# 3.7.2 Přenosová hra a šifrovací principy

| | |
|---|---|
| **Účastníků** | 8 - 20 |
| **Fyzická náročnost** | I |
| **Psychická náročnost** | IV |
| **Autoři** | Markéta Ledvinová, Oliver Velich |
| **Počet uvádějících** | 1-2 |
| **Čas na realizaci** | 90 minut |
| **Čas na přípravu** | 15 minut |
| **Prostředí** | místnost, nezávisle na denní či roční době |
| **Rozdělení** | samotná hra v týmech po 4 účastnících, diskuze celá skupina |

## Cíle

Žák aplikuje známé kódovací a šifrovací principy. Vysvětlí smysl kódování a šifrování na specifických praktických příkladech.

## Sdělení

Šifry a kódování nejsou jenom hračky, ale využívají se při přenosu zpráv na mobilu nebo v počítači.

## Metody

Aktivizace, didaktická hra, soutěž, frontální výuka, diskuze.

Metody a formy

## Klíčové kompetence

- Komunikace v mateřském jazyce je rozvíjena:
  - aktivní komunikací mezi hráči v průběhu tvorby a řešení úloh,
  - rozborem průběhu hry a použitých postupů.

- Matematická schopnost a základní schopnosti v oblasti vědy a technologií jsou rozvíjeny:
  - seznámením se a tréningem použití různých druhů šifer,
  - aplikací známých šifrovacích principů při šifrování a dešifrování krátkých zpráv.
- Sociální a občanské schopnosti jsou rozvíjeny
  - zamýšlením se a diskuzí nad bezpečností dat a obsahu komunikace v IT technologiích,
  - aktivním naslouchání a vyjadřováním názoru.

# Forma a popis realizace

Jedná se o šifrovací hru, kde žáci aktivně šifrují a dešifrují krátké zprávy. Hra je proložena diskuzemi a krátkým výkladem o šifrování a kódování.

# Přizpůsobení SVP

U programu mají žáci možnost přinést do způsobu řešení vlastní znalost při vymýšlení způsobu kódování a testovat svůj způsob uvažování v praxi. V reflektivní části se rozebírá, které použité postupy byly ve výsledku efektivní a které nikoliv. Rozbor má velkou informační hodnotu a je důležitým motivačním prvkem pro další pokračování a udržení zájmu.

# Obsah

Při hře, která probíhá ve dvou sériích kol, se účastníci rozdělí na šifrující dvojice (v každé dvojici je jeden hráč A a jeden hráč B), které mají za úkol domluvit se na způsobu kódování, a záškodníky, kteří mají za úkol kódy rozluštit a zprávu změnit. V každém samotném kole pak A obdrží slovo, zakóduje je, pošle dvojici záškodníků, kteří mají za úkol kód prolomit a vyluštěnou zprávu změnit a znova zakódovat stejným kódem. Poté dostane kódovanou zprávu hráč B, který má za úkol dekódovat přijatou zprávu a rozhodnout, jestli je to zpráva pravá (poslaná hráčem B), či falešná (změněná záškodníky). V druhé sérii kol se role AB a ZZ vymění. Bodování probíhá dle bodovací tabulky, následuje reflexe a rozbor.

Samotná hra je uvedena opakováním a procvičením známých i nových šifrovacích principů a proložena mini výkladem a diskuzí o šifrování v IT technologiích.

# Uvedení

## Příprava

Před schůzkou je třeba vytisknout jednotlivé šifry pro úvodní opakování, každou asi v polovičním počtu, než je v kroužku žáků. Dále budou potřeba veškeré tabulky pro přenosovou hru, stopky na měření času, papíry a psací potřeby. Pokud se schůzka odehrává ve třídě, kde je možné si sednout ke stolům ve dvojicích a trojicích, není třeba místnost zvlášť upravovat. Pokud v místnosti nejsou stoly, je dobré žákům rozdat na psaní tvrdé podložky.

## Realizace

### Opakování šifrovacích principů a ukázka nových - 15 minut

Lektor začne otázkou, jaká znají účastníci kódování (Morse, Braille, vlajková abeceda, polský kříž...). Na co se používala, případně používají a jestli se s nimi už setkali.

Účastníci utvoří skupinky po 2 nebo 3 členech a dostanou postupně k rozluštění 3 šifry obsahující různá kódování.

U první šifry se lektor zeptá, co by mohlo znamenat „HAJOAJSKMETÁ?E“, po chvíli, když někdo přijde na to, že se jedná o prohození dvojic vedlejších písmen a zpráva je „AHOJ JAK SE MÁTE?“ vysvětlí pojem transpoziční šifry. Je to přeskupení písmen zprávy podle určitého klíče nebo i náhodně. Jde o to, že všechna písmena zprávy jsou stále v zašifrovaném textu nezměněná, jen se zamíchalo jejich pořadí. Poté rozdá šifru č. 1 s přesmyčkami. Pro ty, co po dvou minutách stále netuší, může rozdat nápovědu kódovanou Morseovkou.

Následují dvě grafické šifry (č. 2 a 3), které lektor může krátce uvést tím, že v šifrách se také mohou ukrývat graficky písmena nebo různé znaky. Další grafickou šifru má lektor na ukázku (bludiste.pdf).

U šifry č. 4 je možné rozdat buď variantu, kde jsou šifra i tabulka se semaforovou abecedou na jedné straně (lehčí), nebo je možné vytisknout šifru oboustranně a rozdat papír šifrou nahoru, většina luštitelů si druhé strany nevšimne a po chvíli je na ni můžeme upozornit s tím, že často si u šifer všímáme jen těch nejvíce zjevných znaků a podstatné informace nám mohou zůstat skryty přímo před očima.

U páté šifry se lektor zeptá, zda znají Caesarovu šifru, a na jakém principu funguje (substituce), poté účastníci luští substituční šifru.

Poslední je ukázka steganografické šifry (uhel_pohledu.pdf). Dalšími příklady jsou tajné inkousty (citron, mléko, UV, chemické sloučeniny), zmenšení na minci...

Poté, co účastníci dokončí luštění a rozeberou se způsoby řešení, přechází se k další aktivitě - vymýšlení vlastních šifer a jejich předávání.

### Šifro-přenosová hra 1. série kol - 30 min

Účastníci teď musí vymyslet a a domluvit se na efektivní a zároveň dostatečně bezpečné formě komunikace. Seznámí se s pravidly hry a rozdělí se do týmů po 4. V rámci týmu se rozdělí role na 1xA, 1xB, 2xZ. Před samotnou sérií kol se musí v omezeném čase A a B domluvit na zvoleném způsobu šifrování a samostatně si vytvořit šifrovací klíč, kterým budou komunikaci šifrovat. Samotná hra probíhá v 5 kolech, každé kolo se skládá postupně z několika fází (časy pro jednotlivá kola/fáze je dobré upravit podle aktuální pokročilosti skupiny): A šifruje zprávu (slovo ze seznamu); Z se snaží prolomit šifru a vytvořit vlastní klíč, může poslat jiné slovo; B dešifruje zprávu a rozhoduje se, jestli byla komunikace infiltrována. Po skončení všech kol se společně diskutují zvolené způsoby šifrování a v jakých aspektech komunikace nejčastěji selhala. V rámci předem uvedeného hodnocení se rozdělí body v rámci týmu a vyhodnotí se úspěšnost komunikace v rámci rolí A,B vs. Z.

### Jak se šifruje v mobilu nebo v počítači - 10 min

Následuje krátká diskuze, v níž se žáci zamyslí nad způsobem, jakým chrání obsah své komunikace v digitálním prostředí a vyjmenovávají způsoby, jakými komunikují v digitálním prostředí. Zamýšlí se

nad tím, jakým způsobem může být jejich komunikace napadena nebo odposlouchávána. Lektor představí rozdíl mezi kódováním a šifrováním ve smyslu výpočetní techniky. Účastníci se zamýšlí nad tím, proč se informace kódují a kdy je vhodné je také šifrovat.

V krátkém doplňujícím mini výkladu lektora se dozvědí, že šifry a kódování nejsou jenom hračky, ale využívají se při přenosu zpráv na mobilu nebo v počítači. Lektor připomene koncept prvočísel a představí, jak problém rozložení složeného čísla na prvočísla je základním kamenem šifrovacích algoritmů.

Poté se skupina navrací k druhé sérii kol přenosové hry.

**Šifro-přenosová hra 2. série kol - 25 min**

Ve druhé sérii si účastníci vyzkouší druhou roli celé problematiky. Důraz na efektivní domluvu, důsledné dodržování šifrovacího klíče a výměna role šifrujících a záškodníků umožňuje zachovat zajímavost 2. série. Žáci na základě zkušeností z předchozího běhu hry musí upravit sofistikovanost svých šifer, aby byly bezpečnější, nebo efektivnější.

Kromě prohození rolí jsou prohozeni žáci i mezi týmy. Ještě jednou se připomenou základní pravidla. Po domluvě mezi A a B probíhá standardně 5 kol. Zavede se paralelní průběh, aby se hra zrychlila. Ve hře se šifrují delší slova.

### Uzavření

Uzavření schůzky probíhá formou reflexe hry a použitých postupů.

### Poznámky

Smysl této aktivity spočívá ve zopakování kódování a šifrovacích postupů (substituce, transpozice, grafické šifry), které už žáci znají, a také ve vytvoření prostoru, v němž mohou žáci své znalosti aplikovat i jiným způsobem, než vlastním luštěním zadaných úkolů. Znalosti skupiny tak může lektor na úvod schůzky do jisté míry sjednotit a přidat nějaké nové postupy, například steganografické šifry. Důležité je věnovat se na úvod takovým principům, které pak žáci budou schopni skutečně použít v rámci přenosové hry, tedy víceméně jednoduchým.

Vysvětlování a samotná přenosová hra se může protáhnout. Druhé kolo je možné provádět rychleji s větším překryvem jednotlivých kroků. Je potřeba dostatečný čas pro A a B na domluvu klíče. Ideální jsou 4 hráči = A + B + 2xZ, kteří se ve druhém kole přehodí Z1=A, Z2=B, A,B=Z. Po skončení přenosové hry je důležité a přínosné, když dojde k rozboru hry - jak hra probíhala, jaké žáci použili postupy, které z nich byly efektivní a které ne, apod. Žáci mají zpravidla o tento rozbor zájem, protože jsou zvědaví, jak hra probíhala v jiných skupinkách a chtějí zhodnotit svůj výkon prakticky. Zvláště v případě nedostatku času je vhodné tento rozbor upřednostnit před podrobným vyhodnocováním a určováním vítěze, protože má pro žáky zásadnější informační hodnotu vzhledem k rozvoji jejich kompetencí a vnitřní motivaci v tématu pokračovat.

## Odkazy

- https://www.pruzkumnik.cz/praxe/sifry/tabulky.html - ukázky kódovacích tabulek

- https://hackernoon.com/how-does-rsa-work-f44918df914b - vysvětlení principu RSA
- https://play.google.com/store/apps/details?id=cz.absolutno.sifry&hl=cs&gl=US - aplikace pro dešifrování základních typů šifer
- https://chlyftym.cz/pomucky/ - přehledné pomůcky pro šifrování od Chlýftýmu

# Pomůcky a materiál

| Položka | Počet | Popis |
|---|---|---|
| vytištěné šifry | 1 od každého druhu/dvojice | úvodní šifry, úhel pohledu, bludiště |
| papíry | v počtu účastníků + rezerva | |
| tužky / psací potřeby | v počtu účastníků + rezerva | |
| tabulka bodování AB | 1ks/dvojice | |
| tabulka bodování Z | 1ks/dvojice | |
| seznam slov | | |
| abeceda | | |
| Morseova abeceda | | |
| tabulka ASCII | | |
| stopky | 1 ks | Pro lektora na měření času |

# Přílohy

### Obsahové přílohy

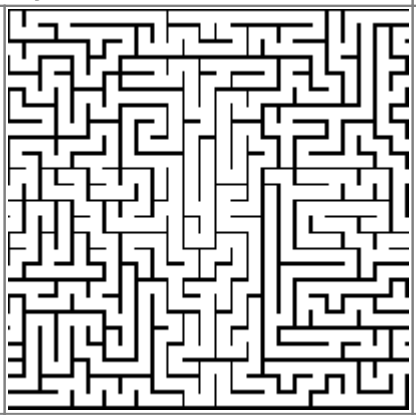
| # | Soubor | Popis |
|---|---|---|
| 010.20.02 | abeceda.docx | abeceda pomůcka |
| 010.20.03 | abeceda.pdf | abeceda pomůcka - tisk |
| 010.20.04 | ascii.docx | ASCII tabulka pomůcka |
| 010.20.05 | ascii.pdf | ASCII tabulka pomůcka - tisk |
| 010.20.06 | bludiste.docx | bludiště - ukázka grafické šifry |
| 010.20.07 | bludiste.pdf | bludiště - ukázka grafické šifry - tisk |
| 010.20.08 | bodovani.docx | bodovací tabulka přenosové hry |
| 010.20.09 | bodovani.pdf | bodovací tabulka přenosové hry - tisk |
| 010.20.22 | ceske_braillovo_pismo.pdf | české Braillovo písmo pomůcka - tisk |
| 010.20.23 | ceske_braillovo_pismo.svg | české Braillovo písmo pomůcka |
| 010.20.10 | morse.docx | Morseova abeceda pomůcka |
| 010.20.11 | morse.pdf | Morseova abeceda pomůcka - tisk |
| 010.20.12 | prubeh.docx | časový rozvrh průběhu přenosové hry |
| 010.20.13 | prubeh.pdf | časový rozvrh průběhu přenosové hry - tisk |
| 010.20.26 | sifry_uvodni_4_oboustranne.pdf | úvodní šifry - šifra č.4 oboustranná - tisk |
| 010.20.24 | sifry_uvodni_opakovani.pdf | šifry - úvodní opakování šifrovacích principů - tisk |
| 010.20.14 | skoreab.docx | tabulka pro zapisování skóre hráčů A a B |
| 010.20.15 | skoreab.pdf | tabulka pro zapisování skóre hráčů A a B - tisk |
| 010.20.16 | skorez.docx | tabulka pro zapisování skóre záškodníků |
| 010.20.17 | skorez.pdf | tabulka pro zapisování skóre záškodníků - tisk |
| 010.20.18 | slova.docx | seznam slov pro přenosovou hru |
| 010.20.19 | slova.pdf | seznam slov pro přenosovou hru - tisk |

| | | |
|---|---|---|
| 010.20.21 | uhel_pohledu.pdf | ukázka steganografické šifry - tisk |
| 010.20.20 | uhel_pohledu.svg | ukázka steganografické šifry |
| 010.20.25 | uvodni_sifry.zip | zdrojové soubory SVG k editaci |

**Metodické přílohy**

| # | Soubor | Popis |
|---|---|---|

# Zdroje

| # Přílohy | Zdroj | | Popis | Autor | Původ | Licence | Datum |
|---|---|---|---|---|---|---|---|
| 010.20.06 | 01 |  | bludiště | Sven Dražan | Vlastní tvorba | CC BY-SA | 2021-04-19 |