Šifrování

Informatika | 7. třída

Cíle hodiny

- Žák vysvětlí základní principy šifrování a jeho význam pro bezpečnost dat.
- Žák samostatně používá jednoduché šifrovací metody pro zakódování a dekódování zpráv.

1. Evokace (10 minut)

- **Tajná zpráva pro třídu: Rozluštění zašifrovaného vzkazu pomocí jednoduché substituční šifry**

  Čas: 10 minut
  Pomůcky: Zašifrovaná zpráva pro každého žáka

  1. Motivační aktivita - rozluštění tajné zprávy

     - Rozdám každému žákovi zašifrovanou zprávu
     - Text zprávy: "VITEJTE V HODINE SIFROVANI"
     - Šifrování: Každé písmeno posunuto o 3 pozice v abecedě (Caesarova šifra)
     - Zašifrovaný text: "YLWHMWH Y KRGLQH VLIURYDQL"

  2. Postup luštění

     - Žáci samostatně zkoumají text, hledají vzory
     - Po 2 minutách: Nápověda - text obsahuje slovo "HODINE"
     - Po další 1 minutě: Nápověda - všechna písmena jsou posunuta stejným směrem

  3. Kritéria úspěchu

     - Žák rozluští zprávu
     - Žák vysvětlí princip šifrování, který byl použit

ADHD:
- Asistent sedí vedle žáka
- Pomáhá udržet pozornost na textu
- Poskytuje dílčí nápovědy při hledání vzorů
- Rozděluje text na menší části pro snazší analýzu

Původní písmeno	Zašifrované písmeno
A	D
B	E
C	F
D	G
E	H
F	I
G	J
H	K
I	L

J	M
K	N
L	O
M	P
N	Q
O	R
P	S
Q	T
R	U
S	V
T	W
U	X
V	Y
W	Z
X	A
Y	B
Z	C

2. Uvědomění (30 minut)

- **Příběh o šifrování v historii a současnosti s ukázkami využití v běžném životě**

  Čas: 15 minut
  Pomůcky: Pracovní list, projektor

  1. Interaktivní příběh (7 min)

  - Projekce obrázků moderních technologií (mobil, počítač, platební karta)
  - Žáci zapisují do pracovního listu, kde všude potřebujeme hesla/šifrování
  - Společná kontrola, doplnění dalších příkladů

Kde používáme šifrování?	Proč je důležité?
Mobilní telefon - odemykání	Ochrana osobních dat a aplikací
Internetové bankovnictví	Zabezpečení peněz a plateb
Email, sociální sítě	Soukromá komunikace
Wi-Fi síť	Bezpečné připojení k internetu

  2. Rozdíl mezi šifrováním a kódováním (8 min)

  - Demonstrace na příkladech:
    - Kódování: převod do Morseovy abecedy (SOS = ... --- ...)
    - Šifrování: záměna písmen podle klíče (AHOJ → BIPK)

- Žáci ve dvojicích zkoušejí určit, zda jde o šifrování nebo kódování

Příklad	Šifrování/Kódování	Vysvětlení
Vlajková signalizace	Kódování	Každá vlajka = jeden význam
Přesmyčka KOAL → KOLA	Šifrování	Změna pořadí písmen podle pravidla
QR kód	Kódování	Převod textu do čtvercového vzoru

Kritéria úspěchu:

- Žák uvede 3 příklady využití šifrování v běžném životě
- Žák správně rozliší mezi šifrováním a kódováním na konkrétních příkladech

ADHD: Asistent pedagoga:
- Pomáhá s udržením pozornosti při vyplňování pracovního listu
- Kontroluje správnost zápisů
- Podporuje aktivní zapojení do diskuze
- Pomáhá s organizací práce ve dvojici

Systém ověřování a tisku NSA Punch
Zdroj: WikiMedia

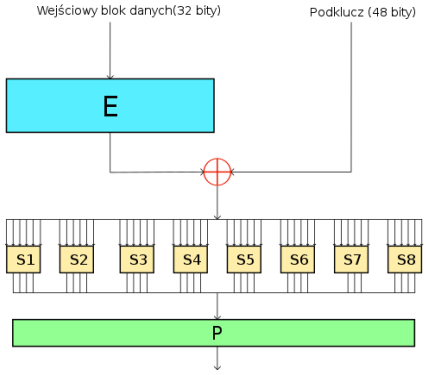

Diagram Data Encryption Standard
Zdroj: WikiMedia

Kryptografie - Wikipedie: https://cs.wikipedia.org/wiki/Kryptografie

Moderní šifrování - ČT edu: https://edu.ceskatelevize.cz/video/13811-matematika-kolem-nas-moderni-sifrovani

- **Praktické procvičení šifrovacích metod - Caesarova šifra a zrcadlové písmo**

1. Stanoviště pro šifrování (4 stanoviště, žáci rotují po 3-4 minutách)

- Rozdělení do 4 skupin po 3-5 žácích
- Každá skupina začíná na jiném stanovišti
- Časomíra na projektoru / tabuli

Stanoviště 1: Caesarova šifra

Původní text	Zašifrovaný text (posun +3)
KOCKA	NRFND
PES	SHV
MYSKA	PBVND

Stanoviště 2: Zrcadlové písmo

Původní text	Zrcadlově
MOBIL	ꓶIꓭOM
TABLET	TƎꓶꓭAT
POCITAC	ↃATIↃOꟼ

Stanoviště 3: Morseova abeceda

Text	Morseovka
SOS	... --- ...
AHOJ	.- .... --- .---
MAMA	-- .- -- .-

Stanoviště 4: Znaková řeč

Slovo	Znak
AHOJ	Mávání pravou rukou
PROSÍM	Krouživý pohyb pravou rukou na hrudi
DĚKUJI	Pohyb ruky od brady směrem vpřed

2. Kritéria úspěchu

- Skupina vyřeší min. 2 příklady na každém stanovišti
- Správně použije šifrovací metodu
- Dokáže vysvětlit princip šifrování ostatním

ADHD: Asistent pedagoga:
- Rotuje mezi stanovišti
- Pomáhá s udržením pozornosti na aktuálním úkolu
- Poskytuje dodatečné vysvětlení
- Kontroluje správnost řešení
- Pomáhá s organizací práce ve skupině

Seznam šifer - Skaut Kostelec: http://dakota.skautkostelec.cz/skautska_stezka/praxe/seznam_sifer.htm

Procvičování šifrování - Umíme informatiku: https://www.umimeinformatiku.cz/cviceni-sifry

- Aktivita - AlfaBox (~10 minut, zařadit podle tempa hodiny)

3. Reflexe (5 minut)

- **Šifrovací soutěž: Vytvoření a výměna tajných zpráv ve dvojicích s použitím naučených metod**

  Praktické procvičení šifrovacích metod

  Pomůcky:

- Papíry A4
- Tužky
- Abecední tabulka s očíslovanými pozicemi písmen

Aktivita - Caesarova šifra:

1. Ukázka principu:

Původní text	Posun +3
A B C D	D E F G
AHOJ	DKRM

2. Dvojice žáků:

- Každá dvojice dostane papír rozdělený na dvě části
- První žák napíše krátkou zprávu (max 5 slov)
- Zašifruje pomocí posunu o 3 písmena
- Předá spolužákovi k rozluštění

Kritéria úspěchu:

- Správné zašifrování zprávy (všechna písmena posunuta o 3)
- Úspěšné rozluštění zprávy spolužákem
- Vysvětlení použitého postupu

ADHD: Asistent pedagoga:
- Sedí mezi dvojicemi žáků s ADHD
- Pomáhá s počítáním posunu písmen
- Kontroluje správnost šifrování
- Poskytuje vizuální pomůcku - abecední tabulku s očíslovanými pozicemi

Jak vytvářet kódy a šifry - wikiHow: https://www.wikihow.cz/Jak-vytvářet-kódy-a-šifry

- Aktivita - Zpětná vazba

Nápady k samostatné práci pro žáky

Procvičte si šifrování a luštění tajných zpráv:

1. Rozluštěte následující zprávy zašifrované Caesarovou šifrou (posun o 3 písmena):
a) VNROD MH NUDVQB
b) SURJUDPRYDQL
c) VLIQRYDFL NOLF

2. Zašifrujte pomocí Caesarovy šifry (posun o 3 písmena) tato slova:
a) POCITAC
b) TELEFON
c) INTERNET

3. Přepište do zrcadlového písma:
a) ROBOT
b) PROGRAM

4. Rozluštěte text v Morseově abecedě:

....-.. ---

5. Vytvořte krátkou zprávu (maximálně 3 slova) a zašifrujte ji dvěma různými způsoby, které jsme se naučili.

Tento úkol přímo navazuje na stanovené cíle hodiny a prohlubuje získané znalosti a dovednosti:

1. Podporuje pochopení principů šifrování tím, že žáci aktivně používají různé šifrovací metody (Caesarova šifra, zrcadlové písmo, Morseova abeceda).
2. Rozvíjí praktické dovednosti v šifrování a dešifrování zpráv, což odpovídá druhému cíli hodiny - samostatné používání jednoduchých šifrovacích metod.
3. Úkol postupuje od jednodušších příkladů ke složitějším a kombinovaným, což umožňuje žákům postupně si upevnit znalosti všech probraných šifrovacích metod.
4. Poslední úkol podporuje kreativitu a syntézu získaných znalostí, když žáci musí sami vytvořit zprávu a aplikovat různé šifrovací metody.