1. Pomocou transpozičnej šifry dešifrujte text.

Transpozícia patrí k základným spôsobom šifrovania a jej princípom je zmena pozície znaku v texte. Príkladom transpozičnej šifry môže byť tzv. Fleißnerova mriežka, ktorú vidíte nižšie na obrázku. Tento šifrovací systém vynájdený v 16. storočí popisoval okrem iných aj Jules Verne vo svojom románe Matyáš Sandorf.

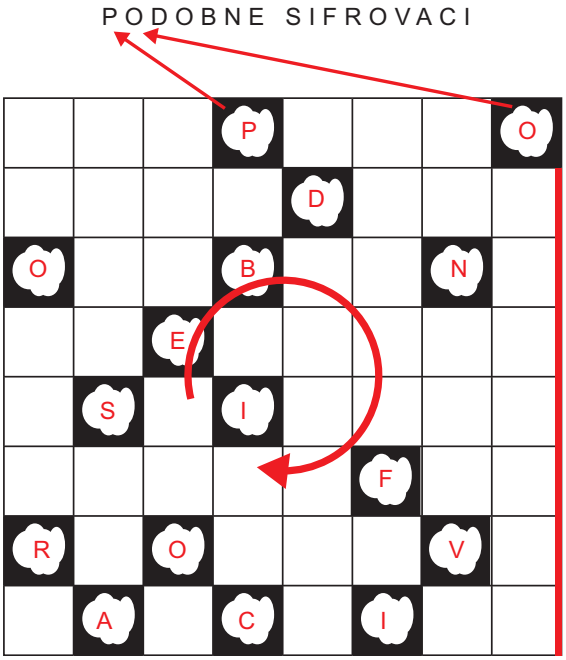
Nasledujúca správa bola zašifrovaná jednoduchou transpozičnou šifrou. Na jej dešifrovanie je nutné si pripraviť dešifrovaciu mriežku. Dešifrovanie prebieha správnym pohybom dešifrovacej mriežky a postupným vypisovaním znakov viditeľných cez dešifrovaciu mriežku v políčkach.

Do prázdnej mriežky (nižšie) prepíšte zašifrovaný text zľava doprava a zhora nadol. Priložte dešifrovaciu mriežku. Po opísaní znakov sa mriežka pootočí o 90° a postup s opísaním znakov sa opakuje. Mriežka sa trikrát pootočí. Správny pohyb spočíva v správne zvolenom smere otáčania a počiatočnej polohy mriežky.

Pozor! Mriežku je možné otáčať buď doprava alebo doľava a nepoznáte počiatočnú polohu mriežky.

NEPPR MVORE EIDJN SOEVB ZENMK EEYEP TOCSK IAOUA ZVIRE FMJRL OVAAV DOAAC JIXV
PODOBNE SIFROVACIE MRIEZKY POUZILA V PRVEJ SVETOVEJ VOJNE NEMECKA ARMADA

V počiatočnej polohe bola horná hrana mriežky (zvýraznená silnejšie) napravo. Mriežka sa pri šifrovaní otáčala doprava. Rozdelenie šifrovaného textu na bloky pochádza z histórie, kedy sa pri prenose platilo podľa počtu prenášaných slov (a nie podľa počtu znakov) a priemerná dĺžka slov v anglickom jazyku je 5 znakov. Text je bez diakritiky.



Program celoživotného vzdelávania

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).