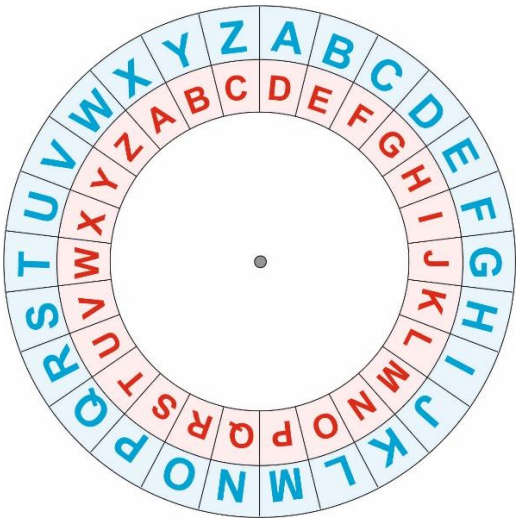
Šifry 1 – řešení

1. Ve videu se mluví o proslulé Caesarově šifře, o které se Caesar zmiňuje ve svém díle „Zápisky o válce galské“. Princip šifry spočívá v posunu písmen abecedy o předem daný počet. Caesar standardně posouval písmena abecedy o 3. Pro urychlení procesu šifrování a dešifrování se užíval tzv. Caesarův kotouč (schéma je na obr. 1). Po okrajích dvou kruhovitých desek byly vyryty znaky abecedy. Natočením kotoučů do správné polohy je na vnějším kotouči běžná abeceda a na vnitřním kotouči abeceda (posunutá) zašifrovaná.



Obr. 1. Caesarův kotouč – nastavení posunu o 3 písmena

a) Zašifrujte Caesarovskou šifrou text:

GAIUS JULIUS CAESAR

b) Dešifrujte následující text, o kterém víte, že byl zašifrován Caesarovskou šifrou:

SURWL EOERVWL L ERKRYH ERMXML PDUQH

a) K zašifrování uvedeného textu využijeme nastavení kotoučů na obr. 1. Vstupní text budeme číst na modrém kotouči (běžná abeceda), zašifrovaný text dostaneme na kotouči červeném. Tedy G zašifrujeme jako J, A šifrujeme jako D, atd. Zašifrovaný text je tedy tvaru

JDLXV MXOLXV FDHVDU

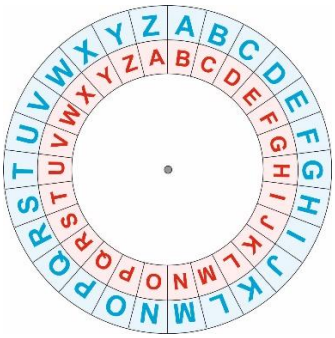
b) V tomto případě opět využijeme nastavení kotoučů na obr. 1. Zašifrovaný text budeme zadávat na červeném kotouči, dešifrovaný text budeme číst na kotouči modrém. První zašifrované písmeno je S, což dešifrujeme jako P. Druhým zašifrovaným písmenem je U, což dešifrujeme jako R, atd. Dešifrovaný text je

PROTI BLBOSTI I BOHOVE BOJUJI MARNE

2. V předchozí úloze jsme věděli, že k zašifrování textu byla použita Caesarova šifra s posunem o 3 písmena. V takovém případě je dešifrování textu poměrně jednoduché. Zkuste nyní dešifrovat níže uvedený text, o které víte jen, že k jeho zašifrování byl použit Caesarův kotouč.

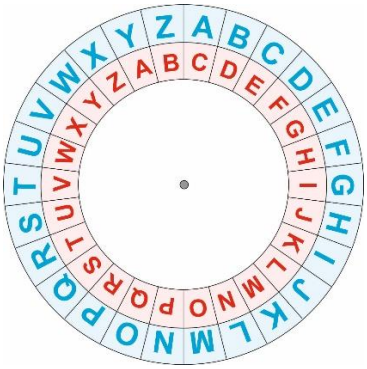
MOLQF EILRMLPQF PB JRPF YLGLSXQ XIB SVEOXQ PB KBAX

V tomto případě nezbývá, než postupovat „hrubou silou“, tj. postupně zkoušet různá nastavení kotoučů tak dlouho, až dostaneme smysluplný text. Začneme posunem o jeden znak, tj. natočíme kotouče do polohy na obr. 2.



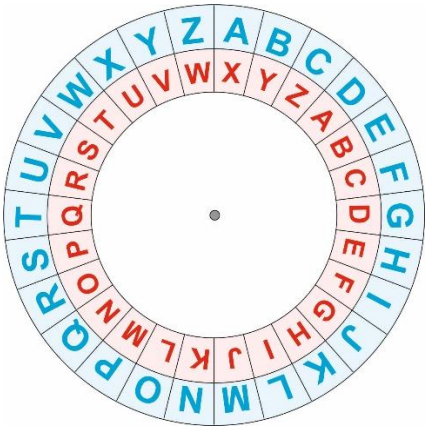
Obr. 2

a zkusíme dešifrovat text: M = L, O = N, L = K, Q = P, F = E. Slovo LNKPE nedává smysl, tedy toto nastavení kotoučů nebude správné. Zkusíme posun o 2 znaky, tj. natočíme kotouče do polohy na obr. 3.



Obr. 3

a dešifrujeme text: M = K, O = M, L = J, Q = O, F = D. Ani slovo KMJOD nedává smysl, tedy ani toto nastavení kotoučů nebude správné. Zkoušíme další a další nastavení kotoučů a postupně vylučujeme jednotlivé možnosti. Až při nastavení kotoučů do polohy na obr. 4 dostaneme:



Obr. 4

M = P, O = R, L = O, Q = T, F = I. Slovo PROTI dává smysl, tj. zřejmě nyní máme kotouče ve správné poloze. Dešifrování celého textu dostaneme hledanou zprávu:

PROTI HLOUPOSTI SE MUSI BOJOVAT ALE VYHRAT SE NEDA