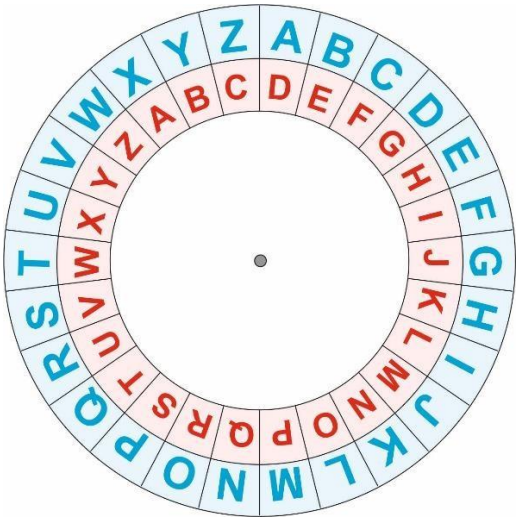
Šifry 1 – Pracovní list

Kryptologie jako věda o utajení obsahu zpráv má velmi zajímavou a dlouhou historii a provází lidskou společnost už od samého vzniku písma. Prolomení tajné šifry několikrát v dějinách zásadním způsobem ovlivnilo vývoj lidské civilizace. V prvním pracovním listu začneme nejjednodušší šifrou, kterou používal slavný římský vojevůdce Julius Caesar. Podívejte se na video a vyřešte následující úlohy. Video odkaz

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

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