STARŠIE KÓDOVACIE SYSTÉMY

V minulom čísle ste si mohli prečítať krátky úvod do kódovania. Možno ste tam nenašli to, čo si pod kódmi či šiframi zvyčajne predstavujete – viac či menej náhodné zhluky číslic, písmen či obrázkov. V tejto časti seriálu o kódovaní si však prídete na svoje – zameriame sa v ňom na jednoduchšie šifry používané v minulosti i súčasnosti.

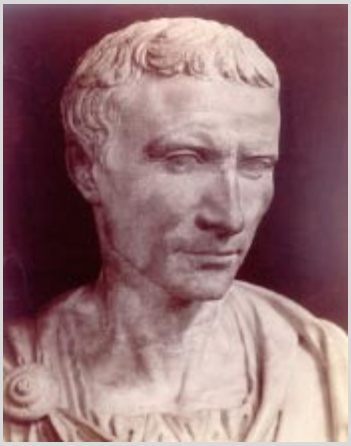
Medzi najjednoduchšie šifry, ktoré si môžete vyskúšať, je písanie textu zrkadlovo. Keď píšete dostatočne škaredo týmto spôsobom, nepovolaná osoba len ťažko zistí, čo ste napísali. Ak však príde na to, že má váš text čítať v zrkadle, môžete sa spoliehať už len na svoj škrabopis, čo v niektorých prípadoch môže byť stále veľmi bezpečnou šifrou. Jedným z prvých, ktorí tento spôsob písania používali a dochovala sa nám o tom aj písomná zmienka, bol Leonardo da Vinci.

Skytalé

Tento spôsob utajovania informácií sa používal v starovekom Grécku a Sparte. Princíp šifrovania údajov spočíva v tom, že sa na drevený valec vopred dohodnutého priemeru namotal pásik pergamenu alebo kože a v smere hlavnej osi valca sa naň napísal text od jedného konca k druhému. Po jeho odmotaní na ňom zostali písmená, ktoré nedávali spolu zmysel. Jediným spôsobom, ako dešifrovať zašifrovaný text, bolo namotanie pásika na valec rovnakého priemeru. Čoskoro sa však našli aj spôsoby, ako text dešifrovať – stačilo pásik namotať na kužeľ a postupne ho na ňom posúvať, až kým sa nenašiel vhodný priemer použitého valca.

Skytalé

V tomto článku sa budeme často stretať s prevodom písmen na čísla a naopak, a tak si hneď na úvod tento prevod zobrazíme v tabuľke – každému písmenu abecedy priradíme jeho poradie v abecede:



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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Cézarova šifra

Princíp Cézarovej šifry je veľmi jednoduchý, ale vo svojom čase geniálny a dlho neprekonaný. Princípom tejto šifry je posunutie každého písmena na písmeno, ktoré je v abecede o tri miesta za ním (v našej tabuľke doprava). Tak sa napríklad písmeno **A** zmení na písmeno **D**, písmeno **B** na písmeno **E**, ..., písmeno **W** na písmeno **Z**, písmeno **X** na písmeno **A** (keď prídeme na koniec abecedy, pokračujeme na jej začiatku) atď. Dešifrovanie prebieha naopak – každé písmeno posunieme o 3 písmená v abecede späť – doľava. Posun si môžeme, samozrejme, zvoliť ľubovoľný. Na rýchle šifrovanie slúži otočné koliesko – na začiatku si nastavíme, na ktoré písmeno sa zobrazí písmeno **A** a potom už len pozeráme na vytvorené páry písmen: Vo vonkajšom prstenci hľadáme písmená nezašifrovaného textu a vo vnútornom nachádzame ich zašifrovanú podobu. Na obrázku vidíme posun o 3 písmená doprava. Táto šifra sa ľahko dešifruje, pretože ak vieme, že ide len o posun v abecede, tak nám stačí vyskúšať 25 možností posunutia (prípadne aj viac, ak používame inú abecedu), čo na počítači nerobí žiaden problém. Ak by sme chceli zvýšiť bezpečnosť tejto šifry, môžeme sa dohodnúť, že napríklad prvé písmeno bude posúvané o 4 doprava, druhé o 5 doľava, tretie o 3 doprava a túto skupinu troch posunutí budeme za sebou opakovať.

Polybiov štvorec

Tento kód môžete nájsť v literatúre aj pod menom fakľový ďalekopis. Grécky historik Polybios (210 – 120 p. n. l.) vymyslel spôsob, ako zasielať správy na veľké vzdialenosti pomocou svetelnej signalizácie. Základom bola tabuľka políčok, do ktorej vpísal 25 písmen abecedy. Keďže abeceda, ktorú používame, má 26 pís-

men, môžeme jedno z písmen vynechať alebo dať dve do jedného políčka. Zvyčajne sa tak robí s písmenami Q a W, ktoré sa u nás veľmi často nevyskytujú a z kontextu je vždy jasné, o ktoré písmeno ide. V angličtine sa napríklad zlučujú písmená I a J.

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

Ak by sme potrebovali prenášať viac písmen, stačí rozšíriť tabuľku na príslušné rozmery (nemusí byť ani štvorcová). Týmto usporiadaním vieme charakterizovať každé písmeno usporiadanou dvojicou riadok-stĺpec. Sám autor odporúčal, aby sa správa podávala ďalej tak, že počet faklí v ľavej ruke určuje číslo riadka a počet faklí v pravej ruke číslo stĺpca daného písmena. Takýto prenos však mohol sledovať hocikto a odchytiť vysielanú správu. Jednou z možností bolo správu najprv nejakou inou technikou zašifrovať a odosielať už zašifrovanú správu. Inou možnosťou je zvoliť si náhodné usporiadanie písmen v štvorci. Ďalšia metóda spočíva v tom, že si zvolíme kľúčové slovo, ktoré napíšeme do prvého riadka, prípadne aj ďalších, pričom použité písmená už neopakujeme. Ostatné písmená sa potom doplnia tak, ako idú v abecede, pričom písmená, ktoré už sú v štvorci, v našom kľúčovom slove, napísané, vynechávame. Ak si zvolíme ako kľúčové slovo slovo **MLADY VEDEC**, dostaneme takúto tabuľku (písmená DE zo slova VEDEC sme už nepísali, pretože sa v spojení Mladý vedec vyskytli už skôr):

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

V tejto šifre je každé písmeno zakódované dvoma číslicami, ide o tzv. *digrafickú šifru*. Môžeme sa na ňu pozerať aj ako na jednoduchú substitučnú šifru, kde každému písmenu priradíme dvojciferné číslo, ktorého cifry sú len 1, 2, 3, 4 alebo 5.

Existuje veľa šifier, ktoré sú založené na Polybiovom štvorci. Jedna z nich bola používaná aj vo väzeniach, kde si väzni vyťukávali jednotlivé súradnice písmen na mreže. Prenášanej správe tak rozumeli len tí, ktorí poznali správny kľúč. Medzi ďalšie patria Zlomková a Čínska šifra.

Zlomková šifra

Na šifrovanie pomocou zlomkovej šifry sa používa Polybiov štvorec, pričom sa jednotlivé písmená kódujú vo forme zlomkov, kde čitateľ udáva číslo riadka a menovateľ zlomku udáva číslo stĺpca, teda táto šifra predstavuje len iný zápis vysielania pomocou fakieľ. Teda napríklad slovo **AHOJ** by sme pomocou základného Polybiovho štvorca zakódovali ako **1/1, 2/3, 3/5, 2/5**. Čítanie môžeme trochu sťažiť tým, že zlomky nebudeme uvádzať v takom tvare, akom nám vyjdú, ale upravíme ich na základný tvar. Tým sa dekódovanie samozrejme stane nejednoznačným, ale na druhej strane sa dá ľahko nájsť správne písmeno, pretože nemáme veľa možností krátenia.

Čínska šifra

Táto na prvý pohľad veľmi efektná a ťažko dešifrovateľná šifra vychádza taktiež z Polybiovho štvorca. Jednotlivé písmená v nej šifrujeme pomocou zvislých a vodorovných čiar tak, že počet vodorovných čiar udáva riadok a počet zvislých čiar udáva stĺpec, v ktorom sa písmeno nachádza v zvolenom Polybiovom štvorci. Zároveň tieto čiary volíme tak, aby neboli rovnako dlhé a ani nemali rovnaký sklon. Zároveň tieto čiary môžeme aj rozlične zakriviť na ich koncoch, prípadne môžeme urobiť aj vlnovky – podľa inšpirácie, chuti a estetického cítenia – fantázii sa medze nekladú. Tu si treba dávať pozor len na to, aby ste vedeli rozlíšiť, či sú jednotlivé čiary sú zvislé alebo vodorovné. Ako príklad si zvolíme Polybiov štvorec pre slovo **CINSKA SIFRA** (po vynechaní rovnakých písmen ostane už len **CINSKAFR**):

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

Zašifrujme pomocou tohto štvorca slovné spojenie **Mladý vedec**, teda bez diakritiky **MLADY VEDEC**. Prvé písmeno, **M**, sa nachádza v štvrtom riadku a prvom stĺpci. To znamená, že musíme urobiť štyri vodorovné čiary a jednu zvislú. Písmeno **L** sa nachádza v treťom riadku a piatom stĺpci, teda urobíme tri vodorovné a päť zvislých čiar. Takto opakujeme postup, až prídeme k písmenu **C**, ktoré sa nachádza v prvom riadku a prvom stĺpci, takže urobíme už len jednu vodorovnú a jednu zvislú čiaru.

Dešifrovanie tejto šifry je pre človeka, ktorý ju pozná, veľmi ľahké – stačí počítať zvislé a vodorovné čiary a potom už len nájsť príslušné pozície písmen v štvorci. Na zmätenie nepriateľa môžete do tejto šifry vložiť miestami bodky, o ktorých budete len vy vedieť, že nič neznamenajú.

Posuvný kód

Princíp tohto kódu je veľmi jednoduchý a pre človeka, ktorý nepozná systém kódovania, nezrozumiteľný a nedekódovateľný. Východiskom pre kódovanie je dostatočne dlhý text. Môže ním byť text piesne, úryvok z básne alebo aj celá kniha. My si za náš pomocný text zoberieme úvodný odsek tohto článku:

```
V minulom čísle ste si mohli prečítať
krátky úvod do kódovania. Možno ste tam
nenašli to, čo si pod kódmi či šiframi
zvyčajne predstavujete – viac či menej
náhodné zhluky číslic, písmen či obrázkov.
V tejto časti seriálu o kódovaní si však
prídete na svoje – zameriame sa v ňom na
jednoduchšie šifry používané v minulosti
i súčasnosti.
```

Text, ktorý budeme kódovať, bude:

KODUJEME POSUVNYM KODOM.

Postup spočíva najprv v prevode písmen našej správy na čísla vyjadrujúce ich poradie v abecede na základe tabuľky uvedenej v úvode článku:

K	O	D	U	J	E	M	E
11	15	4	21	10	5	13	5

P	O	S	U	V	N	Y	M
16	15	19	21	22	14	25	13

K	O	D	O	M
11	15	4	15	13

Prevod robíme do abecedy bez diakritiky kvôli jednoduchosti. Nič vám však nebráni použiť plnú abecedu s diakritikou, interpunkciou a medzerami – princíp kódovania ostane ten istý.

Ako prvé ideme zakódovať písmeno **K** – je na 11. mieste v abecede, a tak jeho kódom bude 11. písmeno v poradí v našom pomocnom texte, pričom medzery preskakujeme. Bude to písmeno **S**. To si zapíšeme. Teraz ideme zakódovať ďalšie písmeno v poradí – písmeno **O**. Začneme písmenom nasledujúcim v texte za už nájdeným **S** a odpočítame 15 znakov. Dostaneme tak písmeno **E**. Pokračujeme ďalej rovnakým spôsobom, pričom za znak považujeme aj bodku, čiarku či pomlčku, a dostaneme, že prvé slovo je po zakódovaní **SEAIEEPD**. Za týmto slovom dáme medzeru a pokračujeme ďalej až po predposledné kódované písmeno **O**: **SEAIEEPD ATNČSNMN ŠNIO**. Tu náš pomocný text skončil – pri počítaní posledných 13-tich písmen by sme už nemali odkiaľ čerpať písmená. Prejdeme však opäť na začiatok textu a môžeme pokračovať – 4 znaky nám ostali do konca textu, a tak na začiatku textu musíme nájsť deviaty znak $(13-4=9)$ – je to písmeno **Č**. Výsledný kód je **SEAIEEPD ATNČSNMN ŠNIOČ**.

Teraz sme však pred otázkou: Ako tento zakódovaný text dekódujeme? Na prvý pohľad by sa zdalo, že stačí nájsť prvé písmeno **S** v našom pomocnom texte, vypočítať, ktoré je to písmeno v poradí a podľa tohto čísla určiť písmeno v abecede. Pri tomto písmene nám vyjde 11, a teda prvé písmeno bude **K**. Druhé zakódované písmeno je však **E**. Najbližšie E za písmenom S je už na druhej pozícii, a tak by malo byť dekódovaným písmenom písmeno **B**, čo ale nie je správne. Kde sa stala chyba? Problém je v tom, že v texte sa nám bude často stávať, že sa budú písmená v pomocnom texte často opakovať. A ak použijeme dlhšiu abecedu (napr. s diakritikou), potom to bude ešte výraznejšie. Tým je znemožnené jednoznačné dekódovanie. Na prvý pohľad sme dostali nepoužiteľný systém kódovania, pretože ho nevieme dekódovať. Avšak aj takéto kódy majú svoj význam.

Kedysi v stredoveku si učenci posielali výsledky svojho bádania tak, že zoradili písmená celej vety alebo textu abecedne za sebou. Napríklad z vety *„Dnes je pekný deň.“* by ste dostali *„ddeeeejknnňpsý“*, čo už veľmi zrozumiteľné nie je. Krátke texty sa však dajú rozobratím viacerých možností dekódovať, pomôckou býva často aj to, že viete, z akej oblasti text pochádza. Dlhšie texty sa však veľmi ťažko dekódujú, navyše dekódovanie ani nie je jednoznačné. Takéto kódy, ktoré sa dajú jednoznačne zakódovať a nedajú sa jednoznačne dekódovať, nazývame *jednosmerné*. Ich využitie spočíva v utajení skutočností a ich neskoršom overení – takto sa môžu kódovať napríklad heslá v počítači. Istým algoritmom je heslo zakódované a uložené. Keď chceme neskôr zistiť, či sme zadali správne heslo, tak počítač zakóduje nami zadaný reťazec písmen a výsledok porovná s uloženým reťazcom. Ak sa zhodujú, zadali sme správne heslo. Ak nie, heslo nebolo správne.

Ako by sme mohli modifikovať tento posuvný kód, aby sa dal jednoznačne dekódovať? Jedným z riešení je počítať, ktoré v poradí z daných písmen máme použiť, aby sme dostali to správne, a toto číslo pripísať ku každému písmenu. Ukážeme si to na našom príklade: Písmeno **K** zakódujeme na **S**. Od začiatku nášho pomocného textu po toto písmeno S sa nevyskytuje žiadne iné písmeno S, preto k písmenu **S** pripíšeme číslo **1** (naše **S** je prvé S v poradí). Pri druhom písmene, **O**, dostávame, že bude zakódované ako **E**. Od písmena **S** po toto písmeno **E** sa nachádzajú ešte 2 písmená E (v slove „čísle“ a „ste“), teda naše **E** je tretie v poradí. Preto k písmenu **E** pripíšeme číslo **3**. Opakovaním tohto postupu dostaneme:

S1 E3 A1 I1 E1 E1 P1 D2 A2 T2 N3 Č2 S2 N1 M1 N1 Š1 N1 I1 O2 Č1.

Pri dekódovaní už nebudeme mať problém – v tomto prípade si nájdeme prvé písmeno **S** v pomocnom texte, zapíšeme si jeho poradie, za ním nájdeme tretie písmeno **E** a zapíšeme si jeho poradie za písmenom **S**, za ním nájdeme prvé písmeno **A** atď. (modrou je znázornené prvé prechádzanie textom, červenou druhé):

```
V minulom ČíSle ste si mohli prEčítAť
krátky úvod do kódovanIa. Možno stE tam
nEnašli to, čo si Pod kóDmi či šiframi
zvyčAjne predstavujeTe – viac či menej
náhodNé zhluky číslic, písmen Či obrázkov.
V tejto časti Seriálu o kódovaNí si však
prídete na svoje – zaMeriame sa v ňom Na
jednoduchŠie šifry používaNé v mInulosti
i súčasnOsti.
```

Takto sme dostali pomerne bezpečnú šifru. Jediným problémom je to, aby mali obidve strany rovnaký pomocný text. To sa dá zabezpečiť rôznymi spôsobmi – jeho zaslaním či výmenou, ale dajú sa použiť aj iné dohody – napríklad sa bude kódovať na základe vydania dohodnutých novín v danom dni.

Martin Hriňák