ŠIFROVANIE – METÓDY TAJNÝCH AGENTOV

Tematický celok / Téma	*ISCED / Odporúčaný ročník*
• **Reprezentácie a nástroje – informácie**	ZŠ / 5-6.ročník – 3. vyučovacia hodina zo série 4 metodík 1 vyučovacia hodina

Požiadavky na vstupné vedomosti a zručnosti

Vedomosti a zručnosti podľa ŠVP - informatika pre primárne vzdelávanie:
- zakódovať informáciu podľa pokynov do konkrétnej reprezentácie
- dekódovať informáciu z jednoduchých reprezentácií
- čítanie s porozumením

Ciele

Žiakom osvojované vedomosti	*Žiakom rozvíjané zručnosti a spôsobilosti*
Reprezentácie a nástroje – informácie • **kódovať informáciu podľa pokynov do konkrétnej reprezentácie** • **dekódovať informáciu z jednoduchých reprezentácii** Šifrovanie, ako nástroj utajenej a bezpečnej komunikácie: • aplikovať metódy šifrovania (Fleissnerova otočná mriežka, Caesarova šifra, Šifrovací disk, Vigenerova šifra) • formulovať nové, vlastné pravidlá kódovania	Informatické myslenie: • (ALG2) **vykonávať algoritmus** (šifrovať podľa známych pravidiel) • ALG4) **vytvárať vlastné algoritmy**, ktoré pracujú s množinou dát (vytvoriť vlastné šifrovacie pravidlá) • (DEK1) lineárna dekompozícia – **lineárne rozdeliť** prácu pre členov tímu • VYH1) **vybrať kritériá** pre vyhodnotenie výsledkov algoritmu (bezpečnosť systému) Bádateľské spôsobilosti: • formulovať otázku/problém • zdieľať a prezentovať výsledky pred spolužiakmi • diskutovať/obhajovať výsledky

Riešený didaktický problém

Je dôležité uvedomiť si určité zákonitosti a princípy šifrovania, kedy sa používajú šifry, šifrované správy v bežnom živote. Pri tvorbe šifrovanej (zamaskovanej) správy musíme zvoliť spôsob alebo metódu ako správu z čitateľnej podoby pretvoriť do nečitateľnej (zašifrovanej) podoby. Dnes používané kryptografické metódy pre ochranu dôverných informácií sú vytvorené na základe známych historických metód šifrovania a dešifrovania. Žiaci si majú uvedomiť, že otázka zabezpečenia dát je veľmi dôležitá, aj dáta na domácom počítači je vhodné zabezpečiť.

Dominantné vyučovacie metódy a formy	*Príprava učiteľa a pomôcky*
• Bádateľská metóda (učebný cyklus 5E) • práca v štvorčlenných skupinách pomocou pracovného listu – kooperatívna metóda mozaiky expertov • riadený rozhovor	• Pracovný list pre každého žiaka • Šifrované správy - vystrihnuté z prílohy č.1 • Poradové čísla pre členov v skupine – používané v prvej metodike

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

	• Pre každú skupinu nasledovné pomôcky vystrihnuté podľa prílohy č.2: Fleissnerova otočná mriežka Pásiky písmen pre Caesarovu šifru Šifrovací disk Tabuľka pre Vigenerovu šifru
Diagnostika splnenia vzdelávacích cieľov	
Žiaci počas fázy skúmania spoznávajú metódy šifrovania a vytvárajú aj vlastné šifrované správy v skupinách expertov. Na základe kooperatívnej metódy mozaiky expertov vysvetľujú osvojené metódy svojim spolužiakom, a zároveň a prehĺbia svoje poznatky. Pomocou sebahodnotiacej karty na konci pracovného listu si zhodnotia svoje vedomosti a zároveň to slúži ako spätná väzba pre učiteľa o splnení vzdelávacích cieľov.	

Úvod

Tretia metodika v tejto sérii metodík sa zaoberá **so šifrovaním**, kde formou zábavných aktivít predstavíme význam šifrovanej informácie v poňatí bezpečnej komunikácie na internete, počítačovej bezpečnosti a ochrane údajov.
Na základnej škole pri narábaní s kryptografiou úplne vystačíme iba s papierom a perom, tak ako to bolo aj v počiatkoch tohto odvetvia.
Téma šifrovania sa nenachádza v štátnom vzdelávacom programe, teda táto metodika je nad rámec vzdelávacieho štandardu, ale považujeme to za veľmi zaujímavú a obľúbenú oblasť informatiky, kde si žiaci môžu nadobudnúť zručnosti a skúsenosti z tradičnej kryptografie, a rozvíjajú aj algoritmické myslenie a schopnosti riešenia problémov.
Metodika je rozvrhnutá na základe učebného cyklu 5E, a podobne, ako v prvej metodike aj tu použijeme kooperatívnu metódu mozaiky expertov, ktorá už je známa pre žiakov.

Priebeh hodiny:

1. **Zapojenie:** Aktivita Špióni – motivačná hra (10 min)
2. **Skúmanie:** Známe šifrovacie metódy (15 min)
3. **Vysvetľovanie:** Žiaci – Experti predstavia pridelenú metódu šifrovania v skupine (10 min)
4. **Rozšírenie:** Vlastné šifry (5 min)
5. **Vyhodnotenie:** Sebahodnotiaca tabuľka (3 min)

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu
a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

ZAPOJENIE (CCA 10 MIN):

Aktivita špióni – motivačný príbeh
Postup pri aktivite: Žiakom rozdáme šifrované správy. Majú vytvoriť skupiny po štyroch tak, že všetci v tíme majú mať rovnakou metódou šifrovanú správu.
Porozprávame im motivačný príbeh:

"Každý z vás je špiónom nejakej veľmoci, snažiaci sa získať utajenú správu. Ste po štyroch v skupine patriacej k tej istej veľmoci, ale nepoznáte sa navzájom. Správa sa skladá zo 4 viet, pričom každý zo skupiny má rozdielnu vetu. Všetky tri skupiny majú rovnakú správu!
Úlohou každej skupiny je získať celú správu a vyriešiť jej obsah. Aby nepriatelia nezistili obsah vašej správy, tie sú zašifrované. Každá skupina **má vlastný spôsob šifrovania**, teda vašou úlohou je nájsť všetkých tých, ktorí majú zašifrovanú správu rovnakou metódou. Pozor, môže sa stať, že ak vašu správu dostane nepriateľ, je schopný ju po čase rozlúštiť."
Huraj, L.: Vyučovanie Internetu na základnej škole. Bratislava: MC Bratislava, 1997, 56 s.,ISBN 80-8052-022-4 (str. 15).

Víťazom je skupina, ktorá nájde všetkých svojich členov, a bude mať ako prvá celú správu vylúštenú. (poradie viet nie je podstatné)

Spôsob šifrovania, pre skupinu **James Bond**: (Šifrovanie spočíva v napísaní písmen v opačnom poradí)
OTALZ DAN ĽOS
SOĽ NAD ZLATO

Spôsob šifrovania, pre skupinu **Matahari**: (Šifrovanie spočíva v napísaní každého slova v opačnom poradí)
ĽOS DAN OTALZ
SOĽ NAD ZLATO

Spôsob šifrovania, pre skupinu **Casanova**: (Šifrovanie spočíva v napísaní číslice od 1 do 9 postupne medzi písmená)
S1O2Ľ3 N4A5D6 Z7L8A9T1O
SOĽ NAD ZLATO

Šifry skupín nie sú až také ťažké, dá sa prísť na každú z nich.
Učiteľ má pripraviť šifrované správy, jednotlivé vety rozdá žiakom na papierikoch.
V prílohe uvádzame možné zadanie so správou, zašifrované podľa horeuvedených metód:

1. ÚTEK Z VÄZENIA JE PLÁNOVANÝ NA ZAJTRA
2. PRIPRAVTE LANÁ A REBRÍKY
3. STRÁŽCA JE NA NAŠEJ STRANE
4. PRED VÄZNICOU NÁS ČAKÁ HELIKOPTÉRA

SKÚMANIE: ZNÁME ŠIFROVACIE METÓDY (15 MIN)

Pracovný list – 1. úloha

Použijeme kooperatívnu metódu mozaiky expertov, rozdelíme žiakov do štvorčlenných skupín, alebo skupiny môžu byť vytvorené aj na základe predchádzajúcej úlohy. Pomocou farebných kartičiek s číslami, podobne ako na prvej hodine, rozdelia si jednotlivé metódy.

Každý žiak dostane pracovný list a začne študovať svoju pridelenú metódu šifrovania podľa poradového čísla. (cca. 3 min)

Do každej skupiny rozdáme vystrihnuté pomôcky šifrovania:

- Flessnerovu otočnú mriežku
- Pásiky písmen pre Caesarovu šifru
- Šifrovací disk
- Tabuľku pre Vigenerovu šifru

Následne skupiny sa prerozdelia, a žiaci začnú pracovať ako skupina expertov pre jednotlivé metódy šifrovania, bádateľsky dešifrujú a šifrujú správy.

Poznámka pre učiteľa
Pravdepodobne metóda šifrovania Vigenerovou šifrou je najkomplikovanejšia. Ak učiteľ považuje to za neprimerané pre daných žiakov, môže to aj vynechať. Prílohou metodiky je pracovný list v docx formáte, vytlačiť PL môžete aj bez tejto metódy.

Uvádzame metódy v pracovnom liste s riešeniami:

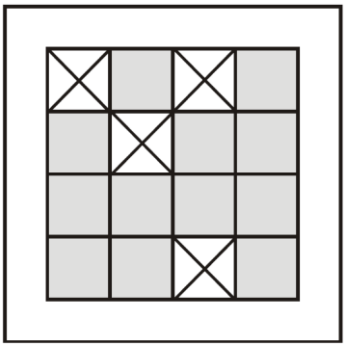
Úloha 1

Naštudujte jednu metódu šifrovania – každý člen skupiny svoju vybranú metódu

1. Fleissnerova otočná mriežka

Položte mriežku na tabuľku so zašifrovaným textom, ktorú ste dostali. Šifrovací kľúč je mriežka s otvorom. Počas prvej svetovej vojny bol tento šifrovací systém používaný aj v praxi nemeckou armádou, a použil to aj Jules Verne v knihe "Nový gróf Monte Christo".

Podľa mriežky vyberte písmená na pozíciách otvorov v mriežke. Tie tvoria šifrovaný text, potom mriežku otočte v smere hodinových ručičiek a v otvoroch postupne prečítajte ďalšie písmená.



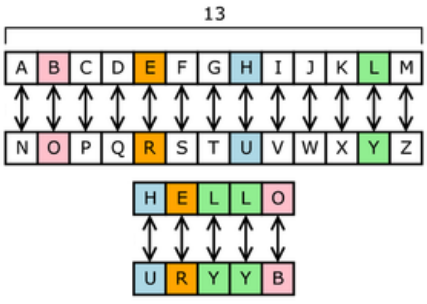
Napíšte riešenie zadanej šifry:

NEBOJME SA ŠIFRY

Vytvorte vlastnú zašifrovanú správu pomocou danej mriežky. Použite priloženú prázdnu mriežku.

2. Caesarova šifra

Je to druh šifry, pri ktorej je každé písmeno správy je posunuté o danú pozíciu ďalej v abecede.
Napríklad pri posunutí doprava o 13 miest písmeno A bude nahradený písmenom N. V prípade písmena vyskytujúceho sa na konci abecedy sa toto písmeno posunie opäť na začiatok abecedy.
Táto šifra patrí medzi najznámejšie a najstaršie šifrovacie systémy, používal ho rímsky cisár Caesar pred 2000 rokmi.



Najprv tu vytvorte vhodnú dešifrovaciu tabuľku na posunutie o 3 miesta.

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
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

*Odšifrujte nasledovnú utajenú správu, kde šifra používa **posunutie o 3 miesta**.*

L	Á	S	K	A	H	O	R	Y	P	R	E	N	Á	Š	A
O	D	V	N	D	K	R	U	B	S	U	H	Q	D	V	D

Vymyslite vlastnú zašifrovanú správu:

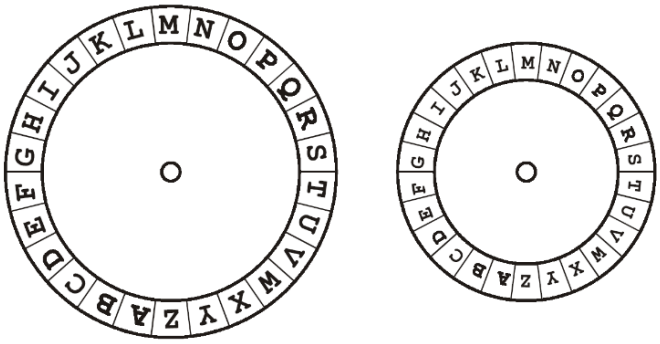
Vytvorte vlastnú dešifrovaciu tabuľku s vlastným posunutím.

Posunutie nech je:	

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

Správa:	
Zašifrovaná správa:	

3. Šifrovací disk



Je to šifrovacia pomôcka skladajúca sa z dvoch otočných kotúčov. Na každom z nich je napísaná abeceda. Vonkajšia predstavuje znaky abecedy a vnútorná šifrovú abecedu. Pootočením vnútorného kruhu o niekoľko políčok pod vonkajším písmenom sa nachádza vnútorné písmeno, čo predstavuje šifru daného písmena.

Šifrovací disk pôvodne slúžil na šifrovanie pomocou Caesarovej šifry.

*Odšifrujte nasledovnú správu pomocou šifrovacieho disku, **kde A → F***

Použite priložené šifrovacie disky.

Správa:	L	A	S	T	O	V	I	C	K	A
Zašifrovaná správa:	**Q**	**F**	**X**	**Y**	**T**	**A**	**N**	**H**	**P**	**F**

Vymyslite vlastnú zašifrovanú správu:

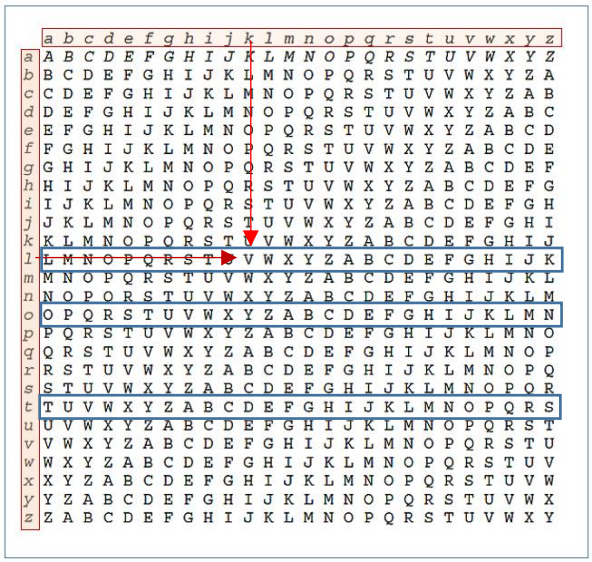
Správa:	
Zašifrovaná správa:	

4. Vigenerova šifra

Táto šifra používa 26 abecied posunutých o 1 miesto. Šifrovanie prebieha tak, že sa zvolí kľúčové slovo. Daný kľúč určuje, pomocou ktorej abecedy sa bude šifrovať.

*Pri šifrovaní sa používajú **riadky**, ktoré začínajú písmenami tvoriacimi kľúč. Nech je kľúč slovo LETO.*

*V **stĺpcoch** sa nachádzajú písmená správy.*



Správa:	K	O	S	I	C	E
Kód:	L	E	T	O	L	E
Zakódovaná správa:	V	S	L	W	N	I

Pomocou kľúča JAR odšifrujte správu:

Správa:	M	E	D	V	E	D
Kód:	J	A	R	J	A	R
Zakódovaná správa:	V	E	U	E	E	U

Vymyslite vlastnú zašifrovanú správu:

Správa:															
Kód:															
Zašifrovaná správa:															

Poznámka pre učiteľa:

Žiaci v skupinách majú spoločne vymyslieť vlastné správy a zašifrovať ich. Každý si napíše do svojho pracovného listu spoločné riešenie tímu a keď sa vrátia do svojich pôvodných skupín, ostatní to budú dešifrovať.

VYSVETĽOVANIE (CCA 15 MIN):

Počas tejto fázy žiaci sa vrátia do svojich pôvodných skupín a **každý člen predstaví ostatným** svoju pridelenú metódu šifrovania.
Experti dajú vyriešiť vlastnú zakódovanú správu vytvorenú v 2. úlohe svojim spolužiakom v skupine, nadiktujú im zašifrované správy, a ostatní členovia to zapíšu do svojho pracovného listu. Takto všetci precvičia šifrovanie každou predstavenou metódou.

ROZŠÍRENIE (CCA 5 MIN):

Pracovný list – 2. úloha
Žiaci opäť pracujú v skupinách, majú vymyslieť novú, jednoduchú metódu šifrovania, a zašifrovať tajnú správu pre spolužiakov. Dôležité je originálny spôsob šifrovania.
Správa by nemala byť dlhšia, ako 10 znakov, aby v ďalšej fáze vyhodnotenie to mohli šikovne prezentovať.
Môžu to dokončiť aj ako domácu úlohu.

Možné riešenia:
Transpozičné metódy:

1. AKČIVOTSAL – písanie slov odzadu
2. **LBACSDTFOGVHIJČZKXA** – zo správy treba čítať vždy len každé druhé (k-te) písmeno
3. Čítanie slov v tabuľke po stĺpcoch:

K	R	M	M	P	M	E	D
T	U	U	U	E	D	J	N
O	H	J	K	S	O	P	E
D	É	A	O	Á	N	A	

Substitúcia foneticky znejúcich hlások:
AGO ZI UZDELIEŽ, DAG PUDEŽ ZBAĎ

Vernamova šifra – je podobná ako Vigenerova šifra, ale náhodne vygenerovaný šifrovací kľúč je tak dlhý, ako samotná správa a použije sa len raz. Takmer nerozbitná šifra, najčastejšie sa používa v kryptografii.

Skytalé – šifrovací valec, ktorý sa omotá tenkým prúžkom papiera. Na tento papier sa napíše správa zvyčajne zľava doprava. Keď sa prúžok odmotá, výsledkom je rad nesúvisiacich znakov. Na rozlúštenie potrebujete rovnako hrubý valec, aby sa písmená zobrazili v správnych riadkoch.

VYHODNOTENIE (CCA 3 MIN):

Skupiny majú predstaviť svoje vlastné metódy šifrovania. Predpokladáme, že vedené aktivity sú pre žiakov zaujímavé, podnecujú ich zvedavosť.
Prípadne môžeme zadať **za domácu úlohu** vymyslieť ďalšie metódy šifrovania, ktorú odprezentujú na nasledujúcej hodine.

Žiaci si majú uvedomiť, že cieľom šifrovania je utajenie správy, pričom má byť jednoznačné dané pravidlo a šifrovací kľúč. Odšifrovať správu dokáže len ten, kto pozná tento kľúč.
Žiaci by mali vedieť uviesť príklady potreby šifrovania v bežnom živote.
(elektronické bankovníctvo, zašifrovaný výpis účtu z banky , elektronický podpis, dokumenty, ochrana osobných údajov)

Na sebahodnotenie slúži sebahodnotiaci test a tabuľka:

SEBAHODNOTIACI TEST

Úloha 3

Označte správne tvrdenie ☒ ***:***

- ☒ *Cieľom šifrovania je utajenie správy.*
- ☒ *Účelom šifrovania je utajenie pre bezpečnú ochranu údajov.*
- ☐ *Šifrovanú správu hocikto môže dešifrovať.*

SEBAHODNOTIACA TABUĽKA

Otázky na hodnotenie Vašej práce:	**áno**	**čiastočne**	**nie**
Viem kedy a kde sa používajú šifry?			
Viem šifrovať pomocou Fleissnerovej otočnej mriežky?			
Viem šifrovať pomocou Caesarovej šifry?			
Viem šifrovať pomocou šifrovacieho disku?			
Viem šifrovať pomocou Vigenerovej šifry?			