ŠIFROVACÍ KROUŽEK - 3. hodina

1. Myszkowskiho transpozice – tuto vymyslel Émile Victor Théodore Myszkowski roku 1902. Principem je zvolit si klíč, který má opakující se písmeno. V našem případě zvolíme klíč např. BFAB … naše pořadí znaků klíče tedy bude 2 3 1 2

   2312
   SIFR
   OVAC
   IKRO
   UZEK

   Nyní sloupce s neopakujícími se čísly (1 a 3) prezentujeme stejně jako v jednoduché sloupcové transpozici, tedy od shora dolů, zatímco sloupce s opakujícím se číslem (2) zapisujeme postupně zleva-doprava ... tedy:

   Výsledek: **FARE SROC IOUK IVKZ**

Text, který budeme šifrovat je např.: **Myszkowski to vymyslel**

Vybereme si klíč, např. slovo: "**NEBE**" a připravíme si text, který chceme zašifrovat do řádek, které jsou stejně dlouhé jako klíč, v našem případě tedy čtyři:

M Y S Z
K O W S
K I T O
V Y M Y
S L E L

Ke klíči si přiřadímě pořadí sloupců, podle abecedy, tedy:

N E B E
3 2 1 2

A nyní tvoříme výslednou šifru tak, že u neopakujících se sloupečků (tedy první a třetí) přepíšeme text po sloupečkách a opakující se zapisujeme postupně zleva doprava u dvou stejných sloupečků (tedy druhý a čtvrtý), princip je podobný jako u sloupcové. Rozebereme si to pomalu.

Začneme třetím sloupcem, protože má abecední číslo 1. Ten přepíšeme jako v klasické sloupcové transpozici jako sloupeček.

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

SWTME

Dále máme dva sloupečky s číslem dvě, ty jsou tím pádem hned za sebou a vytvoříme je tak, že jejich znaky zadáme postupně po řádcích, tedy:

YZOSIOYYLL

A můžeme je samozřejmě v půlce rozdělit, aby to nebylo pro luštitele nápadné:

YZOSI OYYLL

A následuje poslední část, tedy sloupeček s číslem tři, tedy první sloupeček:

MKKVS

Výsledná šifra je tedy: **SWTME YZOSI OYYLL MKKVS**

Nyní dešifrovat:

Máme tuto šifru:

SWTME YZOSI OYYLL MKKVS

a máme klíč: "NEBE"

Nejprve si zjistíme abecední pořadí v klíči:

N	E	B	E
3	2	1	2

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.QuEst
Pořádá RADIOKLUB OK1KPI Písek

Dále si zapíšeme šifrovaný text do řádek pod sebe a každou řádku si očíslujeme. Šifra nám převedla text z řádků do sloupců nyní musíme tady zase obráceně zabývat se řádky, nikoli sloupci. Musíme brát v úvahu, že dva prostřední sloupce mají stejné číslo, označíme si je hvězdičkou.

1 S W T M E

2* Y Z O S I

2* O Y Y L L

3 M K K V S

Nyní se dáme do dešifrování. Podle klíče vidíme, že první řádka bude řádka s číslem 3 (tedy ve skutečnosti čtvrtá poslední:

M K K V S

Dále máme první z řádek, které jsou šifrované jinak a tyto musíme dešifrovat tak, že ve druhém řádku výsledku budou lichá písmena. Ze dvou řádků z hvězdičkou tedy vybereme lichá: **Y** Z **O** S **I** O **Y** Y **L** L

Y O I Y L (liché)

Podle klíče následuje první řádek, tedy:

S W T M E

A nakonec druhá část dvou řádků s hvězdičkou, tentokrát sudá písmena: Y **Z** O **S** I **O** Y **Y** L **L**

Z S O Y L (sudá)

Výsledek tedy je:

M K K V S
Y O I Y L
S W T M E
Z S O Y L

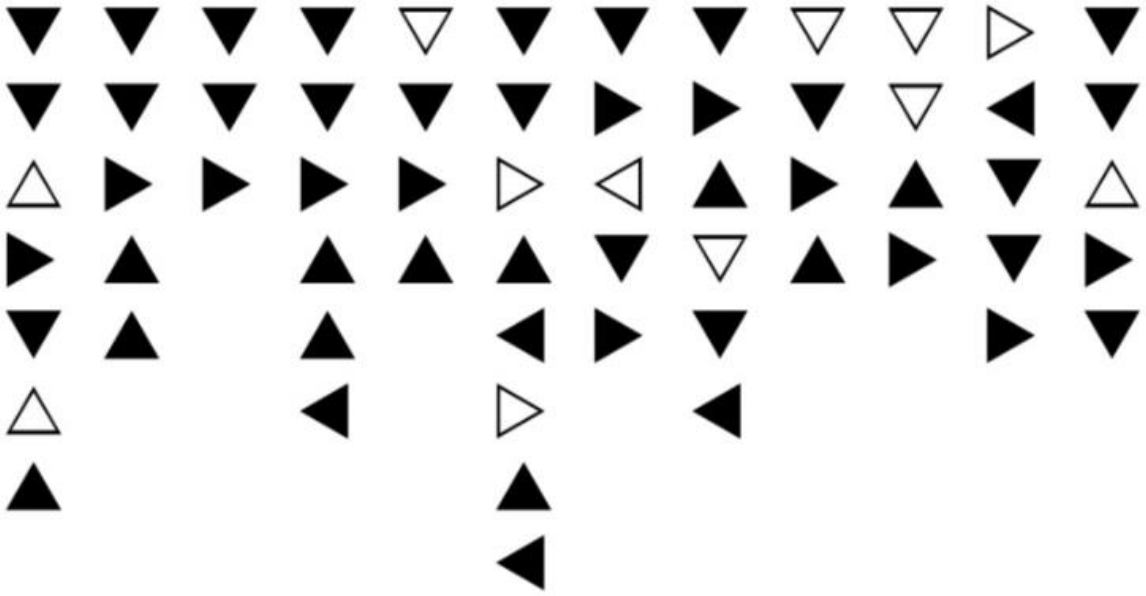
A nyní můžeme dešifrovaný text číst po sloupcích, zleva doprava, od vrchu dolů.

MYSZKOWSKITOVYMYSLEL

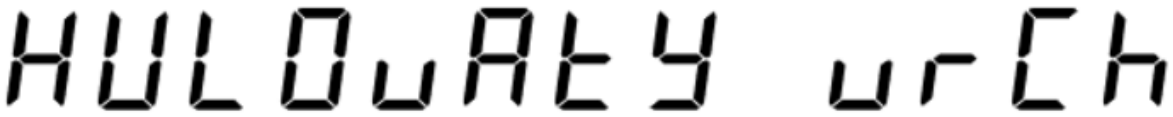
Ačkoli to vypadá složitě, je to velmi jednoduché :)

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

Jedna z šifer ze soutěže I.Quest:



Jedná se o jednoduchou šifru, kde šipky vpodstatě navigují tužku a každý sloupeček je jeden znak ve formátu 7 segment display – tedy klasického digitáního sedmisegmentového displaye, který určitě znáte z digitátek od veksláků a z vtipu o policajtech s pointou „pendrek pendrek stolička sněhulák". Šifra je postavena tak, že každý znak začíná v levém horním rohu znaku pomyslného displeje a černá šipka znamená piš, bílá posuň bez psaní. Dostanete tak snadno tento nápis:



Tedy Kulovatý vrch.

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

Cvičení:

1. **Rozluštěte Myszkowskiho transpozici s klíčem: CERCANY**

ELSKSDI TLNSIJI ARJDULT OETFOOU JOITMVL HJERUSS EZSEEYI

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.QuEst
Pořádá RADIOKLUB OK1KPI Písek