7.2 Přenosová hra a šifrovací principy

- Obsah
- Metodika

Načítám ...
>> Jít na tuto stránku.

Metody

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

Metody a formy

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.

Obsah

Úvodní opakování šifrovacích principů

Dnes se podíváme na několik základních druhů kódování a šifer a zahrajeme si hru, kde si tyto principy budete moci rovnou vyzkoušet.

Znáte nějaké druhy kódování nebo šifer?

- Braille - hmatové písmo používané nevidomými či slabozrakými osobami, vyvinul jej Francouz Louis Braille roku 1824 v 15 letech poté, co oslepl. Znaky sestávají z dvou sloupců po 3 polohách, které mohou a nemusí obsahovat vraženou tečku. Krom písmen obsahuje také znaky pro interpunkci, závorky, přepínání notací a rozšířenou verzi 2×4, která se však používá jen zřídka. Národní podoby abecedy se mírně liší na základě různé frekvence znaků v různých jazycích.
- Morseova abeceda - systém pro kódování písmen abecedy a číslic pro použití v telegrafní komunikaci, vymyslel ji asistent Samuela Morse a byla používána v námořní dopravě k nouzové komunikaci až do konce 20. století.
- Námořní vlajková abeceda - signální vizuální komunikační kód používaný dodnes v námořní dopravě.
- Semafor - slouží ke komunikaci mezi osobami na větší vzdálenost s přímou viditelností, je dodnes součástí nouzové námořní komunikace.
- Enigma - šifrovací stroj vyvinutý Německem používaný během druhé světové války, mechanicko-elektrický, používal několik míchacích kotoučů, které se otáčely a měnily tak po každém úderu klávesy substituční schéma. Byl prolomen polskými kryptoanalytiky a posléze

prvním elektronickým počítačem speciálně sestrojeným Brity pod vedením Alana Turinga. Časté opakování zpráv o počasí na frontě umožnilo zjistit denní nastavení kotoučů.
- Binární kódování - způsob reprezentace znaků jako čísel v binární soustavě uvnitř počítače.
- Polský kříž - grafické uspořádání abecedy do tabulky s možností jednoduchého grafického zápisu.

Kódování je způsob zápisu informací vhodný pro přenos nebo záznam na určitém médiu. Je veřejně známý, a proto není prakticky vhodný pro utajování důležitých informací. V šifrovacích hrách se používá, protože umožňuje převést zprávu do prezentace, kterou je možné dále upravovat.

Šifrování je způsob přeměny zprávy do podoby, která je pro osoby neznalé určitého tajemství nečitelná. Tajný může být vlastní způsob přeměny informace nebo jen určitý parametr daného schématu, např. klíč v podobě čísla o kolik jsou písmena v abecedě posunuta.

Teď se prosím rozdělte do dvojic nebo trojic a dostanete postupně několik šifer, které se můžete pokusit rozluštit.

Než vám rozdám první, zkuste zapřemýšlet, co by mohl znamenat tento nápis „HAJOAJSKMETÁ?E“.

Ano máte pravdu, písmenka jsou proházena ve dvojicích tak, jak byla ve zprávě vedle sebe. Tomuto druhu šifry, kdy písmenka zamícháme podle určitého schématu, se říká transpozice. Tady je ta transpozice lineární, ale pokud bychom zprávu zapsali do mřížky, dává nám to spoustu možností, jak je přeházet v ploše.

Teď vám rozdám šifru č. 1, pokud si nebudete po pár minutách vědět rady, tak tu mám taky nápovědu, kterou si určitě zvládnete dekódovat.

Jednalo se o přesmyčky, to je jistý druh náhodné transpozice. Schéma míchání není dáno, prostě zkoušíme přeházet písmenka, dokud nevyjde něco smysluplného. POKEC → KOPEC, PRACH → CHRPA, MALTA → TLAMA, SIMKA → MISKA, PANEL → PLENA, celkově tedy vychází PRASE, což je slovo, které samo o sobě má 3 smysluplné přesmyčky, ačkoliv u jedné přidáváme háček. Docela dobrý je online nástroj https://anagrammer.org, který vám najde všechny možné přesmyčky daného textu v různých jazycích.

Další šifra je zase jiná a můžete u ní zjistit, že přeházení písmenek není jediný způsob, jak získat smysluplnou zprávu. Opět máme připravenou kódovanou nápovědu, pokud byste ji potřebovali.

Jak je vidět, některé pojmy mají v našem jazyce předem dané pořadí, ve kterém se nejčastěji uvádějí, a to nám umožňuje v daném pořadí objekty spojit, čímž můžeme něco nakreslit.

Šifra č. 3 je tak trochu podobná, i když jiná. Pro případ potřeby máme k ní zakódovanou nápovědu, kterou snad zvládnete přečíst, i kdybyste byli slepí.

V třetí šifře šlo o to použít fantazii a každý z pojmů si představit, podobají se písmenům a ty už stačí jen přečíst odshora dolů. U druhé i třetí šifry jsme se nevyhnuli použití textu, o to se pokouší tato bludišťová šifra (princip převzatý z TMOU 6 stanoviště 3). Zkuste se na ni podívat a říct mi své nápady, jak by se dala řešit nebo možná, jak by v ní mohla vůbec být ukryta nějaká smysluplná informace.

Někteří z vás to možná uviděli. Pro nás ostatní, co se dělá s bludišti? Bloudí se v nich, tak to zkusme, budeme si kreslit, jak se v bludišti dá chodit. Sice nevíme, odkud kam se chceme dostat a to spoustu lidí odradí od toho, aby vůbec něco zkoušeli, ale tím se nesmíme nechat odradit. Po čase zjistíme, že některé oblasti jsou nedostupné a ty nám dají písmenka.

Čtvrtou šifru vám teď rozdám na lavice, podívejte se na ni, zda vám něco nepřipomíná. Někteří z vás možná už tuší.

Je to zpráva v kódování známém jako semafor. To, proč jsem vám ji ale rozdal, teď nevidíte. Tak se zkuste pořádně podívat. Vidíte, klíč k řešení byl celou dobu na druhé straně. Občas se necháme zmást tím, co nám někdo dá přímo před oči a zapomeneme na to, že se na všechno dá dívat z různých úhlů pohledu.

Už jste někdy slyšeli o Césarova šifře, Caesar posunul písmena v abecedě o 3 pozice doprava, takže A se stalo D. Ačkoliv nám to může připadat jako jednoduchá hříčka, v té době asi nikoho nenapadla a divili byste se, že ještě v roce 1915 byla používána v ruské armádě a dokonce v roce 2011 na základě jejího použití byli odsouzeni osoby připravující teroristický útok.

Pátá šifra vám snad nedá moc práce. Kdybyste nemohli dostat nápad, je tu nápověda.

Ano, jednalo se o posun o jedno doleva, proto tam bylo tolik těch Z. Výsledek je taková trochu zeměpisná hádanka, tu jste jednoduše uhodli, takže už víte, co je řešení.

Poslední šifru, kterou vám teď nabídneme, si pořádně prohlédněte. Chce to dobrý nápad a potom se dá vyluštit během chviličky, jen se na ní musíte správně podívat.

Pár z vás to zvládlo a těm ostatním zopakuji, co jsem říkal u oboustranné šifry. Někdy jde o úhel pohledu, v tomto případě musí být hodně ostrý.

Zkuste mi říci, co si z těchto několika šifer odnášíte.

Přenosová hra

Teď je potřeba, abyste se rozdělili ideálně do čtveřic, pokud to nevyjde, tak uděláme pětice nebo trojice. V rámci vaší skupiny si teď rozdělte role označené jako A, B a dva záškodníky Z. A a B dostanou minutku na to, aby se domluvili, jak spolu budou komunikovat a další dvě minuty na to, aby si nasdíleli tajné klíče. Poté už spolu budou moci komunikovat jen skrze zprávy. Bude probíhat několik kol, v každém kole bude nejprve jedna minuta na to, aby A vyrobilo šifru pro B a stejně tak B pro A, šifrovat budete slova, která vám dáme až poté, co se A a B rozejdou. Poté, co šifry pošlete, ale budou zachyceny záškodníky a ti mají 2 minuty na to, aby je rozluštili a případně pozměnili tak, aby to příjemce nepoznal. Následně mají příjemci minutu na to, aby přijatou zašifrovanou zprávu dešifrovali a určili, zda byla pozměněná nebo je původní. Časové schéma je tady vyvěšené (prubeh.pdf). Výsledky bude každý zapisovat do své tabulky (skoreab.pdf, skorez.pdf). Celkem bude tato první série kol trvat 30 minut. Poté se prohodíte. Podle toho, jak budete úspěšní ve svých rolích, můžete získat body uvedené v této tabulce (bodovani.pdf).

Šifro-přenosová hra 1. série kol - 30 min

Teď se podíváme, jak se vám dařilo, kolik zpráv záškodníci rozluštili, kolik podvrhli a na kolik z nich jste přišli. Podělte se prosím o svoje postupy, jaký způsob šifrování jste zvolili a jaké jste měli klíče? Jak se dařilo záškodníkům? Co byste příště udělali jinak a co se vám osvědčilo?

Jak se šifruje v mobilu nebo v počítači - 10 min

Ještě než se vrhneme do druhé série kol a vyměníte si role, rád bych se vás zeptal, jaké informace, s kterými každý den pracujete, jsou šifrované? Vidíte, kolik vás toho napadlo, telefonní hovory, placená satelitní televize, internetové stránky, bankovnictví, platby kartou. Myslíte si, že by někdo mohl tuto komunikaci odposlechnout a jak by to dělal?

Při komunikaci se využívá jak kódů, tak šifer. Kódy jsou veřejné známé způsoby přepisu nebo reprezentace dat a slouží k zajištění bezchybného přenosu dat. Tady vidíte ASCII tabulku (ascii.pdf), která ukazuje, kterým znakům v počítači jsou přiřazené jaké číselné hodnoty. Počítače potřebují mít všechno reprezentované jako čísla. Nakonec se dojde na to, že jsou to jen série nul a jedniček. Proto, aby bylo jasné, kdy má který elektrický nebo radiový signál znamenat nulu a kdy jedničku, existují ještě kódování na úrovni hardwaru, ale podstatné je, že krom samotných informací se posílají ještě dodatečné kontrolní součty, podle kterých lze zjistit, zda někde na cestě nedošlo ke změně jedničky na nulu. Kódování se nesnaží zabránit cílené sabotáži, je to proto, aby se překonaly přirozeně se vyskytující rušení, jako jsou výboje, blesky, zkraty, indukované napětí, kosmické záření a kvantové fluktuace.

Naopak šifrování se používá tam, kde chceme zajistit, aby komunikaci nikdo nemohl odposlouchávat, nebo aby mu odposlechnuté informace byly k ničemu bez znalosti tajného klíče. Možnost domluvit se bezpečně na společném sdíleném tajemství, např. skrze tajnou schůzku, je v současné době digitální komunikace nepraktická, proto byly vynalezeny způsoby, jak si tajemství vyměnit bez možnosti bezpečné komunikace.

Jedna z možností je na principu dvou zámků s dvěma klíči. Představme si, že Alice a Bob si chtějí poslat kufr s tajemstvím, Alice nejdřív kufr zamkne svým zámkem a zamčený ho pošle Bobovi, ten na kufr přidá svůj zámek s jiným klíčem a zamčený oběma zámky jej pošle zpět. Poté Alice odemkne svůj zámek a odstraní jej a pošle kufr s jediným zámkem zpět Bobovi, ten už jen odemkne svůj zámek a kufr může otevřít. Celou dobu byl kufr zamčený zámky, ke kterým nikdo jiný neměl klíč, takže byl v bezpečí. Toto schéma má nevýhodu, že vyžaduje poslat si kufr třikrát tam, zpátky a tam a také samotné zamykání musí umožňovat, aby se zámky vzájemně neovlivňovaly a bylo je možné zamykat a odemykat v libovolném pořadí. Tím, že klíč k zamčení a odemčení daného zámku je ten stejný, nazývá se tento způsob symetrická kryptografie.

Existují však matematické postupy, díky kterým lze vytvořit dvojici klíčů, jeden se zveřejní a druhý se ponechá soukromý a tajný. Když vám někdo bude chtít poslat tajnou zprávu, vezme ji a zamkne vašim veřejným klíčem. Pouze váš soukromý klíč ji dokáže odemknout. Jeden z postupů, který to umožňuje, je založen na velkých prvočíslech, jejichž součin není vůbec jednoduché rozložit na původní součinitele. Pro malá čísla třeba 13 * 7 = 91 nám vyzkoušet několik čísel nezabere příliš dlouho, avšak když by se jednalo o čísla se stovkou cifer, už bude takový úkol trvat mnoho let i rychlým počítačům. Zkuste si třeba na kalkulačce zjistit z jakých prvočinitelů se skládá číslo 3233, nebo třeba číslo 65537 (je to prvočíslo, takže byste museli vyzkoušet čísla do 255).

Zkusme se teď zamyslet, kdy se nám hodí informace kódovat a kdy naopak šifrovat.

- sonda posílá fotky z povrchu Marsu,
- posílám vzkaz kamarádovi přes celou třídu,
- maminka mi posílá nákupní seznam,
- vojenský dron přijímá signál o tom kam letět,
- klíč od auta vysílá signál, aby se otevřelo.

Teď si vyměníte role a opět si zahrajeme přenosovou hru. Záškodníci se stanou rolemi A a B a z těchto se stanou záškodníci. Protože jste teď nabrali více zkušeností, budou také přenášená slova trochu delší. A a B pusťte se do domluvy způsobu komunikace, máte na to 1 minutu, poté budete mít 2 minuty na domluvu klíče.

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

Podíváme se, jak se vám dařilo v této druhé sérii a jak jste zvládli šifrovat, nabourávat a rozpoznávat.

Prosím podělte se o to, co vám fungovalo. Podařilo se vám do druhého kola zapracovat některý z postupů, o kterých jsme si říkali?

Je něco, co by vás o kódování a komunikaci nebo skutečných šifrách ještě zajímalo?

Pomůcky a materiál

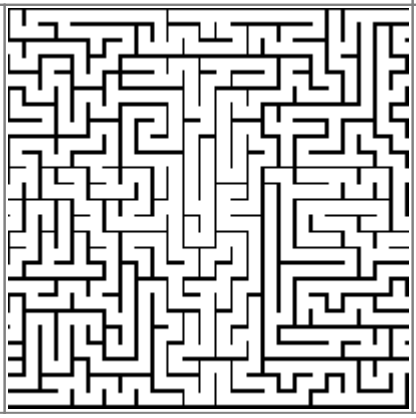
Položka	Počet	Popis
vytištěné šifry	1 od každého druhu/dvojice	úvodní šifry, úhel pohledu, bludiště
papíry	v počtu účastníků + rezerva	
tužky / psací potřeby	v počtu účastníků + rezerva	
tabulka bodování AB	1ks/dvojice	
tabulka bodování Z	1ks/dvojice	
seznam slov		
abeceda		
Morseova abeceda		
tabulka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

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

Zdroje

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

>> Jít na tuto stránku.