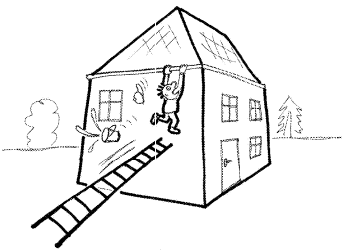
INFORMATIKA

Využitie IKT pri rozvíjaní kompetencie modelovania vo vyučovaní matematiky

STANISLAV LUKÁČ

Prírodovedecká fakulta UPJŠ v Košiciach

(*Dokončení*)

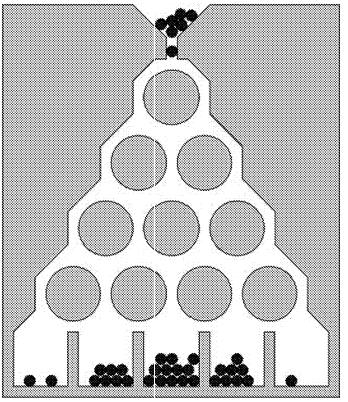


Príklad 4. Posledný vybraný príklad je zameraný na modelovanie a skúmanie pohybu guľky medzi prekážkami. Na pozorovanie pohybu skutočných guliek medzi prekážkami existuje zaujímavá pomôcka na výučbu pravdepodobnosti známa ako Galtonova doska.

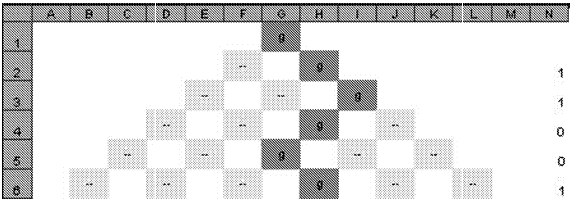
Základom tejto učebnej pomôcky je doska, na ktorej sú v radoch umiestnené kolíčky valcovitého tvaru, pričom počet kolíčkov v radoch sa postupne zväčšuje. Guľky sa spúšťajú z vrchnej strany dosky medzi kolíčky, na ktoré postupne narážajú a náhodne sa vychyľujú vľavo alebo vpravo. Po prekonaní poslednej prekážky umiestnenej v dolnom rade padajú guľky do priehradiek vytvorených pod prekážkami. Žiaci môžu pozorovať výsledky náhodných pokusov, ktorými sú pády guliek do niektorej z priehradiek. Schematicky možno Galtonovu dosku zobraziť pomocou obrázka 3 (http://commons.wikimedia.org/wiki/File:Galton_Board.svg).

Vzniká prirodzená otázka, či budú guľky padať do priehradiek pod prekážkami približne rovnako často, alebo budú do niektorých priehradiek padať častejšie. Zamyslime sa najprv, ako by sme mohli modelovať dráhu guľky na papieri alebo na tabuli. Po zakreslení prekážok a priehradiek by sme mohli pri každej prekážke hodiť mincu. Ak padne číslo, posunieme

guľku vľavo, ak padne znak, posunieme guľku vpravo a tak budeme pokračovať, až kým guľka nespadne po vychýlení na poslednej prekážke do niektorej priehradky. Na základe opísaného postupu možno vytvoriť tabuľku pomocou tabuľkového kalkulátora. Na obrázku 4 predstavujú prekážky biele políčka a dráha guľky je reprezentovaná znakmi „g“. Guľka môže po postupnom odchyľovaní na piatich prekážkach spadnúť do jednej zo šiestich priehradiek.



Obr. 3



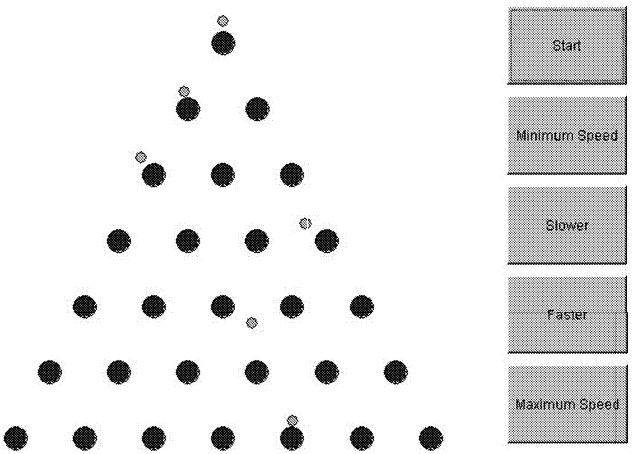
Obr. 4

Výsledky hádzania mincou sú uložené v stĺpci N, pričom v bunke N2 je zapísaný vzorec: `=IF(RAND()<0,5;0;1)`. Využíva sa v ňom matematická funkcia RAND, ktorej výsledkom je náhodné číslo z intervalu $\langle 0, 1)$ generované na základe rovnomerného rozdelenia pravdepodobnosti. Ak je v stĺpci N hodnota 0, guľka sa má posunúť vľavo a ak hodnota 1, guľka sa má posunúť vpravo. V bunke F2 je zapísaný vzorec, v ktorom sa na

základe náhodného čísla v tom istom riadku v stĺpci N a na základe pozície guľky v predchádzajúcom riadku rozhodne, či sa do bunky zapíše znak „g“ alebo znak „-“:

```
=IF(AND(E1="g";$N2=1);"g";IF(AND(G1="g";$N2=0);"g";"-"))
```

Uvedený vzorec je skopírovaný do buniek so sivým pozadím. Po opätovnom stláčaní klávesu F9 sa možno presvedčiť, že guľka padá častejšie do prostredných priehradiek. Je to spôsobené tým, že zatiaľ čo do krajných priehradiek existuje len jedna cesta, do prostredných priehradiek existuje viac ciest, ako sa môže do nich guľka dostať. Na internete možno nájsť applety, ktoré umožňujú nielen pozorovať pohyb guliek, ale aj určovať početnosti guliek v jednotlivých priehradkách. Na obrázku 5 je zobrazená časť okna appletu dostupného na stránke www.jcu.edu/math/isep/Quincunx/Quincunx.html.

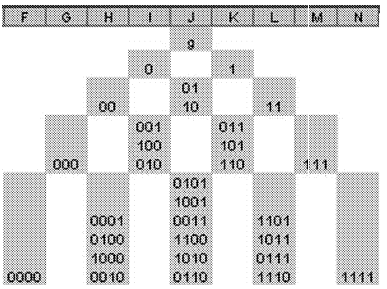


Obr. 5

V okne appletu sa dá nastaviť počet priehradiek aj počet guliek, ktoré budú postupne padať do jednotlivých priehradiek. V spodnej časti okna sa vykreslí histogram početnosti, na základe ktorého môžu žiaci vypočítať relatívnu početnosť guliek padnutých do jednotlivých priehradiek.

Pre porovnanie nameraných relatívnych početností s teoretickými hodnotami pravdepodobnosti je potrebné vypočítať pravdepodobnosť pádu

guľky do jednotlivých priehradiek. Pri výpočte využijeme základné myšlienky z modelu vytvoreného v prostredí tabuľkového kalkulátora. Základom výpočtu je určovanie počtu rôznych ciest guliek do jednotlivých priehradiek. Pre reprezentáciu ciest guliek využijeme postupnosti 0 a 1. Vetvenie ciest na prvej prekážke budeme reprezentovať 0 alebo 1. Pri rozdelení ciest na druhej prekážke dopíšeme k prvému číslu znova 0 alebo 1. Pri vetvení ciest na ďalších prekážkach budú vznikať stále dlhšie postupnosti 0 a 1. V každej k-tici z 0 a 1 je takýmto spôsobom zakódovaná celá cesta guľky pomedzi k prekážkami. Obrázok 6 zobrazuje výpis všetkých ciest do jednotlivých pozícií medzi prekážkami.



Obr. 6

Na k-tej úrovni vetvenia je spolu 2^k rôznych ciest do $k+1$ priehradiek. Z obrázka 6 vidno, že po odchýlení na 4 prekážkach môže guľka padnúť do jednej z 5 priehradiek, pričom do prostrednej priehradky existuje 6 rôznych ciest. Počet všetkých ciest guliek do jednotlivých pozícií na doske odpovedá číslam v Pascalovom trojuholníku, pričom aj v schéme na obrázku 6 vidno, že počet ciest do vybranej pozície je určený súčtom počtu ciest do susedných pozícií v predchádzajúcom riadku. Na obrázku 5 mohla guľka padnúť do jednej z ôsmich priehradiek, preto pre výpočet pravdepodobnosti pádu guliek do jednotlivých priehradiek by sme využili odpovedajúce čísla z 8. riadku Pascalovho trojuholníka.

Po podrobnejšom preskúmaní k-tic v jednotlivých pozíciách na doske si možno všimnúť, že všetky k-tice na jednej pozícii obsahujú rovnaký počet 1 (aj 0). Je to pochopiteľné, lebo pri ceste do n-tej priehradky zľava sa musela guľka odchýliť na prekážkach $n-1$krát vpravo. Pre výpočet pravdepodobnosti, že guľka padne do tej priehradky z 8 priehradiek, v ktorej

reprezentácia ciest obsahuje s jednotiek a $7-s$ núl, využijeme Bernoulliho schému. Platí:

$$p(s) = \binom{7}{s} \cdot \left(\frac{1}{2}\right)^{s} \cdot \left(\frac{1}{2}\right)^{7-s} = \binom{7}{s} \cdot \left(\frac{1}{2}\right)^{7}$$

pričom $s = 0, \ldots, 7$. Vo výsledku sú čísla z 8. riadku Pascalovho trojuholníka.

Záver

Modelovaniu sa možno učiť len aktívnou praktickou činnosťou. Preto by mal byť venovaný vo vyučovaní matematiky dostatočný priestor rôznym druhom modelovacích aktivít, ktoré môžu byť aj súčasťou práce na projektoch. Pri plánovaní modelovacích aktivít je potrebné pripravovať námety na prácu s rôznymi typmi modelov, počnúc od aritmetických, geometrických a grafických až po algebraicko-analytické. Niekedy sa vo vyučovaní matematiky rýchlo prechádza k využívaniu algebraického modelu, aj keď žiaci ešte nemajú dostatočné zručnosti z využívania jednoduchších modelov. Treba si však uvedomiť, že jednoduché aritmetické a geometrické modely poskytujú základ pre zložitejšie a viac sofistikované modely využívané v geometrii, algebre a analýze.

Literatura

[1] *Blum, W. – Galbraith, P. L. – Henn, H., W. – Niss, M.*: Modelling and applications in mathematics education: the 14th ICMI study. New ICMI Study Series Volume 10, Springer, 2007.

[2] *Jančařík, A. – Hošpesová, A. – Dvořák, P.*: Využití programu MS Excel v práci učitele matematiky. Univerzita Karlova v Praze, 2007.

[3] *Jedinák, D.*: James Sylvester – matematik hrdý na svoju poéziu, Obzory matematiky, fyziky a informatiky, 3/2009, ročník 38.

[4] *Sekerák, J.*: Kľúčové kompetencie v matematickom vzdelávaní. Matematika Informatika Fyzika, Metodicko - pedagogické centrum Prešov a PF UPJŠ v Košiciach, číslo 29, str. 132 – 137, 2007.

[5] *Žilková, K.*: Školská matematika v prostredí IKT. Univerzita Komenského Bratislava, 2009.

(Autorkou úvodní ilustrace je MGr. Jaroslava Čermáková.)

Počítačová bezpečnost ve výuce informatiky

(5. část: cesta k polyalfabetické substituci)

MICHAL MUSÍLEK – ŠTĚPÁN HUBÁLOVSKÝ

Přírodovědecká fakulta Univerzity Hradec Králové

Ve třetí části našeho seriálu jsme se naučili luštit šifrový text (zašifrovaný jednoduchou záměnou) pomocí frekvenční analýzy a ve čtvrté jsme popsali algoritmus zdokonalující a výrazně zefektivňující tuto metodu rozšířením frekvenční analýzy také na bigramy (dvojice písmen). Také jsme se zmínili o tom, jak zdatnými kryptoanalytiky byli po celý středověk Arabové. V roce 1412 dokončil učenec *Šihább al-Qalqašandí* čtrnáctidílnou encyklopedii pro úředníky, ve které popisuje mimo jiné celou řadu steganografických metod a šifrovacích postupů a abeced. V části věnované kryptoanalýze popisuje nejen frekvenční analýzu, ale také využití bigramových vztahů [4]. Evropští učenci nezůstávají zpět, a jednoduchá záměna postupně ztrácí pověst bezpečného způsobu utajení obsahu zprávy. Kryptologové jsou nuceni svými protivníky kryptoanalytiky ke zdokonalování šifrovacích systémů.

Jednou z možností jak oklamat frekvenční analýzu je použití tzv. homofonní substituce. Často se vyskytující znaky v ní budeme vyjadřovat ne jedním, ale několika různými znaky. Tím zmateme luštitele textu hned dvakrát. Jednak bude mít taková šifrová abeceda více „písmen“ než abeceda používaná pro příslušný otevřený text, jednak budou v šifrovém textu chybět výrazně frekventované znaky, k nimž bychom přiřadili nejčastěji se vyskytující písmena (víme, že v českém jazyce jde o písmena E, A, O, I a N). Zkusme takovou důkladnou homofonní substituci navrhnout. Vraťme se k tabulce četností písmen v českém textu (tab. 1).

Vydělíme četnosti stejným číslem (např. číslem 1,5) a výsledek zaokrouhlíme na celé číslo. Vyjde-li nám nula, uvedeme ovšem jedničku, protože každé písmeno otevřeného textu musíme alespoň jedním způsobem umět nahradit. Vyjde-li 5 nebo 7, uvedeme 6 kvůli náhodnému generování použité záměny. Sečteme-li počty různých nahrazení u jednotlivých

Tabulka 1

A	B	C	D	**E**	F	G	H	**I**	J	K	L	M
8,8	1,7	3,6	3,6	**10,5**	0,4	0,3	2,3	**7,7**	2,0	3,8	4,1	3,3
N	**O**	P	Q	R	S	T	U	V	W	X	Y	Z
6,7	**8,3**	3,5	0,0	5,2	5,4	5,6	3,8	4,4	0,1	0,1	2,7	3,1

písmen abecedy, dostaneme číslo 72, což je potřebný počet znaků šifrové abecedy.

Tohoto počtu můžeme dosáhnout například tak, že k 26 písmenům mezinárodní abecedy přidáme číslice 1 až 9 (nulu vynecháme, pletla by se s písmenem O), 10 písmen řecké abecedy (Γ, Δ, Θ, Λ, Ξ, Π, Σ, Φ, Ψ, Ω), 10 písmen cyrilice (Б, Ж, И, Ц, Ч, Ш Щ, Э, Ю, Я) a 17 různých značek a znamének ($, £, ¥, †, ‡, €, ∞, ∩, ∫, ≈, ≡, ⊕, ⊖, ∗, §, #).

Převodová tabulka pro šifrování otevřeného textu bude zohledňovat nejen nahrazované písmeno, ale také náhodnou volbu určenou hodem kostkou (s výjimkou znaků, které mají pouze jedno možné nahrazení). Při šifrování budeme házet běžnou hrací kostkou, kterou známe např. ze hry Člověče nezlob se, a podle výsledku hodu provedeme náhradu. Převodová tabulka pak pro šifrování může vypadat například viz tab. 2.

Zkuste dešifrovat: Ξ£Λ#Q ΨΛЧМИ §Φ1∫∩ λ9ЧЭЦ M⊖M£Z G∩#4F Ю⊕A2Ω #K⊖.

Je zřejmé, že práce s homofonní šifrou je o dost komplikovanější než s běžnou jednoduchou záměnou. Při šifrování musíme náhodně vybírat konkrétní záměnu z několika možností. Při dešifrování má převodová tabulka mnohem více sloupců, v našem případě 72 místo 26. Šifrová abeceda musí používat méně obvyklé znaky, které je třeba si osvojit. Frekvenční analýza u ní nevede k cíli tak přímočaře jako u jednoduché záměny, ale při zachycení většího množství zpráv, jež jsou šifrovány podle stejné převodové tabulky, je i homofonní substituce luštitelná.

Možnou cestou k zjednodušení homofonní substituce je použít k nahrazení každého písmene místo jednoho znaku z mohutné šifrové abecedy dvouciferné číslo, tedy dvě číslice. Šifry, které každý znak abecedy otevřeného textu nahrazují dvojicí znaků šifrové abecedy, nazýváme digrafické substituce. V naší převodové tabulce bychom použili 72 náhodně vybra-

Tabulka 2

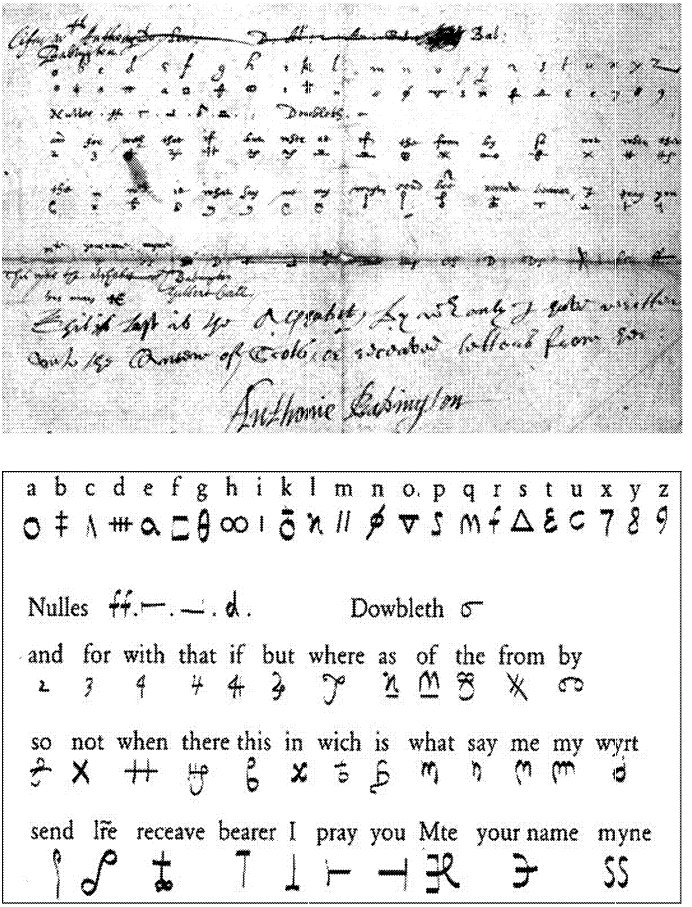
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	$		Λ	Π	Φ				X		≈	T	A
2	3				8			U	N				
3	Ш	§			⊖	F	Я		P	D	Σ	‡	
4	2				Ш				#				
5	И		G	R	7			I	V		K	E	☪
6	Ψ				∩				5				

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	Θ	₤			W	Б	Ц	Z	Y				
2	9	J	∫			Э	Г					₤	⋆
3	4	6		L	¥	Ж	Ω	S	Δ	C	B		
4	≡	†				O	Ǫ						
5	**nový**	Ю	Ξ		⊕	**nový**	**nový**	∞	M			H	L
6	**hod**	Ч				**hod**	**hod**						

ných dvojciferných čísel, ale všech dvouciferných čísel je 90. Jak naložit s těmi zbývajícími?

Využití volných dvouciferných čísel či volných znaků rozsáhlé šifrové abecedy je v principu dvojí. Buď je přimícháme náhodně do šifrového textu, aniž by nesly jakoukoliv informaci, pak se jim říká klamače a slouží pouze ke ztížení frekvenční analýzy šifrového textu, nebo se pomocí jednotlivých znaků kódují celá často se vyskytující slova. Kombinace šifry, kódů a klamačů byly používány po dobu více než pěti století a mají své vlastní pojmenování, říká se jim nomenklátory. První nomenklátory vytvořil pro vyslance vzdoropapeže Klementa VII. italský kryptograf *Gabreli di Lavinde* v roce 1379. Šlo o kombinace homofonních šifer a kódů [4].

Jiný nomenklátor, složený z jednoduché záměny, 35 kódů, 4 klamačů a symbolu označujícího zdvojené písmeno („dowbleth“) se stal osudným skotské královně Marii Stuartovně. Tajná korespondence mezi Marií Startovnou a vůdcem spiklenců Anthony Babingtonem byla bohužel zachycována, opisována a postupně rozluštěna kryptoanalytikem *Thomasem Phelippesem*. Tím, že v jednom z dopisů vyslovila souhlas s plánem na zavraždění anglické královny Alžběty, si Marie podepsala vlastní rozsudek



Obr. 1 Nomenklátor Marie Stuartovny – originál rukopisu Anthony Babingtona a význam značek

smrti. Tomuto dramatickému příběhu z dějin kryptologie věnuje Simon Singh první kapitolu své knihy [3].

Přestože použití homofonních substitucí a nomenklátorů značně ztížilo luštění, byly i takovéto šifrové systémy luštitelné při zachycení většího množství zpráv a při odhadnutí jejich obsahu z kontextu. Bylo potřeba přijít s novým nápadem. Přišel s ním italský renesanční humanista a polyhistor *Leon Battista Alberti*, který kolem roku 1466 na podnět papežského

tajemníka Leonarda Data sepsal práci o utajené komunikaci, ve které mimo jiné navrhuje použití dvou a více různých převodových tabulek k šifrování zprávy. Taková substituce, která se skládá z několika jednoduchých záměn, které jsou podle dohodnutého systému postupně používány na jednotlivé znaky otevřeného textu, se nazývá polyalfabetická substituce. Alberti sestrojil také mechanickou pomůcku – šifrovací disk, který umožnil vzájemným pootočením vnitřního a vnějšího kotouče posun abecedy o libovolný počet znaků. Abecedu doporučuje posunout po každých třech až čtyřech slovech.

Obr. 2 Blaise de Vigenére

V roce 1518 vyšla tiskem první kniha o kryptologii. Knihu začal psát roku 1508 benediktýn *Johannes Trithemius*. Nabízí v ní jinou pomůcku pro šifrování, tabulku posunutých abeced nazývanou *tabula recta*. Tritheimus vylepšuje Albertiho systém doporučením měnit šifrovou abecedu po každém písmenu. Polyalfabetickou substituci propagoval italský šlechtic *Giovan Battista Bellaso* ve své knize *La cifra*, vydané roku 1553, v níž rozvíjí myšlenky Albertiho a Trithemia a zavádí systémy založené na utajení klíče (nikoliv metody šifrování). Jedním ze systémů je polyalfabetická šifra s periodicky se opakujícím heslem, známá pod jménem Vigenérova šifra. Francouz *Blaise de Vigenére* ji popsal ve své knize *Traicté des chiffers*, vydané v roce 1586.

Ukažme si jak takové šifrování pomocí Vigenérovy šifry probíhá. Pro zašifrování použijeme část myšlenky z knihy Alberta Einsteina [1] a jako heslo použijeme název této knihy. Nejprve přepíšeme otevřený text: „Ještě v sedmnáctém století byli vědci a umělci v celé Evropě tak spjati s ...“ bez diakritiky a bez mezer a nad něj zapíšeme stejným způsobem heslo tolikrát, kolikrát je ho zapotřebí.

```
JAKVIDIMSVETJAKVIDIMSVETJAKVIDIMSVETJAKVIDIMSVETJAKVIDIMSVE
JESTEVSEDMNACTEMSTOLETIBYLIVEDCIAUMELCIVCELEEVROPETAKSPJATI
SECOMYAQVHRTLTOHAWWXWOMUHLSQMGKUS PQXUCSQKHTQWQVHYEDVSVXVSOM
```

Jednotlivé znaky šifrového textu pak získáme použitím Trithemiovy tabulky tabula recta tak, že v řádku začínajícím příslušným písmenem hesla, a ve sloupci začínajícím příslušným písmenem otevřeného textu najdeme odpovídající znak šifrového textu. Pak už zbývá pouze přepsat výsledný šifrový text do pětimístných skupin:

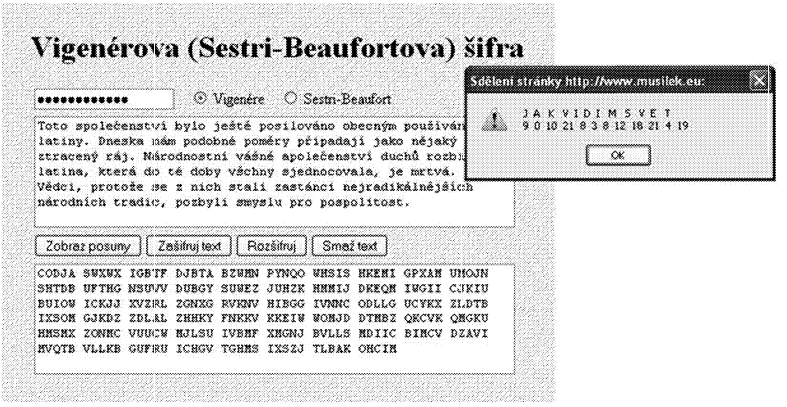
TABULA RECTA

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

Dešifrování probíhá tak, že v řádku začínajícím příslušným písmenem hesla najdeme určité písmeno šifrového textu a odpovídající písmeno otevřeného textu je pak v prvním řádku téhož sloupce. Vyzkoušejte si dešifrování na druhé části Einsteinovy myšlenky:

```
BPYGM FVKED MWNAV DAWQO CTQBY OEOGC MVWEM VQSZJ TXXDS XMIXL
SOQFS QMYEE XSDDB HUQJI IFXHV TVDPX GYEM
```

Velmi podobná Vigenérově šifře je *Sestri-Beaufortova* šifra, kterou jako první popsal roku 1710 *Giovanni Sestri* [4], ale je známa spíše pod názvem Beaufortova varianta Vigenérovy šifry. Šifruje se v ní stejným způsobem, jakým se ve Vigenérově šifře dešifruje a naopak. Obě uvedené šifry můžeme realizovat také pomocí počítače, např. využitím skriptu na webu [2]. Vzhled webového rozhraní vidíte na obr. 3. Je třeba vyplnit heslo a otevřený text nad tlačítky, přitom otevřený text může být zapsán s diakritikou a interpunkčními znaménky. Stiskem tlačítka „Zašifruj text“ se provede šifrování a výsledek se objeví v dolním textovém poli, již rozdělený do pětimístných skupin. Dešifrování probíhá analogicky, je třeba vyplnit heslo, šifrový text se zapíše do horního textového pole a stiskem tlačítka „Rozšifruj“ se provede dešifrování, a výsledek se zobrazí v dolním textovém poli. Zde ovšem musíme provést dělení do slov a doplnění diakritiky ručně. Přepínání mezi systémem Vigenére a Sestri-Beaufort provádíme pomocí radiových tlačítek vedle okénka s heslem. Implicitní hodnota je Vigenére.



Obr. 3 Webové rozhraní skriptu pro šifrování a dešifrování pomocí Vigenérovy a Sestri_Beaufortovy šifry.

Třetím podobným způsobem šifrování je systém Beaufort, který popsal anglický admirál sir *Francis Beaufort* (známý svou stupnicí síly větru) a popularizoval ji jeho bratr, který tabulku tabula recta prodával společně s návodem k použití a tvorbě hesla za šest pencí od roku 1857. Výhodou Beaufortova systému proti předchozím je stejný postup při šifrování a dešifrování. Heslo si opět napíšeme periodicky nad otevřený text, ale postup hledání záměny je teď jiný. Vybereme řádek tabulky začínající daným písmenem otevřeného textu, v něm najdeme daný znak hesla a ve stejném sloupci přečteme písmeno v prvním řádku tabulky. To zapíšeme jako znak šifrového textu. Analogický postup platí i pro dešifrování. Heslo si napíšeme periodicky nad šifrový text, vybereme řádek tabulky začínající daným písmenem šifrového textu, v řádku najdeme příslušný znak hesla a ve stejném sloupci v prvním řádku najdeme odpovídající písmeno otevřeného textu. Ukažme si to na příkladu:

```
JAKVIDIMSVETJAKVIDIMSVETJAKVIDIMSVETJAKVIDIMSVETJAKVIDIMSVET
DNESKASEOCITAMETVARIVTVARDRTIVESKUTECNOSTIZENOSITELIMYSLENKY
GNGDYDQIETWAJOGCNDREXCJTSXTCAIEUIBLPHNWDPVJIFHMLQWZNWFQBOIUV
```

Všechny tři výše uvedené šifrové systémy shrnul a matematicky jednoduše formalizoval roku 1888 francouzský učenec *Marquis Gaetan Henri Leon Viarizio de Lesegno*. Převedl písmena abecedy na čísla (A = 0, B = 1, C = 2, ., Y = 24, Z = 25) a odvodil, že pro znak klíče K, znak otevřeného textu O a znak šifrového textu Š platí převodové vzorce [4]:

	Šifrování	Dešifrování
Systém Vigenére	Š = O + K	O = Š − K
Systém Beaufort	Š = K − O	O = K − Š
Systém Sestri-Vigenére	Š = O − K	O = Š + K

Z tabulky převodových vzorců je dobře vidět vztah mezi systémy Vigenére a Sestri-Baufort, stejně jako stejný postup šifrování i dešifrování u systému Beaufort. Uvedené vztahy můžeme snadno zabudovat do programů, které šifrování i dešifrování zautomatizují.

Polyalfabetické substituce s periodickým heslem byly dlouho pokládány za velmi bezpečné šifrovací systémy. Příště si ale ukážeme, že i takové

šifry lze, zejména při použití krátkého hesla u dostatečně dlouhého šifrového textu, poměrně snadno luštit. Nabízí se otázka, zda vůbec existuje absolutně bezpečný systém šifrování.

Absolutně bezpečný šifrový systém

Roku 1843 vyslovil americký spisovatel Edgar Alan Poe domněnku, že dokáže-li lidský rozum nějakou šifru vymyslet, dokáže ji i rozluštit. Roku 1917 však jiný Američan *Gibert S. Vernam* vymyslel šifrovací systém založený na použití jednorázového náhodně vygenerovaného hesla, které má stejnou délku jako zpráva sama [4]. Takový systém je skutečně absolutně bezpečný, ale pouze při dodržení velmi přísných podmínek. Heslo musí být skutečně zcela náhodnou sekvencí znaků, nikoliv např. náhodně zvoleným úsekem z textu písně, či knihy. Heslo musí být použito pouze jednou. Už při dvojím použití hesla k zašifrování dvou různých zpráv znají kryptoanalytici postup, který může vést k prolomení šifry [3]. Příprava velkého množství jednorázových hesel a jejich bezpečná distribuce je velmi náročná. Proto se tento systém používá zcela výjimečně. Matematický důkaz absolutní bezpečnosti Vernamovy šifry podal teprve roku 1949 americký matematik a elektronik *Claude Elwood Shannon* [5].

Literatura

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

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

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

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

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