém mohou žáci pracovat a který mohou různě vylepšovat, např. zavést kontroly korektnosti vstupů, úpravy tisku údajů, apod. a nakonec posuzovat, v čem je jejich verze programátorsky nebo uživatelsky lepší než zde předložená základní verze.

Literatura

[1] *Běloun, F. a kol.*: Sbírka úloh z matematiky pro základní školu (7. vydání). Prometheus, Praha 1992.

Autorkou úvodní ilustrace je Mgr. Jaroslava Čermáková.

Počítačová bezpečnost ve výuce informatiky

(2. část – jednoduchá záměna –monoalfabetické šifry)

MICHAL MUSÍLEK – ŠTĚPÁN HUBÁLOVSKÝ

Přírodovědecká fakulta Univerzity Hradec Králové

V článku [1] jsme se zmínili, že *Mistr Jan Hus* psal z vězení v Kostnici šifrované dopisy, k jejichž zašifrování použil jednoduchou substituční šifru [2], [5]. Šifroval pouze samohlásky, a to tak, že je nahradil písmenem následujícím v abecedě po dané samohlásce. Jeho šifrovací systém lze tedy znázornit tabulkou:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	F	F	G	H	J	J	K	L	M	N	P	P	Q	R	S	T	V	V	W	X	Z	Z

Příklad šifrového textu: PZCHB JFST KPRFN J PPCBTFK VSFCH HRJCHVV Z NJZ VZCHPDJ NFPPSLVSFNSTVJ SVBRPVF SMJLNPST, PPKRZTFCTVJ B PRBZDNB CHVBLB.

Otevřený text, který vznikne dešifrováním podle tabulky, jsme umístili až na konec tohoto článku, abychom čtenáři nepokazili radost ze samostatného vyřešení úlohy. Při dešifrování si jistě uvědomíte, že použitý systém je poměrně slabý a navíc je vzhledem k dešifrování nejednoznačný, protože v šifrovém textu mohou písmena B, F, J, P, V a Z mít dva různé významy. Naštěstí se dá z kontextu správný význam (zda jde o samohlásku, nebo souhlásku) zpravidla snadno určit.

Pojmenování „otevřený text“ a „šifrový text“ dobře vystihují podstatu. Otevřený text představuje zprávu před šifrováním, v běžné, každému čitelné a srozumitelné podobě. Šifrový text naopak má být pro nepovolaného člověka nečitelný, má se mu jevit jako náhodná změť písmen či jiných znaků. Jednou z možností, jak získat z otevřeného textu šifrový text, je znak po znaku provádět náhradu podle tzv. převodové tabulky. Převod šifrového textu zpět na otevřený text nazýváme dešifrování. Provádíme je

podle stejné tabulky jako šifrování, znaky pro náhradu ovšem nehledáme v horním, nýbrž ve spodním řádku tabulky.

Převodové tabulky.

Šifra Mistra Jana Husa byla jednoznačná vhledem k šifrování, ale vzhledem k dešifrování byla nejednoznačná. Uvedeným nedostatkem netrpěly o mnoho starší šifry, použité ve Starém zákoně, kde snad opisovatel Bible chtěl zanechat v textu své znamení a např. místo Babel (Babylon) napsal občas Šešach. Toto zašifrování vyplynulo ze záměny písmen ze začátku hebrejské abecedy za písmena z jejího konce, tedy *alef* za *tav*, *bet* za *šin* až *kaf* (ch) za *lamed*. Protože v hebrejském textu se často zapisují pouze souhlásky a samohlásky se doplňují z kontextu, vešla tato šifra ve známost pod názvem *atbaš* [3], [5]. Uplatníme-li stejný princip na latinku (budeme používat mezinárodní abecedu s 26 písmeny bez diakritiky), dostaneme systém daný převodovou tabulkou:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Tento systém má oproti předchozí šifře dvě výhody. Je jednoznačný vzhledem k dešifrování a navíc lze použít pro šifrování stejnou tabulku jako pro dešifrování. To nám umožní zkrátit převodovou tabulku na polovinu:

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

V hebrejské literatuře se pak objevují ještě další dva podobné systémy, nazývané *albam* a *atbah* [6]. Šifra *albam* rozdělila nejprve hebrejskou abecedu na dvě poloviny a pak přiřadila prvnímu písmenu z první poloviny první písmeno z druhé poloviny, druhému druhé, třetímu třetí atd. V hebrejské abecedě se tedy zaměnilo *alef* za *lamed*, *bet* za *mem* atd., odtud *albam*. Převodovou tabulku šifry albam

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

lze opět zapsat i ve zkrácené podobě:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Poslední jmenovaná šifra *atbah* souvisí se zápisem čísel v hebrejských textech, kdy písmena byla současně používána jako číslice. Přitom prvních devět písmen hebrejské abecedy představovalo číslice 1 až 9, zatímco druhých devět číslice 10 až 90. Šlo o nepoziční číselnou soustavu (podobně jako u římských číslic). Šifra k sobě přiřazovala písmena tak, aby jejich součet byl pro první devítičlennou skupinu 10 a pro druhou 100. V hebrejské abecedě zbývají už jen čtyři písmena (celkem má 22 znaků pro souhlásky). V latince zbývá osm písmen, se kterými obvykle naložíme podobně jako s předchozími dvěma devíticemi:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	H	G	F	E	D	C	B	A	R	Q	P	O	N	M	L	K	J	Z	Y	X	W	V	U	T	S

I tuto převodovou tabulku je možné zkrátit, ale nikoliv na polovinu:

A	B	C	D	E	J	K	L	M	N	S	T	U	V
I	H	G	F	E	R	Q	P	O	N	Z	Y	X	W

Zkuste dešifrovat texty zašifrované v šifrách atbaš a albam (řešení je na konci článku):

Atbaš: `EVOPB NRWVZ OFNMV HGZXR QVMPI RWOZN FHRNR`
`GRKIL HGLIA MVSLA YBEAO VGOBS VNRMT DZB`
Albam: `WRQVA LZFXH GRPAL ZOBUN GFGIV ZPYBI RXNWR WRUBB`
`FBOAB FGXGR ENIRQ RWRUB PVALV ZLFYR AXLPN CRX`

Všechny šifry, o kterých jsme doposud mluvili, nahrazují určité písmeno abecedy jiným jednoznačně daným písmenem dle převodové tabulky. Tomuto typu šifry se říká *jednoduchá záměna*, nebo také *monoalfabetická šifra*. Nabízí se otázka, kolik existuje navzájem různých jednoduchých záměn, jestliže vyloučíme šifry nejednoznačné vzhledem k dešifrování (tedy i šifru Mistra Jana Husa). Každou takovou šifru můžeme popsat tabulkou, která má v prvním řádku abecedu seřazenou v obvyklém abecedním pořadí

(A, B, C, ... , Z) a ve druhém řádku jsou písmena uspořádána v libovolném pořadí. Počet různých pořadí, tedy permutací z písmen mezinárodní abecedy je

$$26! = 26 \cdot 25 \cdot 24 \ldots 3 \cdot 2 \cdot 1 = 403\,291\,461\,126\,605\,635\,584\,000\,000,$$

tedy přibližně 403 kvadriliónů.

Šifry atbaš i albam mají společné určité omezení, které však přináší výhodu stejného postupu při šifrování i dešifrování zpráv. Je jím vytvoření dvojic písmen, které se vzájemně zastupují (proto stačí k popisu těchto šifer tabulka s 13 sloupci namísto 26). Opět se nabízí otázka, kolik je takových šifer, které k sobě vzájemně přiřazují dvojice písmen? Řečeno matematickou terminologií se jedná o zobrazení, která jsou sama k sobě inverzní. Představíme-li si, že postupně volíme jednotlivé dvojice písmen, můžeme psát:

$$\binom{26}{2}\binom{24}{2}\binom{22}{2}\cdots\binom{4}{2}\binom{2}{2} = \frac{26!}{2^{13}} = 49\,229\,914\,688\,306\,352\,000\,000.$$

Šifer typu atbaš – albam je sice 2^{13}krát (přibližně osmtisíckrát) méně než všech jednoduchých záměn, ale pořád jich je $49 \cdot 10^{21}$ (49 000 triliónů).

Pro úplnost přehledu běžných monoalfabetických šifer musíme zmínit tzv. *Caesarovu šifru*. Šifra je pojmenována po slavném římském vojevůdci Caesarovi, který ji používal při svém válečném tažení do Galie. Spočívá v posunutí abecedy o 2 písmena, tedy prvnímu písmenu A v otevřené abecedě odpovídá písmeno C jako první písmeno v šifrové abecedě. Převodová tabulka:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Tuto šifru lze samozřejmě obměnit tak, že místo o 2 písmena posunujeme šifrovou abecedu o 1, 3, 4, 5, ... , 24, 25 písmen. Posunutím o 26 písmen bychom již získali abecedu identickou s otevřenou abecedou, takže text by nebyl zašifrován, šlo by vlastně o nulové posunutí. Šifer založených na nenulovém posunutí je tedy 25, včetně Caesarovy šifry. Jde tedy o poměrně slabý šifrový systém.

Jiné znaky v šifrové abecedě

Šifru můžeme nepovolaným osobám ještě více zkomplikovat, jestliže místo stejných znaků (26 písmen mezinárodní abecedy) použijeme v šifrové abecedě částečně, nebo zcela jiné znaky. Příklad takové šifry si ukážeme opět pomocí převodové tabulky:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	ζ	D	p	2	η	E	o	3	α	F	n	4	β	A	m	5	γ	B	l	6	δ	C	L	7	ε

Musíme si ovšem dát pozor, abychom nezaměnili šifrování za kódování. To lze velmi snadno provést např. použitím semaforové abecedy, která je všeobecně známým kódem. Nahrazení polohy rukou odpovídajícími polohami ručiček na symbolickém ciferníku hodin sice pomůže skrýt obsah zprávy před nezkušeným člověkem, ale zkušený luštitel zprávu velmi snadno dešifruje – viz převodová tabulka kódu „semaforová abeceda pomocí hodin“:

A	B	C	D	E	F	G	H	I	J	K	L	M
												
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
												

Obr. 1

Jaký je rozdíl mezi šifrou a kódem? Zdánlivě žádný, protože obojí můžeme vyjádřit převodovou tabulkou. Zásadní rozdíl je ovšem v účelu převodu. Je-li jeho smyslem utajení zprávy a převodová tabulka představuje tajný klíč, který by měl být známý pouze pisateli a adresátovi zprávy, jedná se o monoalfabetickou šifru. Je-li naopak převodová tabulka nějakým způsobem zveřejněna či dokonce obecně známa, jedná se o kód. Příkladem kódu je např. ASCII (*American Standard Code for Information Interchange*):

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Kódy podle kříže

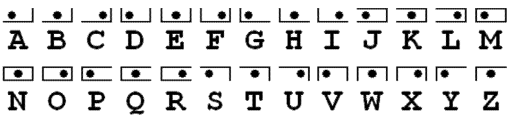
Poměrně snadno čitelné jsou kódy podle kříže (někdy méně poeticky nazývané kódy prasečích chlívků). Ukažme si vytvoření jednoho z těchto kódů, který nese pojmenování *velký kříž*. Místo tradiční převodové tabulky umístíme písmena otevřené abecedy do tabulky 3×3 pole, a to po třech znacích:

ABC	DEF	GHI
JKL	MNO	PQR
STU	VWX	YZ_

Abychom dostali ty správné „chlívky“, odstraníme vnější ohraničení tabulky a vnitřní naopak zvýrazníme:

ABC	DEF	GHI
JKL	MNO	PQR
STU	VWX	YZ_

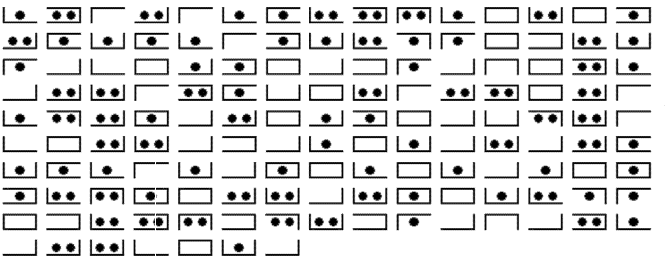
Znaky kódu získáme z čar ohraničujících danou skupinu písmen otevřené abecedy a z tečky vyznačující umístění písmene v příslušném „chlívku“ (vlevo, uprostřed, či vpravo):



Obr. 2

Kódy podle kříže mohou být příjemným zpestřením v současnosti velmi populárních her, jimž se říká šifrovací, ale úkoly v nich zadávané jsou jen někdy šiframi. Často se zde jedná také o luštění kódů, steganografickými metodami ukrytých zpráv, rébusů a hlavolamů. Jsou-li úlohy spojeny s aktivním pohybem v přírodě, jedná se o ušlechtilou zábavu rozvíjející řecký ideál kalokagathia (harmonický soulad tělesného i duševního rozvoje, čestnosti a statečnosti). Nicméně po prvním seznámení se takový systém pro znalého luštitele stává pouhým kódem, nikoliv šifrou.

Pro luštění jsme pro vás připravili text zakódovaný pomocí kódu *malý kříž*. Zkuste sami přijít na systém vytvoření grafických znaků tohoto kódu. Malá nápověda: poslední slovo otevřeného textu je „čeká“ (tedy vlastně „CEKA“).



Obr. 3

Použití ve škole

Pokud bude chtít učitel informatiky připravit pro své žáky zprávy zašifrované pomocí různých typů jednoduché záměny, může využít jednoduché programy, které najde na webu [4]. Už se žáky základní školy je možné v rámci výuky informatiky probrat některé klasické monoalfabetické šifry známé z historie, vysvětlit jim princip jednoduché záměny a vyzvat je k sestavení vlastní převodové tabulky.

Na středoškolské úrovni můžeme žákům zadat úkol vytvořit makro v jazyce Visual Basic for Aplications, které text zapsaný do textového editoru Microsoft Word zašifruje podle některé zvolené monoalfabetické šifry.

Řešení předložených úloh

Otevřený text šifry Mistra Jana Husa

Pýcha jest kořen i počátek všech hříchův, z níž vychodí neposlušenství, svárové, smilnost, pokrytectví a prázdná chvála.

Otevřený text šifry atbaš

Velkým ideálům nestačí jen křídla, musí mít i prostor, z něhož by vzlétly. *Hemingway*

Otevřený text šifry albam

Jediným skutečným bohatstvím člověka je jeho osobnost, která vede jeho činy i myšlenky. *Čapek*

Otevřený text šifry malý kříž

Lví silou, vzletem sokolím kupředu kráčejme a drahé vlasti v oběti své síly snášejme. A byť i cesta daleká, ta Sokolíka neleká, jen mužně, statně kupředu, vždyť drahá vlast čeká!

Literatura

[1] *Musílek, M. – Hubálovský, Š.*: Počítačová bezpečnost ve výuce informatiky (1. část – Tvorba hesel a steganografie). MFI 20 (2010/11), č. 3.

[2] *Bíč, J.*: Jak mistr Jan Hus kódoval dopisy z Kostnice? History revue, roč. 2, č. 12.

[3] *Klíma, V.*: Utajené komunikace – 2. díl. CHIP: magazín informačních technologií, roč. 4, č. 6.

[4] *Musílek, M.*: Šifry a kódy [online]. 2010 [cit. 2010-01-31] Dostupné z: <http://www.musilek.eu/michal/sifry.html?menu=mat>

[5] *Singh, S.*: Kniha kódů a šifer. 2. vyd., Argo a Dokořán, Praha: 2009.

[6] *Vondruška, P.*: Kryptologie, šifrování a tajná písma. 1. vyd. Albatros, Praha: 2006.

ZPRÁVY

Praemium Bohemiae studentům již po desáté

Obr. 1 Medaile Bohuslava Jana Horáčka (1924 – 2002)

Dne 4. prosince 2010 byly v zámeckém divadle státního zámku Sychrov uděleny studentům prestižní ceny Praemium Bohemiae. Stalo se tak letos již po desáté, když nejlepším českým talentům v přírodních vědách byly uděleny tyto prestižní ceny. Jak jsou čtenáři našeho časopisu každoročně informováni, ceny od roku 2001 uděluje *Nadace Bohuslava Jana Horáčka Českému ráji* z úroků finančních prostředků, které pocházejí z celoživotního podnikání jejího zakladatele mecenáše Bohuslava Jana Horáčka v den výročí jeho narození (narodil se 4. prosince 1924 v Radvánovicích u Turnova). Nadace oceňuje cenami Praemium Bohemiae ty nejlepší, kteří i přes svůj nízký věk dokázali proslavit naši republiku ziskem medaile na světové přírodovědné olympiádě.

Letošní rok je mimořádný v tom, že Nadace ocenila studenty již po desáté. Za deset ročníků Nadace studentům udělila 208 cen Praemium Bohemiae v celkové