

Základy šifrování

Šifry se používají již od dávných dob. Například Julius Caesar používal šifry pro vojenskou komunikaci. Používal posun o tři místa, obecně je ale za Caesarovu šifru označováno jakékoli šifrování na principu prostého posunu písmen (znaků) o konstantní hodnotu. My se v tomto dílu MAKOSA některé základní šifry naučíme řešit.

1) Šifry s posouváním písmen

Používá se základní abeceda bez diakritiky.

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

Posunujeme o dvě, tři i více písmen, nebo kombinujeme

KYIMQM – posunem každého písmena o dvě písmena po směru abecedy dostaneme MAKOSO

2) Šifry s posouváním písmen a daným klíčem

246138 →

Číslo nad šipkou určuje o kolik jsou písmena v abecedě posunuta. To znamená, že první písmeno je posunuté o 2 písmena druhé o 4 až šesté o 8 písmen. Při delším textu se klíč nad šipkou opakuje, až do konce rozluštění dané šifry

OEQP VW - MAKOSO

3) Šifry v nichž se používají místo písmen přirozená čísla

A=1 B=2 C=3 D=4.....Z=26. Jednotlivá čísla se oddělují středníkem. Jiná možnost je čísla psát římskými čísly. Někdy se používá i nadefinování

13; 1;11;15; 19; 15 – MAKOSO

Jinak: XIII; I; XI; XV; XIX; XV – MAKOSO

4) Šifry v nichž se používají místo písmen čísla a přitom se využívá klávesnice v mobilním telefonu

Klávesa ABC je s číslem 2; DEF s 3;WXYZ s 9. Podle toho v jakém pořadí je písmeno na klávese, tolik daných číslic je v šifře. Skupiny čísel mohou být, ale nemusí, odděleny mezerou.

6 2 55 666 7777 666 (62556667777666) - MAKOSO