Kódování a šifrování dat
Informatika
|
6. třída
Cíle hodiny

- Žák vysvětlí rozdíl mezi kódováním a šifrováním dat.
- Žák na příkladech demonstruje jednoduché metody kódování a šifrování textu.

1. Evokace (10 minut)

- **Tajná zpráva: Žáci dostanou krátkou zprávu zašifrovanou jednoduchou záměnou písmen a pokusí se ji rozluštit**

    1. Příprava šifry:

        - Metoda: Posun abecedy o 3 písmena (Caesarova šifra)
        - Klíč: A = D, B = E, C = F, atd.

    Caesarova šifra
    Zdroj: WikiMedia

    2. Zašifrovaná zpráva: YLWHMWH GR WDMQHKR NOXEX

    3. Postup: a) Rozdám papíry se zašifrovanou zprávou. b) Vysvětlím úkol: rozluštit tajnou zprávu. c) Tipy pro luštění:

        - Hledání opakujících se vzorů písmen
        - Odhad krátkých slov (např. "DO")
        - Pozorování četnosti písmen

    4. Nápovědy (použiji postupně, pokud žáci mají potíže):

        - Nápověda 1: Jde o posun písmen v abecedě
        - Nápověda 2: Zkuste posunout každé písmeno o několik míst zpět

    5. Diskuze po rozluštění:

        - Jak jste postupovali?
        - Které strategie vám pomohly?
        - Bylo by možné zprávu rozluštit bez znalosti metody?

    6. Vysvětlení principu:

        - Na tabuli ukážu posun abecedy.
        - Představím pojem Caesarova šifra.

    7. Závěr:

        - Shrnu použití jednoduché šifrovací metody.
        - Zmíním existenci složitějších metod pro budoucí lekce.

    Aktivita rozvíjí logické myšlení, schopnost analýzy a řešení problémů. Zároveň propojuje teorii s praxí v oblasti šifrování.

2. Uvědomění (30 minut)

- **Povídání o kódování a šifrování dat: Co to je, k čemu slouží, jaké jsou mezi nimi rozdíly**

Kódování a šifrování dat:

Příklad kódu
Zdroj: WikiMedia

1. Kódování dat:

   - Převod informací do jiné formy nebo formátu
   - Cíl: Usnadnit přenos nebo ukládání dat
   - Příklady:
     - Morseova abeceda
     - Čárový kód
     - QR kód

2. Šifrování dat:

   - Proces skrývání obsahu zprávy
   - Cíl: Ochrana informací před neoprávněným přístupem
   - Příklady:
     - Záměna písmen
     - Caesarova šifra
     - Tajný klíč

3. Hlavní rozdíly:

   - Účel:
     - Kódování: Efektivní přenos a ukládání dat
     - Šifrování: Zabezpečení a utajení informací
   - Znalost metody:
     - Kódování: Veřejně známé
     - Šifrování: Často tajné nebo s použitím klíče
   - Reverzibilita:
     - Kódování: Vždy lze dekódovat se znalostí metody
     - Šifrování: Obtížné dešifrovat bez znalosti klíče

4. Aktivita: "Najdi rozdíly" (10 minut)

   - Rozdělím žáky do dvojic
   - Každé dvojici dám list s příklady kódování a šifrování
   - Úkol: Označit, zda jde o kódování nebo šifrování, a vysvětlit proč
   - Příklady na listu: a) Morseova abeceda (kódování) b) Tajná zpráva napsaná citrónovou šťávou (šifrování) c) Braillovo písmo (kódování) d) Zpráva napsaná pozpátku (šifrování) e) ASCII kód (kódování)
   - Společná kontrola a diskuse o odpovědích

5. Shrnutí klíčových bodů: (5 minut)

   - Kódování mění formu dat pro lepší přenos a ukládání
   - Šifrování chrání obsah zprávy před neoprávněným přístupem
   - Kódování je veřejné, šifrování často využívá tajné metody nebo klíče
   - Oba procesy jsou důležité v moderních technologiích a komunikaci

Tato aktivita propojuje teoretické znalosti s praktickým rozpoznáváním rozdílů mezi kódováním a šifrováním. Podporuje kritické myšlení a spolupráci mezi žáky.

- [ ] Obecný úvod do šifrování dat
- [ ] Rozdíl mezi kódováním a šifrováním
- [ ] Kódování textu a šifrování
- [ ] Šifrování dat - Wikipedie

- **Praktické cvičení: Kódování zpráv pomocí Morseovy abecedy a šifrování pomocí jednoduché záměny písmen**

1. Morseova abeceda (kódování)

   - Ukážu Morseovu abecedu na tabuli nebo rozdám tištěnou verzi

   Písmeno Morseův kód

   A • —

   B — • • •

   C — • — •

   ... ...

   - Vysvětlím princip: tečka = krátký signál, čárka = dlouhý signál
   - Ukážu kódování slova "SOS": • • • — — — • • •

2. Jednoduchá záměna písmen (šifrování)

   - Princip: každé písmeno nahradíme jiným podle předem daného klíče
   - Ukážu klíč na tabuli:

   Původní A B C D E ...

   Nové D E F G H ...

   - Vysvětlím: každé písmeno posuneme o 3 místa v abecedě

3. Praktické úkoly pro žáky: a) Zakódujte pomocí Morseovy abecedy: "AHOJ" b) Zašifrujte pomocí jednoduché záměny (posun o 3): "TAJNE" c) Zakódujte Morseovou abecedou a poté zašifrujte posunem o 3: "SOS"

4. Samostatná práce žáků:

   - Rozdám papíry s tabulkou Morseovy abecedy a klíčem pro záměnu
   - Žáci pracují na úkolech (5 minut)

5. Kontrola výsledků:

   - Společně projdeme správná řešení a) AHOJ: • — / • • • • / — — — / • — — — b) TAJNE: WDMQH c) SOS: • • • — — — • • • → VRV

6. Diskuse o výhodách a nevýhodách obou metod:

   - Morseova abeceda: jednoduchá, univerzální, ale snadno čitelná
   - Záměna písmen: těžší na luštění, ale také na zapamatování klíče

Propojení teorie s praxí a rozvoj kritického myšlení.

7. Bonusový úkol pro rychlejší žáky:

   - Vymyslete vlastní jednoduchý způsob šifrování zprávy
   - Napište krátkou zprávu (max. 5 slov) a zašifrujte ji svou metodou

8. Prezentace bonusových úkolů:

   - Dobrovolníci představí své metody šifrování
   - Ostatní žáci se pokusí zprávy rozluštit

Podpora kreativity a vzájemného učení.

9. Závěrečné shrnutí:
   - Kódování (Morseova abeceda) - veřejně známé, slouží k efektivnímu přenosu

- Šifrování (záměna písmen) - tajné, chrání obsah zprávy

Šifrování dat-KRYPTOLOGIE - učímeseIT.cz Jak vytvářet kódy a šifry - wikiHow

- Aktivita - Co mám na zádech (~10 minut, zařadit podle tempa hodiny)

3. Reflexe (5 minut)

- **Hra 'Kódování nebo šifrování?': Žáci rozhodují, zda uvedené příklady patří ke kódování nebo šifrování**

  Příprava:

  - Kartičky s příklady kódování a šifrování
  - Dvě krabice nebo nádoby označené "Kódování" a "Šifrování"

  Struktura QR kódu
  Zdroj: WikiMedia

  Průběh hry:

  1. Rozdělím třídu do skupin po 3-4 žácích.

  2. Vysvětlím pravidla:

     - Každá skupina dostane sadu kartiček s příklady
     - Úkol: roztřídit kartičky do správných krabic 1 minuta na vysvětlení

  3. Rozdám kartičky s příklady:

     - ASCII kód (Kódování)
     - Tajný inkoust (Šifrování)
     - Čárový kód (Kódování)
     - Zpráva psaná pozpátku (Šifrování)
     - QR kód (Kódování)
     - Nahrazení písmen čísly (Šifrování)
     - Braillovo písmo (Kódování)
     - Binární kód (Kódování)
     - Tajná řeč - pig latin (Šifrování)
     - Semaforová abeceda (Kódování)

  4. Skupiny třídí kartičky 3 minuty

  5. Rychlá kontrola a shrnutí výsledků 1 minuta

  Tato aktivita podporuje aktivní zapojení žáků a vzájemné učení ve skupinách.

- Aktivita - Zpětná vazba

Nápady k samostatné práci pro žáky

1. Vytvořte vlastní jednoduchou šifru a použijte ji k zašifrování krátkého vzkazu pro spolužáka. Napište jak zašifrovaný vzkaz, tak i klíč k jeho rozluštění.

2. Zakódujte následující slova pomocí Morseovy abecedy:
a) INFORMATIKA
b) KÓDOVÁNÍ
c) ŠIFROVÁNÍ

3. Rozhodněte, zda se jedná o kódování nebo šifrování, a své rozhodnutí zdůvodněte:
a) Překlad textu do Braillova písma
b) Použití tajného inkoustu pro napsání zprávy
c) Převod textu do binárního kódu (0 a 1)

4. Rozluštěte následující zašifrovanou zprávu. Nápověda: Každé písmeno je posunuto o 1 místo v abecedě.
"LPEQWBOJ B TJGSPWBOJ KF [BCBWOF"

5. Vymyslete tři situace z běžného života, kde se setkáváme s kódováním dat, a tři situace, kde se využívá šifrování dat. Ke každé situaci napište krátké vysvětlení.

Tento domácí úkol je navržen tak, aby přímo navazoval na cíle hodiny a klíčové body, které byly stanoveny:

1. Úkol s vytvořením vlastní šifry přímo souvisí s cílem "Žák na příkladech demonstruje jednoduché metody kódování a šifrování textu". Žáci zde prakticky aplikují znalosti o šifrování.

2. Kódování slov pomocí Morseovy abecedy opět naplňuje cíl demonstrace jednoduchých metod kódování a zároveň procvičuje jeden z klíčových bodů - Morseovu abecedu jako příklad kódování.

3. Rozhodování mezi kódováním a šifrováním přímo souvisí s cílem "Žák vysvětlí rozdíl mezi kódováním a šifrováním dat". Žáci musí aplikovat své znalosti o definicích a hlavních rozdílech mezi kódováním a šifrováním.

4. Rozluštění zašifrované zprávy opět naplňuje cíl demonstrace jednoduchých metod šifrování a procvičuje klíčový bod - jednoduchou záměnu písmen jako příklad šifrování.

5. Vymýšlení situací z běžného života pro kódování a šifrování dat prohlubuje pochopení rozdílů mezi těmito koncepty a jejich praktického využití, což podporuje oba stanovené cíle hodiny.

Celkově tento úkol pokrývá všechny klíčové body zmíněné v cílech hodiny a nutí žáky aktivně pracovat s koncepty kódování a šifrování, čímž upevňuje znalosti získané během hodiny.