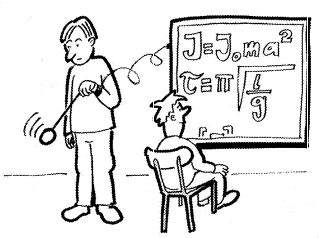
INFORMATIKA

Analýza a vizualizace dat (nejen) ve fyzikálním praktiku

MICHAL ČERNÝ

Přírodovědecká fakulta MU Brno



Fyzikální praktikum patří mezi nezastupitelné prvky gymnaziální výuky, ve které si mohou žáci sami vyzkoušet platnost fyzikálních zákonů a jejich aplikaci na konkrétní děje. Zcela přirozeně se v něm seznamují s tvorbou experimentů, uvažují o chybách, ale také samostatně vyhodnocují naměřené výsledky.

Právě zpracování naměřených výsledků patří u žáků mezi nepříliš oblíbenou činnost a často jde i o velmi silně zanedbávanou stránku. Na tomto místě je nutno říci, že rukou psané protokoly s rýsovanými grafy jsou pro žáky jen málo přínosné. Nezískávají totiž přehled o tom, jak se výsledky zpracovávají v mimoškolním prostředí a nenaučí se psát přírodovědecké texty na počítači, což pro ně může v budoucnu znamenat nemalý hendikep.

Často se setkáváme s tím, že grafy jsou tvořeny a analyzovány v programech, jako je Excel či Calc. Ty jsou však určeny především pro obchodní aplikace a žáci se v nich nenaučí dobrým návykům v oblasti analýzy a vizualizace dat. Grafy mají jen velmi malou variabilitu nastavení, odečítání hodnot je problematické a o možnostech prokládání křivek není třeba příliš mluvit. Žáci jsou tak doslova tlačeni k tomu, aby křivku prokládali nikoli podle funkční závislosti, ale prostě jen tak, aby v dostatečném mě-

řítku papírového protokolu tvarově odpovídala teoretickému předpokladu. Je zřejmé, že takto koncipovaná práce ve fyzikálním praktiku v oblasti vyhodnocování výsledků nemá příliš valnou kvalitu.

Jako optimální se proto jeví speciální nástroje na analýzu a vizualizaci dat. V širším povědomí jsou známy především dva programy, které se však pro školní využití příliš nehodí. Jednak je to *Origin*, který nabízí výborné funkce, pohodlné ovládání a téměř dokonalé výsledky, avšak za cenu, kterou škola ani žák obvykle nejsou schopni zaplatit. Druhým takovým programem je bezplatný *Gnuplot*, který je však vhodný spíše pro výuku informatiky, nežli na běžnou rutinní práci s daty v rámci gymnaziální výuky.

V další části článku si představíme několik aplikací, jež je možno k práci ve fyzikálním praktiku na školách použít, a které jsou dostupné zdarma. Tato okolnost je zvláště důležitá, neboť je žádoucí, aby žáci mohli svá měření zpracovávat doma. Vést je k tomu, aby si ukradli Origin je eticky nepřijatelné (i trestné) a proto jedinou variantou jsou právě bezplatné aplikace.

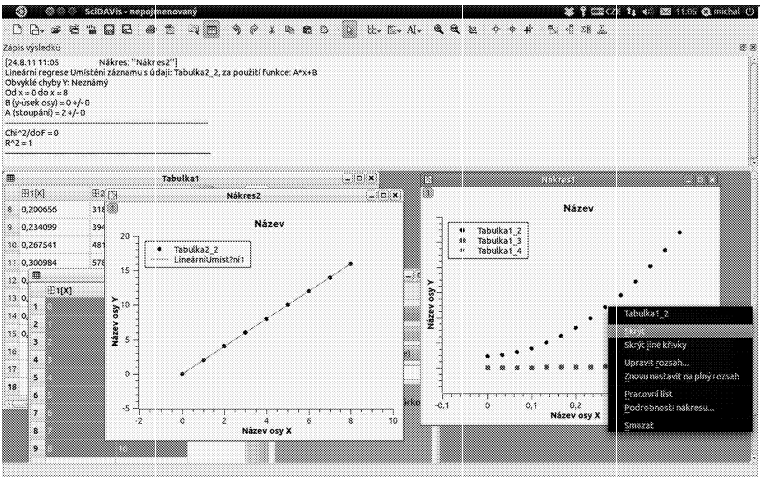
SciDAVis

Velice zajímavým nástrojem pro školní prostředí je SciDAVis [1], který je optimalizovaný speciálně pro vzdělávací účely. Je k dispozici pro Windows, Linux i MAC OS, takže je možno jej snadno provozovat ve škole i na téměř jakémkoli domácím počítači. Velkou výhodu představuje také jeho lokalizace do češtiny. Zvláště začínající uživatel jistě ocení, že přesně rozumí jednotlivým příkazům, má přehled o funkcích atp. Program se poměrně živě vyvíjí, takže jsou neustále doplňovány nové nástroje a odstraňovány chyby.

Ovládání je oproti Originu nepatrně odlišné, ale dle mého soudu je pro žáky lepší a pohodlnější. Vedle okna se sloupci dat se nachází ještě speciální panel, který umožňuje do dalšího sloupce vložit výsledek nějaké funkce. Žáci si tak udělají například jeden sloupec s hmotností tělesa a do druhého přímo prostřednictvím aplikace mohou vložit tíhovou sílu, která na dané těleso působí. Možnosti jsou samozřejmě větší než pouhé sčítání či násobení. Odpadá tak nutnost neustálé komunikace s Excelem.

Z pohledu gymnazijního fyzikálního praktika jsou v oblasti analýzy dat důležité především tři skupiny funkcí – tvorba grafů, odečet hodnot a zjišťování parametrů funkčních závislostí. SciDAVis toho ale zvládá mnohem více – například numericky integrovat či derivovat, statisticky zpracovávat

data apod. Popis těchto vlastností je však mimo spektrum našeho zájmu a pedagog je může vhodným způsobem v případě potřeby žákům ukázat.



Obr. 1 Ukázka možnosti tvorby grafů a lineárního proložení hodnot ve SciDAVis

V oblasti tvorby grafů je připravena základní sada obvyklých typů – nechybí koláčový, sloupcový ani bodový graf. Širší možnosti jsou u grafů, které jsou vyjádřeny křivkou – je možno si nastavit například hladký přechod, schodové spojování, přímé spojení bodů a mnoho dalšího. Z méně obvyklých jsou to pak grafy pro statistické účely (histogram, box plot…), podpora 3D grafů nebo grafů založených na vektorových mapách. Ty však mají význam pouze okrajový a jsou vhodné spíše pro občasné použití. Pro gymnaziální potřeby (ale také například pro základní fyzikální kurz na vysokých školách) jde tedy o nabídku dostatečnou. SciDAVis také nemá problém s umístěním více grafů do jednoho rámečku, s tvorbou zvětšených výřezů nebo s prací s vrstvami. Je tedy možno poměrně jednoduše porovnávat výsledky různých měření. Do grafů lze vkládat také obrázky, automatické tvary, šipky, popisky, legendy, nadpisy a mnohé další prvky.

Nastavování parametrů os se provádí pravým tlačítkem, kterým klikneme na osu a zvolíme položku *možnosti* – na výběr pak máme nastavení druhu písma u popisků, měřítka, velikosti zobrazovaných dílků, barvy osy, průsečíků os nebo nastavení mřížky.

Při analýze dat je k dispozici je také nástroj sloužící k odečtu hodnot na konkrétním místě v grafu (vhodné například pro extrapolaci či interpolaci), odečtu hodnot v konkrétním bodě nebo také umožňuje odstraňovat chybné hodnoty přímo z grafu. Samozřejmě je přítomná funkce pracující se zvětšováním vybrané oblasti grafu.

Z nástrojů pro analýzu dat je nejdůležitější prokládání křivek naměřenými hodnotami. Těchto funkcí je k dispozici poměrně velké množství – od polynomu 1. až 9. řádu, přes různé exponenciály až po Gaussovo rozložení, práci s více píkovými grafy nebo například již zmíněné numerické integrování. Kdykoli je navíc možnost nadefinovat si vlastní funkci, kterou chceme data prokládat. Práce s prokládáním je velice jednoduchá a je otázkou jednoho či dvou kliknutí myší.

Informace o proložení lze vypsat do legendy ke grafu. Současně se automaticky vypisuje do log souboru. V něm je vypsáno vše potřebné, od parametrů a jejich chyb až po třídu přesnosti zpracování dat. Aplikace umí pracovat i s obecnými funkcemi a nabízí možnost statistického zpracování dat.

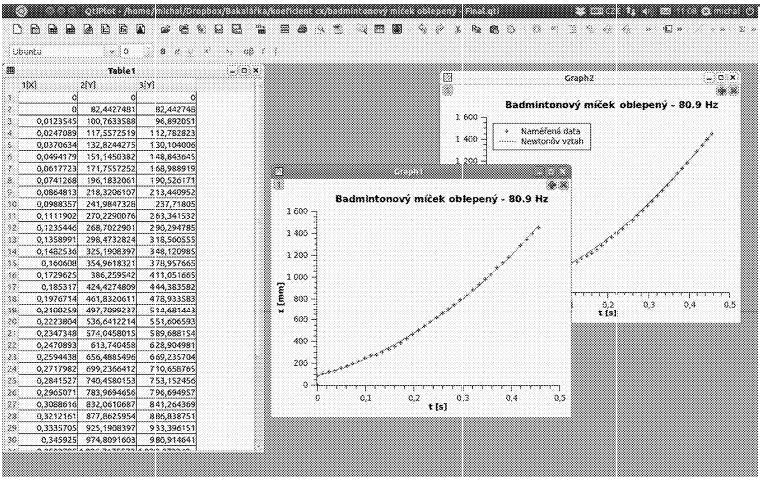
Osobně si myslím, že svou jednoduchostí, přehledností a přitom velice solidní funkční výbavou je pro školní praktikum téměř nejvhodnější volbou. Jistým nedostatkem je však to, že se vzhledově od Originu poměrně liší. Přechod z Originu na SciDAVis je navíc relativně obtížný a nepříliš pohodlný. Opačná cesta je ale podstatně snazší.

QtiPlot a LabPlot

SciDAVis není samozřejmě jedinou aplikací, kterou by bylo možné ve fyzikálním praktiku využít. Proto zde upozorníme ještě na dvě zajímavé aplikace. QtiPlot [2] je nástrojem, který se snaží v maximální možné míře napodobit Origin. Nabízí v podstatě totožnou strukturu menu a ovládání programu je také velice podobné. Pravdou je, že QtiPlot nedisponuje některými grafy (například bublinkovými) nebo statistickými funkcemi (t-Test) a také výsledné grafy nejsou tak esteticky zdařilé jako u Originu; přesto jsou však zdařilejší než u zbytku konkurence. Jinak se jedná o velice kvalitní a komplexní program, který nabízí zcela profesionální funkce. Velkým nedostatkem však je licenční politika, která umožňuje tento program plnohodnotně zdarma používat jen v Linuxu.

LabPlot [3] je nástroj určený pro Linux, ale lze jej spustit také pod Windows. Nabízí základní nástroje pro analýzu dat a poněkud neobvyklé ovládání. Jeho hlavní výhodou jsou 3D grafy, které lze tvořit skutečně ve-

lice dobře. Zajímavou funkcí je také možnost čtení dat přímo z databáze, což se může při automatizovaných měřeních poměrně hodit. Pokud tedy potřebujeme do praktika nástroj, který nabízí základní statistické i analytické nástroje, nabídne základní paletu 2D i poměrně bohatou 3D grafů a je zdarma, pak LabPlot rozhodně stojí za zvážení.



Obr. 2 Pracovní prostředí QtiPlot a graf závislosti polohy na čase při volném pádu badmintonového míčku

Závěr

Existují samozřejmě také další nástroje, které lze k analýze a vizualizaci dat ve fyzikálním praktiku použít. Osobně bych si dovolil doporučit SciDAVis, který se mi jeví pro školní prostředí jako nejvhodnější. Pokud škola používá Linux, pak rozhodně stojí také za zvážení, zda není lepší variantou QtiPlot, který má více funkcí, hezčí grafy a ovládání, které je velmi blízké Originu.

Používání těchto nástrojů nejen může žáky naučit práci s profesionálními programy a říci jim něco více o tom, jak se data skutečně zpracovávají, ale také mohou učinit tvorbu protokolů z měření přesnější a snad také zábavnější.

Jistě není zanedbatelný ani přesah těchto nástrojů do dalších předmětů – matematiky, informatiky, zeměpisu a dalších, ale také do humanitních

věd, pokud zpracovávají nejrůznější dotazníky, výzkumy a další statistické soubory dat.

Literatura

[1] http://scidavis.sourceforge.net
[2] http://soft.proindependent.com/qtiplot.html
[3] http://labplot.sourceforge.net/

Počítačová bezpečnost ve výuce informatiky

6. část: luštění polyalfabetické substituce

MICHAL MUSÍLEK, ŠTĚPÁN HUBÁLOVSKÝ

Přírodovědecká fakulta UHK, Hradec Králové

V minulém díle našeho seriálu jsme se seznámili s polyalfabetickými substitučními šiframi s periodickým klíčem. Dnes si ukážeme, jak lze takové šifry poměrně jednoduše luštit. Máme vyluštit následující šifrový text (zvýraznění některých bigramů podtržením a změnou řezu na tučný si prozatím nevšímejte, jeho důvod bude vysvětlen později).

I**EX**MU	ICDKN	E**MP**YM	Z**AW**CO	**XN**GMG	FV**MQ**U	**OO**IAX	L**UU**LV
LBH**SW**	**CA**DAG	MSNVR	FOETX	**VM**FNG	MV**WZ**L	ISMUD	DFJFM
GLQEV	YCRTM	BXHVL	SZJTD	HBCVL	KFFXF	TKVDL	RMBUE
IQM**UU**	JHWEA	KGCJD	JKVHH	ZFEAB	THSVJ	UTKSU	F**OO**WB
TKSMM	NPLVA	WRFDU	ZTLHZ	SUEYT	XVXLN	VN**MP**A	RZLJG
FPLVP	EWODB	THPBO	AIQGP	YWZUW	BTTRL	IRTZN	WHLPD
UJGCA	EAAMS	**SW**RHT	DLRPP	BDVBC	OHUJM	YUOAU	QBRAR
UGERL	VUJDP	LTHDP	YENVS	IZ**MQ**J	RH**EXN**	LJVLS	**MP**AIO
W**AW**AL	MCIJQ	TJKDO	GERWO	TLZWH	VLPVO	SJACE	JIY**SW**
FUX							

Algoritmus luštění polyalfabetické substituce s periodickým klíčem

Polyalfabetická substituce s periodickým klíčem byla dlouho považována za nerozluštitelnou šifru. Od svého objevu Albertim v 15. století a dokonalého rozpracování Vigenérem o století později odolávala úspěšně luštění až do 19. století, v jehož druhé polovině nezávisle na sobě šifru prolomili dva badatelé. Prvním byl vynikající anglický matematik Charles Babbage, známý jako tvůrce koncepce univerzálního počítače. Postup luštění objevil roku 1854, ale nepublikoval jej, možná na žádost britské rozvědky, která tím získala převahu nad Rusy v krymské válce [4]. Roku 1863 publikoval postup pruský důstojník Friedrich Wilhelm Kasiski v knize *Tajné šifry a umění je dešifrovat* [6]. Zcela jistě neznal Babbageovu práci, takže dále uvedený algoritmus je právem znám jako Kasiského test. Skládá se z pěti kroků:

1. Frekvenční analýzou šifrového textu ověříme, zda v daném případě skutečně může jít o polyalfabetickou substituci.
2. Vyhledáme shodné bigramy a jejich vzdálenosti v šifrovém textu, získaná přirozená čísla rozložíme na prvočinitele a posouzením rozkladů určíme nejpravděpodobnější délku hesla.
3. Šifrový text rozdělíme (rozpočítáme) na skupiny prvních, druhých až k-tých písmen (kde k je délka použitého hesla) a pro každou skupinu určíme nejpravděpodobnější posun šifrové abecedy proti otevřené abecedě.
4. Z jednotlivých písmen zrekonstruujeme heslo a rozhodneme, zda se jedná o systém Vigenére, Sestri-Beaufort, nebo Beaufort. V případě potřeby heslo opravíme.
5. Pomocí získaného hesla a určeného systému dešifrujeme šifrový text. Zjistíme, zda získaný otevřený text dává smysl
   a. Pokud získaný otevřený text nedává smysl, vezmeme další pravděpodobnou délku hesla v pořadí a pokračujeme znovu bodem 3.
   b. Pokud získaný otevřený text dává smysl, rozdělíme text na jednotlivá slova, doplníme diakritiku a interpunkci a jsme hotovi.

Nyní si ukážeme jednotlivé kroky Kasiského testu podrobněji, a to na konkrétním příkladu šifrového textu uvedeného na začátku článku.

Frekvenční analýza šifrového textu

Frekvenční analýzou zjistíme, že šifrový text má celkem 363 znaků a jsou

v něm použita všechna písmena mezinárodní abecedy od A do Z (a nejsou použity žádné jiné znaky). Relativní četnost jednotlivých písmen se pohybuje od 1,9 % do 6,3 %, tedy nevykazuje žádná výrazná maxima odpovídající v otevřeném textu písmenům E, A, O, I a N ani výrazná minima odpovídající písmenům G, F, W, X a Q. Velmi pravděpodobně se jedná o polyalfabetickou substituci.

Určení délky použitého hesla

Pro hledání opakujících se bigramů s výhodou využijeme textový editor a jeho funkci „Najít“ (klávesová zkratka `Ctrl+F`). Nalezené dvojice (trojice, n-tice) bigramů pak označujeme buď změnou řezu písma na tučné a podtržením (tak, jako jsou vyznačeny zde v zadání), nebo ještě lépe zvýrazňovači různých barev. Potom určíme pozice prvních písmen bigramů v šifrovém textu (mezery mezi pětimístnými skupinami nepočítáme), vypočítáme vzdálenosti opakujících se bigramů jako rozdíly příslušných pozic a provedeme rozklad těchto rozdílů na prvočinitele s využitím pravidel dělitelnosti, která jsou učivem základní školy.

Myšlenka vedoucí k určení délky hesla spočívá na dvou skutečnostech. V přirozeném textu se náhodně opakují některé bigramy, některé, jako např. ST, NI, PO, OV, CH, RO, EN, NA, JE, PR, TE, LE, KO, NE, OD poměrně často [2]. Otevřený text byl zašifrován heslem, které má danou délku a periodicky se opakuje. Tak se celkem snadno může stát, že se shodný bigram otevřeného textu zašifruje pomocí stejné dvojice znaků hesla a dvojice shodných bigramů se pak objeví také v šifrovém textu. Očíslujeme-li jednotlivé znaky šifrového textu od 1 do n (kde n je počet znaků šifrového textu; mezery mezi skupinami nepočítáme a nečíslujeme), můžeme vypočítat vzdálenost výskytů shodného bigramu jako rozdíl očíslování prvních znaků bigramu. Vzdálenost pak musí být násobkem délky hesla.

Kdyby stejné bigramy mohly vznikat pouze uvedeným způsobem, stačilo by pak určit největší společný dělitel nalezených vzdáleností a měli bychom hned délku hesla (v nejhorším případě její malý násobek). Bohužel to tak jednoduché není, protože dvojice shodných bigramů může v šifrovém textu vzniknout náhodně i jiným způsobem. Některé bigramy s podezřelými vzdálenostmi můžeme rovnou vyřadit z dalších úvah (v tabulce jsou označeny †), jde o vzdálenosti, ukazující na heslo delší než 30 znaků, nebo kratší než 5 znaků. Ať už vyřadíme některé bigramy, či nikoliv, nemůžeme délku hesla jednoduše určit jako největší společný dělitel,

ale pouze se podíváme, které prvočinitele registrujeme v rozkladech nejčastěji. V naší tabulce vidíme, že jedna trojka se vyskytuje 8krát, dvě trojky 7krát, jedna dvojka 6krát a dvě dvojky 5krát. Všichni ostatní prvočinitelé se pak objevují jen jednou nebo dvakrát. Pravděpodobné délky hesla tedy získáme z rozkladu 3.3.2.2 a vynecháme-li čísla menší než 5 a větší než 30 dostáváme postupně délky: 9, 18, 6, 12. Nejprve tedy vyzkoušíme heslo délky 9 znaků.

Bigram	Výskyt	Rozdíl pozic	Rozklad vzdálenosti (rozdílu pozic) na prvočinitele														
EX	2; 308	306	2	2				3	3	3	3						
MP	12; 193	181														181	†
MP	12; 316	304	2	2	2	2										19	†
MP	193;316	13	2	2												31	†
AW	17; 322	305									5					61	
XN	21; 309	288	2	2	2	2	2	3	3								
MQ	28; 303	275									5	5		11			
OO	31; 157	126	2					3	3				7				
UU	37; 124	87						3								29	†
SW	44; 251	207						3	3							23	
SW	44; 359	315						3	3			5		7			
SW	251;359	108	2	2				3	3	3							
CA	46; 244	198	2					3	3						11		
Četnost výskytu prvočinitelů			**6**	**5**	**2**	**2**	**1**	**8**	**7**	**2**	**1**	**2**	**1**	**2**	**2**	**1**	

Určení posunů pro jednotlivé skupiny znaků šifrového textu

Když jsme odhadli délku hesla, rozdělíme šifrový text na tolik skupin, kolik má očekávané heslo znaků. Podobá se to rozpočítávání, které známe z hodin tělesné výchovy, kde jsme se rozpočítávali na první a druhé. V našem příkladu očekáváme heslo s délkou 9, takže skupin, do nichž rozdělíme šifrový text, bude také 9. Rozdělení provedeme buď ručně, nebo pomocí „Děličky šifrového textu“ na webu [3]. Získáme skupiny:

1. INCMUCRNMLBDXBHJBSSRSNJOIBNCRDYRDNHMLDZJF
2. EEOQUAFGUQXHFUWKTUMFUVGDQTWAHVUUPVEPMOWAU
3. XMXULDOMDEHBTEEVHFMDENFBGTHETBOGLSXACGHCX
4. MPNOVAEVDVVCKIAHSONUYMPTPRLADCAETINIIEVE
5. UYGOLGTWFYLVVQKHVOPZTPLHYLPALOURHZLOJRLJ
6. IMMIBMXZJCSLDMGZJWLTXAVPWIDMRHQLDMJWQWPI
7. CZGAHSVLFRZKLUCFUBVLVRPBZRUSPUBVPQVATOVY
8. DAFXSNMIMTJFRUJETTAHXZEOUTJSPJRUYJLWJTOS
9. KWVLWVFSGMTFMJDAKKWZLLWAWZGWBMAJERSAKLSW

Po rozdělení pro každou skupinu určíme nejpravděpodobnější posun šifrové abecedy proti otevřené abecedě. Ukažme si nejprve, jak to lze udělat bez pomoci počítače. V první skupině spočítáme četnosti všech písmen šifrové abecedy. Skupina má celkem 41 znaků, z toho jsou 4 B, 3 C, 4 D, 1 F, 2 H, 2 I, 3 J, 2 L, 3 M, 5 N, 1 O, 4 R, 3 S, 1 U, 1 X, 1 Y a 1 Z. Ostatních devět písmen se v této skupině nevyskytuje. Přepokládáme, že převodová tabulka vznikla posunutím abecedy o určitý počet znaků. Jak rychle zjistit o kolik? Připravíme si tabulku s četnostmi písmen v dané skupině šifrového textu a ještě jednu tabulku, dvakrát tak dlouhou, ve které vyznačíme červeně (zde šrafováním) písmena E, A, O, I a N a modře písmena G, F, W, X a Q (zde šedou barvou) [5]. Pak posunujeme horní tabulku s četnostmi písmen proti dolní referenční tabulce o 0, 1, 2, ... , 25 sloupců a pro každé posunutí sečteme četnosti u pěti červených (šrafovaných) značek a u pěti modrých (šedých) značek a vypočteme rozdíl těchto dvou součtů („červený“ mínus „modrý“). Nejpravděpodobnější posunutí je to, pro které vyjde rozdíl součtu maximální.

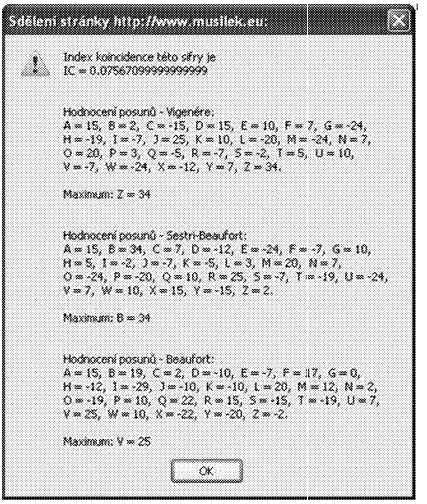
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Polovina referenční 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

Propočítáme-li tyto hodnoty pro první skupinu, dostáváme:

Posun 0 (A nad A) ... $8 - 2 = 6$
Posun 1 (A nad B) ... $15 - 1 = 14$
Posun 2 (A nad C) ... $9 - 6 = 3$
Posun 3 (A nad D) ... $8 - 13 = -5$
Posun 4 (A nad E) ... $3 - 13 = -10$
Posun 5 (A nad F) ... $10 - 13 = -3$
...
Posun 24 (A nad Y) ... $3 - 9 = -6$
Posun 25 (A nad Z) ... $9 - 8 = 1$



Obr. 1 Ohodnocení posunů skriptem

Ze všech 26 vypočítaných hodnot je nejvyšší hodnota pro posun 1 (A nad B, Z nad A). Prvním písmenem hesla by bylo v systému Vigenére písmeno Z (protože Z je nad A), zatímco v sytému Sestri-Beaufort by šlo o písmeno B (protože B je pod A). Pro systém Beaufort bychom museli použít jinou referenční tabulku, ve které by byla písmena řazena opačně (Z, Y, X, ... , B, A) a maximum by pak nastalo pro posun odpovídající V jako prvnímu písmenu hesla. Protože takové ruční počítání posunů je pracné, a tím zdlouhavé, pomůžeme si opět pomůckou na webu [3] (obr. 1), která umí v rámci frekvenční analýzy vypočítat ohodnocení jednotlivých posunů a najít maxima pro všechny tři výše uvedené systémy. Jediný rozdíl oproti ručnímu výpočtu spočívá v tom, že skript počítá s relativními četnostmi v procentech místo absolutních četností a výsledek pak zaokrouhluje na celé číslo. Analýzou jednotlivých skupin dostáváme:

Systém šifrování	Skupina									Heslo
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	
Vigenére	Z	M	T	A	H	I	H	F	S	Nedává smysl
Sestri-Beaufort	B	O	H	A	T	S	T	V	I	BOHATSTVÍ
Beaofort	V	I	F	I	Y	Q	D	H	E	Nedává smysl

Vidíme, že text byl zašifrován systémem Sestri-Beaufort s použitím hesla BOHATSTVÍ.

Dešifrování textu

Text můžeme dešifrovat jedním ze dvou způsobů popsaných v minulém díle našeho seriálu. Ručně s využitím tabulky *tabula recta*, nebo automaticky pomocí počítačového programu. Dešifrováním získáme otevřený text v podobě pětimístných skupin bez diakritiky:

JSEMN AVYSO STPRE SVEDC ENZEZ ADNEB OHATS TVISV
ETANE DOKAZ ELIDS TVEMP OHNOU TVPRE DANIK DYBYH
OMELV RUKOU CLOVE KSEBE VICOD DANYT AKOVE MUCIL
IJENP RIKLA DYVEL KYCHA RYZIC HOSOB NOSTI MOHOU
OSTAT NIDOV ESTKU SLECH TILYM POSTO JUMIS KUTKU
MPENI ZEPRI TAHUJ IJENP ROSPE CHARE AKOHO KOLIV
NEODO LATEL NESVA DEJIK JEJIC HZNEU ZIVAN IUMIS
INEKD OPRED STAVI TMOJZ ISEJE ZISEN EBOGA NDHIH
OTRIM AJICI MESEC NEKOH OTAKO VEHOJ AKOJE CARNE
GIE

Tento text při čtení dává smysl, takže zbývá už jen rozdělit text na jednotlivá slova, doplnit diakritiku a interpunkci a dozvíme se, co si myslel Albert Einstein o bohatství [1]. Tento poslední krok už přenecháme čtenářům.

Literatura

[1] *Einstein, A.*: Jak vidím svět. Praha: Nakladatelství Lidové noviny, s.r.o. 1993. 160 str.

[2] *Kolektiv*: Frekvence písmen, bigramů, trigramů, délka slov [online]. Centrum zpracování přirozeného jazyka Fakulty informatiky Masarykovy univerzity, Brno. [cit. 2010-05-05] Dostupné z: <http://nlp.fi.muni.cz/cs/Frekvence_pismen_bigramu_trigramu_delka_slov>

[3] *Musílek, M.*: Šifry a kódy [online]. 2010 [cit. 2010-05-05] Dostupné z: <http://www.musilek.eu/michal/sifry.html?menu=mat>

[4] *Singh, S.*: Kniha kódů a šifer. 2. vyd. Praha: Argo a Dokořán, 2009. 384 s. (Dokořán).

[5] *Tesař, P.*: Substituce složitá – periodické heslo, srovnaná abeceda. Crypto-World, říjen 2000, roč. 2, č. 12, s. 4–10.

[6] *Vondruška, P.*: Soutěž 2001, II. část – Absolutně bezpečný systém. Crypto-World, říjen 2001, roč. 3, č. 10, s. 2–6.