ŠIFRY A ŠIFROVÁNÍ

1. ŠIFRY S MORSEOVKOU

Opačná morseovka

v opačné morseovce píšeme místo teček čárky a naopak

```
- . / - - - - / . . . / - . . . //  =  AHOJ
```

Čísla

místo teček píšeme čísla od 0 do 4 a místo čárek čísla 5 až 9.

```
16;0403;676;2579  = AHOJ
```

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

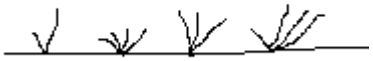
```
AV;IYOU;BLM;EFHK  = AHOJ
```

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.

2. 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 sem 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
```

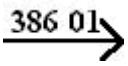
Posun abecedy s pomocným slovem

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 byla písmena víc zpřeházená.

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

Posun abecedy s číselným klíčem



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.

```
AHOJ VODNÍKU  =  1;8;16;11;   23;16;4;15;10;12;22
```

Mezerová šifra

Další velmi jednoduchá šifra, která se dá luštit i bez tabulky. Stačí vědět jak na to. Píšeme najednou do dvou řádek přičemž v první řádce je písmeno, které je v abecedě před tím co chceme zašifrovat a v druhé je písmeno, které je v abecedě po něm. Kdo mě nechápe, ihned pochopí z ukázky.

```
S  Z  A  N  P
U  B  C  P  S

Je zašifrované slovo TÁBOR
```

Samozřejmě by šlo napsat to i takhle:

```
SU  ZB  AC  NP  PS
```

Záměna některých písmen

Zvolí se takový klíč, ve kterém se písmena neopakují a je dost dlouhý. Poté se písmena v klíči očíslují a místo písmen se do zašifrované zprávy píše příslušné písmeno.

```
Klíč     O R I G A N U M
         1 2 3 4 5 6 7 8
Potom   VETS365  1BYV5TEL  PL56ETY  65 P1K25J3
ZH217CE63
je      VETSINA  OBYVATEL  PLANETY  NA POKRAJI
ZHROUCENI
```

Dost slov se dá domyslet i bez klíče, otázka je, zdali to při hře vadí.

3. USCHOVÁNÍ ZPRÁVY V TEXTU

Ob několik písmen

Vždy mezi dvě písmena zprávy napíšeme určitý počet písmen. Ten počet může být pořád stejný, nebo podle zadaného klíče se může měnit.

Ob 2 písmena

AJKHZVOBGJNGVMLODHDLKNRKIQAKBNU

Podle klíče 213

ANJHTONMGJBNVNOFRGDNMNTISEDKGFU

Vždy 2 písmena ze zprávy a 2 jiná ...

AHKLOJNNVŠIJICJHHNLKI

Mezi písmeny slovo

Mezi každé dvě písmena zprávy napíšeme nějaké krátké slovo

ADUBHDUBODUBJDUBVDUBODUBDDUBNDUBIDUBKDUBU

Po určitém písmeni

V textu jsou písmena ze zprávy jen po určitém písmeni. Například po písmenu X.

BNXAMNBXHGZIXOKXJNMMNXVXOGHGXDMXNWEXIXKMNXU

První zepředu, druhé zezadu

Písmena se čtou střídavě z obou konců zprávy. První písmeno je první druhé je poslední třetí je druhé a čtvrté předposlední a tak až doprostřed.

AOVDOUAZJSEIKJKNOJH

Velká písmena

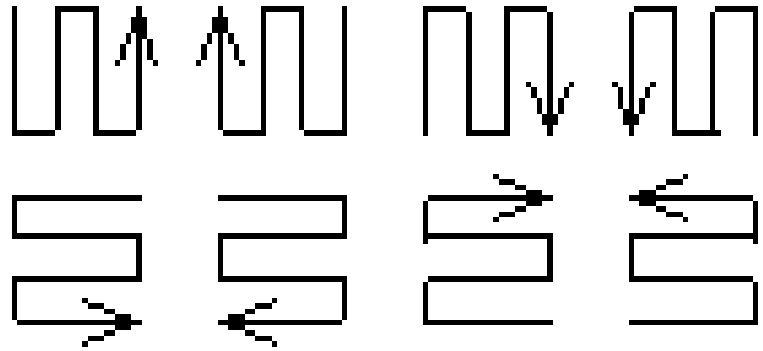
Ve zprávě platí jen velká písmena, popřípadě malá nebo jinak odlišná.

Dvě Oči Ir ceSty = DOPIS

4. RŮZNÉ PSANÍ ZPRÁV

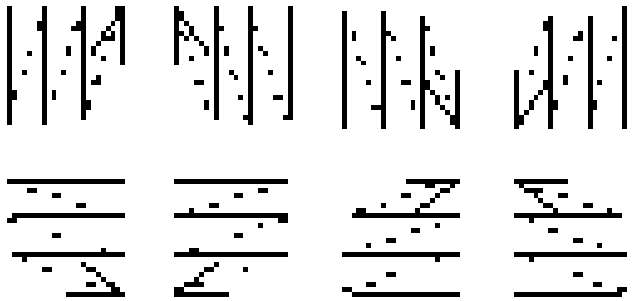
Hadovka

Šifruje a čte se v dohodnutém směru. Zde jsou čtyři základní možnosti. Další možnosti by šly v řádcích.



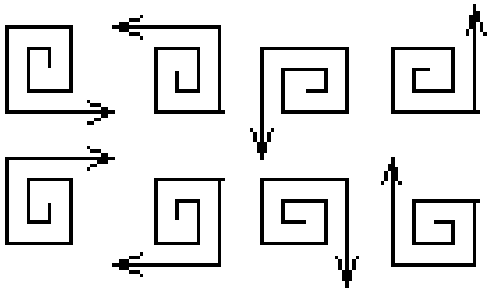
Sloupce

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.



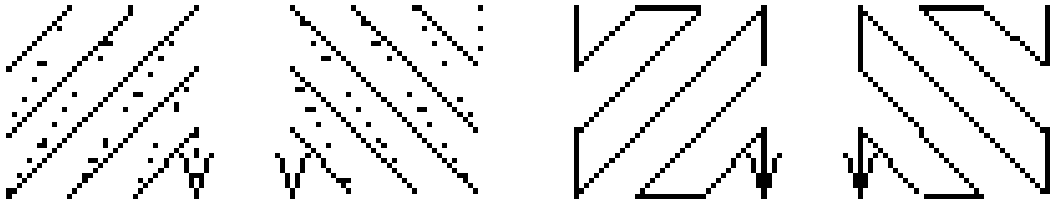
Šnek

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



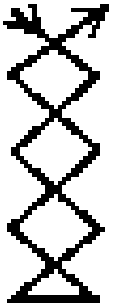
Šikmé sloupce

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.



Trochu složitější psaní

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 někdo bez klíče a návodu vyluštit.

5. 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 A H O J:

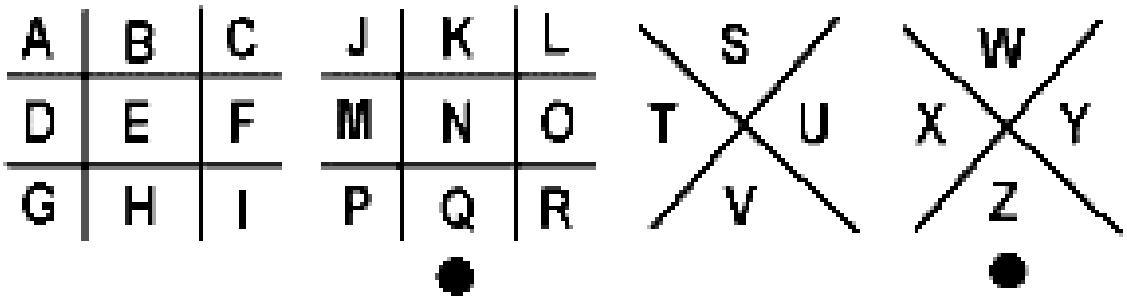
Kříž (Velký polský kříž)

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

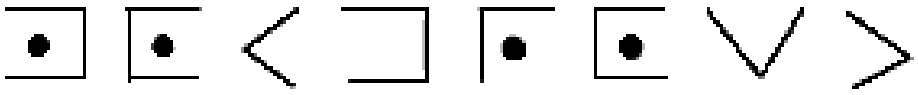
ABC	DEF	GHCh
IJK	LMN	OPQ
RST	UVW	XYZ

V této šifře vypadá slovo **A H O J** takto

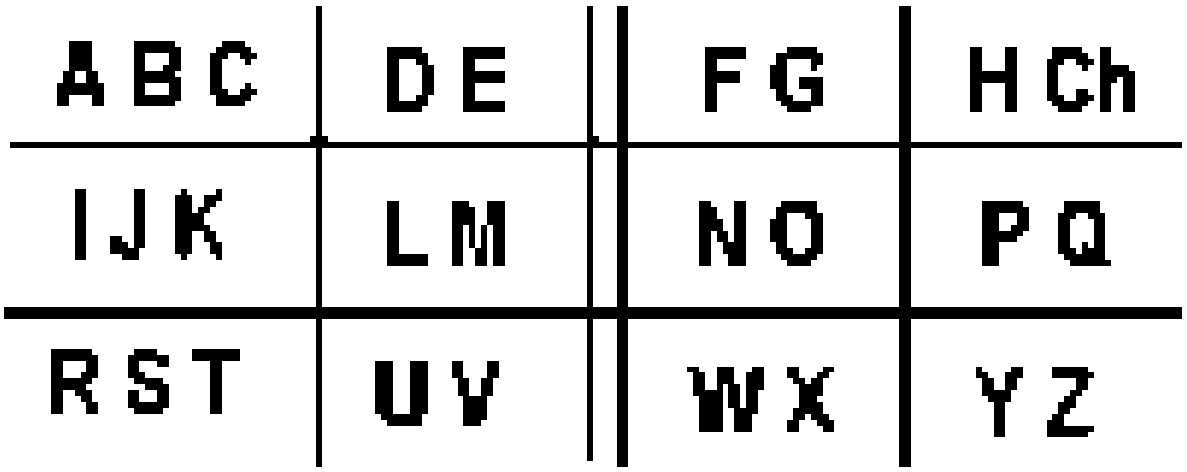
Malý polský kříž



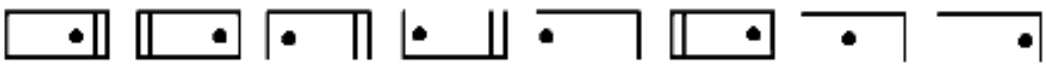
v této šifře vypadá takhle slovo: **moudrost**



"Další kříž"

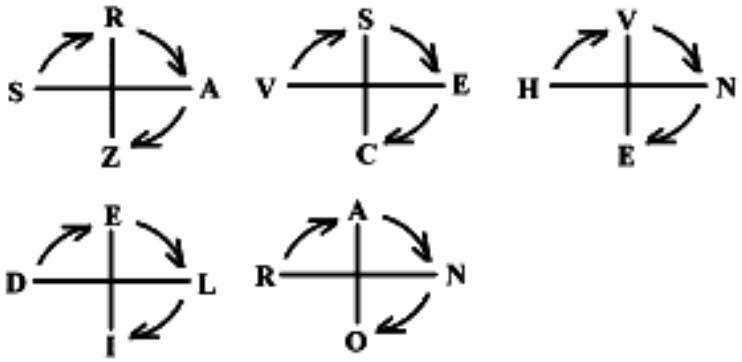


v této šifře vypadá takhle slovo: **moudrost**



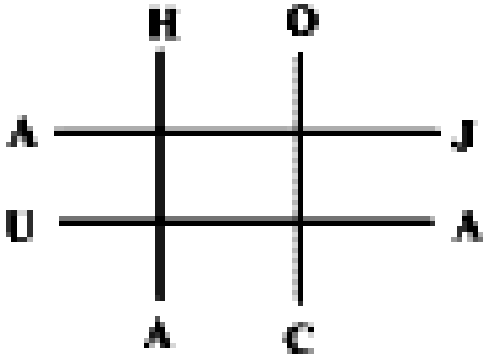
Šifrovací kříže

Zpráva, třeba **"sraz všech v neděli ráno"**, se napíše do takovýchto křížů tak, jak je napsáno v ukázce:



Potom se písmena čtou po řádkách a píší se po skupinkách o pěti písmenech (ještě se tím zmenší šance na vyluštění cizí osobou). Je třeba si předem dohodnout ve kterém místě se bude začínat psát a kolik křížů bude vedle sebe (jinak nastanou trable).
Takto pak vypadá výsledek šifrování: **RSVSA VEHNZ CEEAD LRNIO**

Další možnost je použít **"dvojitý kříž"** ten vypadá asi takto:



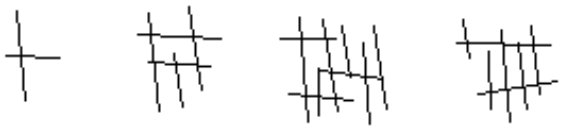
Čínština

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

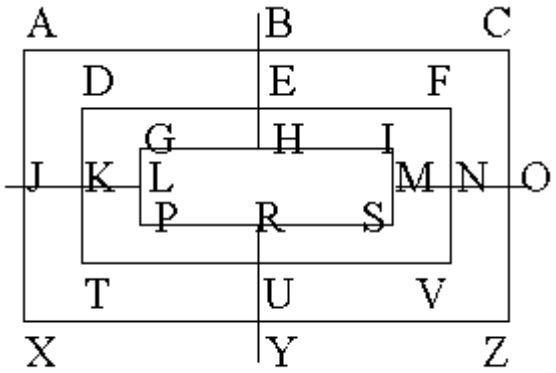
Mimo Ch, Q

Slovo **A H O J** vypadá v čínštině takto:



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.



Mimo Ch, O, W

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

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 (snáz 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.

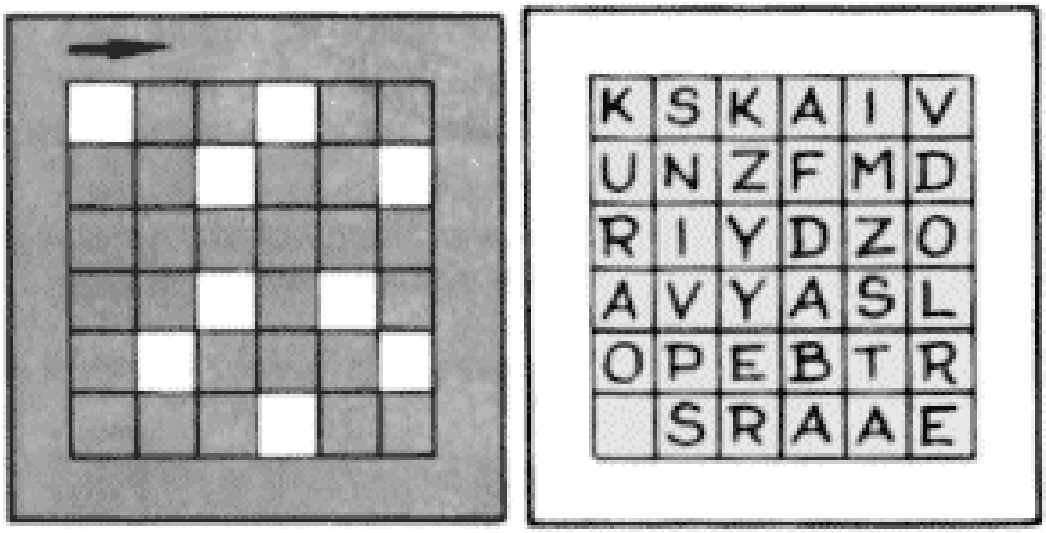
	0	1	6	4	9
V	A	B	C	D	E
O	F	G	H	I	J
D	K	L	M	N	O
A	P	R	S	T	U
K	V	W	X	Y	Z

Mimo Ch, Q

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

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. 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. (Lépe to asi vysvětlit neumím). Zkrátka každý otvor pokrývá 4 místa, tak je třeba si to uvědomit.



6. 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.

Závěrem:

Přípravě tohoto dokumentu jsem věnoval dost, času a budu dost vděčný za případné opravy nebo nové šifry, které používá váš oddíl.

Kontakt e-mail: zoubek@hermes.zcu.cz

OBSAH: