EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

VSTUPNÍ ČÁST

Název komplexní úlohy/projektu

Šifrování zpráv (M)

Kód úlohy

IN-u-4/AE94

Využitelnost komplexní úlohy

Kategorie dosaženého vzdělání

M (EQF úroveň 4)

L0 (EQF úroveň 4)

Vzdělávací oblasti

IN - Informatické vzdělávání

Vazba na vzdělávací modul(y)

Sestavení počítadla – algoritmizace (M)

Škola

VOŠ, SPŠ automobilní a technická, Skuherského, České Budějovice

Klíčové kompetence

Matematické kompetence, Digitální kompetence

Datum vytvoření

03. 10. 2019 21:13

Délka/časová náročnost - Odborné vzdělávání

Délka/časová náročnost - Všeobecné vzdělávání

16

Poznámka k délce úlohy

Ročník(y)

2. ročník, 3. ročník

Řešení úlohy

individuální, skupinové

Doporučený počet žáků

10

Charakteristika/anotace

Žáci se během projektu seznámí se šifrovacími a dešifrovacími metodami dnes i v historii, představí je ostatním ve skupině, vytvoří vývojový diagram pro (de)šifrování zpráv, ten společně odladí a následně ho naprogramují, tedy vytvoří fungující (de)šifrovací aplikaci.

Seznámení s šifrovacími metodami bude probíhat individuálně, resp. ve dvojicích. Žáci si osvojí vyhledávání relevantních zdrojů informací a jejich vhodné převedení pro účely prezentace ostatním. Odladění vývojového diagramu proběhne formou experimentálního ověření; vybrané slovo nebo krátká věta se zašifruje, potom dešifruje a porovnají se hodnoty vstupu a výstupu. Hlavním výstupem je ovšem fungující program, který šifruje a dešifruje slova a krátké věty.

JÁDRO ÚLOHY

Očekávané výsledky učení

Žák:

- vyhledává relevantní a dostatečně přesné informace o šifrovacích metodách na základě zadání;
- převede informace do vhodné podoby pro představení ostatním, přitom dodržuje autorské právo;
- prezentuje informace;
- vytvoří vývojový diagram vybrané šifrovací metody;
- odladí vývojový diagram jiného žáka;
- ve vybraném nástroji naprogramuje aplikaci pro šifrování slov a krátkých vět;
- interpretuje program jiného žáka;
- počítá variace, permutace a kombinace.

Vazba na RVP

Informatické vzdělávání:

- vysvětlí daný algoritmus, program; určí, zda je daný postup algoritmem;
- rozdělí problém na menší části, rozhodne, které je vhodné řešit algoritmicky, své rozhodnutí zdůvodní; sestaví a zapíše algoritmy pro řešení problému;
- ve vztahu k charakteru a velikosti vstupu hodnotí nároky algoritmů; algoritmy podle různých hledisek porovná a vybere pro řešený problém ten nejvhodnější; vylepší algoritmus podle zvoleného hlediska;
- sestaví přehledný program, ten otestuje a optimalizuje;
- používá opakování, větvení programu se složenými podmínkami, proměnné.

Matematické vzdělávání:

- užívá vztahy pro počet variací, permutací a kombinací bez opakování.

Průřezové téma Člověk a digitální svět

Žáci jsou vedeni zejména k tomu, aby:

- vyjadřovali se za pomoci digitálních prostředků a vytvářeli a upravovali vlastní digitální obsah v různých formátech; měnili, vylepšovali a zdokonalovali obsah stávajících děl s cílem vytvořit nový, originální a relevantní obsah;
- získávali data, informace a obsah z různých zdrojů v digitálním prostředí; při vyhledávání používali různé strategie; získaná data a informace kriticky hodnotili, posuzovali jejich spolehlivost a úplnost.

Specifikace hlavních učebních činností žáků/aktivit projektu vč. doporučeného časového rozvrhu

Poznámka k časovému rozvrhu: Délka úlohy je stanovena na 12 hodin pro informatické problémy; poslední úkol, který trvá 2–4 vyučovací hodiny, spadá do hodinové dotace pro matematiku. Měl by také být veden učitelem matematiky.

1. Žáci individuálně hledají informace o šifrovacích metodách, následně si jednu vyberou:

- výběr metody proběhne společně s učitelem, aby žáci nezpracovávali stejné šifrovací metody;
- dvěma žákům je přidělena vždy jedna metoda, takže nadále žáci pracují ve dvojicích.

Upřesnění: kvůli počítačovému zpracování by mělo jít o šifrování textu do textu, případně čísel (bylo by sice možné využít abecedy, v níž se písmena kódují např. pomocí tvaru ruky, ale jen v případě, že by se nepoužil počítač – také by se

muselo změnit zadání přiložené k této úloze).

2. Pro vybranou šifrovací metodu vytvoří žáci ve dvojicích prezentaci: vyhledávají a vybírají relevantní informace, správně citují zdroje; vhodně volí schéma prezentace, využívají obrázky, správně časují případné efekty apod. Ideálně prezentace obsahuje nejen princip samotné šifrovací metody, ale také zajímavosti z historie jejího použití.

3. Žáci ve dvojících představí šifrovací metodu ostatním žákům.

4. Na základě této motivace každý žák vybere nebo vymyslí jednu šifrovací metodu, nemusí si vybrat tu, kterou zpracovával pro prezentaci.

(*První čtyři body dohromady 3 vyučovací hodiny*.)

5. Dalším výstupem je vývojový diagram vybrané šifrovací metody. Detaily metody lze vyhledávat z dostupných zdrojů nebo je samostatně domýšlet. Vybranou metodu žák rozebere na menší části a zapíše ji vývojovým diagramem.

(*1 vyučovací hodina*)

6. Odladění diagramu: žák dostane k dispozici vývojový diagram jiného žáka a pokusí se zašifrovat a následně dešifrovat slovo nebo krátkou větu. Porovná vstupy a výstupy, a pokud se neshodují, najde v diagramu chybu a opraví ji. Zkontroluje diagram i v případě, že se výstupy shodují.

(*1 vyučovací hodina*)

7. Hlavním výstupem je program, který bude zprávy šifrovat i dešifrovat. Při tvorbě se vychází z vývojového diagramu. Žák implementuje algoritmus ve vybraném programovacím prostředí. Součástí programu je i vhodné uživatelské prostředí. Program bude umět zprávy šifrovat i dešifrovat.

Programovací prostředí určuje učitel, může se pro jednotlivé žáky lišit podle jejich schopností nebo preferencí.

Po vytvoření programu žák popíše algoritmus jiného žáka.

(*7 vyučovacích hodin*)

8. Při hodinách matematiky se žáci budou zabývat problémy, které souvisí se šifrováním: zejména počty možností s různými požadavky na složitost hesla. Blíže viz zadání přiložené k této úloze.

(*2–4 vyučovací hodiny; dle zvážení učitele matematiky*)

Metodická doporučení

Výběr programovacího jazyka závisí na pokročilosti žáka, slabší žáci mohou využít i tabulkový procesor a jeho vestavěné funkce, ale spíše se doporučuje vizuální programovací jazyk: větší koncentrace na algoritmus, okamžité výstupy, bez striktní syntaxe. Žáci s více zkušenostmi mohou programovat v textovém programovacím jazyce.

I při ladění vývojového diagramu je vhodné myslet na úroveň žáků. Slabší žáci by měli kontrolovat a ladit jednodušší diagramy a naopak.

Je vhodné časově sladit probírání látky v matematice, aby se v době realizace projektu mohli žáci v hodinách matematiky seznamovat s kombinatorikou a zjišťovat počty možností tvorby hesel při různých specifikacích.

Je třeba být připravený na to, že pro žáky je tvorba algoritmu nebo diagramu náročná. Vytvořit fungující program pak zvládne třeba jen několik málo z nich. Cílem však není naučit žáky programovat, ale naučit je přemýšlet abstraktně a přesně, jednoznačně a systematicky.

Způsob realizace

Individuální výuka

Teoretická výuka v učebnách ICT

Pomůcky

Počítač

Software pro tvorbu prezentace

Software pro tvorbu vývojového diagramu (nejlépe volně dostupný program PS diagram, příp. jiný software, v kterém se

dají vytvářet diagramy)

Software na programování (např.: Python, lze využít on-line dostupné prostředí Scratch nebo jeho desktopová verze Snap!, lze také využít tabulkový procesor)

VÝSTUPNÍ ČÁST

Popis a kvantifikace všech plánovaných výstupů

Prezentace na téma související s šifrováním. (Hodnotí se nejen samotný dokument se zpracovanou prezentací, ale i přednes před spolužáky. Přednes může být kvůli časové náročnosti zkrácen.)

Vývojový diagram

Program šifrující a dešifrující zprávy

Kritéria hodnocení

Informatické vzdělávání

prezentace (10 b)

- všechny náležitosti prezentace: 6 b
- prezentační dovednosti: 4 b

diagram (14 b)

- správný zápis vlastního diagramu: 8 b
- testování a oprava diagramu jiného žáka: 6 b

program (16 b)

- správná funkčnost: 12 b
- uživatelské rozhraní (hodnotí se přehlednost a jednoznačnost): 4 b

V součtu za informatické vzdělávání: 40 b

Matematické vzdělávání

správné řešení: 3 b

správný postup: 2 b

x4 úlohy = v součtu za Matematické vzdělávání: 20 b

Celkem za celou úlohu: 60 b

Orientační hodnocení:

- 60–48 b … 1
- 47–36 b … 2
- 35–24 b … 3
- 23–12 b … 4
- 11–0 b … 5

Hodnocení je možné rozdělit na část informatiky a matematiky a známkovat části odděleně v tomtéž nebo podobném poměru jako u celkového hodnocení.

Doporučená literatura

Informatické myšlení. *Informatické myšlení* [online]. Dostupné z: https://imysleni.cz/

Vzdělávací materiály. *Informatické myšlení* [online]. Dostupné z: https://imysleni.cz/ucebnice

Základy informatiky pro střední školy. *Informatické myšlení* [online]. Dostupné z: https://imysleni.cz/ucebnice/zaklady-informatiky-pro-stredni-skoly

Základy programování v jazyce Python pro střední školy. *Informatické myšlení* [online]. Dostupné z: https://imysleni.cz/ucebnice/zaklady-programovani-v-jazyce-python-pro-stredni-skoly

Poznámky

Poznámka k časovému rozvrhu: Délka úlohy je stanovena na 12 hodin pro informatické problémy; poslední úkol, který trvá 2–4 vyučovací hodiny, spadá do hodinové dotace pro matematiku. Měl by také být veden učitelem matematiky.

Obsahové upřesnění

VV - Všeobecné vzdělávání

Přílohy

- zadani-KU_Sifrovani-zprav.docx
- navrh-reseni_Vyvojovy-diagram.png
- navrhy-reseni_Kryptografie.xlsx
- reseni_Matematicke-vypocty.docx
- Dokumentace-z-overovani-KU_Sifrovani-zprav.docx
- Reseni-zaka_prezentace.pptx
- Reseni-zaka_Sifrovani.sb3
- Reseni-zaka_Sifry-1.docx
- Reseni-zaka_Sifry-2.docx

Materiál vznikl v rámci projektu Modernizace odborného vzdělávání (MOV), který byl spolufinancován z Evropských strukturálních a investičních fondů a jehož realizaci zajišťoval Národní pedagogický institut České republiky. Autorem materiálu a všech jeho částí, není-li uvedeno jinak, je Vít Waldhauser.