**Úlohy šifrovanie**

1. Šifrou atbaš sme zašifrovali krátky text. Tu je výsledok: KLPOZW QV FPIBGB KLW HPZOLF. Viete zistiť znenie zašifrovanej správy? (Pomôcka: Použitá je anglická 26-znaková abeceda – tá, ktorú nájdete na klávesnici.)

POKLAD JE UKRYTY POD SKALOU

1. Našli ste papierik s textom VCVQ URTCXC UC FC NCJMQ QFUKHTQXCV. Ide o šifru podobnú Cézarovej, ale odosielateľ použil iný posun v abecede, nie o tri znaky. Viete určiť, aký posun si zvolil, a tento text rozšifrovať? (Opäť je použitá 26-písmenová abeceda z klávesnice. Zašifrovaný text je v slovenčine. Napovieme, že najčastejšie písmeno v slovenskom texte je A. Aké je najčastejšie písmeno v šifrovom texte? A aký posun by tomu zodpovedal?)

TATO SPRAVA SA DA LAHKO ODSIFROVAT (posun o -2)

1. V polovici 16. storočia Blaise de Vigenère na základe prác Leona Battistu Albertiho,vytvoril svoju vlastnú šifru. Jej sila spočívala v tom, že používala 26 abecied, ktoré boli postupne posúvané o jedno písmeno. Ak by sme chceli použiť kompletnú slovenskú abecedu s diakritikou, dostali by sme oveľa väčší štvorec, ale na princípe šifrovania by sa nič nezmenilo. Na šifrovanie sa používa tzv. Vigenèrov štvorec, v ktorom sú všetky abecedy zapísané. Šifruje sa pomocou kľúčového slova (hesla), ktoré pozná len príjemca a odosielateľ. Ak je napríklad kľúčové slovo **HESLO** a šifrovaný text **GYMNAZIUM**, postupujeme takto:

Kľúčové slovo napíšeme nad jednotlivé písmená šifrovaného textu, pričom ho opakujeme podľa potreby. Vo Vigenèrovom štvorci vyznačíme riadky, ktoré budeme používať (sú to riadky, ktoré majú v záhlaví písmená h, e, s, l, o). Prvé písmeno šifrovaného textu G zašifrujeme pomocou riadku h. V tomto riadku nájdeme v záhlaví stĺpcov písmeno g a v priesečníku tohto stĺpca a riadka je písmeno N. Čiže G sme zašifrovali na N. Druhé písmeno šifrovaného textu Y zašifrujeme pomocou riadku e. V tomto riadku nájdeme v záhlaví stĺpcov písmeno y a v priesečníku tohto stĺpca a riadka je písmeno C. Čiže Y sme zašifrovali na C. Takto pokračujeme, kým nezašifrujeme celý text.

Zašifrujte pomocou Vigenèrovej šifry slovo **KONIEC** (kľúčové slovo je **HESLO**).

RSFTSJ

Obrázok, na ktorom je text, snímka obrazovky, číslo, štvorec

Automaticky generovaný popis

a) RSFTJR

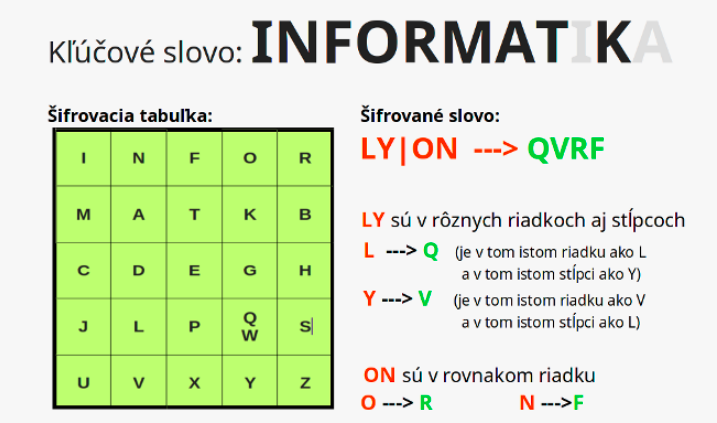
**b) RSFTSJ**

c) DKVXQV

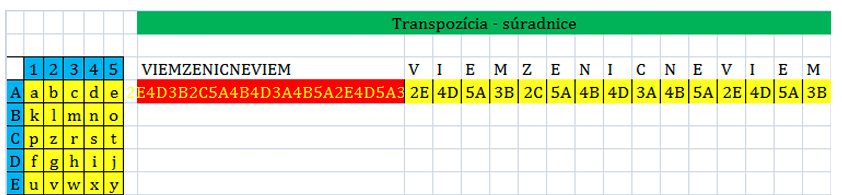
d) JSTFSR

1. Playfairovu šifru navrhol v roku 1854 ju navrhol Charles Wheatstone, názov však získala po barónovi Lyonovi Playfairovi, ktorý ju propagoval. Aj vďaka nemu sa dostala do služieb armády, pričom sa používala ešte aj počas 2. svetovej vojny. Princíp šifry spočíva v nahradzovaní dvojíc písmen inými dvoma písmenami. Text, ktorý chceme zašifrovať, rozdelíme na dvojice písmen (medzery a interpunkciu pre jednoduchosť vynecháme). Na koniec textu môžeme kvôli párnosti pridať ľubovoľné písmeno. Ďalej si navrhneme šifrovaciu tabuľku - Polybiov štvorec, do ktorého najprv napíšeme písmená kľúčového slova. Ak sa v kľúčovom slove opakujú písmená, tak druhý výskyt písmena odignorujeme. Potom doplníme do štvorca zvyšné písmená abecedy (Q,W sú v jednej bunke, ich použitie sa dá v slovenčine odhaliť z kontextu). Postup šifrovania - keďže berieme do úvahy dvojice písmen, môžu nastať tri prípady: 1. Obe písmená sú v rovnakom riadku - každé z nich nahradíme písmenom, ktoré je v riadku od neho napravo. Ak ide o posledné písmeno v riadku, nahradíme ho prvým písmenom v danom riadku. 2. Obe písmená sú v rovnakom stĺpci - každé z nich nahradíme písmenom, ktoré je v stĺpci pod ním. Ak ide o posledné písmeno v stĺpci, nahradíme ho prvým písmenom v tomto stĺpci. 3. Písmená sú v rôznych riadkoch aj rôznych stĺpcoch. Každé písmeno nahradíme takým písmenom, ktoré sa nachádza v priesečníku riadka šifrovaného písmena a stĺpca, v ktorom sa nachádza druhé šifrované písmeno.

Zašifrujte slovo **PLAYFAIR** (ak je kľúčové slovo **INFORMATIKA**).



1. QPKWNTNI
2. QPVKTNNI
3. **QPKVNTNI**
4. PQVKNTIN
5. Vytvorte v tabuľkovom kalkulátore pomocou textových funkcií šifrovací a dešifrovací stroj, ktorý realizuje Cézarovu šifru posunom abecedy o n pozícii. Šifrovanie a dešifrovanie: Do prvého riadku tabuľky zapíšte otvorený text, v druhom riadku bude bunka s posunom, do tretieho riadku vložte funkciu, ktorá hodnotu znaku v tabuľke ASCII posunie o n- pozícii a vzorec nakopírujte do ostatných buniek (šifrovaný text ), v štvrtom riadku použite funkciu na kontrolu, ktorá hodnotu v treťom riadku znovu dešifruje. Dešifrovací stroj: V druhej tabuľke do prvého riadku vložte mnou zadaný šifrovaný text, do druhého riadku vložte hodnotu n (posunutie ) a do tretieho vložte funkciu, ktorá zobrazí dešifrovaný text. Meňte hodnotu n dovtedy, kým text bude mať zmysel. Dešifrovaný text odovzdajte vyučujúcemu.
6. Vytvorte v v tabuľkovom kalkulátore šifrovaciu tabuľku podľa obrázku a zašifrujte zadaný text tak, že nahradíte jednotlivé znaky pracovného textu ich súradnicami v tabuľke - číslom stĺpca a písmenom riadku.



1. Podľa obrázku vytvorte v tabuľkovom kalkulátore tabuľku 5x5, do ktorej zapíšete do riadkov zadaný text, voľné pozície vyplňte náhodnými znakmi. Vyberte prvý stĺpec tabuľky a skopírujte ho do schránky a pomocou „Prilepiť“, „Transponovať“ vložte text do riadku. Postup opakujte s každým stĺpcom tabuľky.

