ŠIFROVACÍ KROUŽEK - 2. hodina

Stereogram ... je optická iluze trojrozměrného zobrazení na dvourozměrném obrázku. Stereogram může být zábavná forma jak schovat nějakou zprávu nebo obrázek.

Příklady: http://www.hidden-3d.com

Další transpoziční šifry:

1. Sloupcová transpozice s klíčem. Nejprve si napíšeme text do tabulky:

   SIFR
   OVAC
   IKRO
   UZEK

   Zvolíme si „klíč" – nějaké slovo o stejném počtu písmen, kolik je sloupců v naší šifře. Pro zjednodušení bude klíč zrovna slovo KLIC. Seřadíme si písmena klíče podle abecedy, tedy: K-3, L-4, I-2, C-1. Tento číselný klíč si napíšeme nad naší tabulku:

   3421
   SIFR
   OVAC
   IKRO
   UZEK

   Nyní šifrujeme po sloupcích a pořadí sloupců je podle klíče: Výsledná šifra je tedy:

   Výsledek: **RCOK FARE SOIU IVKZ**

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

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

2. Šifrovací mřížka: První známá mřížka je od matematika, filosofa, astronoma a astrologa jménem: Hieronymus Cardanus (nebo Gerolamo Cardano), který žil v letech 1501 – 1576.

   Šifrovací mřížku zpopularizoval Jules Verne ve svém románu Matyáš Sandorf. Ještě za první světové války se používala tzv. Fleissnerova mřížka.

   Princip mřížky je jednoduchý, do vytvořené mřížky se zapíše text, poté se mřížka otočí o 90° napíše se pokračování, znovu a znovu. Tak je popsán text celého čtverce a mřížka jej umožňuje číst.

A nyni v praxi: nejprve zašifrovat:

Text, který budeme šifrovat je např.: **Sloupcová transpozice**

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

S L O U P
C O V A T
R A N S P
O Z I C E

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

M E S I C
4 2 5 3 1

A nyni tvoříme výslednou šifru tak, přepíšeme text po sloupečkách a pořadí sloupců je podle abecedy klíče, tady v našem případě je první pátý sloupec, druhý je druhý sloupec, třetí je čtvrtý sloupec, čtvrtý je první sloupec a pátý je třetí sloupec. Dostaneme tedy takový text:

PTPE LOAZ UASC SCRO OVNI

Nyní dešifrovat:

Máme tuto šifru:

PTPE LOAZ UASC SCRO OVNI

a máme klíč: "MESIC"

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

Nejprve si zjistíme abecední pořadí v klíči:

M E S I C
4 2 5 3 1

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:

1 P T P E
2 L O A Z
3 U A S C
4 S C R O
5 O V N I

A nyní se můžeme pustit do dešifrování. Přeházíme si řádky podle klíče, tzn. že první bude řádka 4, druhá bude řádka 2, třetí bude řádka 5, čtvrtá bude řádka 3 a poslední bude řádka 1. Výsledek pak tedy vypadá takto:

4 S C R O
2 L O A Z
5 O V N I
3 U A S C
1 P T P E

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

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

Cvičení:

1. **Rozluštěte sloupcovou šifru s klíčem: CMELAK**

   JZLPLVR NEUVVUU NRTJICI SLSROOU IOIISOF YMSONPS

2. **Zašifrujte libovolný text pomocí mřížky a dejte přečíst postupně ostatním.**

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

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

Úkol: Zkuste rozšifrovat, klíč je slovo: **SIFROVANE**

BNCUIDNZEEC LSSIRSTPSKX IERONARNPVE NRFRAVFJVMV YYIZFEIRVCE
MOVPKIVCEEA GNOJYNOYRNV EPITVOIAAIU ASAOSAAHDML

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

I.QUEST
Pořádá RADIOKLUB OK1KPI Písek