ŠIFROVACÍ KROUŽEK - 1. hodina

Pokud Vás zajímá I.Quest – šifrovací soutěž, kterou pořádáme, více informací i šifry najdete zde.

Odkazy: www.i-quest.cz

Na konci roku si uděláme malou jednoduchou šifrovací soutěž také.

Šifrování se řekně cizím slovem **kryptografie**. Pochází z řečtiny – ***kryptós*** znamená **skrytý** a ***graphein*** znamená psát.

Kryptografie je nauka o metodách utajování smyslu zpráv a to převedením do formy, která je čitelná jenom s určitou speciální znalostí.

Informace můžeme schovat nebo utajit velkým množstvím různých způsobů, mezi které patří i třeba hádanky, rébusy a další. Kroužek se bude zabývat nejrůznějšími z nich.

Cvičení během kroužku: Autobus, Puzzle, Test selektivní pozornosti

Naše první šifra:

Při šifrování obvykle nepoužíváme diakritiku, protože komplikuje šifrování i de-šifrování.

TRANSPOZIČNÍ – transpozice znamená přenos, nebo změna vzájemné polohy. Jedná se o šifru, ve které jsou správná písmenka na jiných než původních místech textu.

Příklad textu, který budeme šifrovat: „SIFROVACIKROUZEK" nebo na dvou řádcích:

```
SIFROVAC
IKROUZEK
```

Při šifrování se velmi často pro pořádek i pro zmatení dešifrujícího výsledný text zapisuje ve skupinách, nejčastěji po pěti písmenech. Náš text má celkem 16 znaků, což je ideální k zápisu ve skupinách po čtyřech.

www.sifrovacirkouzek.cz
Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569

1. **Psaní textu odzadu**: Na této šifře není co vysvětlovat, píšeme text odzadu dopředu.

   KEZUORKICAVORFIS

   Výsledek: **KEZU ORKI CAVO RFIS**

2. **První – poslední:** V této šifře je vždy první písmeno na začátku textu, poslední druhé na konci. Třetí je druhé, čtvrté předposlední, atd.

   SFOAIRUEKZOKCVRI

   Výsledek: **SFOA IRUE KZOK CVRI**

3. **Ob písmeno:** K výrobě této šifry nám pomůže původní text napsaný ve dvou řádkách. Lichá písmena textu jsou první řádek, sudá pak druhý.

   SIIKFRROOUVZAECK

   Výsledek: **SIIK FRRO OUVZ AECK**

4. **Hradby:** V této šifře zapisujeme text do dvou řádek, ve tvaru hradeb, snadno rozlušíte:

   SROCIOUK
   IFVAKRZE

   Výsledek: **SROC IOUK IFVA KRZE**

5. **Uhlopříčka:** V této šifře zapisujeme text do čtverce v úhlopříčkách, čteme zleva:

   ARZK
   RCOE
   IOIU
   SFVK

   Výsledek: **ARZK RCOE IOIU SFVK**

6. **Každé x-té písmeno ve sloupci:** V této šifře používáme každé x-té písmenko. Můžeme sifrování zjednodušit zápisem do sloupečků:

   Pokud nám při potřebě seřadit šifrovaný text do nějakého vzorce nevychází potřebný počet písmenek, doplníme na konec nějaké málo používané písměno, většinou X

   SIFR
   OVAC
   IKRO
   UZEK

   Výsledek (každé čtvrté): **SOIU IVKZ FARE RCOK**

   SIFROV
   ACIKRO
   UZEKXX

   Výsledek (každé třetí): **SAU ICZ FIE RKK ORX VOX**

7. **Šnek:** V této šifře se piše odstředu dokola (doprava nebo doleva).

   ACIK
   VSIR
   ORFO
   KEZU

Seskupování písmen:

Zašifrovaný text se většinou seskupuje po určitém počtu písmenek (často je to 5), aby se znesnadnilo dešifrování. My jsme si dosud seskupili písmenka po takových skupinách, aby se nám naopak snadno šifrovalo i dešifrovalo.

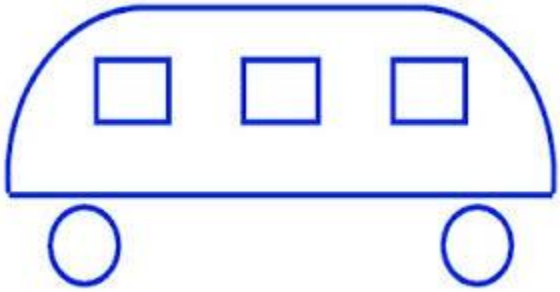
Seskupování může být i zajímavá varianta, rozlušíte tento text?

ANY NIV IDI TEJ EDE NZE ZPU SOB UJA KZA SIF ROV ATN EJA KYT EXT

www.sifrovacirkouzek.cz
Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569

Cvičení č. 1

Kterým směrem jede autobus? Nebo na které straně má předek?



Cvičení č. 2

Mláďata

E	D	M	K	I	P	E	N	R
								

Kam jít zjistíte podle dospělých

Cvičení č. 3: Selektivní pozornost

Úkoly na příště:

1. Zkuste vymyslet nějakou vlastní transpoziční šifru. Zašifrujte do ní text:

JSEMTENNEJLEPSISIFRANTVCERCANECH

Na příští hodině ukážete šifru ostatním.

2. Pohledejte pomocí internetového vyhledávače transpoziční šifry. Zkuste najít nějaký další druh transpoziční šifry, zkuste pochopit jak funguje, zašifrujte do ní stejný text jako ve cvičení 1. Když nebudete vědět, napište mi mail, rád poradím.

3. Zkuste najít nebo vymyslet nějakou zajímavou hádanku, rébus, chyták, cokoli – připravte si na příští hodinu.

4. Zkuste si dešifrovat následující jednoduchou šifru:

AZB UDU VEL KYS TAN USE SIF RAN TEM

5. Pokud se to povedlo, pak následující zvládnete také

OST RAD MIT DOU EBU ZEM ICE ROD

www.sifrovacirkouzek.cz
Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569