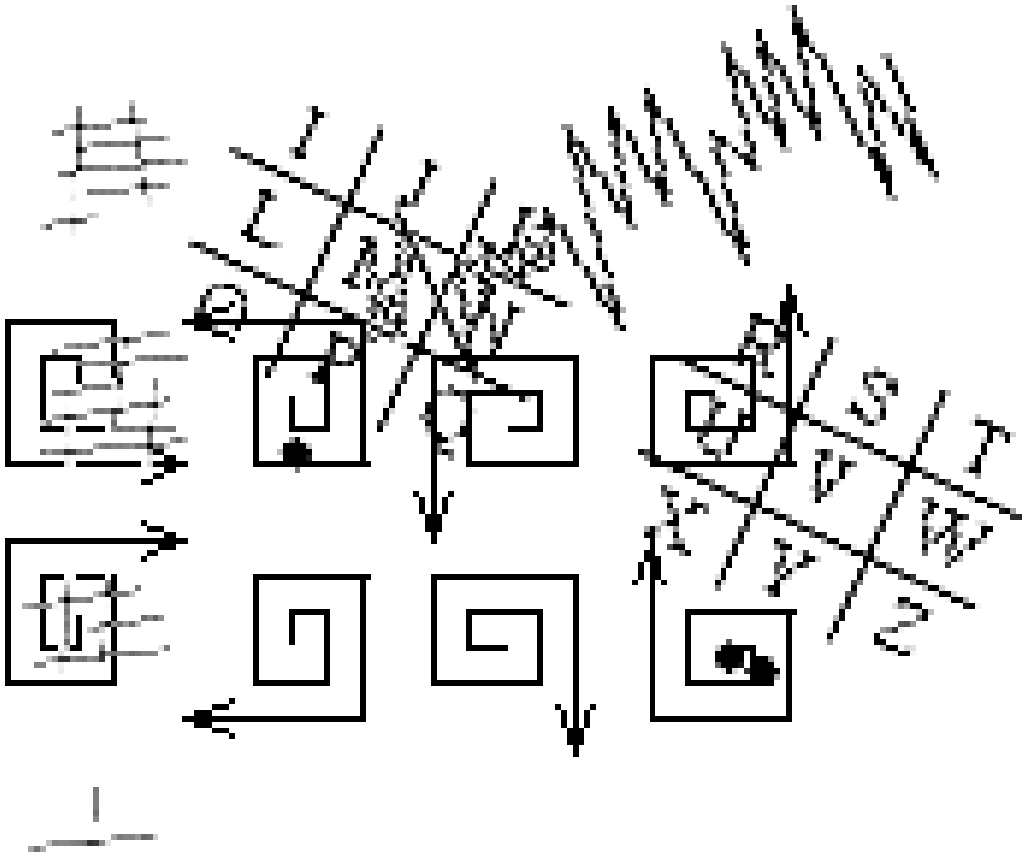
Šifrování



Obsah

Tato knížečka obsahuje popis šifer, které používá náš oddíl při hrách. Jsou rozděleny do několika kategorií podle toho jak se šifrují.

Morseova abeceda

Je způsob předávání zpráv systémem čárek a teček, který byl objeven na konci minulého století. Má značný význam zejména v námořnictví a v armádě. My jí používáme při hrách.

A	.-	Akát	N	-.	Nástup
B	-...	Blýskavice	O	---	Ó náš pán
C	-.-.	Cílovníci	P	.--.	Papírníci
D	-..	Dálava	Q	--.-	Kvílí orkán
E	.	Erb	R	.-.	Rarášek
F	..-.	Filipíny	S	...	Sobota
G	--.	Grónská zem	T	-	Trám
H	....	Hrachovina	U	..-	Učený
Ch	----	Chvátá k nám sám	V	...-	Vyučený
I	..	Ibis	W	.--	Vagón klád
J	.---	Jasmín bílý	X	-..-	Xénokratés
K	-.-	Krákorá	Y	-.--	Ýgar mává
L	.-..	Lupíneček	Z	--..	Známá žena
M	--	Mává			

1	.----	6	-....
2	..---	7	--...
3	...--	8	---..
4	....-	9	----.
5	.....	0	-----

Ostatní znaky

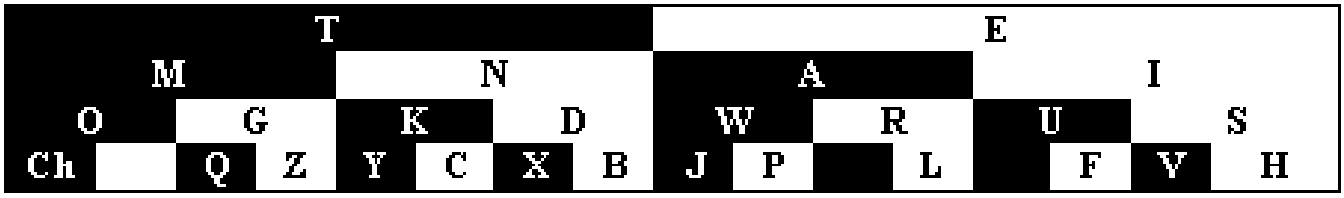
?	..--..	otazník	-	-....-	pomlčka
, !	--..--	čárka, vykřičník		.-----.	odsuvník, tabelátor
.	.-.-.-	tečka	( )	-.--.-	závorka
;	-.-.-.	středník	“ ”	.-..-	uvozovka
/	-..-.	zlomková čára	:	---...	dvojtečka
=	-...-	rovnítko	_	..--.-	podtrhnutí

Zkratky

73	radioamatérský pozdrav
99	“zmizni”
SOS	tísňové volání (Save Our Souls, angl. Spaste naše duše)

Klíč na luštění morseovky

Skvělá pomůcka pro ty co neumí morseovku, při luštění se postupuje z hora dolů vybarvené políčko znamená čárku prázdné znamená tečku.

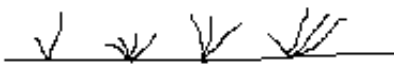


Šifry s morseovkou

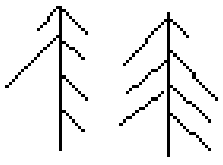
Různé psaní morseovky

- opačná morseovka – místo teček píšeme čárky a naopak
  `-./----/.../-...//  =  AHOJ`
- zrcadlová morseovka – každé písmeno napíšeme zrcadlově
  `.-/-./..--/..-/-./.-.//` = NAZDAR
- čísla – místo teček píšeme čísla od 0 do 4 a místo čárek čísla 5 až 9.
  `16;0403;676;2579  = AHOJ`
- čísla – místo teček píšeme lichá čísla jednomístná čísla a místo čárek sudá .
  `16;1357;446;4773  = AHOJ`
  obě varianty můžeme samozřejmě použít i opačně
- písmena – místo teček napíšeme samohlásky a místo čárek souhlásky
  `AV;IYOU;BLM;EFHK  = AHOJ`
- písmena – místo teček píšeme malé písmena a místo čárek velká
  `vlaK jEDe tAm a Sem  =  VPŘED`
  tyto dvě varianty jdou také použít opačně

Grafická morseovka

Morseovku lze nakreslit jako trsy trávy 

jako zuby na pile  nebo 



jako stromy v lese jako klínové písmo, jako noty v osnově, uzlíky na provázku a spousty dalších možností, které si lze jenom představit.

Šifry se záměnou nebo posouváním písmen

A = ?

Do první řádky se napíše celá abeceda a do druhé se napíše abeceda posunutá. Pod písmeno A se napíše to písmeno o které je to posunuto (např. A=M znamená, že a v šifře se rovná M ve skutečnosti). Při šifrování se hledá ve spodní řádce a do šifry se píše to z horní řádky a při luštění se v horní řádce hledá písmeno v šifře a v dolní je písmeno ze zprávy

Pro A=M vypadá tabulka takto :

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

potom : NUCX ICQBWYCh je AHOJ VODNÍKU

Substituce pomocí slovního klíče

(divnej název, ale někde jsem to tak přečetl). Je to vlastně složitější varianta předchozí šifry. Jednotlivá písmena budou posouvat různě např. A=AHOJ tzn., že pro první písmeno je posun A=A pro druhé A=H až pro čtvrté A=J a od pátého písmene se to opakuje.

ANDT VVRXIRI = AHOJ VODNIKU při klíči A=AHOJ

Abeceda převrácená

Pořadí písmen v abecedě je převráceno

A	B	C	D	E	F	G	H	Ch	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	Ch	H	G	F	E	D	C	B	A

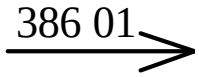
AQChZUZ = ZIRAFA

Posun abecedy s pomocným slovem

Na první řádek si napíšeme normální abecedu. Do spodního řádku pak napíšeme nejprve klíč a po něm po řadě písmena, která se v klíči nevyskytují.. Tím získáme převodní tabulku. Musí se použít slovo ve kterém se neopakují písmen a nejlepší je co nejdelší aby byly písmena víc zpřeházené

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

Potom slovo AHOJ vypadá asi takhle : ChMRO

Číselný posun 

Číslo nad šipkou určuje o kolik jsou písmena v abecedě posunuta. To znamená, že první písmeno je posunuté o 3 písmena druhé o 8 až páté o 1 písmeno od šestého písmene se to opakuje až do konce zprávy. Šifruje se proti směru šipky abychom zprávu mohli ve směru šipky luštit.

```
XZIJ  ULVChIJR  =  AHOJ VODNÍKU
```

Místo písmen čísla

Jedna z nejjednodušších šifer místo písmen se do zprávy napíší čísla A=1 B=2 ... Jednotlivá čísla se oddělují středníkem. jiná možnost je čísla psát římskými čísly. Také je možnost čísla neoddělovat středníkem, ale potom se luštění značně zkomplikuje.

```
VODNÍK  =  23;16;4;15;10;12
VODNÍK  =  XXIII;XVI;IV;XV;X;XII
VODNÍK  =  (23+16)/4+15*(10-12)
```

Mezerová šifra

Další velmi jednoduchá šifra, která se dá luštit i bez tabulky. Stačí vědět jak na to. Píšeme najednou dvě písmena. První je písmeno, které je v abecedě před šifrovaným písmenem a druhé je písmeno, které následuje. Psát můžeme po pravidelných či náhodných skupinách, v jednom či ve dvou řádcích.

YA ChJ QS ZB EG ZB = Y AChJ QS ZBEG ZB = ZIRAFA

Částečná záměna

Zvolí se takový klíč, ve kterém se písmena neopakují a je dostatečně dlouhý (maximálně však 10 písmen) dlouhý. Poté se písmena v klíči očíslují a místo písmen se do zašifrované zprávy píše příslušné písmeno. Nevýhodou je, že si lze hodně slov domyslet i bez klíče, otázka je zdali to při hře vadí.

H	Y	P	E	R	B	O	D	L	A
0	1	2	3	4	5	6	7	8	9

L6K6M6TIV9 V3Z3 7V3 ZI49F1 = LOKOMOTIVA VEZE DVE ZIRAFY

Uschování zprávy v textu

Přeskakování písmen

- přeskakuje se vždy *n* písmen. Začíná se buď tím správným nebo blokem právě *n* špatných písmen. Končí se buď správným písmenem nebo blokem maximálně *n* špatných písmen.
  ZJT**I**PN**R**AH**A**SK**F**VP**A** = ZIRAFA
- vždy se střídá *n* písmen z šifry a *n* špatných písmen
- mezi *a* správných písmen *b* špatných písmen (pro *a*=2, *b*=3)
  zildk**ra**gff**fa**zgt = zirafa
- počet přeskakovaných písmen se určuje podle klíče (pro klíč 213)
  ZPU**I**Z**R**JDP**A**AB**F**N**A** = ZIRAFA
- čte se každé *k*-té písmeno slova (počítáno od začátku či od konce slova), zbytek se přeskakuje. Slova musí mít pochopitelně minimálně *k* písmen.
  (pro *k*=1) **z**uzana **i** **r**enata **a**nalyzovaly **f**alešného **a**meričana = ZIRAFA
- čte se každé první a poslední písmeno slova
- ze zprávy se čte a-té písmeno slova, pak a+1 písmeno dalšího slova. Není-li ve slově dostatek písmen, začíná se počítat opět od začátku slova.
- vynechává se vždy určitá (může být předem dohodnutá) skupina písmen či krátké slovo
  abžir**ab**a**ab**fa = žirafa
- čtou se pouze velká (či jinak odlišená) písmena (ŽId RAdil FAkt dobře = žirafa)
- písmena ze zprávy následují jen po určitém písmeni
  (bn**x**žmnb**x**igzi**x**rk**x**abum**x**f**x**ahj = žirafa)
- v novinovém článku propícháme dírky pod písmeny, která tvoří šifru.

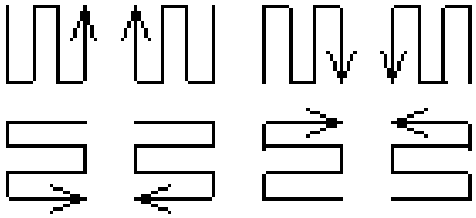
Zamotané psaní

- bez mezer (žirafažužlážvýkačku)
- se špatnými mezerami (ži rafaž už lážvý kačku)
- celá zpráva pozpátku (ukčakývž álžuž afariž)
- každé slovo pozpátku (afariž álžuž ukčakývž)
- od prostředního znaku střídavě na jednu a na druhou stranu
  (frž.iaa ážž.ul kaýž.vkču)
- od krajních znaků střídavě na jednu a na druhou stranu
  (žrfaai žžálu žýakučkv)
- šifra je změť písmen a od každého písmene vede ukazatel na jeho následníka

Různé psaní zpráv

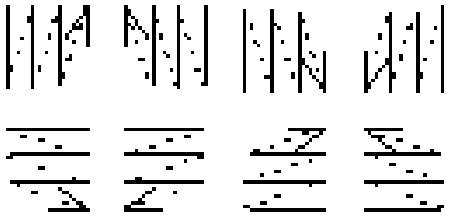
Hadovka

Šifruje a čte se v dohodnutém směru. Zde je pár základní možnosti. Další možnosti by šli např. vždy po dvou řádkách.



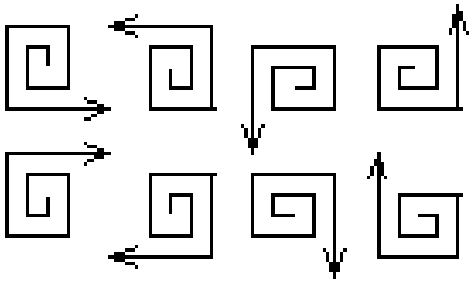
Sloupce

Píše se do sloupců. Další varianta je, že bude jeden sloupec platit druhý ne atd. To samé lze udělat v řádkách, ale musí se psát odzadu jinak by to moc šifra nebyla. I tady by šlo šifrovat vždy po dvou řádkách.



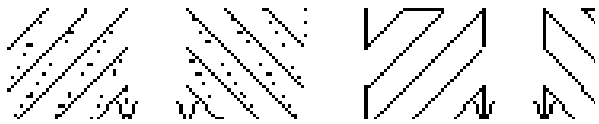
Šnek

Začátek je v prostředku a zpráva se píše dokola, konec zprávy nemusí být na první řádce, záleží na tom jak je zpráva dlouhá.

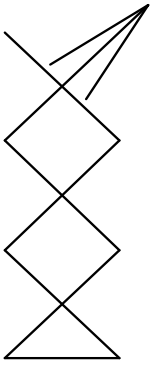


Šikmé sloupce

Zpráva se píše šikmo, začíná se jednom rohu a v protilehlém rohu se končí.



Klikatice



Zpráva se píše střídavě do prvního a druhého sloupce. Takže to vypadá asi takhle, zpráva se tedy píše do sudého počtu sloupců. Možností takto šifrovat je zase spousta, podle místa, kde se začne šifrovat. Dost obtížně se na to přichází, není od věci při prvním použití dát jako nápovědu podobný nákres.

Psaní podle slovního klíče

Dejme tomu, že chceme zašifrovat "sraz všech v neděli ráno" za použití klíče "PRAHA". Napíšeme zprávu takto :

P	R	A	H	A	–	klíč
4	5	1	3	2	–	pořadí písmen v klíči podle abecedy
S	R	A	Z	V	–	zpráva
S	E	C	H	V		
N	E	D	E	L		
I	R	A	N	O		

Poté zpřeházíme (seřadíme) sloupce podle čísel :

1	2	3	4	5
A	V	Z	S	R
C	V	H	S	E
D	L	E	N	E
A	O	N	I	R

A teď, aby to nebylo jednoduché napíšeme vše po sloupcích a to do skupinek po pěti písmenech. Nakonec tedy vznikne : ACDAV VLOZH ENSSN IREER. No ať si to zkusí nikdo bez klíče a návodu vyluštit.

Psaní podle číselného klíče

Klíčem k šifře bude číslo, v němž se žádná číslice nevyskytuje dvakrát. Zprávu napíšeme pod toto číslo a sloupce pak seřadíme podle velikosti. Vzniklou šifru opíšeme po náhodných či pravidelných skupinkách.

4	6	3	9	1	7
S	R	A	Z	J	E
Z	I	T	R	A	U
Z	I	R	A	F	Y

1	3	4	6	7	9
J	A	S	R	E	Z
A	T	Z	I	U	R
F	R	Z	I	Y	A

JA SREZ A TZU IRFR Z IYA = SRAZ JE ZITRA U ZIRAFY

Psaní podle číselného klíče

V každém slově se přehází písmena a pod ně se napíší buď pořadí jednotlivých písmen jak jsou ve zprávě nebo pořadí příslušného písmene ve zprávě (něco jako přesmyčky s klíčem).

J	K	A		E	S		Š	M	Á		B	O	E	N	L	B	U
1	3	2		2	1		3	1	2		3	4	7	6	2	1	5
1	3	2		2	1		3	1	2		6	5	1	2	7	4	1
J	A	K		S	E		M	Á	S		B	L	B	O	U	N	E

Takhle to nevypadá nic moc, ale když se oddělí ty čísla od těch písmen tak se to může někdy hodit

Šifry s tabulkami

Hebrejština

Šifruje se podle následující tabulky. Místo písmene, které chceme zašifrovat nakreslíme čáry, které jsou okolo písmene. Abychom odlišili písmena, které jsou v jiné tabulce, ale na jiném místě píšeme doprostřed tečky u první tabulky žádnou u druhé jednu a u třetí dvě tečky.

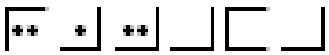
A	B	C
D	E	F
G	H	Ch

I	J	K
L	M	N
O	P	Q

●

R	S	T
U	V	W
X	Y	Z

●●



Takto potom vypadá zašifrované slovo ŽIRAFA :

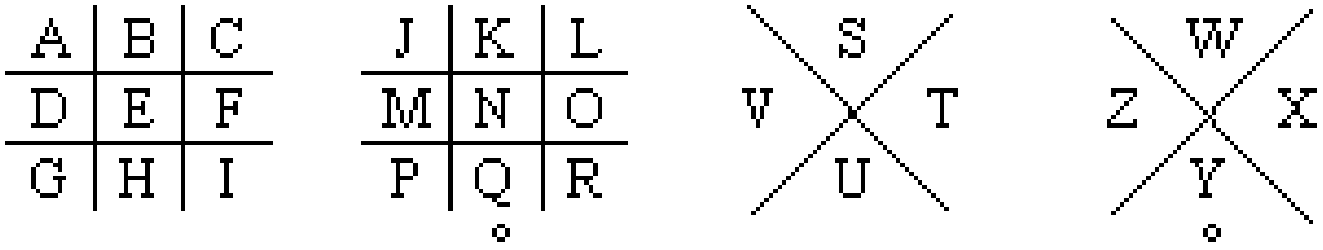
Kříž (Velký polský kříž)

Kříž je velmi podobný hebrejštině, ale všechno je v jedné tabulce. Poloha tečky určuje, které písmeno ze tří platí.

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

v této šifře vypadá slovo ŽIRAFA takto :

Malý polský kříž



a takhle vypadá slovo ŽIRAFA :

Jiný kříž

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

této šifře vypadá takhle slovo ŽIRAFA :

v

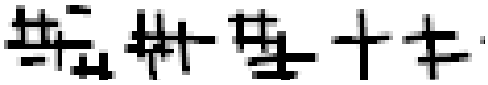
Čínština

Čínština je šifra, která se podobá čínským znakům, ale v žádném případě není tolik složité se ji naučit. Písmeno (např. N), které chceme zašifrovat, si najdeme v tabulce (N je ve čtvrtém sloupci a ve třetí řádce) a podle toho v kolikátém je sloupci tolik napíšeme svislých čar a podle řádek napíšeme vodorovné čary. Čáry ale nepíšeme stejně dlouhé, protože by šifra vypadala spíš jako plot. V každé tabulce se musí vynechat alespoň dvě písmena, ty se dohodnou buď předem, nebo je pak pod zašifrovanou zprávou napsáno, které písmena v tabulce nejsou.

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

Mimo Ch, Q

Takto vypadá v čínštině slovo ŽIRAFA



Zlomky

Používá se stejná tabulka jako u čínštiny, tedy 5x5 políček, vynechávají se dvě písmena. Souřadnice šifrovaného písmene se píšou jako zlomek, první se udává číslo sloupce a druhé číslo řádky. Případně lze použít i takovéto tabulky (lépe se to tak vysvětluje dětem, co nechápou zlomky).

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

Větička AHOJ VODNÍCI je pak takto
1/1 3/2 5/3 5/2 2/5 5/3 4/1 4/3 4/2 3/1 4/2
Při použití tabulky mimo Ch, W.

Šifrovací tabulka

Tabulka je velmi podobná čínštině a zlomkům. šifruje se stejně jako u zlomků, ale místo souřadnic písmene v číslech se píší písmena a čísla (písmeno od řádky a číslo od sloupce). Slova nebo čísla ve sloupcích a řádcích musí být předem dohodnuta jako to , která písmena v tabulce chybí.

	0	1	6	4	9
V	A	B	C	D	E
O	F	G	H	I	J
D	K	L	M	N	O
A	P	R	S	T	U
K	V	W	X	Y	Z

Mimo Ch, Q

Při tabulce bez Ch, Q znamená V0 O6 D9 O9 K0 D9 V4 D4 O4 V6 O4 AHOJ VODNÍCI

Šachová šifra

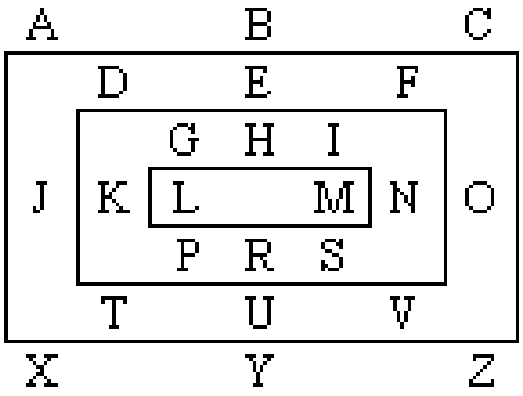
Do libovolné tabulky *m* x *n* napíšeme standardním způsobem (po řádcích) celou abecedu (třeba i několikrát za sebou). Šifra se skládá z písmene označujícího řádek a z číslice označující sloupec.

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

D6 B3 C5 A1 A6 D7 = ZIRAF

Pavoučí síť

Místo písmen ze zprávy se píšou dvě písmena sousední buď ve sloupci nebo v řádku. V každé tabulce musíme vynechat minimálně tři písmena. Ty jsou předem dohodnuté a nebo jsou napsány za zašifrovanou zprávou.



Pak napíšeme AHOJ VODNICI takto
BC EB MN KL NF ZC KT MO MS AB GH

Šifrovací kříže jednoduché

Šifrovaná zpráva se napíše do několika křížů (znak +). Při psaní zašifrovaného dopisu se potom písmenka čtou po řádcích a píší po pravidelných či nepravidelných skupinkách (tím se ještě zmenší šance na vyluštění cizí osobou). Je třeba se předem dohodnout, ve kterém místě se bude začínat psát a kolik křížů bude vedle sebe.

```
    R         Z         A
S       A       R       I       I       U
    Z         T         Z

    R
Y       A
    F
```

RZA SARI IUZTZRY AF = SRAZ ZITRA U ZIRAFY

Šifrovací kříže dvojité

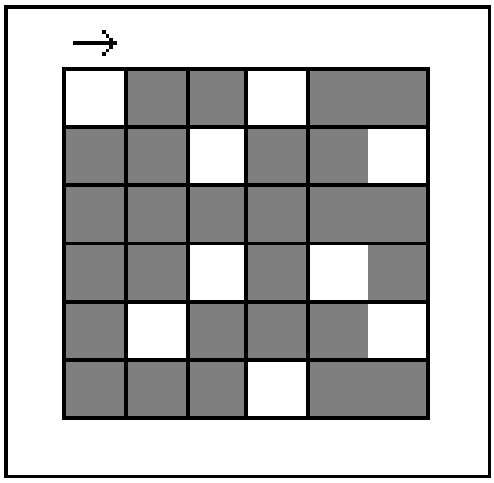
Princip je obdobný jako i jednoduchých šifrovacích křížů. Písmenka však nyní tvoří dvojité kříže (znak #).

```
    R   A             U   Z
S           Z       A           I
R           Z       Y           R
    T   I             F   A
```

RAUZ SZAI RZYR TIFA = SRAZ ZITRA U ZIRAFY

Šifrovací mřížka

Šifruje se tak že se píší písmena skrz tabulku na čistý papír, pak se tabulka otočí v dohodnutém směru o 90 stupňů a píše se dál. Luští se úplně stejně. Následuje ukázka tabulky a s ní zašifrované zprávy (je to oskenované ze zálesáka). Při výrobě tabulky je třeba si dát pozor co se má vyříznout. Nejlepší asi je vždy po vyříznutí nového otvoru na čistý papír proškrtat ty body, které už použít nemůžeme. Nejlíp první tabulku dělat na průhledný papír, aby bylo vidět co jsme již zaškrtali. Zkrátka každý otvor pokrývá 4 místa tak je třeba si to uvědomit.



K	S	K	A	I	V
U	N	Z	F	M	D
R	I	Y	D	Z	O
A	V	Y	A	S	L
O	P	E	B	T	R
	S	R	A	A	E

Sympatetické inkousty

To jsou inkousty, které lze číst pouze po použití nějakých chemikálií, případně, které lze vyvolat působením tepla. Ke psaní používáme čistý papír, který dobře saje a čisté pero nebo štěteček. Samozřejmě, že čistý papír v obálce by byl velmi nápadný. Proto sestavíme obyčejný dopis a pak mezi řádky, na nepopsaný konec a na druhou stranu můžeme psát tajnou zprávu.

Inkousty, které vyvoláváme teplem

- mléko
- kostka cukru rozpuštěná v lžíci vody
- šťáva z cibule, citronu nebo třešní
- ocet
- roztok jedlé sody
- 8 g chloridu nikelnatého a 2 g chloridu kobaltnatého se rozpustí v 90 ml vody. Zahřátím písmo zezelená a po ochlazení opět zmizí.
- 20 %-ní roztok chloridu měďnatého ve vodě. Nápis zahřátím zežloutne a po ochlazení zmizí.

- 1 g chloridu kobaltnatého a 2 g glycerinu se rozpustí v 90 ml vody. Písmo zahřátím zmodrá.
- 1 g kyseliny sírové a 2 g cukru se rozpustí ve 100 ml vody. Písmo zahřátím zčerná. !! kyselinu nutno lít do vody a ne opačně !!

Inkousty, které vyvoláváme chemicky

Černé písmo

- 1 g síranu železnatého se rozpustí v 25 ml vody. Písmo zčerná potřením roztokem taninu nebo kyseliny galové ve vodě.
- 1 g octanu olovnatého se rozpustí v 25 ml vody. Písmo se vyvolá sírovodíkem nebo sírovodíkovou vodou.
- 3 g octanu olovnatého se rozpustí ve 100 ml vody. Písmo se vyvolá potíráním roztokem sirníku draselného.
- 5 g dusičnanu nebo octanu olovnatého se rozpustí ve 100 ml vody. Písmo vyvoláme roztokem 10 g sirníku sodného ve 100 ml vody.

Modré písmo

- 1 g ferokianidu draselného se rozpustí v 25 ml vody. Písmo vyvoláme roztokem chloridu železitého.
- 1 g chloridu kobaltnatého se rozpustí v 25 ml vody. Písmo vyvoláme roztokem chloridu železitého ve vodě.
- 10 - 15 g bramborového škrobu ve 100 ml vody. Vyvoláme roztokem jódu.

Červené písmo

- 1 g fenoftaleinu se rozpustí v 25 ml lihu. Vyvoláváme roztokem uhličnanu sodného nebo draselného (soda, potaš)
- 5 g chloridu železitého se rozpustí v 25 ml vody. Vyvolá se slabým okyseleným roztokem rhodanidu draselného.

Poznámky :

Šifrování

- verze 2.1
- 20. květen 1999

Autoři :

- Vilém Zoubek (zoubek@students.zcu.cz)
- Petr Z. Gotthard (xgotha00@stud.fee.vutbr.cz)

Použitá literatura :

- Lexikonu pro turisty a táborníky, Fin Book Manufacture, 1994
- Zálesácký zápisník, Česká pojišťovna
- Pionýrská stezka, Česká rada Pionýra, 1997
- Aktuality (Cucka, Dam), Městská rada Pionýra Brno, 1997

Název :	Šifrování
Autor :	Ema a Zajíc
Vyšlo :	
Počet stran :	16
Počet obrázků :	29
Počet příloh :	-
Vydání :	III.
Náklad :	
Grafická úprava :	Ema
Tiskárna :	
Cena :	Nevyčíslitelná