Šifry

Od té doby, kdy si lidé začali posílat důležité zprávy, snažili se jiní lidé tyto zprávy zachytit. Jednou z možností, jak ochránit své vzkazy před zvědavci bylo zajistit jim silný (pokud možno ozbrojený doprovod), druhou možností pak napsat zprávu tak, aby na první pohled nedávala smysl – **zašifrovat** ji.

Jenže lidé byli (jsou a budou) zvědaví, proto se snažili tajné zprávy rozluštit – **dešifrovat**. Dodnes však existují šifry, které ještě nikdo nerozluštil. Například některé spisy slavného vědce, anglického mnicha Rogera Bacona, který žil ve 13. století, dosud čekají na svého čtenáře.

Dnes je šifrování (cizím slovem **kryptografie**) složitá věda, v níž se velmi často uplatňují nejlepší a nejvýkonnější superpočítače. To ovšem není náš problém. Proto na počítače při šifrování a dešifrování zapomeneme a budeme se raději více spoléhat na svoji vlastní hlavu.

Rozdělení šifer:

1. Šifry transpoziční – princip tohoto způsobu spočívá v zdánlivě nesouvislé směsi písmen, která však zůstávají ve svém původním významu, jen jsou všelijak přeházena nebo poskládána do různých obrazců.

2. Šifry substituční – zde je každé písmeno nahrazeno jiným písmenem, znakem nebo číslicí.

3. Šifry kombinované – tyto patří mezi šifry složitější, vznikají kombinací předešlých skupin. Patří sem i šifry vícenásobně zašifrované, pochopitelně pokaždé jinak. A taky šifry – „chameleoni“, což jsou šifry, které se tváří jako jiné, než ve skutečnosti jsou.

Obvykle používáme tzv. mezinárodní abecedu (bez háčků, čárek a „ch“), která má 26 písmen. Na to se dost často zapomíná. Ale pozor – „obvykle“ neznamená „vždy“!

Někdy stačí drobná úprava a i celkem jednoduchá šifra nám může dát dost zabrat. Např. když zašifrovaný text rozdělíme do skupin po 5 písmenech a tyto skupiny napíšeme za sebe na řádek. To se pak dost těžko hledá, jak to správně poskládat, aby se to dalo dešifrovat.

Dále uvedené šifry jsou pouze ty nejčastěji používané a nejznámější. Šifer existuje samozřejmě nepřeberná řada. Postupné ovládnutí známých šifer je v podstatě jen cvik k tomu, abychom později dokázali úspěšně luštit i šifry neznámé. A samozřejmě taky vymýšlet šifry nové – tohle jde velice dobře zejména matematikům, a nejen těm profesionálním.

Tak, dost povídání, a s chutí do toho!

1. Transpoziční šifry

a) Pozpátku

KÍLÁRK = KRÁLÍK

b) Hradby

♦ kolmé

K L Í E V K U
R Á K J E N X = KRÁLÍK JE VENKU X

♦ šikmé

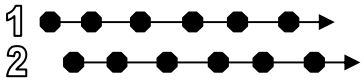
K M Á D Í J
A R O L E K = KRÁLÍK JE DOMA

c) Ob jedno či více písmen

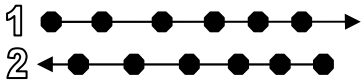
Je několik možností. To, že doskáčete na konec, ještě nemusí znamenat, že jste vyluštili celou šifru.

KDRFÁGLGÍXK = KRÁLÍK

KJREÁDLOÍMKA = KRÁLÍK JE DOMA



KARMÁOLDÍEKJ = KRÁLÍK JE DOMA



d) První - poslední

♦ na jednom řádku

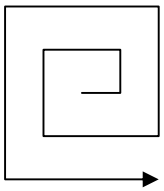
K Á Í K L R = KRÁLÍK
1 3 5 6 4 2

♦ na dvou řádcích

K Í D O K R
Á J M A E L = KRÁLÍK JE DOMA
1 5 6 2
3 7 8 4

e) Šnek

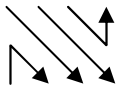
A B A N A
L Í L Á N
K K K R K
O J E U O
N Ě C H A



= KRÁLÍK JE U OKNA NA BALKONĚ CHA

f) Šikmo

L E E U
R Í K T
K Á Č J



= KRÁLÍČEK JE TU

g) Velká/malá

kDSráKHGlKFík = KRÁLÍK

h) Dělení slov

kR áLíč EkjEd oMauO knA = KRÁLÍČEK JE DOMA U OKNA

i) Mřížky (šifra pro pokročilé)

Mřížka je čtverec o jistém počtu polí, z nichž některá jsou vyříznuta, a to tak, aby po čtyřnásobném otočení mřížky byla pokryta všechna pole. Princip sestrojování mřížek: jednotlivá pole si označíme čísly tak, aby při otáčení mřížky všechna pole, pokrytá jedním vyříznutým okénkem, dostala stejné číslo. Každé číslo se tedy v tabulce vyskytuje čtyřikrát. Pak vyřízneme jedno libovolné pole označené č.1, jedno pole č.2, jedno pole č.3 atd. až vyčerpáme všechna čísla.

Luštění: mřížku položíme na tabulku a přečteme (vypíšeme) jednotlivá písmena po řádcích zleva nahoře doprava dolů. Poté mřížku otočíme po směru hodinových ručiček a opět stejným způsobem vypíšeme písmena, která vidíme. Celý postup ještě dvakrát zopakujeme. Otáčíme vždy jen mřížkou, ne papírem s tabulkou!

♦ sudé
(uprostřed není žádné volné pole)

1	2	3	4	5	1
5	6	7	8	6	2
4	8	9	9	7	3
3	7	9	9	8	4
2	6	8	7	6	5
1	5	4	3	2	1

K	K	O	O	R	K
M	N	Á	O	C	D
N	Ě	L	A	N	A
Í	O	B	M	K	Ř
A	B	A	Á	J	L
E	S	E	X	U	E

KLÍČ:
1/1 1/5
2/3
3/3
4/1 4/5
5/5
6/3 6/5

= KRÁLÍK JE U OKNA NA BALKONĚ A MÁ SE MOC DOBŘE X

♦ liché

uprostřed je jedno volné pole, kam nelze napsat žádné písmeno ze šifrované zprávy. Na závěr šifrování tam můžeme dopsat jakékoli písmeno, nebo toto políčko přeskočíme jakoby tam nebylo (když přepisujeme šifru do skupin po pěti, tak tenhle fígl dá někdy při luštění pořádně zabrat!).

1	2	3	4	1
4	5	6	5	2
3	6		6	3
2	5	6	5	4
1	4	3	2	1

K	K	O	A	R
J	Á	N	E	U
A	O	W	N	L
Ě	X	Í	B	Y
A	K	K	L	N

KLÍČ:

1/2 1/5
2/2
3/5
4/3
5/2

= KRÁLÍK JE U OKNA NA BALKONĚ XY

j) Sloupcová šifra (šifra pro pokročilé)

Postup šifrování: zvolíme si heslo (klíč), např. HARDY, určíme pořadí písmen podle abecedy, a šifrujeme:

H A R D Y	= heslo (klíč)
3 1 4 2 5	= číselné pořadí
P O K L A	= text, který chceme zašifrovat
D J E U R	
Y B N I K	
A K A C E	
R V D U T	
E V R B E	

Tabulku s textem přepíšeme do řádku nebo skupin, které budou tvořit konečnou podobu šifry. Začneme sloupcem č.1, pak 2 atd. Výsledek tedy bude vypadat takto:
OJBKV VLUIC UBPDY AREKE NADRA RKETE

♦ Luštění se znalostí klíče:

Spočítáme písmena (30), podělíme počtem písmen klíče (5), tedy 30:5=6, pročež pod každé písmeno klíče přijde 6 písmen. Přepíšeme zašifrovaný text do sloupců po 6 písmenech pod písmena klíče podle číselného pořadí a vodorovně si přečteme zprávu.

♦ Luštění bez znalosti klíče:

Spočítáme písmena (30) a podělíme toto číslo všemi děliteli tak, abychom dostali výsledek beze zbytku. V tomto případě 2, 3, 5, 6 a 15. Tolik písmen může mít heslo. Dvou, tří a 15ti písmenné heslo pro začátek zavrhneme jako nejméně pravděpodobné a zkusíme štěstí s ostatními. Přepíšeme text do sloupců s patřičným počtem písmen a zkoušíme v řádcích sestavit nějaké slovo, které dává smysl. Pokud se nám to povede, ověříme si systém na dalších sloupcích. Funguje-li to, máme vyhráno. Pokud ne, zkusíme pokračovat s heslem o jiném počtu písmen. Při dostatečné trpělivosti na to jednou přece musíme přijít! (Pokud je ovšem text zašifrován touto metodou ...).

2. Substituční šifry

a) Obrázkové morseovky

Možnosti jsou nepřeberné – pila, klínové písmo, příroda (slunce, mraky, tráva) …

klínové písmo: KRÁLÍK

slunce: KRÁLÍK
mrak: JE DOMA U OKNA A
stromy: DÍVÁ SE VEN

b) Morse v písmenech nebo v číslech

- Velké písmeno = čárka, malé písmeno = tečka (nebo naopak)

MgE zKm sY fKfd nn MhR = KRÁLÍK

– . – | . – . | . – | . – . . | . . | – . –

- Lichá číslice = tečka, sudá = čárka (nebo naopak)

238 561 92 5417 53 816 = KRÁLÍK

– . – | . – . | . – | . – . . | . . | – . –

c) Obrácená morseovka

Tečka = čárka, čárka = tečka

. – . | – . – | – . | – . – – | – – | . – . = KRÁLÍK

d) Morse – vyměněné znaky

Poněkud složitější varianta předchozí šifry. Prostou záměnou znaků | a – se obyčejný morseovkový zápis promění v něco, co se tváří jako morseovka, ale je to strašně nepřehledné… (a přitom tak prosté!)

| . | – . | . – . | – . | . . – . . – | . | – – . | | | – . – – | . . – | | | – | | – . | = KRÁLÍK JE DOMA

Podobně by se daly zaměnit třeba všechny znaky navzájem. To by byl chaos!

e) Dvojčíslí

Podle pořadí písmene v abecedě. Místo písmene napíšeme příslušné dvojčíslí. Jedno číslo nestačí, to by pak nebylo poznat, jestli se má vzít jedno číslo nebo dvě; i když i takto by se šifra dala vyluštit, dalo by to ale víc práce – takže budete-li chtít někoho trochu potrápit…

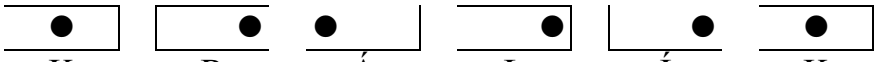
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

111801120911 = KRÁLÍK

f) Kříže

- jeden kříž

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	



K R Á L Í K

- tři kříže

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

K R Á L Í K

g) Doplnění písmene

Šifra se tváří jako dvouřádková, ale není, je potřeba doplnit mezilehlé písmeno.

A
B = C J Q Z K H J
L S B M J L = KRÁLÍK

h) Součet čísel

Stejný princip jako e), sečtu číslice a dostanu pořadí písmene v abecedě: např. 247: 2+4+7=13 nebo: 319: 3+1+9=13 = M

263 873 010 417 315 164 = KRÁLÍK

i) Caesarova šifra

Tuto šifru vymyslel již ve starém Římě Caesar, proto je po něm pojmenována. Princip je jednoduchý: každé písmeno je nahrazeno nějakým znakem (mohou to být i písmena, číslice), např: A = □, B = ◆, C = ↗, D = ⍁, E = ●, atd. Pokud je zašifrovaný text dostatečně dlouhý, a slova nebyla nijak rozdělena (např. do skupin po pěti písmenech), dá se tato šifra vyluštit i bez klíče, a není to až tak složité. Z jednotlivých osamocených písmen nebo dvojic je možno vytipovat několik málo spojek či předložek, postupně trpělivě odhalovat další písmena a dosazovat je do

dosud neznámých slov. Je-li zašifrovaný text rozdělen, je to mnohem horší a komplikovanější.

Teď dvě tabulky, s jejichž pomocí nám půjde luštění Caesarovy šifry lépe od ruky. První tabulka udává rozdělení českých souhlásek, jejich postavení ve slovech:

1	souhlásky, které mohou stát ve dvojicích prvé, málokdy druhé	C, (H), P, S, Z, Ž
2	souhlásky, které stojí ve dvojicích většinou jako druhé, málokdy prvé	L, N, R, Ř
3	souhlásky, které ve dvojicích stojí často jako prvé i druhé, i samostatně mezi samohláskami	D, H, K, T
4	souhlásky, které stojí méně často ve dvojicích souhláskových, ale častěji mezi samohláskami (samotné)	M, Š, V
5	souhlásky, které jsou málokdy ve dvojicích (ani jako prvé nebo jako druhé), ale většinou mezi dvěma samohláskami	Č, J
!!!	souhláska H jako taková patří do skupiny 1, ale ve spojení s C stává často jako druhá, tedy skupina 3	

Luštění také usnadní tzv. **frekvenční tabulka**, která udává, kolikrát se dané písmeno průměrně vyskytuje v českém textu (v %). Pamatujte, že čím je text delší, tím větší je spolehlivost této tabulky. (To platí u většiny šifer: čím delší, tím lépe se luští.)

E	11%	S, T	5%	Č, H, Ř, Š, Ž	1%
A	9%	L, R, U, V	4%	Ď, Ť, Ň	0,5%
O, I	8%	D, K, M, P, Y	3%	F, G	velmi zřídka
N	7%	C, B, J, Z	2%	Q, W, X	cizí slova

j) Posun písmen

- jednoduchý posun o pevný počet písmen

Jedná se o tzv. posunutou abecedu. Klíč (pokud je uveden) vypadá obvykle takto: A = C. Což znamená, že každé písmeno v šifře je posunuto o 2 písmena dopředu či dozadu – nutno vyzkoušet (obvykle dopředu: šifruji A+2=C, dešifruji C-2=A).

Při luštění se s výhodou uplatní **šifrovací kolečko**: z tvrdého papíru vystřihneme 3 různé kruhy (rozdíl poloměrů asi 1 až 2 cm). Kruhy rozměříme na 26 stejných výsečí (po 13,8°). Na první kruh napíšeme abecedu ve směru hodinových ručiček, a pod každé písmeno příslušné číslo (podle šifry e), na druhý kruh opět abecedu ve směru hodinových ručiček a pod tato písmena třeba smluvené značky k Caesarově šifře, a na třetí kruh abecedu tentokrát proti směru hodinových ručiček. Středy kruhů spojíme cvočkem a náš jednoduchý šifrovací stroj je na světě.

- datumová šifra

Bez klíče pro nás nevyluštitelná. Je-li uveden klíč, např. 6.5.1994, znamená to, že první písmeno je posunuto o 6, druhé o 5, třetí o 1, čtvrté a páté o 9, šesté o 4, a znovu dokola sedmé o 6, osmé o 5 atd.

- jiné posuny

Např. dvě abecedy (A = Z) proti sobě, fantazii se meze nekladou.

k) Tritheimova šifra

Johann Tritheim, opat benediktinského kláštera, byl pro svoje kryptografické znalosti za svého života považován za čaroděje. V roce 1508 napsal spis „Stenographica“.

Tritheim vyšel z toho, že Caesarova šifra se dá pomocí frekvence písmen poměrně jednoduše vyluštit, je-li text dostatečně dlouhý, aby se dala použít frekvenční tabulka. Řekl si, že čím kratší text, tím hůře luštitelný a tak postupně přišel na to, že jedna zpráva by se dala psát několika různými abecedami. V tehdejší době to byla pro nezasvěcence nevyluštitelná šifra. Dnes však už existuje metoda, kterou se dá tato šifra vyluštit, i když neznáme klíč – jenže pro nás je to zbytečně složité a nepoužitelné.

	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
	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**
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Šifrování:

H A R D Y = heslo

K R Á L Í Pod heslo napíšeme do řádků text, který chceme zašifrovat. Potom
S S S P H ke každému písmenu prvého sloupce vyhledáme v šifrovací tabulce ve sloupci H (č.8) příslušné písmeno, tedy K=S, A=I.

K J E U O Postupujeme vždy ve sloupcích! Pak přijde na řadu druhý sloupec
S K W Y N pod písmenem A (č.1): R=S, J=K, N=O, S=T. A tak dále až do konce.

K N A A M
S O S E L

Á S E O K
I T W S J

Zašifrovaný text pak rozdělíme skupin po pěti, přičemž postupujeme po řádcích: SSSPH SKWYN SOSEL ITWSJ.

Luštění pomocí klíče: přesně opačným způsobem, než jsme šifrovali.

3. Kombinované šifry

a) Kombinace transpoziční a substituční šifry

Možných kombinací je spousta, z těch jednodušších jsou to třeba: obyčejná morseovka psaná pozpátku, obrácená morseovka pozpátku, dvojčíslí na hradbách atd. Luštění může dát někdy trochu zabrat, ale obvykle se to dá zvládnout i bez klíče.

Složitější kombinace už jsou ale bez nápovědy prakticky nevyluštitelné – představte si třeba datumovku v mřížce, když neznáte ani datum, ani konstrukci mřížky…

b) Vícenásobné transpoziční šifrování

Neznáme-li, jaké šifry byly použity, může nám i kombinace dvou velmi lehkých transpozičních šifer připravit hodně perné chvilky. Třeba ob jedno písmeno tam a zpět na jednom řádku, a výsledek zamotaný do šneka. Příjemnou zábavu…!

c) Vícenásobné substituční šifrování

Zašifrování jednoho textu pomocí dvou různých substitučních šifer po sobě není takový problém, ale luštění, to už je opravdu práce pro vraha. Fantazii se opět meze nekladou: datumovka + dvojčíslí, písmenová Caesarovka (= každé písmeno nahradím jiným písmenem bez jakéhokoliv systému) + Tritheim, no upřímnou soustrast… Bez znalosti klíče nebo aspoň použitých šifer v našich podmínkách nevyluštitelné.

d) Chameleon

Taková šifra se tváří jako nějaká ze známých šifer, ale když ji takto luštíme, tak výsledek buď nedává smysl (slabší povahy okamžitě propadají panice a začnou pomýšlet na nejhorší, tj. vícenásobné zašifrování) nebo nám vyjde text sice smysluplný, ale naprosto neočekávaný – třeba „takhle se to neluští“ (to je ta lepší varianta, protože už víme, že jsme narazili na chameleona; taky by to mohl být chyták nebo spíš podraz, kdy napoprvé vyluštíme třeba „Zpráva je u potoka“, ale ve skutečnosti tam je zašifrováno „Zpráva je na Králičím vrchu“ – na to se dá přijít snad jedině tehdy, když u potoka nic nenajdeme…).

Pro lepší představu jedna ukázka:

11 | 1 80 | 11 2 09 | 1 1 1 0 | 0 50 4 1 | 5 || 1 3 0 | 1 || 21 | 15 11 14 || 01 0 | 1 | 1 30 1 1 | 9 0 51 | 3 1 5 | 03 | 0 4 || 1 5 0 2 | 1 8 05 |||

Ten, kdo podlehne optickému klamu, že se jedná o morseovku (tj. všichni…), nejprve získá text „TAKHLE SE TO NELUŠTÍ HU“. A jen ten, kdo bez ohledu na rozdělení číslic mezerami a svislicemi z nich udělá dvojice, zjistí, že se jedná o

dvojčíslí a správný text je „KRÁLÍK JE DOMA U OKNA A MÁ SE MOC DOBŘE“.

Hodně štěstí a málo chyb při šifrování i dešifrování Vám přeje Zico.