Šifry 2

V pracovním listu „Kouzelná čísla“ jsme viděli, že kouzlit s čísly není zase tak obtížné. Ukázali jsme si, jaké matematické principy stojí v pozadí těchto efektních triků. Samozřejmě, že existují i triky opírající se o složitější úvahy. Můžete se znovu podívat na video a potom vyřešit příklady uvedené v pracovním listu.

- Video odkaz

1. Ve videu se mluví o tzv. transpozičním šifrování. Tento způsob šifrování zachovává soubor použitých písmen textu, který chceme zašifrovat, avšak zamění (promíchá) jejich pořadí dohodnutým způsobem. K přeházení písmen můžeme například použít tabulku se třemi sloupci. Otevřený text zapisujeme do tabulky po sloupcích, zašifrovanou zprávu čteme po řádcích. Na obr. 1 je ukázka zašifrování textu „TRANSPOZICNI SIFRA NENI BEZPECNA“ a výsledná šifra.

T	N	I
R	I	B
A	S	E
N	I	Z
S	F	P
P	R	E
O	A	C
Z	N	N
I	E	A
C	N	

TNIRI BASEN IZSFP PREOA CZNNI EACN

Obr. 1.

a) Zašifrujte stejný text, ale pomocí tabulky s pěti sloupci.

b) Dešifrujte následující text, o kterém víte, že byl zašifrován transpoziční šifrou (tabulkou o 10 sloupcích).

KKKYU ECTKP DJMBK TOTTR YEAYA AJOOI ZDKLA KECMP UNOAB MAOUA ZOUKY ANNVD CUKDB BEEME LJAYY YMNNC OETZL TAIOH VTAKA TBJHJ EABOJ OYAAE

2. V předchozí úloze jsme znali počet sloupců šifrovací tabulky. Pokud tuto informaci nemáme, stačí postupně zkoušet různé rozměry tabulky tak dlouho, dokud nedostaneme smysluplný text. To je důvod, proč není transpoziční šifra považovaná za bezpečnou. Snadné vylepšení poskytuje použití tajného klíče, který vepíšeme do záhlaví tabulky. Po zapsání textu uspořádáme sloupce tabulky abecedně podle písmen klíče. Šifrovanou zprávu pak čteme po řádcích.

   a) Zašifrujte text „DNES JE KRASNY DEN“ klíčem SOK.

   b) Jaký text ukrývá zpráva „OKZKU YEOVJ NSRSYT“ zašifrovaná klíčem SEDM?