

## 1. Pomocí transpoziční šifry dešifrujte text.

Transpozice patří k základním způsobům šifrování a jejím principem je změna pozice znaku v textu. Příkladem transpoziční šifry může být tzv. Fleißnerova mřížka, kterou vidíte níže na obrázku. Tento šifrovací systém vynalezený v 16. století popisoval mimo jiné i Jules Verne ve svém románu Matyáš Sandorf.

Následující zpráva byla zašifrována jednoduchou transpoziční šifrou. K jejímu dešifrování je nutné si připravit dešifrovací mřížku. Dešifrování probíhá správným pohybem dešifrovací mřížky a postupným vypisováním znaků viditelných skrz dešifrovací mřížku v políčkách.

Do prázdné mřížky (níže) přepište šifrovaný text zleva doprava a shora dolů. Přiložte dešifrovací mřížku. Po opsání znaků se mřížka pootočí o 90° a postup s opsáním znaků se opakuje. Mřížka se třikrát pootočí. Správný pohyb spočívá ve správně zvoleném směru otáčení a výchozí poloze mřížky.

**Pozor!** Mřížku lze otáčet buď doprava, nebo doleva a neznáte výchozí polohu mřížky.

EMPPR RVOIN NZDIE SOKVB YMNEP CEOEU TZKSA IAOIR VVAME FAVRL OADAV  
ALAXC CIXV

**PODOBNE ŠIFROVACÍ MRÍŽKY POUŽIVALA V PRVNÍ SVETOVÉ VALCE NEMECKÁ ARMADA**

**V počáteční poloze byla horní hrana mřížky (silněji zvýrazněná) napravo. Mřížka se při šifrování otáčela doprava. Rozdělení šifrovaného textu na bloky pochází z historie, kdy se při přenosu platilo dle počtu přenášených slov (nikoliv dle počtu znaků) a průměrná délka slov v anglickém jazyce je 5 znaků. Text je bez diakritiky.**

