

→ **Objasnite transpozíciu ako metódu šifrovania, dešifrujte text šifrovaný stĺpcovou transpozíciou 8 x 4: PINUOEIZZ EANZ XANJXVAEXAM XCERX**

TRANSPOZÍCIA je presúvanie jedného alebo viacerých znakov správy (v prípade počítačov môže ísť i o posun už binárne kódovanej správy - teda bitov).

STĹPCOVÁ TRANSPOZÍCIA je najjednoduchšou transpozíciou, ktorú popísal vo svojom diele "Cryptomenytices Patefacta" John Falconer v roku 1518. Správa sa napísala do obdĺžnika po riadkoch, a potom bola prepísaná po stĺpcoch. Kľúčom sú rozmery obdĺžnika v znakoch.

Riešenie: POZNAVACIE ZNAMENIE JE RUZA

RAIL FENCE ŠIFRA je forma transpozíčnej šifry, ktorá dostala svoje meno podľa spôsobu, akým je kódovaná. V Rail Fence šifre sa pôvodný text (plaintext) píše zostupne na "koľaje" idúce za sebou. Ak sa dostaneme na poslednú "koľaj" imaginárneho plotu, pokračujeme ďalej smerom nahor. Správa sa potom číta v riadkoch. Napríklad použijeme tri "koľaje" a správu "BOLI STE ODHALENI. HNED UTECTE", šifra sa zapíše takto:

```
B...S...D...E...N...T...E
.O.I.T.O.H.L.N.H.E.U.E.T.
..L...E...A...I...D...C..
```

→ **Vyhľadajte na Internete a spustite videoprednášku s tematikou IKT.**

→ **Stručne popíšte, ako sa využívajú počítače v športe, obchodovaní, umení a v zábave.**

Šport, umenie, zábava

Počítače už dávno zaujali tvorcov a používateľov počítačových hier. Tie sú veľmi náročné na rýchlosť a kvalitu grafiky. Aj vďaka tomu výrobcovia hardvéru musia stále vylepšovať svoje produkty. V digitálnom fotoaparáte riadi počítač temer všetky funkcie, aj zápis obrazu do pamäte. Fotografie sa dajú pomocou počítača upraviť, starý film sa dá vyfarbiť. Počítače umožňujú vytvoriť rôzne efekty i celé scény vo filmoch, pomáhajú pri tvorbe animovaných filmov a aj filmy sa v nich upravujú do konečnej podoby. V divadle sa využívajú pri osvetľovaní javiska, návrhu choreografie. V hudobnom priemysle sa využívajú na mixovanie a úpravu nahrávok. Staré nahrávky sa pomocou nich dajú opraviť, tento proces sa nazýva **remastering**. Počítače sú ukryté aj v hudobných nástrojoch – syntetizátoroch, ktoré môžu komunikovať s počítačom prostredníctvom jazyka MIDI. Možnosti, ktoré ponúka počítač, zaujali aj výtvarníkov a sochárov, ktorí pomocou CAD systému môžu navrhnuť štúdiu nového diela. Digitálny záznam športových výkonov zasa pomáha športovcom pri tréningu.

DT zmenili prístup k informáciám. Získavanie informácií o kultúrnych podujatiach, doprave, komunikácia s inštitúciami, vrátane štátnej a verejnej správy, rezervácie ubytovania a cestovných lístkov, hľadanie zaujímavosti v nejakej lokalite alebo zisťovanie o otváracích hodinách múzeí a mnohé ďalšie, nám dovoľujú lepšie plánovať a využívať voľný čas.

Obchod

Na obale každého tovaru nájdeme **čiarový kód**, ktorý obsahuje informáciu, o aký tovar ide, kde bol vyrobený a pod. Pokladnica (čiže počítač) vie, čo sa míňa a koľko ešte čoho má obchod na sklade. Vie teda, čo treba objednať. Čoraz viac sa rozvíja obchod cez Internet. Vznikajú virtuálne predajne, ktoré nepotrebujú miestnosti a nemusíme do nich chodiť. Tovar nám však niekto musí priniesť. Od základov sa mení **práca s peniazmi**. Čoraz viac peňažných operácií sa uskutočňuje na diaľku, cez Internet, cez mobil, z domu **bezhotovostne**. Objavili sa bankomaty, vďaka ktorým máme prístup k svojim peniazom cez bankomatovú kartu, po identifikácii sa **PIN** (Personal Identification Number) kódom. Pribúdajú operácie, ktoré ešte pred pár rokmi neexistovali, ako homebanking a internetbanking.