Úloha Vigenèrova šifra

Úloha je umístěna v kapitole **Řešíme problémy s daty**.
https://pracesdaty.zcu.cz/index.php/resime-problemy/11-resime-priklad-1

Určení

2. stupeň (7. třída).

Tip na hodinu

Úlohu je dobré zařadit po úloze Datík a prohlížeče na závěr práce se vzdělávacím materiálem. Kvůli náročnosti ale zároveň i zajímavosti jí lze vyhradit samostatnou hodinu.

Cíl

Popsat vlastními slovy konkrétní situaci, co je o ní známo.

Zhodnotit zda je k dispozici vše k řešení problému.

Znázornit řešení problému.

Výstup

Žák popíše počáteční situaci při (de)šifrování textu.

Žák vyřeší v jednotlivých krocích (de)šifrování textu.

Žák využije pomocnou tabulku pro (de)šifrování textu.

Popis

Žáci zjistí, jak funguje Vigenèrova šifra. (De)šifrování je záměrně udělané písmeno po písmenu, aby žáci dokonale poznali její princip. Pokud by se jim nedařilo při opakování písmen klíče si zapamatovat, co již (de)šifrovali, je vhodné žákům umožnit rozepsat text a pod něj opakovaně klíč po písmenech do buněk v tabulkovém kalkulátoru (Google Tabulky, LibreOffice Calc, Microsoft Excel apod.), nebo využít čtverečkovaný papír. Žáci mohou sice díky kontrole šifrování celého textu používat úlohu sami, ale kvůli její obtížnosti to výrazně nedoporučujeme. Při vedení v hodině podle níže popsaného využití lze předpokládat, že se spíše k úloze budou vracet jako k zajímavému nástroji.

Ovládání

Do prvního pole se vyplní text, který je třeba (de)šifrovat. Pod něj se vyplní klíč, s jehož pomocí bude (de)šifrování prováděno. V obou polích jsou písmena automaticky převedena na velká. Při **šifrování** se v rozbalovacím seznamu vybere písmeno podle textu zprávy a jako pomůcka se automaticky vyznačí v šifrovací tabulce odpovídající sloupec. Dále se vybere v rozbalovacím seznamu písmeno podle (opakovaného) klíče a jako pomůcka se automaticky vyznačí v šifrovací tabulce příslušný řádek. Písmeno šifrovaného textu je v průsečíku vyznačeného sloupce. Po kliknutí na tlačítko *Šifruj* se písmeno zapíše do šifrované zprávy. Při **dešifrování** se v rozbalovacím seznamu písmeno podle textu ze šifrované zprávy a jako pomůcka se automaticky vyznačí v šifrovací tabulce všechny jeho výskyty. Dále se vybere v rozbalovacím seznamu písmeno podle (opakovaného) klíče a jako pomůcka se automaticky vyznačí v šifrovací tabulce příslušný řádek. Písmeno dešifrovaného textu se červeně zbarví v záhlaví sloupců. Po kliknutí na tlačítko *Dešifruj* se písmeno zapíše do dešifrované zprávy. Tlačítko *Kontrola* slouží v obou případech pouze ke kontrole správnosti celé (de)šifrované zprávy. Tlačítko *Zpět* v obou případech odstraňuje jedno (de)šifrované písmeno.

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Metodický list vznikl jako součást beta verze vzdělávacího materiálu Práce s daty za podpory projektu Podpora rozvíjení informatického myšlení reg. číslo CZ.02.3.68/0.0/0.0/16_036/0005322 spolufinancovaného Evropskou unií.

Využití v hodině

Pro umocnění rozvoje příslušných částí informatického myšlení je dobré projít všechny níže naznačené kroky.

Upozornění:

- Při použití prohlížeče Microsoft Edge mohou nastat problémy s vykreslováním pomocného vyznačování v šifrovací tabulce, které bylo popsáno v sekci Ovládání.

Šifrování

Otázky do diskuse:

1. Proč s daty pracujeme někdy tak, že je šifrujeme?
2. K čemu slouží při šifrování klíč?
3. Co mám udělat, když chci šifrovat slovo INFORMACE a jako klíč použít slovo DATA?

Pokyny:

- První otázka vede k navození pochopení, co se bude v hodině odehrávat. Nechejte žáky pokud možno samotné dojít k tomu, že šifrování je užitečné, když chceme předat nějaké tajné informace. Uděláme to ve formě dat, kterým má porozumět pouze někdo. Jinému má zůstat jejich skutečný obsah skryt.
- Opověď na druhou otázku naleznou žáci přímo v textu. Můžete samozřejmě pro jistotu rozebrat ještě více v diskusi.
- Ke třetí otázce si připravte jako pomoc následující tabulku:

Zpráva	I	N	F	O	R	M	A	C	E
Klíč	D	A	T	A					
Šifrovaná zpráva									

Důležité je, nechat žáky, aby vám z textu úlohy dokázali poradit, že klíč je třeba opsat vícekrát podle počtu písmen zprávy. Vysvětlete způsob šifrování a nechejte si diktovat písmena šifrované zprávy z průsečíku od různých žáků.

Poznámky:

- Žáci by měli dokázat vysvětlit účel šifrování.
- Žáci by měli popsat výchozí situaci při šifrování textu zprávy.
- Žáci by se měli při řešení problému dokázat soustředit na detail v rámci celku.
- Žáci by měli využít správně klíč při šifrování textu zprávy.
- Žáci by měli poznat výhody automatizace provádění kroků při šifrování.

Samostatná práce:

- Žáci samostatně šifrují zprávu PRACESDATYJE<slovo> klíčem SIFROVANI.

Pokyny:

- Zobrazte žákům zprávu, kterou mají šifrovat s tím, že další slovo si do ní mají vymyslet sami. Přidejte klíč.
- V případě potřeby doplňte ještě jednou informace k ovládání (vybrat písmeno ze zprávy, z klíče a kliknout na tlačítko *Šifruj*, v případě potřeby se lze tlačítkem *Zpět* rušit po jednom šifrovaná písmena, tlačítko *Kontrola* použít až na konci).
- Doporučte žákům, aby si přepsali zprávu s (opakovaným) klíčem vedle do tabulky.
- Nechejte všem opravdu dostatek času.

Otázky do diskuse:

1. Do kterého řetězce znaků se zašifrovala část zprávy, kterou jsme měli všichni stejnou?
2. Které slovo jste do věty doplnili a zašifrovali?
3. Co je zajímavé na textu šifrované zprávy?

Pokyny:

- U první otázky si nechejte někým nadiktovat příslušnou zašifrovanou část (jedná se o HZFTSNDNBQRJ). Případně se zeptejte, zda všichni došli k témuž.
- U druhé otázky vyberte více žáků a převeďte pro kontrolu šifrování jejich slova písmeno po písmenu v návaznosti na předchozí část zprávy (případně to nechejte předvést je samotné). V případě počátečního ostychu mějte do zásoby připravené na úvod nějaké vlastní slovo.
- U třetí otázky nespěchejte a snažte se od žáků získat co nejvíce postřehů. Případnými doplňujícími otázkami se snažte dojít k tomu, že se v něm sice nachází stejná písmena (přinejmenším ve společné části jsou to dvě N), ale při pohledu zpět na text původní zprávy je patrné, že na odpovídajících místech byla písmena různá. Podobně si lze všimnout, že i když se některá písmena v textu původní zprávy opakovala (ve společné části např. E, A), v textu šifrované zprávy jsou na příslušných místech písmena různá.
- Snažte se, aby se dostali ke slovu různí žáci (i podle toho, kdo mluvil na začátku).

Poznámky:

- Žáci by se měli při řešení problému dokázat soustředit na detail v rámci celku.
- Žáci by měli dokázat dát jasné instrukce, které povedou ke znázornění šifrování.
- Žáci by měli využít správně klíč při šifrování textu zprávy.
- Žáci by měli dokázat opakovaně využít pro ně již známý postup.
- Žáci by měli osvědčit vytrvalost při práci na složitém problému.
- Žáci by měli poznat výhody automatizace provádění kroků při šifrování.
- Žáci by měli dokázat popsat řešení jejich problému.
- Žáci by si měli vyzkoušet popis analytického postupu myšlení.

Dešifrování

Otázky do diskuse:

1. Dorazila mi zpráva UOUWDGAMQU. Co v ní je?
2. Co mám udělat, když chci zprávu dešifrovat a jako klíč použít slovo DATIK?
3. Co je zajímavé na dešifrovaném textu zprávy?

Pokyny:

- První otázka má vést primárně k tomu, jestli si žáci již uvědomili, že pro rozluštění budou potřebovat znát klíč. Je opět dobré je k tomu nechat dojít samotné. Samozřejmě se lze zmínit potom zmínit o tom, že teprve bez znalosti klíče jsou v pozici člověka, který provádí kryptoanalýzu, což si ale ještě případně vyzkouší v posledním úkolu.
- Ke druhé otázce si připravte jako pomoc následující tabulku:

Šifrovaná zpráva	U	O	U	W	D	G	A	M	Q	U
Klíč	D	A	T	I	K					
Dešifrovaná zpráva										

- Důležité je, nechat žáky, aby vám z textu úlohy dokázali poradit, že klíč je třeba opsat vícekrát podle počtu písmen zprávy. Vysvětlete způsob dešifrování a nechejte si diktovat červeně vyznačená písmena dešifrovaného textu zprávy od různých žáků.
- U třetí otázky nespěchejte a snažte se od žáků získat co nejvíce postřehů. Případnými doplňujícími otázkami se snažte dojít k tomu, že se v něm sice nachází stejná písmena (O, T), ale při pohledu zpět na šifrovaný text je patrné, že na odpovídajících místech byla písmena různá. Podobně si lze všimnout, že i když se písmeno U v šifrovaném textu opakovalo třikrát, pokaždé bylo dešifrováno jako jiné písmeno. Novou zajímavostí je, že ze zcela jinak vypadajícího slova jsme za pomoci klíče dešifrovali část textu stejnou jako klíč.
- Snažte se, ať se ke slovu dostane co nejvíce žáků.

Poznámky:

- Žáci by měli popsat výchozí situaci při dešifrování šifrovaného textu zprávy.
- Žáci by se měli při řešení problému dokázat soustředit na detail v rámci celku.
- Žáci by měli využít správně klíč při dešifrování šifrovaného textu zprávy.
- Žáci by měli poznat výhody automatizace provádění kroků při dešifrování.
- Žáci by si měli vyzkoušet popis analytického postupu myšlení.

Práce ve dvojicích:

- Žáci ve dvojici šifrují zadané zprávy, které souvisejí s činnostmi s daty.
- Žáci ve dvojici dešifrují zprávy od jiné dvojice.

Pokyny:

- Připravte si na papíru napsaná slova, která představují činnosti, které v souvislosti s daty žáci v průběhu práce se vzdělávacím materiálem dělali (např. HLEDAME, EVIDUJEME, KONTROLUJEME, TRIDIME, FILTRUJEME, RADIME, PREZENTUJEME, POROVNAVAME atd.) a rozdejte je i s klíčem DATIK mezi dvojice s výzvou, aby si je nesdělovali.
- Připomeňte případně, že ovládání je stejné, jako když šifrovali při první samostatné práci.
- Až budou všechny dvojice hotovy, vyzvěte je, aby si mezi sebou vyměnily pouze šifrované zprávy bez klíče. Následně mají šifrovanou zprávu dešifrovat.
- Připomeňte v případě potřeby žákům způsob ovládání při dešifrování.
- Pokud by nějaká dvojice tápala ohledně klíče, pokuste se je navést, co by asi mohli zkusit jako první (klíč, který použili při šifrování sami).
- Ponechejte všem na vše dostatek času.

Poznámky:

- Žáci by se měli při řešení problému dokázat soustředit na detail v rámci celku.
- Žáci by měli dokázat dát jasné instrukce, které povedou ke znázornění (de)šifrování.
- Žáci by měli využít správně klíč při (de)šifrování.
- Žáci by měli dokázat opakovaně využít pro ně již známý postup.
- Žáci by měli osvědčit vytrvalost při práci na složitém problému.
- Žáci by měli poznat výhody automatizace provádění kroků při šifrování.
- Žáci by měli dokázat popsat řešení jejich problému.
- Žáci by si měli vyzkoušet popis analytického postupu myšlení.
- Žáci by měli spolu komunikovat pro dosažení společného cíle.

Otázky do diskuse:

1. Jaká slova jste (de)šifrovali?
2. Popište, v čem jednotlivé činnosti spočívají? Proč je s daty děláme?

Pokyny:

- Nechte si nadiktovat od žáků slova a případně jejich šifrovanou podobu. Můžete opět porovnávat shody písmen atd.
- U druhé otázky nechejte žáky vlastními slovy popsat, na co si v souvislosti s jednotlivými činnostmi vzpomenou. V případě potřeby doplňujte, korigujte, vraťte se k příslušné části vzdělávacího materiálu apod.
- Snažte se, aby se dostali ke slovu různí žáci.

Poznámky:

- Žáci by měli dokázat popsat jejich řešení problému.
- Žáci by měli porovnat výchozí situaci a řešení problému.
- Žáci by se měli při řešení problému dokázat soustředit na detail v rámci celku.
- Žáci by si měli vyzkoušet popis analytického postupu myšlení.
- Žáci by měli dokázat zopakovat, v čem spočívají jim známé postupy práce s daty.

Kryptoanalýza

Otázky do diskuse:

1. Dorazila mi zpráva QHCDSRPHQWHCHGDWDMVRXYVXGHNROHPQDV. Co v ní je?
2. Na co se potřebujete zeptat?

Práce ve dvojicích či větších skupinách:

- Žáci si ve dvojicích, či větších skupinách zahrají na kryptoanalytiky, kteří chtějí dešifrovat zadanou zprávu.
- Za každou skupinu se může chodit ptát pouze jeden zvolený zástupce.

Pokyny:

- Předejte žákům příslušnou šifrovanou zprávu (na papíru, nebo sdílením na počítači např. v tabulce nebo v dokumentu).
- Zdůrazněte, že klíč jim nemůžete prozradit, ale můžete jim říci něco o jeho vlastnostech, když se vhodně zeptají. Zásadní by pro ně měl být moment, kdy je napadne se zeptat na délku klíče (ta je rovna jedné, čili se vlastně problém redukuje na klasickou Caesarovu šifru a při dešifrování stačí vybrat pouze jeden správný řádek ze šifrovací tabulky). Následně by jim mělo již stačit pouze několik pokusů pro nalezení správného písmene, které je klíčem (D).
- Připomeňte užitečnost používání tlačítka *Zpět* po postupné vracení dešifrovaných písmen.
- NEZAPOMENTEZEDATAJSOUVSUDEKOLEMNAS

Poznámky:

- Žáci by měli porovnat výchozí situaci a řešení problému.
- Žáci by se měli při řešení problému dokázat soustředit na detail v rámci celku.
- Žáci by měli umět položit vhodné otázky k řešení problému.
- Žáci by si měli vyzkoušet kryptoanalytický postup.
- Žáci by měli využít správně klíč při dešifrování textu zprávy.
- Žáci by měli dokázat dát jasné instrukce, které povedou ke znázornění dešifrování.
- Žáci by měli dokázat opakovaně využít pro ně již známý postup.
- Žáci by měli dokázat zopakovat, v čem spočívají jim známé postupy práce s daty.

Závěrečné otázky:

1. Jak jste při snaze o kryptoanalýzu postupovali, jak jste uvažovali?
2. Co je při způsobu šifrování, který jste si vyzkoušeli, nejobtížnější?

Pokyny:

- U první otázky nechejte projevit co nejvíce žáků. Měli by popsat i to, jak dospěli k otázkám, které budou pokládat. Berte v potaz i to, že ne všechny skupiny museli při řešení posledního problému uspět.
- U druhé otázky by žáci měli dokázat sami zopakovat, že tím nejdůležitějším byl klíč. V momentě, kdy byl znám a věděli, jak je šifrování konstruováno, neměli s ním problém. Zásadní je tedy u tohoto typu (symetrické) šifry, si předat klíč tak, aby ho nikdo nezachytil. Dalším problémem ve skutečnosti bývá i fakt, že obecně nemusí být známo, jaký typ šifry byl použit.
- Snažte se, aby se dostali ke slovu různí žáci.

Poznámky:

- Žáci by měli dokázat popsat jejich řešení problému.
- Žáci by měli identifikovat nejdůležitější problém symetrického šifrování.
- Žáci by si měli vyzkoušet popis analytického postupu myšlení.