Moderné vzdelávanie pre vedomostnú spoločnosť / Projekt je spolufinancovaný zo zdrojov EÚ

Mgr. Ján Hanuliak

# VYUČOVANIE TÉMY ŠIFROVANIE INFORMÁCIÍ NA STREDNEJ ODBORNEJ ŠKOLE

Osvedčená pedagogická skúsenosť edukačnej praxe

Prešov

2013

| | |
|---|---|
| **Vydavateľ:** | Metodicko-pedagogické centrum, Ševčenkova 11,<br>850 01 Bratislava |
| **Autor OPS:** | Mgr. Ján Hanuliak |
| **Kontakt na autora**: | Stredná odborná škola, Kušnierska brána 349/2, 060 01 Kežmarok,<br>jan.hanuliak@gmail.com |
| **Názov OPS:** | Vyučovanie témy Šifrovanie informácií na strednej odbornej škole |
| **Rok vytvorenia OPS:** | 2013 |
| **Odborné stanovisko vypracoval:** | Mgr. Monika Karoľová |

Za obsah a pôvodnosť rukopisu zodpovedá autor. Text neprešiel jazykovou úpravou.

Táto osvedčená pedagogická skúsenosť edukačnej praxe bola vytvorená z prostriedkov národného projektu Profesijný a kariérový rast pedagogických zamestnancov.

Projekt je financovaný zo zdrojov Európskej únie.

## Kľúčové slová

Informácia, kódovanie, dekódovanie, šifrovanie, dešifrovanie, kryptológia, symetrická šifra, asymetrická šifra, substitučná šifra, transpozičná šifra, steganografia, Pascal s programovacím prostredím Lazarus, Delphi, myšlienková mapa, tabuľka ASCII, otvorený text, šifrovacia funkcia, šifrovací kľúč, šifrový text, šifrovacia mriežka.

## Anotácia

Cieľom mojej práce bolo spracovať analýzu učiva témy Šifrovanie informácií na strednej odbornej škole, vytvoriť okomentovanú zbierku riešených úloh a projektov, prepracovať metodiku výučby témy, stanoviť učebné ciele, vytvoriť vlastný systém gradovaných učebných úloh, popísať použité vyučovacie metódy, učebné pomôcky, didaktickú techniku a spôsoby hodnotenia učebných výsledkov žiakov. Vytvorenú metodiku overiť vo výučbe v prvom a druhom ročníku strednej odbornej školy a dať odporúčania pre pedagogickú prax.

## OBSAH

ÚVOD ..... 5

1 OPIS OSVEDČENEJ PEDAGOGICKEJ SKÚSENOSTI ..... 7

2 PREHĽAD O SÚČASNOM STAVE VYUČOVANIA ŠIFROVANIA NA STREDNEJ ODBORNEJ ŠKOLE ..... 11

2.1 Štátny vzdelávací program ..... 11

2.2 Školský vzdelávací program ..... 11

2.3 Učebné osnovy ..... 11

3 NÁVRH METODIKY VYUČOVANIA ŠIFROVANIA ..... 13

3.1 Východiská pre vyučovanie šifrovania ..... 13

3.2 Vyučovacie metódy ..... 13

3.3 Organizačné formy vyučovania ..... 14

3.4 Materiálne prostriedky vyučovania ..... 14

3.5 Základné pojmy ..... 14

3.6 Štruktúra učiva podľa tematických celkov ..... 15

3.7 Systém úloh ..... 15

4 OVERENIE NAVRHNUTEJ METODIKY ..... 31

4.1 Odporúčania pre pedagogickú prax ..... 31

ZÁVER ..... 33

Zoznam príloh ..... 37

# ÚVOD

Šifrovanie, ktoré bolo v minulosti iba výsadou tajných služieb, armád, špionáže, sa dnes hlavne vďaka rýchlemu rozvoju informatizácie stáva každodennou súčasťou nášho života. Čím viac sa otvárame svetu, narastá potreba ochrany nášho súkromia, duševného, ale aj fyzického majetku. Pri komunikácii s bankou cez Internetbanking, používaním mobilu alebo bezdrôtového pripojenia počítača prebieha naša komunikácia šifrovane. Tento fakt si bežný používateľ dnes ani neuvedomuje. Na jednotlivých príkladoch a projektoch ukážem postupnosť šifrovania v MS Word, MS Excel a v programovacom jazyku Pascal , ktoré som overil so žiakmi. Náročnosť jednotlivých úloh a samotných projektov postupne rastie.

Hlavné ciele mojej práce na tému „Vyučovanie témy Šifrovanie informácií na strednej odbornej škole“ sú:

1) Spracovať analýzu učiva o šifrovaní.
2) Stanoviť učebné ciele, vytvoriť systém gradovaných učebných úloh.
3) Popísať použité vyučovacie metódy, učebné pomôcky, didaktickú techniku a spôsoby hodnotenia učebných výsledkov žiakov.
4) Vytvorenú metodiku overiť vo výučbe informatiky v prvom a druhom ročníku strednej odbornej školy na predmete informatika a dať odporúčania pre pedagogickú prax.
5) Preskúmať a navrhnúť možnosti vizualizácie procesu šifrovania a dešifrovania pre rôzne triedy substitučných a transpozičných šifier.
6) Realizovať programové prostriedky na šifrovanie textov pomocou vybraných klasických šifier a vizualizáciu tohto procesu.

V prvej časti sa venujem popisu základných údajov mojej osvedčenej pedagogickej skúsenosti, špecifikácii cieľovej skupiny a vymedzeniu kompetencií, v druhej časti práce popisujem súčasný stav vyučovania šifrovania v strednej odbornej škole, v tretej časti navrhujem metodiku vyučovania šifrovania, štvrtá časť sa zaoberá overením navrhnutej metodiky a v záverečnej časti som zhrnul poznatky z procesu realizácie.

Pre väčšiu flexibilitu na vyučovacích hodinách som pripravil súbor úloh na šifrovanie pomocou jednoduchých substitučných a transpozičných šifier vo forme zošitu Excel. V prílohe sa nachádzajú ďalšie úlohy zamerané na systematizáciu šifier z rôznych hľadísk. V programovacom prostredí Lazarus som vypracoval sadu alternatívnych úloh na šifrovanie. Myšlienková mapa v programe FreeMind poskytuje prehľad o šifrovacích technikách v minulosti.

# 1 OPIS OSVEDČENEJ PEDAGOGICKEJ SKÚSENOSTI

## Kontext a rámec

V hlavnej časti práce som predstavil súbor metodických materiálov, ktoré boli odučené v rámci vyučovania povinného predmetu informatika na strednej odbornej škole v triedach prvého a druhého ročníka, konkrétne v študijnom odbore mechanik počítačových sietí a dopravná prevádzka. V súlade so štátnym vzdelávacím programom a školským vzdelávacím programom sa v týchto študijných odboroch týždenne vyučujú dve hodiny informatiky v prvom aj druhom ročníku. Okrem toho sa informatika vyučuje aj v týchto odborných predmetoch - programové vybavenie počítačov, technické vybavenie počítačov, programovanie a počítačové siete.

Škola disponuje tromi multimediálnymi počítačovými učebňami, každá pre 12 - 15 žiakov. Vo všetkých učebniach školy je možné využiť digitálne technológie, sú pokryté signálom wifi, je v nich možné použiť notebooky, dataprojektor, interaktívne tabule e-beam a Mimio. Každý učiteľ na škole má k dispozícii notebook alebo stolový počítač vo svojom kabinete.

## Špecifikácia cieľovej skupiny

- **Kategória:** učiteľ
- **Podkategória pedagogických zamestnancov podľa § 13 zákona č. 317/2009 Z. z. o pedagogických zamestnancoch a odborných zamestnancoch a o zmene a doplnení niektorých zákonov:** učiteľ pre úplné stredné všeobecné vzdelávanie a učiteľ pre úplné stredné odborné vzdelávanie (učiteľ strednej školy)
- **Žiak:** žiak strednej odbornej školy
- **Vzdelávacia oblasť:** matematika a práca s informáciami
- **Škola, ročník:** stredná odborná škola, 1. a 2. ročník
- **Vyučovacie predmety:**
  informatika,
  programové vybavenie počítačov,
  technické vybavenie počítačov,
  programovanie,
  počítačové siete.
- **Tematický okruh:**
  Informácie okolo nás.
  Postupy, riešenie problémov, algoritmické myslenie.
- **Tematický celok, učivo:** Kódovanie, šifrovanie informácií.
- **Názov programu kontinuálneho vzdelávania:**
  Využitie informačno-komunikačných technológií vo vyučovaní – inovačné.
  Premena školy: Cesta od tradičného vyučovania k aktívnemu učeniu sa žiakov – inovačné.
  Informatická výchova – kvalifikačné.
  Informatika pre stredné školy – kvalifikačné.
  Informatika pre 2.stupeň ZŠ – kvalifikačné.

## Cieľ práce

Poskytnúť učiteľom informatiky a odborných informatických predmetov metodický materiál a zbierku úloh na tému šifrovanie informácií pre tvorivejšie a pestrejšie sprístupnenie učiva na vyučovacej hodine.

## Vymedzenie kompetencií

Absolvovaním hodín s popísanou metodikou budujem u žiakov nasledovné kompetencie:

### Komunikatívne a sociálne interakčné spôsobilosti

- sprostredkovať informácie vhodným spôsobom (video, text, hovorené slovo, schéma) tak, aby každý každému porozumel,
- vyjadriť alebo formulovať (jednoznačne) vlastný názor a záver,
- aktívne používať odborný jazyk,
- kriticky hodnotiť informácie (kniha, internet a iné),
- správne interpretovať získané fakty, vyvodzovať z nich závery a dôsledky.

### Interpersonálne a intrapersonálne spôsobilosti

- rozvíjať prácu v kolektíve, v družnej a priateľskej atmosfére,
- osvojiť si pocit zodpovednosti za seba a spoluzodpovednosti za prácu v kolektíve,
- hodnotiť a rešpektovať svoju vlastnú prácu a prácu druhých,
- rozvíjať schopnosti kooperácie a komunikácie -naučiť sa spolupracovať v skupine pri riešení problému, zostaviť plán práce, špecifikovať podproblémy, distribuovať ich v skupine, vysvetliť problém ďalšiemu žiakovi, riešiť podproblémy, zhromaždiť výsledky, zostaviť ich do celkového riešenia, verejne o ňom referovať.

### Schopnosti riešiť problémy

- rozpoznávať problémy v priebehu vzdelávania využívaním všetkých metód a prostriedkov, ktoré majú žiaci v danom okamihu k dispozícii (pozorovanie, experimentovanie, grafické prostriedky, tabuľky a pod.),
- vyjadriť alebo formulovať (jednoznačne) problém, ktorý sa objaví v ich vzdelávacom procese,
- hľadať, navrhovať alebo používať ďalšie metódy, informácie alebo nástroje, ktoré by mohli prispieť k riešeniu problému,
- posudzovať riešenie daného problému z hľadiska jeho správnosti, jednoznačnosti alebo efektívnosti a na základe týchto hľadísk prípadne porovnávať aj rôzne riešenia daného problému,
- korigovať nesprávne riešenia problému,
- inovovať zaužívané postupy pri riešení úloh,
- odstraňovať stereotypy pri vyučovaní,
- používať osvojené metódy riešenia problémov aj v iných oblastiach vzdelávania žiakov, pokiaľ sú dané metódy v týchto oblastiach aplikovateľné.

**Spôsobilosti využívať informačné technológie**

- získavať informácie v priebehu vzdelávania využívaním všetkých metód a prostriedkov, ktoré majú žiaci v danom okamihu k dispozícii,
- zhromažďovať, triediť, posudzovať a využívať informácie, ktoré by mohli prispieť k riešeniu daného problému alebo osvojiť si nové poznatky,
- sprístupniť základné pojmy a techniky používané pri práci s údajmi a pri tvorbe algoritmov a výpočtových procesov. Vyučovanie v spojení s informačnými technológiami vytvára platformu pre všetky ďalšie predmety. Dostupné technológie majú poskytnúť vyučovaniu informatiky široký priestor na motiváciu a praktické projekty,
- rozvíjať metakognitívnu kompetenciu - t. j. učiť sa tým, že objavujem; učiť sa tým, že učím druhých; uvažovať o vlastných schopnostiach, definovať reálne ciele, rozmýšľať o procese učenia sa, kriticky posudzovať svoje poznatky, žiaci si majú uvedomiť zodpovednosť za svoje vzdelanie, získať vnútornú potrebu ďalšieho vlastného štúdia,
- rozvíjať si svoju osobnosť a tvorivosť.

**Spôsobilosti byť demokratickým občanom**

- formulovať a prezentovať svoje postoje v priebehu vzdelávania využívaním všetkých metód a prostriedkov, ktoré majú žiaci v danom okamihu k dispozícii,
- preukázať vlastnú zodpovednosť za zverené veci, za svoje vlastné správanie sa, zdravie a spoluzodpovednosť za životné prostredie a bezpečnosť pri práci.

# 2 PREHĽAD O SÚČASNOM STAVE VYUČOVANIA ŠIFROVANIA NA STREDNEJ ODBORNEJ ŠKOLE

Problematikou šifrovania sa zaoberajú oficiálne pedagogické dokumenty: štátny vzdelávací program, školský vzdelávací program, učebné osnovy informatických predmetov, vzdelávací štandard predmetu informatika a odborných informatických predmetov. V nasledovných častiach im budem venovať pozornosť.

## 2.1 Štátny vzdelávací program

V mojej práci vychádzam z požiadaviek štátneho vzdelávacieho programu ISCED 3A pre skupinu odborov 26 Elektrotechnika a ŠVP ISCED 3A pre skupinu odborov 37 Doprava pošty a telekomunikácie. Obsahové zameranie vzdelávacieho programu je orientované na odborné vzdelávanie a praktickú prípravu.

Cieľom vzdelávania v informačných technológiách je naučiť žiakov pracovať s informáciami. Žiaci pochopia základy informačných technológií a naučia sa na užívateľskej úrovni používať operačný systém, kancelársky software a pracovať s bežným aplikačným programovým vybavením vrátane špecifického programového vybavenia, ktoré sa používa v príslušnej odbornej oblasti. Absolvent má ovládať základy práce s operačnými systémami a základy programovania vo vyššom programovacom jazyku (ŠIOV, 2011). Vyučovanie kryptológie tento cieľ dokonale napĺňa.

## 2.2 Školský vzdelávací program

Školský vzdelávací program si školy pripravujú na základe štátneho vzdelávacieho programu. Školský vzdelávací program upravuje obsah a organizáciu vyučovania nad rámec štátom stanoveného minima v učebných osnovách. V práci sa zameriavam na rozbor školského vzdelávacieho programu 2682 K mechanik počítačových sietí z hľadiska problematiky šifrovania. Učivo o šifrovaní sa nachádza v učebných osnovách viacerých povinných predmetov – informatika, programové vybavenie počítačov, počítačové siete, technické vybavenie počítačov a vo voliteľnom predmete programovanie a nepovinnom predmete cvičenie z výpočtovej techniky.

## 2.3 Učebné osnovy

Predmet: Informatika
je súčasťou vzdelávacej oblasti Matematika a práca s informáciami. Tento predmet majú žiaci v 1. a 2. ročníku po jednej vyučovacej hodine. Osobitosťou odborných škôl je, že prevažná časť učiva sa učí aj v rámci odborných predmetov. V samotnom predmete informatike problematiku šifrovania nájdeme iba v dvoch tematických okruhoch.

Tematický okruh č.1: Informácie okolo nás.
- Kódovanie a šifrovanie.

Výkonovým štandardom je:
- demonštrovať digitalizáciu určeného slova použitím kódovacej tabuľky ASCII,
- vysvetliť použitie kódovacích tabuliek,
- opísať niektoré spôsoby kódovania údajov,
- obhájiť potrebu šifrovania informácii,
- demonštrovať použitie šifrovania na jednoduchom príklade,

- vysvetliť rozdiel medzi kódom a šifrou.

Tematický celok č.2: Informačná spoločnosť.
- Riziká informačných technológií.
- Počítačová bezpečnosť.
- Kryptológia.

Výkonovým štandardom je:
- zdôvodniť potrebu ochrany údajov a vysvetliť, aké sú jej spôsoby a prostriedky.

Kryptológia, šifrovanie sa učí v rámci nasledovných odborných predmetov:
Predmet: Programové vybavenie počítačov.
Predmet sa vyučuje v 1.ročníku dve vyučovacie hodiny týždenne a v 2. – 4. ročníku jednu vyučovaciu hodinu týždenne.

Tematický celok: Ochrana informácií v počítačových sieťach, kódovanie.
- Bezpečná komunikácia
- Šifrovanie (typy, princípy)
- Symetrická šifra
- Asymetrická šifra
- Komunikácia typu klient – server (HTTPS)
- Steganografia.

Výkonovým štandardom je:
- vysvetliť pojem šifrovanie, vysvetliť rozdiel medzi šifrovaním a kódovaním, uviesť príklady šifrovania a kódovania,
- vysvetliť princíp bezpečnej komunikácie pomocou protokolu HTTPS,
- vysvetliť pojem steganografia, uviesť príklady metód steganografie a ich použitie v praxi.

Problematike kryptológie sa venujem aj v predmete programovanie, tiež v rámci výučby kancelárskeho balíka v predmete informatika, ale aj v predmete matematika v rámci učiva o prvočíslach a číselných sústavách. V mojej práci sa hlavne kvôli obmedzenému rozsahu budem venovať len základom šifrovania v rámci kancelárskeho balíka MS Office a programovacieho prostredia Delphi /Lazarus.

# 3 NÁVRH METODIKY VYUČOVANIA ŠIFROVANIA

## 3.1 Východiská pre vyučovanie šifrovania

Šifrovanie je príkladom využívania poznatkov z rôznych vedných odborov, čo môžem využiť pri vytváraní a upevňovaní medzipredmetových vzťahov. Spájam poznatky z dejepisu, chémie, fyziky a najmä matematiky. Pri šifrovaní využívam vlastnosti prvočísel, prevody číselných sústav, zobrazenia, funkcie, logické uvažovanie, štatistiku, kombinatoriku. Šifry si vyžadujú výbornú znalosť štruktúry jazyka, slovnej zásoby materinského jazyka, ale aj dobrú znalosť cudzích jazykov.

Mnoho mladých ľudí hľadá spôsoby, ako precvičiť svoj mozog, riešia rôzne krížovky, rébusy, doplňovačky a pod. Iní zasa radi siahnu po napínavej knihe alebo filme so špionážnou zápletkou, šifrovaním, hľadaním tajomstiev, ktoré priamo prekypujú rôznymi šiframi a kódmi (Da Vinciho kód, Anjeli a démoni, Sherlock Holmes a pod.). Žiaci veľmi radi uvítajú každé vytrhnutie z obvyklej jednotvárnosti vyučovacích hodín. Šifrovanie je práve jedným z vítaných spestrení, ktoré ich núti premýšľať, myslieť iným spôsobom, vyžaduje plné sústredenie, núti ich efektívne spolupracovať, analyzovať problémy, rozvíjať logické myslenie, hľadať informačné zdroje a to všetko aj súťažnou formou, bez toho, aby si všimli, že sa vlastne učia. Niektorí žiaci majú problémy s komunikáciou, boja sa povedať svoj názor. Zaujatie hrou v mnohých prípadoch pomáha tieto problémy riešiť a odstraňovať. Táto forma je vhodná aj pre deti so špeciálnymi výchovno-vzdelávacími potrebami (autizmus, vývinové poruchy učenia, poruchy správania ap.), ktoré sú síce inteligentné, ale nedokážu dobre komunikovať a ukázať svoje schopnosti.

Zastávam názor, že vyučovanie kryptológie, šifrovania sa dá pomerne ľahko realizovať v aplikáciách kancelárskeho balíka MS Office a programovacieho prostredia Delphi / Lazarus. Uvedené aplikácie umožňujú postupne vytvárať sadu úloh od najjednoduchších až po veľmi náročné. Mnohé úlohy patria síce medzi náročné, ale nie nezvládnuteľné. Od žiakov sa vyžaduje, aby zvládli základy práce v MS Word a MS Excel, resp. Open Office.

Pri každej preberanej téme je vhodné voliť na začiatku vyučovania jednoduchšie a až neskôr je možné prejsť na zložitejšie úlohy, aby som žiakov neodradil. Niektoré úlohy sa dajú realizovať so žiakmi prvého ročníka, ale náročnejšie až so žiakmi druhého, prípadne vyššieho ročníka na hodinách programovania. Štúdium kryptografických pojmov na strednej odbornej škole som prepojil s programovaním aj preto, lebo ak žiak zvládne samostatne naprogramovať šifrovací algoritmus, pochopí aj jeho činnosť. Pre žiaka je tento spôsob práce omnoho atraktívnejší a následný výklad na odborných predmetoch, pri používaní elektronickej pošty, vytváraní hesiel efektívnejší. Samozrejme predtým, ako začnem so žiakmi šifru programovať, podrobne ju vysvetlím a uvediem konkrétny príklad, napríklad pomocou prezentácie PowerPoint, Wordu alebo Excelu, ktorý bude slúžiť žiakom ako kontrola správnosti ich činnosti.

## 3.2 Vyučovacie metódy

V práci som použil viacero metód, ktoré sú uvedené v jednotlivých úlohách. Dôležité je jednotlivé metódy navzájom kombinovať, meniť a striedať, tak sa určite učivo pre žiakov stane zaujímavejšie a tiež sa vyhnem jednostrannosti vo vyučovacom procese.

### 3.3 Organizačné formy vyučovania

Podľa počtu žiakov zúčastňujúcich sa na vyučovacom procese odporúčam a osvedčila sa mi kombinovaná organizačná forma vyučovania (kombinácia individuálnych a hromadných organizačných foriem) realizovaná v počítačovej učebni.

Podľa stupňa samostatnosti práce žiakov na vyučovacom procese odporúčam využitie individuálnej práce žiakov pri riešení jednoduchých úloh, či s využitím skupinovej práce žiakov pri riešení zložitejších, komplexnejších úloh. Čo sa týka individuálnej práce žiakov, odporúčam zaradiť do vyučovania analogickú, tvorivú a samostatnú prácu žiakov. A čo sa týka skupinovej práce žiakov, navrhujem zoskupovanie žiakov do skupín usmerňovaním zo strany učiteľa o počte 3 až 4 žiakov. Počet žiakov neodporúčam v skupinách zvyšovať, aby sa nestalo, že na riešení zadanej úlohy či projektu budú nakoniec aktívne pracovať maximálne dvaja žiaci a ostatní sa na riešení budú podieľať iba pasívne, resp. vôbec. Jednotlivé skupiny žiakov rozdeľujem podľa úrovne vstupných požiadaviek na vedomosti tak, aby aj slabší žiaci boli platnými členmi skupiny. Slabších žiakov nepodceňujem, lebo často dokážu v skupine prísť so zaujímavými nápadmi aj napriek tomu, že v niektorých činnostiach majú nižšie vedomosti a zručnosti.

### 3.4 Materiálne prostriedky vyučovania

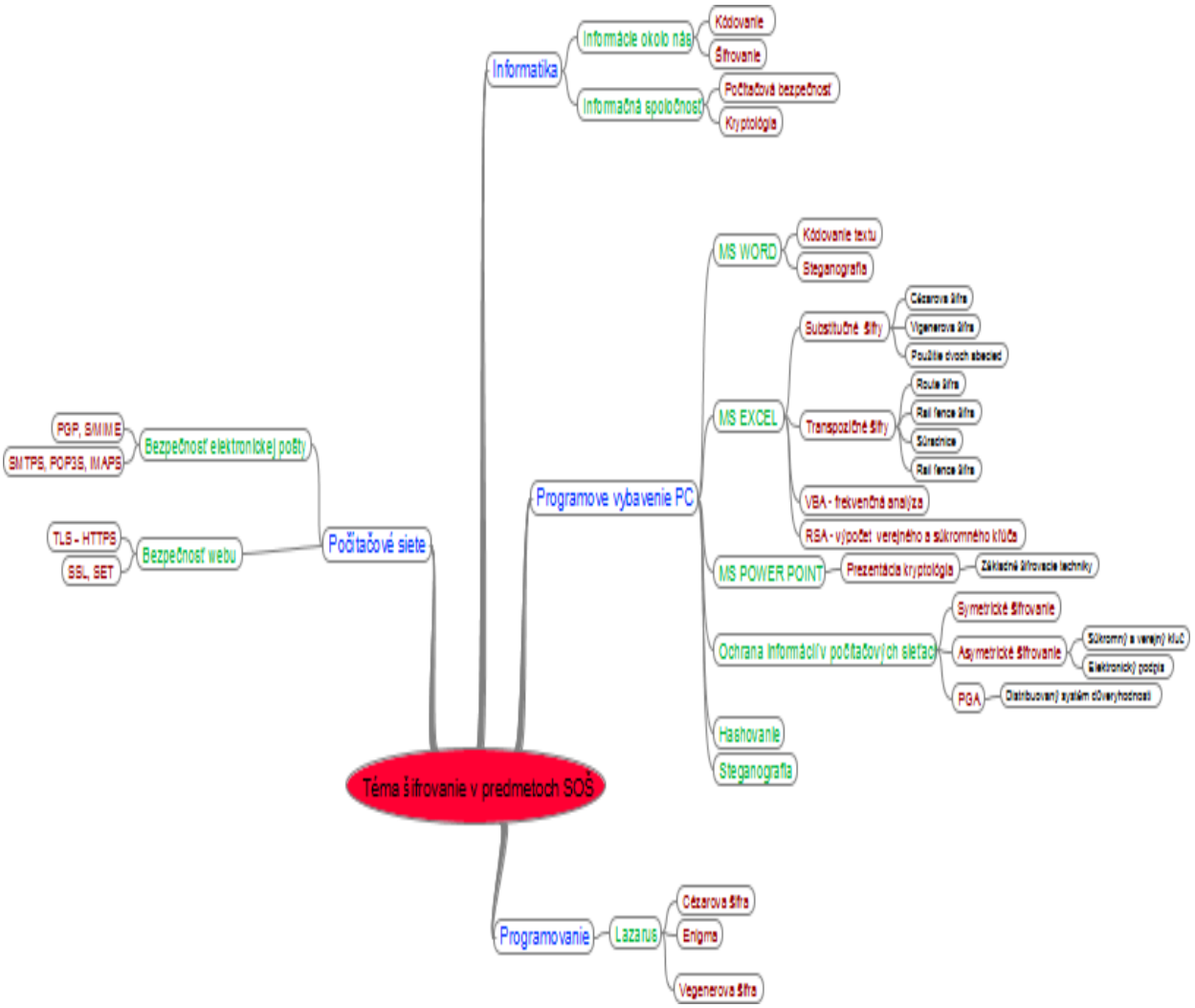
Nevyhnutnou súčasťou vyučovania šifrovania v aplikáciách kancelárskeho balíka je počítač, na ktorom je nainštalovaný MS Office, resp. iný kancelársky balík a programovací jazyk Pascal. Pri vysvetľovaní učiva a prezentácii je veľmi dôležitá interaktívna tabuľa. Pre individuálnu prácu žiakov je vhodnou pomôckou aj ceruzka a štvorčekovaný papier.

### 3.5 Základné pojmy

Otvorený text - text určený k zašifrovaniu.
Steganografia - odbor, ktorý skúma metódy utajenia existencie správy a jej posielanie.
Substitučná šifra - transformuje otvorený text na šifrový náhradou (substitúciou) znakov.
Šifrovacia funkcia - transformuje otvorený text na šifrový.
Šifrovací kľúč - vstupuje do šifrovacej funkcie, je utajovaný prvok bezpečnej komunikácie.
Šifrový text - výsledok šifrovacej funkcie.
Transpozičná šifra - transformuje otvorený text na šifrový zámenou poradia znakov.

Podrobnú analýzu pojmov a ich vzťahov uvádzam v pojmovej mape kryptológia a v prezentácií šifrovanie.pptx.

### 3.6 Štruktúra učiva podľa tematických celkov




Obrázok 1 Myšlienková mapa – šifrovanie v informatike a odborných informatických predmetoch

Prameň: vlastný návrh

### 3.7 Systém úloh

Ako učebnú úlohu som predkladal každú požiadavku na merateľnú činnosť žiaka zameranú na dosiahnutie cieľov učenia sa. Každá úloha má svoje komponenty:

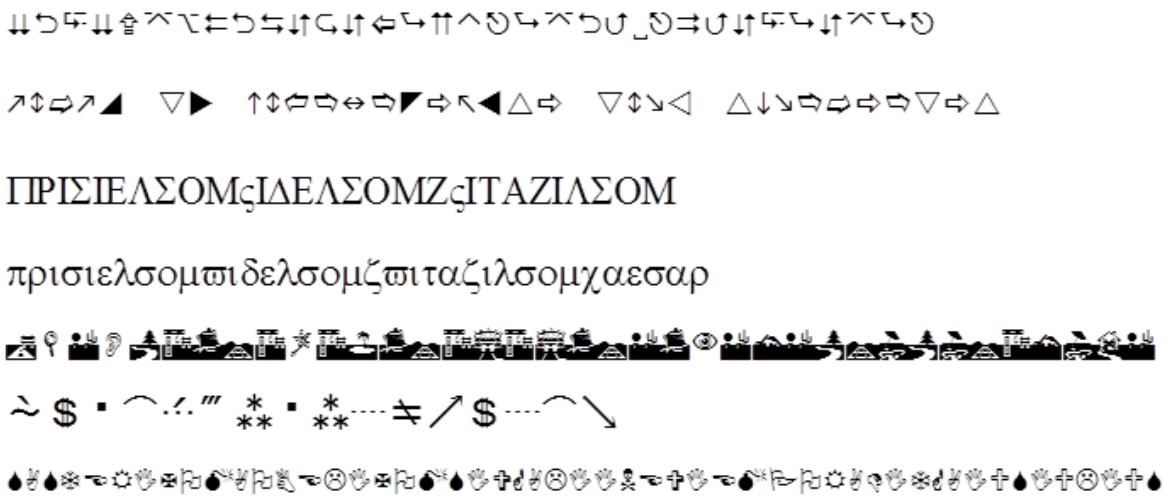
- Štartovacia pozícia (podmienky, zadanie).
- Cesta (postup, riešenie).
- Cieľová pozícia (výsledok).
- Poznatková báza (subjektívny aspekt úlohy).
- Tvorivé úlohy majú otvorené viaceré komponenty.
- Zmena náročnosti úlohy napr. zmenou podmienok (Guniš, 2008).

Systém úloh tvorí postupnosť gradovaných úloh pokrývajúcich výchovné a vzdelávacie ciele zohľadňujúce jednotlivé etapy poznávacieho procesu a rôzne úrovne

požadovaných myšlienkových operácií. Motivuje žiakov a vyžaduje od nich aktívny prístup. Slúži učiteľovi ako návod pri preberaní daného učiva. Pretože moja práca je zameraná na konkrétny študijný odbor, môže si vytvoriť svoj vlastný systém úloh pre nich viac vhodnejší, resp. vhodnejší pre jeho žiakov. Každá úloha v systéme úloh má k sebe pripojený metodický komentár určený pre učiteľa.

Rozdelenie úloh podľa etapy vyučovacieho procesu :
- motivačné úlohy č.1, 2, 3, 4, 5, 6
- expozičné úlohy č. 1, 2, 5, 6
- aplikačné úlohy č. 3, 4, 6
- diagnostické úlohy č. 3, 4.

**Úloha č. 1:**
Ľudia sa už od praveku pokúšali komunikovať pomocou rôznych prostriedkov, ako napr. reč, písmo atď. takým spôsobom, ktorý by zabezpečoval ochranu obsahu pred neželanými osobami a ich vplyvu na prenášané správy. Jednou z možností bolo zašifrovať text tak, že sa zamenilo jedno písmeno iným. Tento spôsob, substitúciu, prvýkrát opísal Július Cézar v svojej knihe Zápisky o vojne v Galii. Poslal list napísaný síce latinsky, ale s použitím gréckych písmen. V dnešnej dobe by to bolo mimoriadne naivné, stačilo by tento text prepísať napr. do Wordu a zmeniť typ písma, nehovoriac o tom, že veľa ľudí grécke písmená pozná. Aj v jeho časoch bola sila tejto šifry založená hlavne na negramotnosti obyvateľstva a nie na šikovnosti nápadu, hoci originalita sa mu uprieť nedá. Žijeme v modernej dobe počítačov a určite nebude problém pre vás vyriešiť podobnú úlohu v programe Word. Zistite, čo skrývajú nasledujúce odkazy:

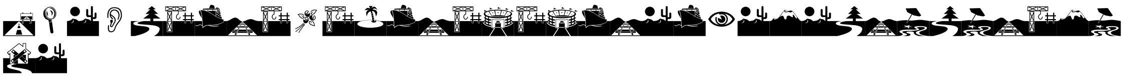


⇊⊃⭋⇊⇮⌅⌥⇇⊃⇆⇅⊂⇅⇦↳⇈^⊘↳⌅⊃∪‿⊘⇉∪⇅⭋↳⇅⌅↳⊘

↗⇕⇨↗◢ ▽▶ ↑⇕⇦⇨⇔⇨◤⇨↖◀△⇨ ▽⇕↘◁ △↓↘⇨⇨⇨⇨▽⇨△

ΠΡΙΣΙΕΛΣΟΜςΙΔΕΛΣΟΜΖςΙΤΑΖΙΛΣΟΜ

πρισιελσομϖιδελσομζϖιταζιλσομχαεσαρ



∻ $ ▪ ⌒∴‴ ⁂ ▪ ⁂---≑／$----⌒＼

💧✌💧❄☜☼✋✠⚐💣✌⚐✍☜☹✋✠⚐💣💧✋✞👌✌☹✋✋☠☜✞✋☜💣🏱⚐☼✌👍✋❄👌✌✋✞💧✋✞☹✋✞💧

**Riešenie:**
Je potrebné označiť text pomocou myši a zmeniť typ písma napr. na Times New Roman, Arial, Cambria a pod.
Použitý typ písma:
Wingdings 3:

⇊⊃⭋⇊⇮⌅⌥⇇⊃⇆⇅⊂⇅⇦↳⇈^⊘↳⌅⊃∪‿⊘⇉∪⇅⭋↳⇅⌅↳⊘
KOCKYSUHODENEZAJTRASOMVRIMECAESAR
↗⇕⇨↗◢▽▶↑⇕⇦⇨⇔⇨◤⇨↖◀△⇨▽⇕↘◁ △↓↘⇨
kockysuhodenezajtrasomv rime

Wingdings 2:

②⑥ഹ②❺ ⑩❶ ⇜⑥ൽ⇝⑤⇝❻ൽ①⓿⑨ൽ ⑩⑥④❷ ⑨⓪④⇝ഹൽ⇝⑩ൽ⑨
KOCKYSUHODENEZAJTRASOMVRIMECAESAR

Symbol:

ΠΡΙΣΙΕΛΣΟΜςΙΔΕΛΣΟΜΖςΙΤΑΖΙΛΣΟΜ
PRISIELSOMVIDELSOMZVITAZILSOM

πρισιελσομϖιδελσομζϖιταζιλσομχαεσαρ
prisielsomvidelsomzvitazilsomcaesar

Webdings:

kleopatrazajtrasastretnemepripyramidecaesar

Bookshelf Symbol 7:

∻ $ ▪ ⌒∴‴ ⁂ ▪ ⁂---≑／$----⌒＼
ajtybrutusmojsyn

Wingdings

| |
|---|
| ♠✌♠❄☜☼✋✠⚐💣✌⚐🖒☜☹✋✠⚐💣♠✋✞✌☹✋✋☠☜✞✋☜💣⚑⚐☼✌☜✋❄✌✋✞♠✋✞☹✋✞♠ |
| SASTERIXOMAOBELIXOMSIVGALIINEVIEMPORADITGAIUSIULIUS |

**Komentár k riešeniu, odporúčania, skúsenosti pre prax:**
Žiakov zaujala úloha dešifrovať (dekódovať) text. Uvedomili si, že text sa dá zakódovať pomocou rôznych obrázkov, obrázkového písma, čiarovým kódom, binárnym kódom .... Zároveň som ich pripravil na tému šifrovanie informácií.

Odporúčam doplniť úlohy otázkami a príkazmi typu:
- Navrhnite iné druhy písma zo sady MS Office. Ktoré typy písma by ste použili na zašifrovanie textu?
- Vymenujte niektoré spôsoby kódovania informácií, ktoré ľudia vymysleli v minulosti .
- Nájdite na Internete iné druhy kódovania, ktoré sa používajú v praxi.
- Nájdite prípady z minulosti, keď odhalenie tajného textu zmenilo dejiny. Našli by ste taký príklad v dejinách?

Úloha splnila motivačnú funkciu a bola prípravnou úlohou pre zavedenie kryptografických pojmov - šifrovanie, dešifrovanie, substitučná šifra. Chcel som ňou u žiakov rozvíjať samostatnosť, logické myslenie, vzťah k histórií a k informatike, rozvíjať prirodzenú snahu odhaľovať tajomstvá a riešiť problémy, čo sa aj podarilo.

**Úloha č. 2**
Rímsky konzul Cézar kódoval správy tak, že posúval písmená o tri miesta v abecede vpravo. Využíval teda dve abecedy, abecedu textu nahradil abecedou správy.

Napr.: GQHVYHFHUEXGHPQDUDQGHVNOHRSDWURX

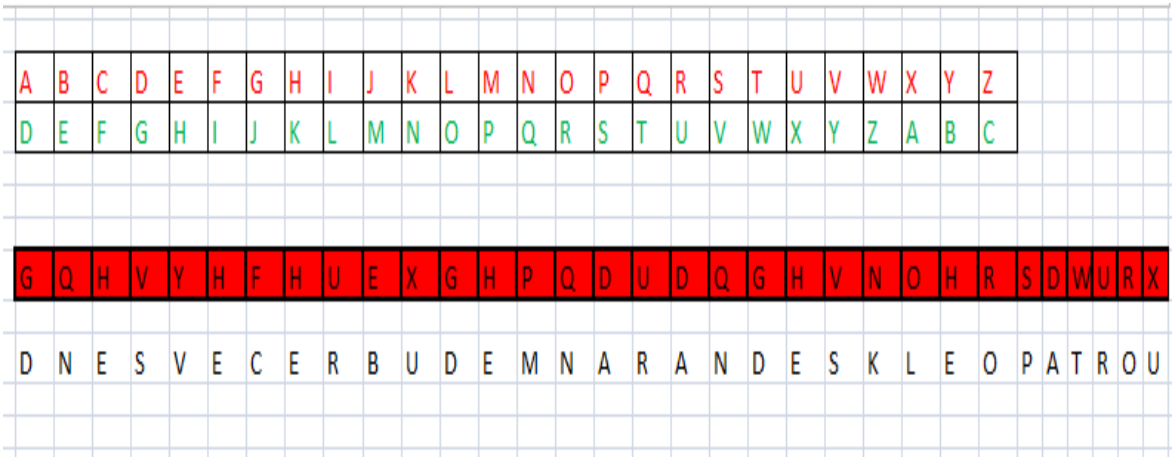
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | | | | | | |

Zistite obsah Cézarovej správy.
a) Doplňte v programe Excel Cézarovu tabuľku podľa zadania posunom o tri znaky.
b) Nahraďte písmená v texte tak, že vymeníte písmená z dolného riadku písmenom horného riadku tabuľky.
c) Napíšte odtajnenú správu.
d) Vytvorte vlastný zoznam z prvého riadku v tabuľke.
e) Vytvorte použitím vlastného zoznamu iné šifrovacie tabuľky posunutím postupne o 4, 5, 6, 7 písmen.
f) Napíšte zašifrovanú správu na papierik pomocou vašej tabuľky a pošlite ju postupne skupine 1-2-3-4-1 a vyučujúcemu.
g) Odovzdajte odšifrovanú správu vyučujúcemu.

Víťazom sa stáva ten, kto má najrýchlejší a najpresnejší preklad.

**Návod:**
Vytvorte vlastný zoznam - označte hodnoty v prvom riadku, choďte na Možnosti programu Excel – Upraviť vlastné zoznamy – Importovať.

**Riešenie:**




Obrázok 2 Cézarova šifra

Prameň: Šifrovanie.xlsx

**Komentár k riešeniu, odporúčania, skúsenosti pre prax:**
Žiaci hravou formou zvládli vytvorenie jednoduchej substitučnej šifry. Naučili sa tvoriť vlastné zoznamy a kopírovať bunky. Vysvetlil som im, že existuje veľa podobných šifier. Úlohu potom vyriešili žiaci podľa návodu, priebežne som im vysvetľoval jednotlivé postupy a ich použitie.

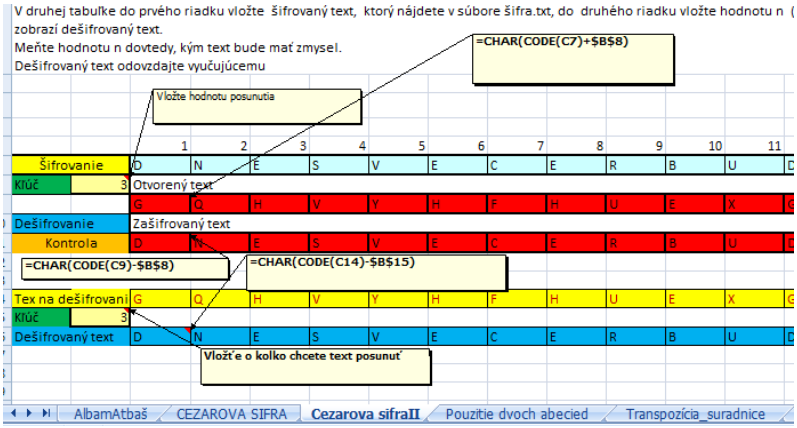
Úlohu odporúčam doplniť otázkami a príkazmi typu:
- Zistite, koľko takýchto možností posunutia písmen existuje.
- Navrhnite, akým spôsobom by sa daná šifra dala skomplikovať.
- Koľkými spôsobmi by sa dala správa zašifrovať takouto šifrou?
- Vymyslite iný spôsob šifrovania textu.

Ide o úlohu na precvičovanie a upevňovanie učiva o substitučnej šifre. Použitím vlastných zoznamov si žiaci precvičili formátovanie buniek a použitie kopírovacieho nástroja bunky. Úlohou som prispel k rozvíjaniu pozitívneho prístupu k učeniu sa v škole, k vyučovaniu informatiky, dejepisu a matematiky.

Pre žiakov som pripravil alternatívne úlohy (Príloha č. 1,2,3,4):
Šifrovanie.xlsx - Albam, Atbaš, Použitie dvoch abecied, Transpozícia_súradnice II, Vigener_princíp.

**Úloha č. 3**
Vytvorte v programe Excel 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.

**Riešenie:**
Použijeme funkcie: na šifrovanie =CHAR(CODE(C7)+$B$8)
Dešifrovanie1: CHAR(CODE(C9)-$B$8), Dešifrovanie2:=CHAR(CODE(C14)-$B$15)



Obrázok 3 Šifrovací a dešifrovací stroj

Prameň: Šifrovanie.xlsx_

**Komentár k riešeniu, odporúčania, skúsenosti pre prax:**
Žiaci si upevnili používanie textových funkcií CHAR, CODE. Sami si vytvorili tabuľku, ktorá bola prehľadná a dalo sa s ňou ďalej pracovať. Jednotlivé časti úlohy žiaci riešili samostatne nezávisle na sebe, resp. s individuálnou konzultáciou so mnou. Úloha podporovala súťaživosť žiakov.

Odporúčam doplniť úlohu otázkami a príkazmi typu:
- Aké vzorce by ste použili pri riešení úlohy?
- Zdôvodnite, prečo by ste použili dané vzorce?
- Dali by sa údaje v tabuľke zobraziť prehľadnejšie?
- Ako by ste obmedzili hodnotu posunutia tak, aby nebola väčšia ako 25 ?
- Čo by sa stalo, keby hodnota posunutia bola 26?

Ide o systemizačnú úlohu, v ktorej si žiaci preverili, či správne používajú skôr osvojené funkcie (CHAR, CODE), kopírovanie vzorcov, formátovanie vzorcov. Súčasne mala úloha diagnostickú funkciu. Hodnotil som splnenie jednotlivých častí úlohy, grafickú úpravu, stupeň samostatnosti. Úloha ukázala, že žiaci majú pozitívny vzťah k informatike a estetickému cíteniu.

Alternatívnu úlohu de Vigenérova šifra (Vigener) predkladám v Prílohe 5.

**Javová analýza:**
V jednotlivých častiach tejto úlohy som hodnotil rôzne javy v závislosti od typu, náročnosti a od úrovne osvojenia konkrétnej úlohy. V tabuľke uvádzam jednotlivé javy, ktoré sú použité v úlohe. Je už len na učiteľovi, ktorý z nasledujúcich javov použije pri hodnotení konkrétnej úlohy. Ak má záujem prihliadať na vyššiu úroveň osvojenia učiva, tak odporúčam jednotlivé javy spájať do jedného.

Tabuľka 1 Javová analýza

| Jav | Bodové hodnotenie |
|---|---|
| vytvorenie tabuľky podľa zadania | 1 |
| vytvorenie šifrovacej funkcie CHAR(CODE(C7)+$B$8) | 2 |
| kopírovanie vzorca | 1 |
| vytvorenie dešifrovacej funkcie CHAR(CODE(C7)-$B$8) | 2 |
| kopírovanie vzorca | 1 |
| vytvorenie dešifrovacej funkcie CHAR(CODE(C14)-$B$15) | 2 |
| zistenie obsahu zadaného šifrovaného textu | 3 |
| aktivita | 0 -3 |

**Hodnotenie:**

| 0 – 3 b | 4 – 5 b | 6 – 7 b | 8 – 9 b | 10 – 15 b |
|---|---|---|---|---|
| nedostatočný | dostatočný | dobrý | chválitebný | výborný |

Prameň: vlastný návrh

Priemerná známka z tejto úlohy podľa uvedenej tabuľky bola 2,23. Štyria žiaci mali výborné hodnotenie.

**Úloha č. 4: Cézarová šifra (Lazarus)**

Cézarova šifra je druh šifry, pri ktorej je každé písmeno správy posunuté o n pozícií ďalej v abecede, pričom n môže byť 1 až M − 1, kde M je počet znakov príslušnej abecedy. Táto šifra bola používaná rímskym vládcom okolo roku 50 pred našim letopočtom. Na tú dobu bola táto šifra veľmi komplikovaná, a preto sa používala aj ďalšie storočia. Princíp pôvodného algoritmu je posunutie každého písmena na písmeno, ktoré je v abecede o tri miesta za ním, čo môžeme vyjadriť matematicky

$y = x + 3 \pmod M$

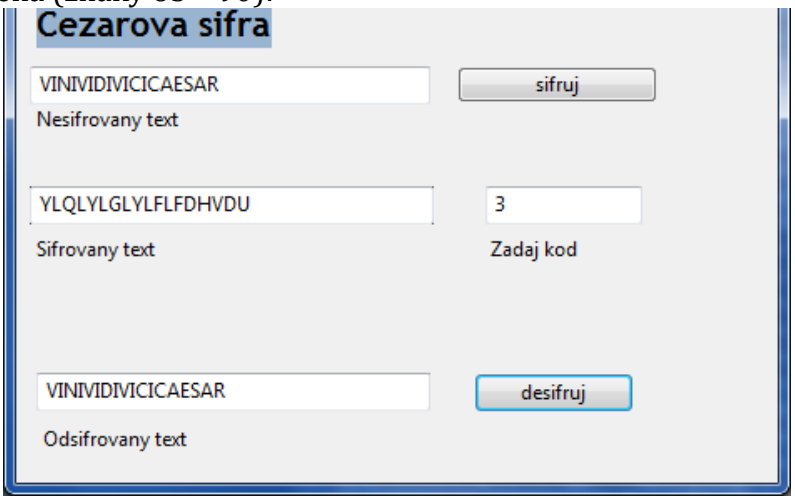
alebo všeobecnejšie

$y = x + n \pmod M$

Vytvorte v Lazaruse aplikáciu s dvoma tlačidlami a štyrmi editovacími políčkami. Prvé tlačidlo premenujte na šifruj a druhé premenujte na dešifruj. Editovacie políčka popíšte labelmi: nešifrovaný text, šifrovaný text, odšifrovaný text, zadaj kód.

V unite vytvorte funkcie EnDeCrypt na zašifrovanie textu pomocou Cézarovej šifry o k pozícií a funkciu DeCrypt na dešifrovanie textu.
Stlačením prvého tlačidla vytvorte procedúru, ktorá do políčka edit2 vloží funkciu na zašifrovanie textu z edit1 a do druhého tlačidla funkciu na dešifrovanie textu z políčka edit2.

**Riešenie:**
Pre veľké písmená (znaky 65 – 90):




Obrázok 4 Cézarova šifra

Prameň: vlastný návrh

Výpis programu Unit:

```
Procedure Button1Click(Sender: TObject);
procedure Button2Click(Sender: TObject);
function EnDeCrypt(const Value : String) : String;
function DeCrypt(const Value : String) : String;
  private
    { private declarations }
  public
    { public declarations }
  end;
var
  Form1: TForm1;
implementation
var CharIndex,k : integer;
{$R *.lfm}
  function TForm1.EnDeCrypt(const Value : String) : String;
begin
Result := Value;
  k:=strtoint(edit4.text);
  for CharIndex := 1 to Length(Value) do
 Result[CharIndex] := chr((ord(Value[CharIndex])-65+k) mod 26 +65 );
 end;
  function TForm1.DeCrypt(const Value : String) : String;
  begin
Result := Value;
k:=strtoint(edit4.text);
 for CharIndex := 1 to Length(Value) do
 Result[CharIndex] := chr((ord(Value[CharIndex])-65-k) mod 26 +65 );
 end;
  procedure TForm1.Button1Click(Sender: TObject);
  begin
 Edit2.Text := EnDeCrypt(Edit1.Text);
```

```
 end;
 procedure TForm1.Button2Click(Sender: TObject);
begin
  Edit3.Text := DeCrypt(Edit2.Text)
   end;
end.
```

**Komentár k riešeniu, odporúčania, skúsenosti pre prax:**
Žiaci si precvičili vytváranie vlastných funkcií (EnDeCrypt, DeCrypt), upevnili si používanie funkcií CHR, ORD, STRTOINT, MOD a prácu s editovacími políčkami. Sami si vytvorili formulár, ktorý bol prehľadný, estetický a dalo sa s ním ďalej pracovať. Úlohu riešili žiaci samostatne a s individuálnou konzultáciou so mnou. Jednotlivé časti úlohy žiaci riešili samostatne, nezávisle na sebe. Úloha podporila súťaživosť žiakov. Cieľom bolo rozvíjať vzťah žiakov k matematike, programovaniu a ku kryptológii.

Odporúčam doplniť úlohu otázkami a príkazmi typu:
Ako upravíte funkcie EnDeCrypt a DeCrypt tak, aby v šifrovanom texte boli ASCII znaky?

- znaky 1 – 256,
- zvlášť sa budú šifrovať čísla a písmená ( znaky 48-57, 65-90, 97-122),
- len veľké písmená,
- len malé písmená.

Aké vzorce by ste použili pri riešení týchto úloh?

- Zdôvodnite, prečo by ste použili dané vzorce?
- Dali by sa údaje vo formuláre a programe zobraziť prehľadnejšie?
- Ako by ste obmedzili hodnotu posunutia tak, aby nebola väčšia ako 127, 256,... ?
- Čo by sa stalo, keby hodnota posunutia pri veľkých písmenách bez diakritiky bola 26?

Alternatívne riešené úlohy v programe Lazarus :
Cezar_subor - šifrovanie a dešifrovanie súboru, Cezar_subor2 - šifrovanie a dešifrovanie pomocou Memo, Cezar_pole - univerzálna šifrovacia a dešifrovacia funkcia použitím polí znakov sú na mojej webovej stránke www.janhanuliak.szm.com.

Žiakom som dal k dispozícii Pracovný list : Enigma – emulácia nemeckého šifrovacieho systému, ktorý sa nachádza v Príloha 6.

**Javová analýza:**
V tabuľke uvádzam jednotlivé javy, ktoré sú použité v úlohe a hodnotil som ich pridelením konkrétneho počtu bodov. Úloha bola pomerne náročná, čo sa prejavilo na priemernej známke 2,54. Len dvaja žiaci vytvorili funkčný program bez chýb.

Tabuľka 2 Javová analýza

| Jav | Bodové hodnotenie |
|---|---|
| vytvorenie TButton a TEdit | 1 |
| nastavenie vlastnosti objektov v inšpektorovi objektov | 1 |
| deklarácia premenných a konštánt | 1 |
| deklarácia procedúr alebo funkcií | 1 |
| vytvorenie funkcie EnDeCrypt | 3 |
| vytvorenie funkcie DeCrypt | 3 |
| načítanie hodnoty TEdit do premennej | 1 |
| zobrazenie premennej v políčku TEdit | 1 |
| priradenie procedúry tlačidlu 1 | 1 |
| priradenie procedúry tlačidlu 2 | 1 |
| ošetrenie prípadných chýb | 1 |
| aktivita | 0-3 |

**Hodnotenie:**

| 0 – 4 b | 5 – 7 b | 8 – 10 b | 11 – 13 b | 14 – 16 b |
|---|---|---|---|---|
| nedostatočný | dostatočný | dobrý | chválitebný | výborný |

Prameň: vlastný návrh

Alternatívne úlohy (neriešené):
Ako by ste naprogramovali šifru Atbaš a Albam, ktoré ste už riešili v programe MS Excel?
Návody:
Atbaš: Princíp algoritmu je zámena prvého znaku za posledný, druhý za predposledný a tak ďalej, čo môžeme vyjadriť funkciou
$y = 25*x + 25 = - x + 25 \pmod M$.
Albam: Základným algoritmom je Cézarova šifra s posunom o 13 znakov.
$y = x + 13 \pmod M$.

**Komentár k riešeniu, odporúčania, skúsenosti pre prax:**
Jedná sa o systemizačnú úlohu, v ktorej si žiaci preverili, či správne používajú skôr osvojené funkcie (chr, ord, mod), modifikovanie funkcií (EnDeCrypt, DeCrypt). Súčasne mala úloha diagnostickú funkciu. Hodnotil som splnenie jednotlivých častí úlohy, grafickú úpravu, stupeň samostatnosti. Úlohou som rozvíjal u žiakov pozitívny vzťah k algoritmickému mysleniu, k presnosti a trpezlivosti pri riešení problémov.

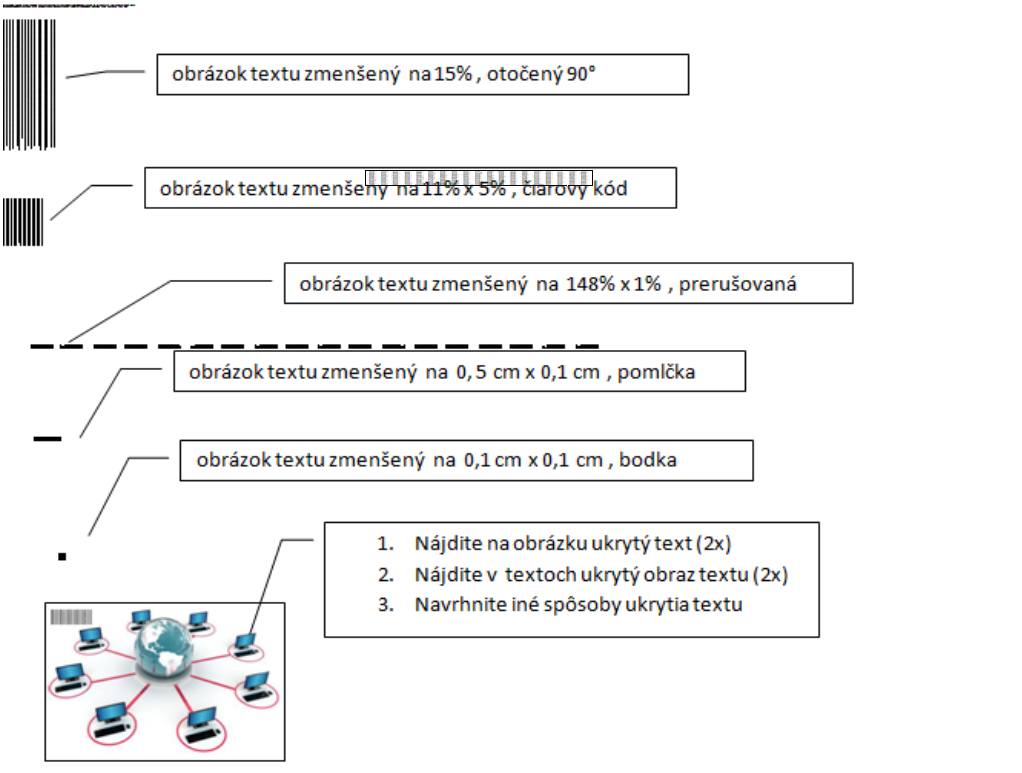
**Úloha č. 5: Steganografia (Skrývanie informácií).**

Proces skrývania údajov do inej formy údajov. Napríklad textový súbor môže byť skrytý „vo vnútri" obrazového alebo zvukového súboru. Pozeraním sa na obrázok alebo počúvaním zvuku by ste nemali spoznať prítomnosť externej informácie.

Skopírujte nasledujúci text do schránky a prilepte ho špeciálne ako obrázok :

Slovo 'steganosgraphein' je gréckeho pôvodu a znamená 'skryté písanie' ('steganos', schovaný a 'graphein', píšem). Prvý krát bola táto technika použitá už niekedy okolo roku 440 pred našim letopočtom. Demeratus (historik, 484-425 p. n. l.) vo svojich dejinách popisuje udalosť, kde práve ukrytie textu postačilo k bezpečnému zaslaniu správy. Varovanie o blížiacom sa útoku na Grécko napísal na drevenú dosku, ktorú potom zalial voskom a poslal ju po poslovi. Stráže, ktoré kontrolovali pri vstupe, ho prepustili, lebo nenašli nič len nepopísanú drevenú dosku. V nasledujúcich obdobiach sa mnoho ľudí inšpirovalo a vymysleli rôzne obmeny ako napr. vkladanie správ do útrob ulovených rýb, ukrývanie textov do malieb, pašovanie drog v telových dutinách a pod. S príchodom výpočtovej techniky sa aj pre steganografiu otvorili nové možnosti .Ideálnym médiom na ukrývanie stegospráv sú v počítačovom svete obrázky Majú obrovskú kapacitu, napríklad obrázok vo formáte BMP s rozlíšením 1024 x 768 bodov v 24-bitových farbách má veľkosť 2,25 MB. Obrázok si možno predstaviť ako maticu čísel, pričom každé z nich predstavuje číslo príslušnej farby. Čiernobiele obrázky majú iba jednu maticu, ktorej čísla predstavujú odtiene sivej. Farebné obrázky sú zložené akoby z troch matíc, každá pre jednu farebnú zložku, ktorými sú červená (R) zelená (G) modrá (B). Každý bod je zložený z týchto troch zložiek. Hodnota odtieňa sivej farby je v rozmedzí od 0 do 255 a takisto každá zložka R, G, B má hodnotu od 0 do 255. Dajú sa teda zakódovať do 8 bitov. Dve farby, ktoré sú v palete v tesnej blízkosti, to znamená, že ich číselná hodnota sa líši o 1, napríklad farba číslo 124 a 125, sú také príbuzné odtiene, že človek si nemusí uvedomiť ich vzájomnú zámenu v obrázku. Informácia je zapísaná v binárnom tvare, a to tak, že do každého LSB bitu každého bajtu obrázka sa zapíše 1 bit stegosprávy Správy je možné ukrývať aj do zvuku. Takisto sa tu využíva nedokonalosť ľudského ucha, ale je potrebné dáva si väčší pozor na výsledok, pretože ľudské ucho je veľmi citlivé. Možno použiť techniku, keď sa dáta ukrývajú do posledného signifikantného bitu (LSB) podobne ako v prípade obrázkov

Po nakopírovaní vykonajte s obrázkom nasledujúce operácie.




Obrázok 5 Steganografia

Prameň: vlastný návrh

**Komentár k riešeniu, odporúčania, skúsenosti pre prax:**

Ide o motivačnú a expozičnú úlohu. Žiaci sa oboznámili s jednoduchou formou ukrývania informácie – steganografie. Úlohu riešili samostatne podľa pracovného listu a potom pomocou interaktívnej tabule. Úlohou som pripravil žiakov na zložitejšie úlohy v

programovacom jazyku, ako je skrývanie informácie do zvukového súboru alebo do rastrového obrázku pomocou funkcie XOR.
Odporúčam doplniť úlohu otázkami a príkazmi typu:

- Aké iné formy skrývania informácie poznáte?
- Čítali ste o použití steganografie v minulosti ?
- Nájdite na Internete príklady použitia steganografie.
- Nájdite na Internete softvér na realizáciu steganografie.
- Program nainštalujte a vyskúšajte.

**Úloha č. 6: Transpozícia**

Leonardo da Vinci bol taliansky renesančný architekt, hudobník, vynálezca, sochár a maliar. Počas celého života používal zrkadlové písanie, písal svoje zápisky tak, že ich bolo možné čítať len s pomocou zrkadla. Wolfgang Amadeus Mozart skladal hravo svoje skladby, vedel hrať na klavíri s opačnou polohou rúk. Dokázal súvisle hovoriť odzadu. Ani oni, ani vy ste zrejme netušili, že používali jednoduchú transpozičnú šifru.

Transpozícia je v podstate poprehadzovanie znakov textu, každý znak si zachováva svoju podobu, ale mení svoju pozíciu. Priebeh transpozície závisí od šifrovacieho algoritmu. Existuje veľké množstvo jednoduchých transpozičných šifier, ale existujú aj odolné šifry bežne používané aj dnes.

**Príklad 1 : Písanie odzadu**
Celá zašifrovaná správa sa prepíše odzadu : Dnes je pondelok – KOLEDNOPEJSEND
Zašifrujte text označený ako text1, ktorý Vám zadá vyučujúci.
**Komentár:**
Očakávanie, že si žiaci upevnia poznanie vlastnosti textu sa splnili.
Odporúčam doplniť úlohu otázkami a príkazmi typu:

- Navrhnite spôsoby, ako by ste túto jednoduchú šifru skomplikovali.

**Príklad 2 : Písanie slov odzadu**
Toto je písanie odzadu – UDAZDO EINASÍP EJ OTOT
Zašifrujte text označený ako text2, ktorý Vám zadá vyučujúci..

**Príklad 3 : Súradnice**
Vytvorte v programe Excel šifrovaciu tabuľku podľa obrázku a zašifrujte zadaný text tak, že nahradíte jednotlivé znaky pracovného textu ich súradnicami v tabuľke - číslom stĺpca a písmenom riadku.

| | | | | | | Transpozícia - súradnice | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | VIEMZENICNEVIEM | V | I | E | M | Z | E | N | I | C | N | E | V | I | E | M |
| A | a | b | c | d | e | 2E4D3B2C5A4B4D3A4B5A2E4D5A3 | 2E | 4D | 5A | 3B | 2C | 5A | 4B | 4D | 3A | 4B | 5A | 2E | 4D | 5A | 3B |
| B | k | l | m | n | o | | | | | | | | | | | | | | | | |
| C | p | z | r | s | t | | | | | | | | | | | | | | | | |
| D | f | g | h | i | j | | | | | | | | | | | | | | | | |
| E | u | v | w | x | y | | | | | | | | | | | | | | | | |

Obrázok 6 Transpozičná šifra – súradnice

Prameň: Šifrovanie.xlsx

Dešifrujte zadaný text.
**Komentár:**
Očakával som, že si žiaci upevnia poznanie vlastnosti absolútnych súradníc. Po dôkladnom vysvetlení žiaci úlohu splnili.
Odporúčam doplniť úlohu otázkami a príkazmi typu:

- Navrhnite spôsoby ako by ste túto jednoduchú šifru skomplikovali?

**Príklad č. 4 Transponovaná matica**
Podľa snímky z prezentácie sifrovanie.pptx vytvorte v programe Excel 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.

Obrázok 7 Transpozičná šifra - transpozícia riadkov a stĺpcov

Prameň: Šifrovanie.pptx

Dešifrujte zadaný text.
**Komentár:**
Žiaci správne pochopili transpozíciu matice.
Odporúčam doplniť úlohu otázkami a príkazmi typu:

- Navrhnite iné spôsoby transpozície.

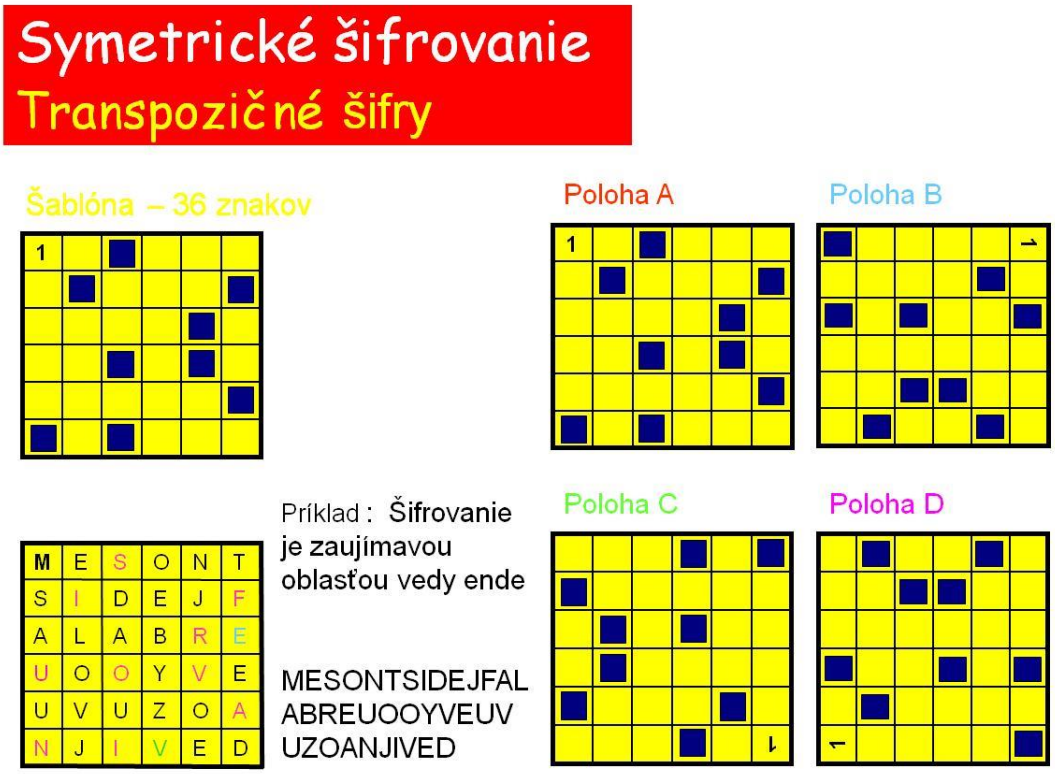
**Príklad č. 5 Šifrovacia mriežka**

Transpozíciu textu správy je možné spraviť aj podľa vopred dohodnutého kľúča alebo šifrovacej mriežky.

Šifrovacia mriežka je mriežka typu n x n (skladá sa z n riadkov, n stĺpcov, pričom n je prirodzené číslo). Najvhodnejšie je použiť párny počet riadkov a stĺpcov. V tejto mriežke sú niektoré (presne určené) štvorčeky vystrihnuté.

Vyberte si jednu šifrovaciu mriežku a položte ju na papier tak, aby prvé prázdne políčko bolo v ľavom hornom rohu (ak sa autor a príjemca správy nedohodnú inak). Do prázdnych políčok šifrovacej mriežky zapíšte časť správy. Šifrovaciu mriežku otočte v dohodnutom smere, napr. v smere hodinových ručičiek alebo proti smeru hodinových ručičiek a vpíšte do prázdnych políčok ďalšiu časť. Opäť otočte v smere mriežku a vpíšte znaky. Po štvrtom otočení šifrovacej mriežky dopíšte poslednú časť správy. Ak vám ostanú prázdne políčka, doplňte ich náhodnými znakmi. Vzniknutú zašifrovanú správu zapíšte do jedného riadku.

Pomocou mriežky zašifrujte krátku otázku a dajte ju spolužiakovi. Spolužiak odpovie zašifrovanou správou. Dešifrujte odpoveď, ktorú Vám poslal spolužiak.




Obrázok 8 Šifrovacia mriežka

Prameň: Šifrovanie.pptx

**Komentár:**
Žiaci si upevnili poznanie vlastnosti textu. Sami si vytvorili tabuľky, ktoré boli prehľadné a dalo sa s nimi ďalej pracovať. Jednotlivé časti úlohy riešili samostatne nezávisle na sebe, resp. s individuálnou konzultáciou so mnou.

Odporúčame doplniť úlohu otázkami a príkazmi typu:

- Zistite, koľko vystrihnutých okienok musí mať šifrovacia mriežka s rozmermi 8x8. Šifrovaciu mriežku otáčame štyrikrát.

- Určte, koľkoznakovú správu je možné zašifrovať šifrovacou mriežkou s dvanástimi riadkami.
- Zistite pomocou Wikipédie, ktorá armáda v 1. svetovej vojne používala Fleissnerovu šifrovaciu mriežku .
- Zistite pomocou Internetu, aký spôsob šifrovania použil francúzsky spisovateľ Jules Verne v knihe Nový Gróf Monte Christo.

# 4 OVERENIE NAVRHNUTEJ METODIKY

Dôležitým cieľom mojej práce – osvedčenej pedagogickej skúsenosti bolo overiť metodiku vo vyučovaní informatiky na strednej odbornej škole. Metodiku som overoval na Strednej odbornej škole v Kežmarku v 1. a 2. ročníku študijných odborov mechanik počítačových sieti, dopravná prevádzka a pracovník marketingu.

V rámci overovania som úlohy č. 1, 5 a 6 riešil so žiakmi v prvých ročníkoch. Žiakom úlohy nerobili problémy a veľmi ľahko vyriešili zadania aj doplnkové zadania. Úlohy č. 2, 3, 4 som riešil v druhom ročníku. Úlohu č. 2 úspešne zvládli všetci žiaci, úspešnosť 3. úlohy bola 60% a úlohu č. 4 bez pomoci učiteľa vyriešilo len 20% žiakov a s pomocou 45%. Nižšiu úspešnosť si vysvetľujem tak, že išlo o nové učivo, ktoré si vyžaduje fixáciu a dlhší čas, aby žiaci získali programátorské skúsenosti. Predpokladám, že riešením podobných úloh sa percento úspešnosti zvýši. Šesť žiakov dosiahlo plný počet bodov, čo svedčí o tom, že je v silách žiakov zvládnuť podobné úlohy, len si to vyžaduje dlhší čas a viac opakovania.
V motivačnej a expozičnej časti sa mi osvedčila prezentácia „sifrovanie.pptx“, podľa ktorej sa pomocou animácii šifier podarilo zvládnuť základné učivo, čo dokázali žiaci pri použití interaktívnej tabule vyriešením úloh č. 1, 2, 3.

## 4.1 Odporúčania pre pedagogickú prax

Na základe skúseností nadobudnutých počas realizácie vyučovania témy šifrovanie informácií odporúčam túto tému vyučovať na stredných odborných školách, najmä v tematických okruhoch „Postupy, riešenie problémov, algoritmické myslenie“ a „Informácie okolo nás“. Odporúčam vyučovať tému šifrovania najskôr v programoch MS Word, MS Excel a Power Point, ktoré poskytujú možnosti pre rôzne formy šifrovania, dešifrovania, steganografie. Použitím ich grafického a výpočtového potenciálu sa šifry stávajú názornými a ľahko realizovateľnými. Veľké množstvo funkcií, ktoré tieto programy obsahujú sa dajú efektívne využiť ako šifrovacie, resp. dešifrovacie nástroje. Sú to hlavne textové funkcie, prevody medzi číselnými sústavami DEC2HEX, DEC2OCT, DEC2BIN, BIN2DEC, štatistické funkcie, vlastné funkcie a iné. Použitie grafov a štatistických funkcií im umožní dešifrovať šifry pomocou frekvenčnej analýzy, ktorá precvičuje logické myslenie a núti žiakov poznať štruktúru jazyka, vlastnosti samohlások a spoluhlások. Nenásilnou formou si žiaci budujú medzipredmetové vzťahy. Sú zaujímavým spestrením vyučovacích hodín a nenápadne pripravujú žiakov na zvládnutie zložitejších algoritmov a prostriedkov programovacích jazykov. Pri svojej práci nevidia nudnú obrazovku vývojového prostredia (FreePascal) alebo množstvo okien (Lazarus), ale prostredie, ktoré dobre poznajú pri svojej práci s operačným systémom Windows a samotným balíkom MS Office.

Pri vyučovaní danej problematiky odporúčam klásť väčší dôraz na praktické riešenie úloh, než na vyučovanie teórie a pasívne prijímanie poznatkov. Aj z vlastných skúseností môžem usúdiť, že pri preberaní teórie sú žiaci znudení a majú menší záujem ďalej sa rozvíjať v tejto oblasti. Úlohou učiteľa by malo byť skôr vytváranie podmienok k poznávaniu ako predkladanie hotových vedomostí. Žiaci skôr uprednostňujú praktickú prácu s počítačom ako samotné prijímanie nových faktov. Samotné vyučovanie tejto témy u väčšiny žiakov vzbudilo záujem o túto problematiku. Po zadaní úlohy odporúčam mať pripravené súbory, prezentácie, aby žiaci kvôli lepšej názornosti videli, čo je cieľom ich práce a čo od nich očakávam.

Počas vyučovania žiaci nemali väčšinou problém pochopiť zadania úloh. Zadania úloh sú pomerne obšírne, robil som to úmyselne, lebo s takýmto spôsobom zadania sa stretávajú napr. v testoch PISA. Najväčšie problémy žiakom spôsobovali chybové hlásenia počas ladenia programu a často zabúdali úlohu na začiatku uložiť. Tu by bolo vhodné, aby sa na hodinách anglického jazyka venovala pozornosť aj technickej angličtine. Najväčšie problémy majú žiaci, ktorí sa učia nemecký jazyk, ktorí majú problémy aj s vyhradenými výrazmi programovacieho jazyka. Odporúčam klásť veľký dôraz pri vysvetľovaní tejto problematiky, pripraviť pre nich preklad najčastejších chybových hlásení a ich zrozumiteľný výklad .
Zbierka materiálov, ktoré sú vhodné na vyučovanie tejto problematiky sa nachádza v prílohe. Tieto úlohy a projekty som vyberal tak, aby boli motivujúce pre žiakov a využiteľné v praxi.

# ZÁVER

Počas práce na tomto projekte som urobil rozbor problematiky šifrovania v informatických predmetoch na strednej odbornej škole. Ako motiváciu som použil niekoľko zaujímavých historických faktov z dejín šifrovania. Pre lepšie zvládnutie jednotlivých spôsobov šifrovania uvádzam v práci ukážky, ktoré majú žiakovi pomôcť ozrejmiť a lepšie pochopiť študované učivo. Svoje získané vedomosti si žiaci overili na úlohách, ktoré im majú zároveň pomáhať rozvíjať tvorivosť, podporiť ich logické a algoritmické myslenie, schopnosť aplikovať získané poznatky, dedukovať, či vedieť vyvodiť a zdôvodniť svoje tvrdenie.

V rámci medzipredmetových vzťahov som okrem historických faktov použil v úlohách výroky známych osobností, ktoré sú zakomponované v jednotlivých úlohách. Pripravil som prezentáciu, ktorá názorne ukazuje problematiku kryptológie, názorne vysvetľuje princípy substitučných a transpozičných šifier, symetrického a asymetrického šifrovania a elektronického podpisu. Je vhodná pri vysvetľovaní jednotlivých šifier najmä v odborných informatických predmetoch. Súbory sifrovanie.xls a sifrovanie.xlsm (makra), obsahujú hárky s úlohami, ktoré sú vhodné na precvičovanie substitučných a transpozičných šifier, frekvenčnej analýzy, tvorby verejného a súkromného kľúča. Ďalšiu časť tvoria projekty vypracované v programovacom prostredí Lazarus (rôzne verzie Cézarovej šifry, emulácia nemeckého šifrovacieho systému Enigma). Myšlienková mapa názorne ukazuje problematiku kryptológie, kryptografie a kryptoanalýzy. Tieto časti sú venované učiteľom informatiky stredných odborných škôl, ktorí majú záujem svoje hodiny obohatiť o tému šifrovania v aplikáciách kancelárskeho balíka a programovacieho jazyka Lazarus. Keďže jednotlivé úlohy a projekty zbierky riešených úloh gradujú, žiaci si na týchto úlohách precvičia a osvoja učivo.

Po každom príklade uvádzam komentár k riešeniu, odporúčania, skúsenosti pre prax a doplňujúce alternatívne úlohy.

Okrem vysvetlenia základného učiva a vytvorenia zbierky riešených úloh bola téma v aplikáciách kancelárskeho balíka odučená na SOŠ v Kežmarku.
Prostredníctvom tejto skúsenosti som sa zdokonalil v oblasti šifrovania. Výučba témy ma obohatila aj po didaktickej stránke. Bola to pre mňa veľká výzva učiť novú, zaujímavú tému, vo vyučovaní ktorej by som chcel pokračovať aj v budúcnosti. Plánujem ju rozšíriť o problematiku frekvenčnej analýzy, asymetrického šifrovania, vytvárania súkromného a verejného kľúča. Pri inovácii školského vzdelávacieho programu sa zameriam na zaradenie týchto tém do vyučovacieho procesu a na tvorbu komplexnejších projektov a úloh využiteľných v praxi.
Dúfam, že táto osvedčená pedagogická skúsenosť pomôže hlavne učiteľom informatiky pri oživení vyučovacích hodín.

# ZOZNAM BIBLIOGRAFICKÝCH ZDROJOV


1. GUNIŠ, J., ŠNAJDER, Ľ. 2008. Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika, didaktika predmetu Informatika 2. ŠPU, Bratislava.2008. ISBN: 978-80-8118-021-7

2. KALAŠ, I., BLAHO, A. 2007. Tvorivá informatika. 1. zošit z programovania. SPN - Mladé letá, Bratislava. 48. s. 2007. ISBN: 80-10-01723-2

3. SINGH, S. 2009. Kniha kódů a šifer. Argo / Dokořán . Edice Aliter,Praha.2009. ISBN: 978-80-7363-268-7


**Internetové zdroje**


4. Kolektív autorov. 2008. Štátny vzdelávací program. Informatika. Príloha ISCED3A [online]. ŠPU, Bratislava. 2008. Dostupné na internete: https://www.iedu.sk/vyucovanie_a_studium/vyucovacie_predmety/xKatalog_Dokumenty/Informatika%20ISCED%203.pdf

5. Štátny inštitút odborného vzdelávania. 2011. Štátne vzdelávacie programy ISCED 3A. [on-line] [citované 2011-04-10] http://www.siov.sk/ext_dok-svp-isced-3a-26/11562c

## ZOZNAM PRÍLOH

Príloha 1 Šifrovanie.xlsx - Albam, Atbaš

Príloha 2 Šifrovanie.xlsx - Použitie dvoch abecied

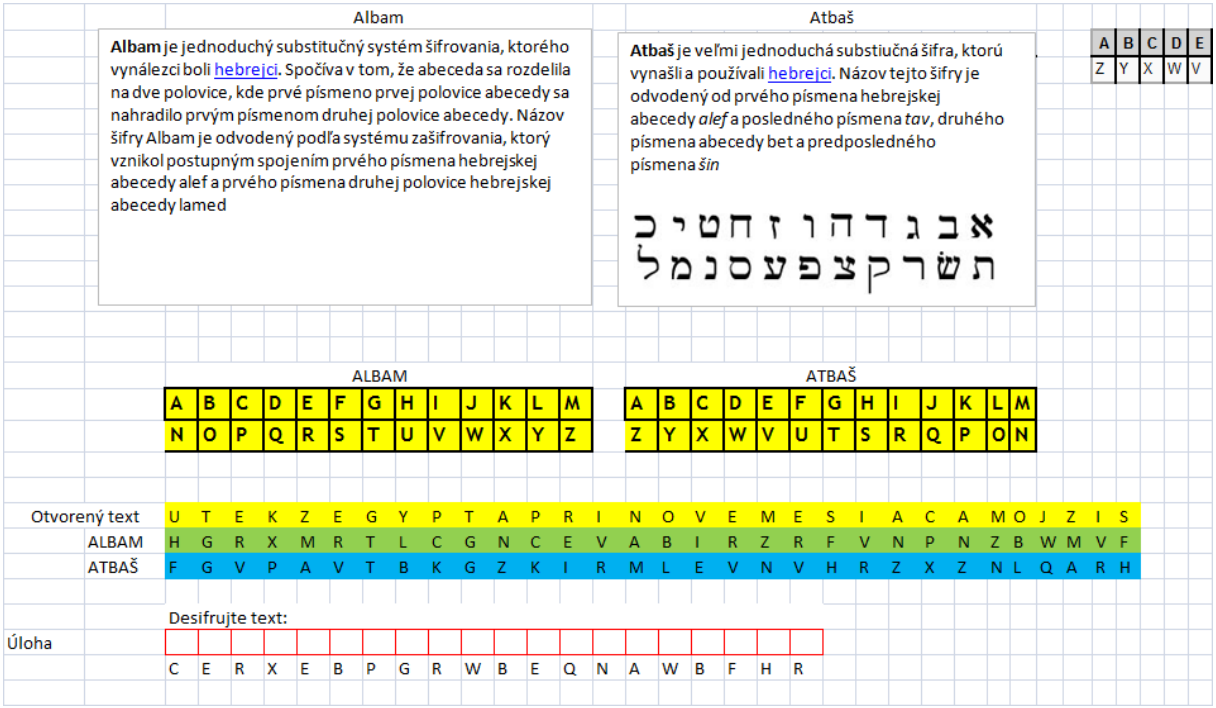
Príloha 3 Šifrovanie.xlsx - Transpozícia_súradnice II

Príloha 4 Šifrovanie.xlsx - Princíp Vigenérovej šifry

Príloha 5 Šifrovanie.xlsx - Vigenérova šifra

Príloha 6 Pracovný list - Enigma

**Príloha 1** Šifrovanie.xlsx - Albam, Atbaš



Albam

**Albam** je jednoduchý substitučný systém šifrovania, ktorého vynálezci boli hebrejci. Spočíva v tom, že abeceda sa rozdelila na dve polovice, kde prvé písmeno prvej polovice abecedy sa nahradilo prvým písmenom druhej polovice abecedy. Názov šifry Albam je odvodený podľa systému zašifrovania, ktorý vznikol postupným spojením prvého písmena hebrejskej abecedy alef a prvého písmena druhej polovice hebrejskej abecedy lamed

Atbaš

**Atbaš** je veľmi jednoduchá substiučná šifra, ktorú vynašli a používali hebrejci. Názov tejto šifry je odvodený od prvého písmena hebrejskej abecedy *alef* a posledného písmena *tav*, druhého písmena abecedy bet a predposledného písmena *šin*

א ב ג ד ה ו ז ח ט י כ
ת ש ר ק צ פ ע ס נ מ ל

| A | B | C | D | E |
|---|---|---|---|---|
| Z | Y | X | W | V |

ALBAM

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

ATBAŠ

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Otvorený text | U | T | E | K | Z | E | G | Y | P | T | A | P | R | I | N | O | V | E | M | E | S | I | A | C | A | M | O | J | Z | I | S |
| ALBAM | H | G | R | X | M | R | T | L | C | G | N | C | E | V | A | B | I | R | Z | R | F | V | N | P | N | Z | B | W | M | V | F |
| ATBAŠ | F | G | V | P | A | V | T | B | K | G | Z | K | I | R | M | L | E | V | N | V | H | R | Z | X | Z | N | L | Q | A | R | H |

Desifrujte text:

| Úloha | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | C | E | R | X | E | B | P | G | R | W | B | E | Q | N | A | W | B | F | H | R |

## **Príloha 2** Šifrovanie.xlsx - Použitie dvoch abecied

Použitie dvoch abecied

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Otvorená abeceda | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Šifrová abeceda 1 | F | Z | B | V | K | I | X | A | Y | M | E | P | L | S | D | H | J | O | R | G | N | Q | C | U | T | W |
| Šifrová abeceda 2 | G | O | X | B | F | W | T | H | Q | I | L | A | P | Z | J | D | E | S | V | Y | C | R | K | U | H | N |
| Dnesveceroosemnu | d | n | e | s | v | e | c | e | r | o | o | s | e | m | n | u | l | a | u | t | o | k | | | | |
| | 12 | | | | | | | | | | | | | | | | | | | | | | | | | |
| | v | z | k | v | q | f | b | f | o | j | d | v | k | p | s | c | p | g | n | y | d | l | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | v | z | k | v | q | f | b | f | o | j | d | v | k | p | s | c | p | g | n | y | d | l | c | x | 7 | 2 |
| Veľké písmena | V | Z | K | V | Q | F | B | F | O | J | D | V | K | P | S | C | P | G | N | Y | D | L | C | X | 7 | 2 |
| Prevod do ASCII | 86 | 90 | 75 | 86 | 81 | 70 | 66 | 70 | 79 | 74 | 68 | 86 | 75 | 80 | 83 | 67 | 80 | 71 | 78 | 89 | 68 | 76 | 67 | 88 | 55 | 50 |
| Prevod do HEX | 56 | 5A | 4B | 56 | 51 | 46 | 42 | 46 | 4F | 4A | 44 | 56 | 4B | 50 | 53 | 43 | 50 | 47 | 4E | 59 | 44 | 4C | 43 | 58 | 37 | 32 |
| | 56 | 5A | 4B | 56 | 51 | 46 | 42 | 46 | 4F | 4A | 44 | 56 | 4B | 50 | 53 | 43 | 50 | 47 | 4E | 59 | 44 | 4C | 43 | 58 | 37 | 32 |
| | 101 | 101 | 100 | 101 | 101 | 100 | 100 | 100 | 100 | 100 | 100 | 101 | 100 | 101 | 101 | 100 | 101 | 100 | 100 | 101 | 100 | 100 | 100 | 101 | 110 | 110010 |

56 5A 4B 56 51 46 42 46 4F 4A 44 56 4B 50 53 43 50 47 4E 59 44 4C 43 58 37 32
1010110 1011010 1001011 1010110 1010001 1000110 1000010 1000110 1001111 1001010 1000100 1010110 1001011 1010000 1010011 1000011 1010000 1000111 1001110 1011001 1000100 1001100 1000011 1011000 110111 110010
ห้าสิบหกบาทถ้วน ## ## ห้าสิบหกบาทถ้วน ห้าสิบเอ็ดบาทถ้วน สี่สิบหกบาทถ้วน สี่สิบสองบาทถ้วน สี่สิบหกบาทถ้วน ## ## สี่สิบสี่บาทถ้วน ห้าสิบหกบาทถ้วน ## ห้าสิบบาทถ้วน ห้าสิบสามบาทถ้วน สี่สิบสามบาทถ้วน ห้าสิบบาทถ้วน สี่สิบเจ็ดบาทถ้วน ## ห้าสิบเก้าบาทถ้วน สี่สิบสี่บาทถ้วน ## สี่สิบสามบาทถ้วน ห้าสิบแปดบาทถ้วน สามสิบเจ็ดบาทถ้วน

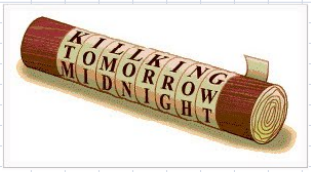
# **Príloha 3** Šifrovanie.xlsx - Transpozícia - súradnice II

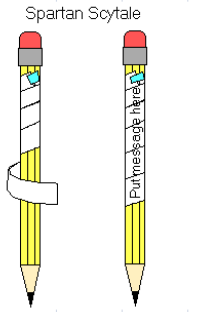
## Rail Fence šifra

BOLI SME NA FILME
B S A M O I M N F L E L E I

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | | | | S | | | | A | | | | M | |
| | O | | I | | M | | N | | F | | L | | E |
| | | L | | | | E | | | | I | | | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | S | A | M | O | I | M | N | F | L | E | L | E | I |



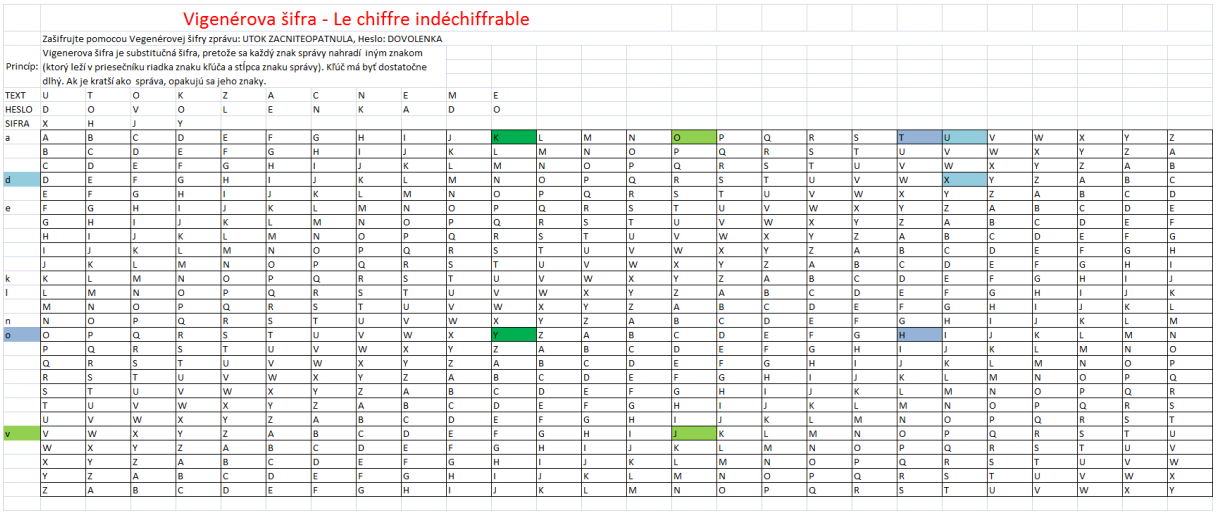

## ROUTE Šifra

BOLISTE ODHALENIZRADCOVIA
B S D E R O O T H N A V L E A I D I I O L Z C A

| | | | | | |
|---|---|---|---|---|---|
| B | S | D | E | R | O |
| O | T | H | N | A | V |
| L | E | A | I | D | I |
| I | O | L | Z | C | A |

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | S | D | E | R | O | O | T | H | N | A | V | L | E | A | I | D | I | I | O | L | Z | C | A |

# **Príloha 4** Šifrovanie.xlsx - PrincípVigenérovej šifry



Vigenérova šifra - Le chiffre indéchiffrable

Zašifrujte pomocou Vegenérovej šifry zprávu: UTOK ZACNITEOPATNULA, Heslo: DOVOLENKA

Princíp: Vigenerova šifra je substitučná šifra, pretože sa každý znak správy nahradí iným znakom (ktorý leží v priesečníku riadka znaku kľúča a stĺpca znaku správy). Kľúč má byť dostatočne dlhý. Ak je kratší ako správa, opakujú sa jeho znaky.

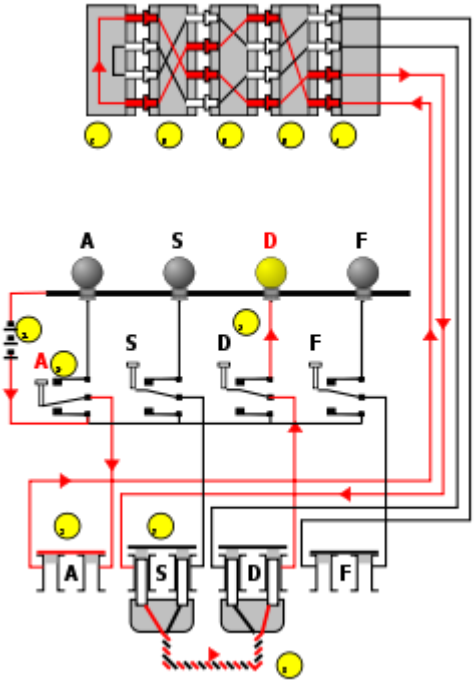
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TEXT | U | T | O | K | Z | A | C | N | E | M | E | | | | | | | | | | | | | | | | | |
| HESLO | D | O | V | O | L | E | N | K | A | D | O | | | | | | | | | | | | | | | | | |
| SIFRA | X | H | J | Y | | | | | | | | | | | | | | | | | | | | | | | | |
| a | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | | |
| | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | | |
| | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | | |
| d | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | | |
| | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | | |
| e | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | | |
| | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | | |
| | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | | |
| | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | | |
| | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | | |
| k | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | | |
| l | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | | |
| | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | | |
| n | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | | |
| o | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | | |
| | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | | |
| | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | | |
| | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | | |
| | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | | |
| | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | | |
| | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | | |
| v | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | | |
| | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | | |
| | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | | |
| | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | | |
| | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | | |

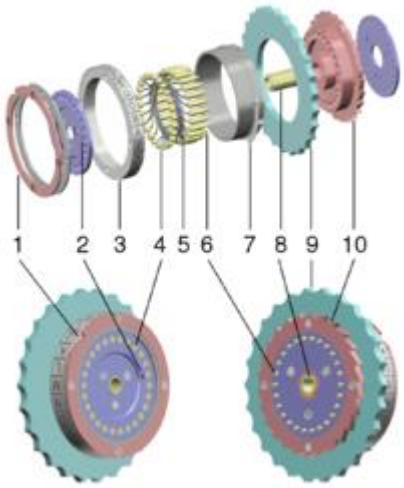
## **Príloha 5** Vigenérova šifra

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Vigenérova šifra - Le chiffre indéchiffrable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | Šifruj 1 | | Dešifruj -1 | 1 | | Šifro | 39 | znakov | | Dĺžka | 9 | | | | | | | | | | | | | | | | | | |
| Stlpec | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Kľúč | dovolenka | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | dovolenkadovolenkadovolenkadovolenkadovolenkadovolenkadovolenkadovolenka | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rozvoj | D | O | V | O | L | E | N | K | A | D | O | V | O | L | E | N | K | A | D | O | V | O | L | E | N | K | A | D | O | V | O |
| KÓD ASCII | 68 | 79 | 86 | 79 | 76 | 69 | 78 | 75 | 65 | 68 | 79 | 86 | 79 | 76 | 69 | 78 | 75 | 65 | 68 | 79 | 86 | 79 | 76 | 69 | 78 | 75 | 65 | 68 | 79 | 86 | 79 |
| Otvorený text | utokzacnemeranopatnulanakotetristodesat | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rozvoj | U | T | O | K | Z | A | C | N | E | M | E | R | A | N | O | P | A | T | N | U | L | A | N | A | K | O | T | E | T | R | I |
| KÓD ASCII | 85 | 84 | 79 | 75 | 90 | 65 | 67 | 78 | 69 | 77 | 69 | 82 | 65 | 78 | 79 | 80 | 65 | 84 | 78 | 85 | 76 | 65 | 78 | 65 | 75 | 79 | 84 | 69 | 84 | 82 | 73 |
| Šifra | 88 | 72 | 74 | 89 | 75 | 69 | 80 | 88 | 69 | 80 | 83 | 77 | 79 | 89 | 83 | 67 | 75 | 84 | 81 | 73 | 71 | 79 | 89 | 69 | 88 | 89 | 84 | 72 | 72 | 77 | 87 |
| Znaky | X | H | J | Y | K | E | P | X | E | P | S | M | O | Y | S | C | K | T | Q | I | G | O | Y | E | X | Y | T | H | H | M | W |
| | X | H | J | Y | K | E | P | X | E | P | S | M | O | Y | S | C | K | T | Q | I | G | O | Y | E | X | Y | T | H | H | M | W |
| Odošli | XHJYKEPXEPSMOYSCKTQIGOYEXYTHHMWDXBNEVOO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | X H J Y K E P X E P S M O Y S C K T Q I G O Y E X Y T H H M W D X B N E V O O | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

# *Enigma*

*(novogr. αίνιγμα - záhada, hádanka) bola prenosným elektromechanickým šifrovacím strojom pracujúcim na princípe otáčajúcich sa rotorov. Používala sa v niekoľkých modifikovaných verziách najmä nemeckými ozbrojenými silami pred vypuknutím a počas druhej svetovej vojny. Šifra Enigmy bola Nemcami považovaná za neprelomiteľnú a absolútne bezpečnú, no už v roku 1932 ju prelomili poľskí kryptológovia, ktorých poznatky využili po vypuknutí vojny spojenecké vojská. Informácia o prelomení kódu bola jednou z najtajnejších. O úlohe Poliakov sa otvorene začalo hovoriť až v roku 1973. Enigma je elektromechanický stroj, ktorý obsahuje 4 ozubené kolieska. Nimi sa zadával šifrovací kľúč (4 znaky abecedy). Šifra sa dala úspešne dešifrovať iba po navolení správneho počiatočného nastavenia ozubených koliesok (šifrovacieho kľúča), ktorým bola zašifrovaná. Išlo teda o symetrické šifrovanie.*




*Princíp:*

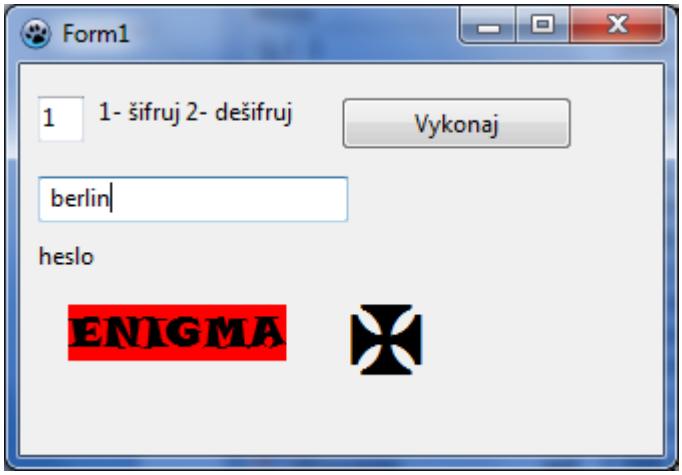
*Šifrovací stroj Enigma kóduje písmená takým spôsobom, že každé z nich môže byť opísané matematicky ako výsledok permutácie. Zjednodušme si princíp fungovania Enigmy takto: K jednotlivým znakom správy budeme pripočítavať znaky šifrovacieho kľúča, keď dôjdeme na koniec kľúča, začneme od začiatku. Napríklad, nech je kľúč* ***panzer*** *(tank) správa, ktorú ideme šifrovať: „ Richtung Stalingrad".(Smer Stalingrad). Šifru vytvoríme takto: r+**p**, i+**a**, c+**n**, , h+**z**, t+**e**, u+**r**, n+**p**, g +a, +**n**, s+z t+**e**, a+**r**, l+**p**, i+**a**, n+**n**, g+**z**, r+**e**, a+**r**, d+**p**,*

*Príklad:*

*Vytvorte novú aplikáciu. Do formulára aplikácie vložte Label1 s obsahom: „1-šifruj, 2-dešifruj", Label2 s obsahom „heslo", prázdne editovacie políčka Edit1 a Edit2, jedno tlačidlo Vykonaj. Program načíta text na zašifrovanie holy_text.txt, a uloží ho do súboru sifr_text.txt. Dešifrovaný text uloží do súboru*'desifr_text.txt*. Program načíta hodnoty 1 alebo 2 z edit1 a heslo z edit2. Použite cyklus, funkcie char, ord.*

*Program ošetrite tak, že na šifrovanie a dešifrovanie použijeme len 26 znakov.*

Riešenie:




Unit.pas

```
type

 { TForm1 }

 TForm1 = class(TForm)
  Button1: TButton;
  Edit1: TEdit;
  Edit2: TEdit;
  Label1: TLabel;
  Label2: TLabel;
  Label3: TLabel;
  Label4: TLabel;
  procedure Button1Click(Sender: TObject);
 private
  { private declarations }
 public
  { public declarations }
 end;

var
 Form1: TForm1;

implementation

{$R *.lfm}

{ TForm1 }

procedure TForm1.Button1Click(Sender: TObject);
var f1,f2:TextFile;
   h:char;
   i,kod,dkod:integer;
   key:string;
```

```
begin
  kod:=StrToInt(Edit1.Text);
  key:=Edit2.Text;
  if kod=1 then AssignFile(f1,'holy_text.txt') else AssignFile(f1,'sifrov_text.txt');
  reset(f1);
  if kod=1 then AssignFile(f2,'sifrov_text.txt') else AssignFile(f2,'desifr_text.txt');
  rewrite(f2);
  dkod:=length(key);
  i:=1;
  while not EOF(f1) do
    begin
    read(f1,h);
    if kod=1 then h:=char(ord(h)+ord(key[i]))
          else h:=char(ord(h)-ord(key[i]));
    write(f2,h);
    if i=dkod then i:=1




          else inc(i);
    end;
  CloseFile(f1);
  CloseFile(f2);
end;
end.
```