

Univerzita Karlova
Pedagogická fakulta
Katedra matematiky a didaktiky matematiky

BAKALÁŘSKÁ PRÁCE

Digitální kompetence ve výuce matematiky na SŠ se zaměřením na
bezpečnost na internetu

Digital Competencies in Mathematics education at Secondary Schools with a
Focus on Internet Safety

Lukáš Hylský

Vedoucí práce: Mgr. David Janda, Ph.D.

Studijní program: Matematika se zaměřením na vzdělávání (B0114A170007)

Odevzdáním této bakalářské práce na téma Digitální kompetence ve výuce matematiky na SŠ se zaměřením na bezpečnost na internetu potvrzuji, že jsem ji vypracoval pod vedením vedoucího práce samostatně za použití v práci uvedených pramenů a literatury. Prohlašuji, že jsem při její tvorbě nepoužil nástrojů umělé inteligence jiným způsobem, než je uvedeno ve vyjádření, které je součástí textu práce. Dále potvrzuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 13. 4. 2025

Chtěl bych poděkovat svému vedoucímu práce doktorovi Davidovi Jandovi za jeho cenný čas, užitečné rady a ochotu se kterou mi po celou dobu tvorby této práce vypomáhal.

ABSTRAKT

Bakalářská práce je zaměřená na zařazení digitálních kompetencí do výuky matematiky na středních školách. Na základě současného pojetí digitálních kompetencí, definovaných v kurikulárních dokumentech, vytvářím podklady pro projektovou výuku v rámci předmětu matematika, zaměřené na vybraná témata z bezpečnosti na internetu a ochrany osobních údajů. Práce je členěná do kapitol. V první kapitole se věnuji historii, vzniku a zařazení digitálních kompetencí do kurikulárních dokumentů. Dále jsou podle těchto dokumentů digitální kompetence rozřazeny a blíže popsány. Druhá kapitola obsahuje popis projektové výuky, její charakteristické znaky, výhody a nevýhody. Ve třetí kapitole vytvářím materiály k projektové výuce. Nejdříve se věnuji tématům hesel, jaká je náročnost prolomení, jak vytvořit silné heslo a jaká jsou rizika slabého hesla. Dále specifikuji některé kybernetické útoky společně se způsoby, jak se proti nim bránit. Následně jsou popsány vybrané typy šifrování, pomocí kterých jsou chráněna data na internetové síti. Nakonec zapojuji všechny tyto části do konkrétních bloků projektové výuky, které lze využít jako podklady ve výuce matematiky. Cílem je vytvořit sadu aktivit, které propojují teoretické poznatky z těchto oblastí s matematickým obsahem a umožňují jejich aplikaci v rámci projektové výuky. Výsledné materiály slouží jako konkrétní podklady pro pedagogy, kteří chtějí efektivně rozvíjet digitální kompetence svých žáků přímo v hodinách matematiky, a zároveň zvyšovat jejich povědomí o rizicích digitálního prostředí.

KLÍČOVÁ SLOVA

Digitální kompetence v matematice, ochrana osobních údajů, bezpečnost na internetu, projektová výuka

ABSTRACT

The bachelor's thesis focuses on the inclusion of digital competencies in mathematics teaching in secondary schools. Based on the current concept of digital competencies, defined in curriculum documents, I create materials for project-based learning within the subject of mathematics, focused on selected topics from Internet security and personal data protection. The work is divided into chapters. In the first chapter, I discuss the history, origin and inclusion of digital competencies in curriculum documents. Furthermore, digital competencies are classified and described in more detail according to these documents. The second chapter contains a description of project-based learning, its characteristics, advantages and disadvantages. In the third chapter, I create materials for project-based learning. First, I address the topics of passwords, how difficult it is to crack, how to create a strong password and what are the risks of a weak password. I also specify some cyber attacks together with ways to defend against them. Subsequently, selected types of encryption are described, with which data on the Internet are protected. Finally, I integrate all these parts into specific blocks of project-based learning that can be used as materials in mathematics teaching. The goal is to create a set of activities that connect theoretical knowledge from these areas with mathematical content and enable their application within project-based learning. The resulting materials serve as specific materials for educators who want to effectively develop their students' digital competences directly in mathematics lessons, while at the same time raising their awareness of the risks of the digital environment.

KEYWORDS

Digital competencies in mathematics, personal data protection, internet safety, project-based learning

Obsah

Úvod	7
1 Digitální kompetence.....	8
1.1 Historie, vznik a zařazení do výuky	8
1.2 Rozdělení digitálních kompetencí	9
1.2.1 Využití a zapojení	10
1.2.2 Informace a komunikace	11
1.2.3 Tvorba a vyjádření.....	11
1.2.4 Efektivita a inovace	12
1.2.5 Přínos a vývoj	12
1.2.6 Bezpečnost a etika	13
2 Projektová výuka	14
3 Materiály k projektové výuce	16
3.1 Hesla a náročnost jejich prolomení	16
3.2 Tvorba bezpečného hesla.....	16
3.3 Kybernetické útoky na účty chráněné heslem	19
3.4 Ochrana hesel a šifrování	21
3.5 Osnova projektové výuky	23
3.5.1 Motivační aktivity	23
3.5.2 Kybernetické útoky.....	26
3.5.3 Šifrování a prolamování jednoduchých šifer.....	27
3.5.4 Závěrečná hra – Útěk z hackerského doupěte	31
Závěr.....	37
Seznam použitých informačních zdrojů	38

Úvod

Žijeme v době velkého technologického rozvoje, kde internet představuje jeden z nejdůležitějších nástrojů komunikace moderní doby. Dokázal propojit miliardy lidí a zařízení po celém světě. Jako všechny pokroky, nese i tento řadu nevýhod a rizik a s těmi vzrůstá i tlak na vzdělání v oblasti bezpečnosti na internetu ve školách.

Ve školách je proto do výuky předmětů zahrnuto sedm klíčových kompetencí. Jednou z nich je digitální kompetence, jež připravuje žáky a učí je, jak zacházet s digitálními technologiemi včetně bezpečnosti.

Motivací pro dané téma je snaha ukázat žákům, že je třeba mít se na pozoru, pokud cokoliv dělám v internetovém prostředí, a přispět k rozvoji digitálních dovedností žáků z hlediska jejich schopnosti se bezpečně a eticky pohybovat v internetovém světě.

Tato práce se zaměřuje na zařazení problematiky bezpečnosti a ochrany osobních dat do hodin matematiky v rámci projektové výuky. Konkrétně je zaměřena na téma ochrany osobních údajů pomocí hesel, šifrování a ochranu před kyberútoky. Cílem práce je vytvořit úlohy a aktivity zaměřené na tato témata vhodné pro projektovou výuku matematiky (např. formou projektového dne), ale i s možným použitím přímo v hodinách matematiky.

První kapitola se zaměřuje na seznámení s digitálními kompetencemi. Je uvedeno něco málo z historie a dále jsou rozděleny do šesti kategorií.

Druhá kapitola obsahuje základní charakteristiku a principy projektové výuky.

Ve třetí kapitole jsou již vypsány zásady ochrany osobních údajů na internetu. Následuje propojení těchto principů s matematikou. Tato část slouží jako podklad projektové výuky a obsahuje úlohy a aktivity. Ty jsou detailně popsány, jak by s nimi učitelé matematiky měli ve výuce zacházet.

K celé problematice se často vyjadřuje mnoho různých institucí formou online materiálů, kurzů a podobně. Z toho důvodu je třeba brát některé zdroje s rezervou.

1 Digitální kompetence

V této části se práce věnuje objasnění významu a funkce digitálních kompetencí ve výuce. Dále jsou rozděleny do několika odvětví a charakterizovány.

1.1 Historie, vznik a zařazení do výuky

V dnešní době, kdy technologie stále více pronikají do našich životů, se stává nezbytným, abychom se jim učili rozumět již od útlého věku. S Evropským doporučením o klíčových dovednostech z roku 2006, byly digitální kompetence uznány jako jedna z osmi klíčových kompetencí¹ potřebné pro celoživotní učení (Ferrari et al., 2013). Důsledkem tohoto doporučení, vznikl projekt DIGCOMP. Iniciovala ho Evropská komise a měl za cíl vytvořit jednotný rámec pro digitální gramotnost. Na studii se podílelo devadesát pět expertů z přibližně čtyřiceti zúčastněných stran. Od roku 2013 se tak můžeme seznámit s vypracovaným rámcem pro výuku digitálních kompetencí. Ten se stal podkladem pro následný rozvoj a implementaci v jednotlivých zemích.

V roce 2018 byl Evropský rámec již z velké části přeložen do českého jazyka. Ministerstvo školství, mládeže a tělovýchovy (zkr. MŠMT) následně přidalo v roce 2021 do kurikulárních dokumentů novou klíčovou kompetenci. „Klíčové kompetence představují soubor vědomostí, dovedností, schopností, postojů a hodnot, které jsou důležité pro osobní rozvoj jedince, jeho aktivní zapojení do společnosti a budoucí uplatnění v životě.“ (MŠMT, 2021a, s. 8) V rámcovém vzdělávacím programu (zkr. RVP) pro školy se vyskytovalo šest klíčových kompetencí. Byly to tyto: kompetence k učení; kompetence k řešení problémů; kompetence komunikativní; kompetence sociální a personální; kompetence občanská; kompetence pracovní v RVP pro základní školy (MŠMT, 2021b) a kompetence k podnikání pro střední školy a gymnázia (MŠMT, 2021a). Sedmá přidaná kompetence je kompetence digitální.

¹ Nejedná se o klíčové kompetence tak, jak je známe z RVP. Jsou to komunikace v mateřském jazyce, komunikace v cizím jazyce, matematická kompetence, základní kompetence ve vědě a technice, digitální kompetence, učení se k učení, sociální a občanské kompetence, kompetence k podnikání. Průnik s klíčovými kompetencemi je zejména v kompetencích digitální, k podnikání, sociální a občanské.

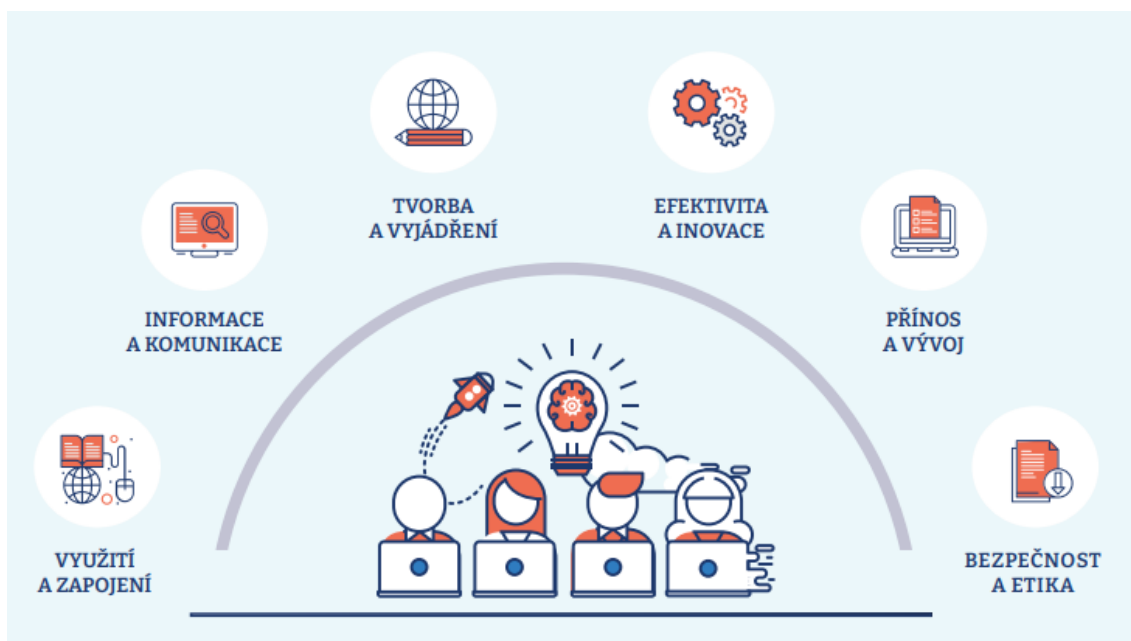
„Znamé tvrzení praví, že dnes je úkolem učitelů vést žáky k tomu, aby byli schopni nástroji, které nebyly ještě vynalezeny, řešit problémy, o kterých zatím nikdo netuší, že problémy jsou.“ (Altmanová et al., 2010, s. 56) Konkrétně tento problém lze interpretovat jako jednu z dílčích kompetencí digitální kompetence, jež má za úkol naučit žáky, jak se zorientovat v neznámých systémech.

Klíčové kompetence by měly být zastoupeny ideálně ve všech vyučovaných předmětech, i když míra zastoupení se jistě může lišit. Některé předměty jsou pro konkrétní kompetence vhodnější než jiné. Každý předmět má své specifické cíle a zaměření, a proto míra zapojení digitální kompetence do dané výuky může značně lišit. Matematika a informatika jsou pro ně však jako stavěné. Úzkou souvislost zmiňuje například Bendl (2023): „Digitální technologie otevírají možnosti ke konstruktivistickému pojetí výuky matematiky a k její individualizaci. Interaktivní simulace důkazů a názorné představení algoritmů vede k pochopení principů matematiky a jejich ukotvení.“ (Bendl, 2023)

1.2 Rozdělení digitálních kompetencí

Abychom mohli říct, že jsme relativně digitálně kompetentní², musíme podle záměru popsaného výše, ovládat dílčí klíčové kompetence spadající do různých oblastí, viz Obrázek 1. Jednotlivá témata se vzájemně prolínají, a tak je někdy těžké je od sebe řádně oddělit. Spíše než jako soupis nutných znalostí lze vnímat podobné zdroje jako sumář témat, kterým je potřeba věnovat patřičnou pozornost.

² Obecně považuji za problematický dichotomický pohled, podle kterého rozhodujeme, zda je člověk digitálně kompetentní nebo nikoliv. Spíše lze na tuto problematiku nahlížet tak, že sbíráme zkušenosti dílčích kompetencí a tím přispíváme k něčemu, co pak nazýváme digitální kompetencí. I toto je však měřitelné velmi problematicky, pokud vůbec.



Obrázek 1: Infografika digitální kompetence (Národní pedagogický institut České republiky, 2021)

V následujícím textu rozliším digitální kompetenci do šesti odvětví dle schématu na Obrázku 1. Každá část obsahuje analýzu dané tematiky v kontextu současného RVP pro gymnázia. Následuje komentář v kontextu matematiky.

1.2.1 Využití a zapojení

Odvětví digitální kompetence dle RVP: „Žák ovládá potřebnou sadu digitálních zařízení, aplikací a služeb, využívá je při školní práci i při zapojení do veřejného života; digitální technologie a způsob jejich použití nastavuje a mění podle toho, jak se vyvíjejí dostupné možnosti a jak se mění jeho vlastní potřeby“ (MŠMT, 2021a, s. 11)

Využívání digitálních technologií nesporně patří k dnešní době. Ve výuce matematiky se nám hodí mnoho nástrojů. Například GeoGebra je jednoduchý, volně dostupný program, s jehož pomocí se dá názorně vyučovat mnoho matematických témat. Využití má GeoGebra ve výuce funkcí, planimetrie, stereometrie nebo třeba analytické geometrie. Nejedná se však pouze o softwarové nástroje. Spadá sem i využívání kalkulačků.

V dnešní době je využívání digitálních technologií naprosto běžnou záležitostí, a to i v rámci matematiky libovolného stupně vzdělávání. „Při řešení reálných problémů žádný odborník

nepočítá na papíře, nekreslí si na čtverečkovaný papír grafy. Počítačové algebraické systémy (CAS – Computer Algebra Systems) jsou již více než půl století neodmyslitelnou součástí aplikované matematiky. “ (Bendl, 2023)

1.2.2 Informace a komunikace

Odvětví digitální kompetence dle RVP: „Žák, získává, posuzuje, spravuje, sdílí a sděluje data, informace a digitální obsah v různých formátech; k tomu volí efektivní postupy, strategie a způsoby, které odpovídají konkrétní situaci a účelu.“ (MŠMT, 2021a, s. 11)

Jedním z aktuálně nejdůležitějších témat v této oblasti jsou dezinformace, je proto potřeba s tím ve výuce pracovat. Gilbert (2017) ve své studii ukazuje, že práce s informacemi je považována za velmi důležitou a žádanou i v následujícím pracovním životě. Je třeba umět vyhodnocovat informace a kriticky je posuzovat. Dalším tématem z daného odvětví je schopnost komunikovat s ostatními prostřednictvím digitálních technologií a implementovaných komunikačních platforem.

Přesah do výuky matematiky můžeme dnes pozorovat každý den. Žáci musí při samostatném studiu matematiky vyhodnocovat pravdivost různých zdrojů (včetně zdrojů založených na jazykových modelech AI), bylo by možné (a vhodné) se tomuto tématu v rámci výuky věnovat explicitně, např. zorientovat se v množství předem vybraných informací sdílených v rámci MS Teams či Google Classroom.

Toto odvětví bylo hojně využíváno během distanční výuky za pandemie COVID-19.

1.2.3 Tvorba a vyjádření

Odvětví digitální kompetence dle RVP: „Žák vytváří, vylepšuje a propojuje digitální obsah v různých formátech; vyjadřuje se za pomoci digitálních prostředků.“ (MŠMT, 2021a, s. 11)

Současný stav technologií nám otevřel dveře ke kreativitě. Můžeme nyní využívat mnoha grafických i jiných programů na tvorbu libovolného obsahu. „Digitální technologie proces tvorby jako takové významně proměnily, co se týče forem (učitel dnes může pracovat s chatboty, nelineárními interaktivními příběhy, reálnými daty, může tvořit infografiky či programovat) i jejich variability.“ (Černý, 2023, s. 37)

Toto téma není vyhrazeno pouze pro tvorbu nového obsahu, ale také na úpravu již stávajícího. Cílem je naučit se pracovat s obsahem v různých formátech a s využitím různých digitálních technologií (Růžicková et al., 2020). V rámci matematiky můžeme vést žáky k využívání tabulkových editorů jako je MS Excel, které jsou vhodné například na statistické vyhodnocování určitých jevů nebo vypracování protokolů k záznamům pozorování či měření. Dále sem také patří programy na vytváření 3D grafiky, 3D tisk, geometrická a výpočetní prostředí nebo využívání programovacích jazyků. Jistě by ale bylo možné zařadit i další oblasti spadající mezi digitální technologie.

1.2.4 Efektivita a inovace

Odvětví digitální kompetence dle RVP: „Žák navrhuje prostřednictvím digitálních technologií taková řešení, která mu pomohou vylepšit postupy či technologie; dokáže poradit s technickými problémy.“ (MŠMT, 2021a, s. 11)

Toto téma se velmi prolíná s předchozími. Snahou je ukázat žákům, že technologie jsou v dnešní době pro práci nezbytné. Nejedná se pouze o zdroj zábavy, nýbrž o způsob, jak si ulehčit práci a dosáhnout lepších výsledků. Chceme-li si například ohlídat termín odevzdání práce, můžeme si nastavit v mobilním telefonu upomenutí do kalendáře, které se nám připomene i týden předem, abychom měli dostatek času na vypracování. Asi aktuálně nejmodernějším způsobem inovace jsou nástroje využívající umělou inteligenci. Tyto nástroje nám umožňují rychle a efektivně pracovat. Když si potřebujeme rychle najít nějaké informace, stačí se zeptat AI. Ta nám během sekund vyhodí odpověď. Jelikož se ale stále jedná o technologii v rozvoji, je třeba jí brát s velkou rezervou. Není nutné tyto inovativní technologie využívat, avšak jejich používání nám velmi zefektivňuje naši práci.

1.2.5 Přínos a vývoj

Odvětví digitální kompetence dle RVP: „Žák se vyrovnává s proměnlivostí digitálních technologií a posuzuje, jak vývoj technologií ovlivňuje různé aspekty života jedince a společnosti a životní prostředí, zvažuje rizika a přínosy.“ (MŠMT, 2021a, s. 11)

S rychlým vývojem se mění i možnosti, které digitální technologie mohou poskytnout vzdělávání. Technologie si jsou vzájemně podobné v obecných funkcích, ale liší se v detailech fungování. K základnímu porozumění nových softwarů nám pomůže znalost

řady dalších, jelikož právě obecné funkce jako jsou otevření či vložení souboru jsou generalizované. Jsme nuceni se neustále setkávat s novými technologiemi a musíme se v nich zorientovat. Patří sem i kritické posouzení, jak vývoj technologií ovlivňuje různé aspekty života jedince, společnosti a životní prostředí. Dále pak zvážení přínosů a rizik. (MŠMT, 2023)

1.2.6 Bezpečnost a etika

Odvětví digitální kompetence dle RVP: „Žák předchází situacím ohrožujícím bezpečnost zařízení i dat, situacím ohrožujícím jeho tělesné a duševní zdraví; při spolupráci, komunikaci a sdílení informací v digitálním prostředí jedná eticky, s ohleduplností a respektem k druhým.“ (MŠMT, 2021a, s. 11)

Bezpečné zacházení s technologiemi je důležité, protože může mít bezprostřední dopad na život jedince. Nejde však pouze o ochranu osobních dat, bankovního účtu nebo přístupu na sociální sítě. Pod toto téma spadá například i ochrana fyzického a duševního zdraví, které mohou být ohroženy třeba nadměrným množstvím informací. „Informací je na internetu velké množství, možná více, než bychom potřebovali. Proto se někdy hovoří o informační záplavě.“ (Černý, 2023, s. 31) Tento přebytek informací může být zahlcující, zvláště pak když se na nás takto hrnou negativní zprávy. Pocit zahlcení je obvykle spojován se ztrátou kontroly nad situací a někdy i s pocitem přemožení. V krajním případě může vést až k poškození zdraví (Bawden & Robinson, 2009).

Důležité je také brát ohledy na ostatní, jelikož naše aktivita na internetu může mít daleko větší dosah, než jsme původně zamýšleli. Navíc je třeba si uvědomovat, že v moment, kdy se něco přidá na internet, stává se to potažmo majetkem všech. Takové věci se z internetu již nejspíše nikdy neztratí a vždy tam budou někde existovat. Altmanová et al. (2010) tvrdí, že pokud bude ve výuce opomíjen kyberprostor, svět sociálních sítí a problematika on-line bezpečí, půjde o zanedbání vzdělávacího obsahu.

Propojení tohoto tématu s matematikou je ústředním tématem této práce a je rozepsáno v dalších kapitolách.

2 Projektová výuka

Tato kapitola se krátce věnuje vysvětlení a popisu projektové výuky.

Projektová výuka je vyučovací metoda, která je obzvláště vhodná pro dosažení trvanlivějších kontextových výsledků u žáků (Gary, 2015). Nejedná se o běžnou metodu učení. Jak název napovídá, jedná se o projekt, na kterém se s žáky pracuje. Časové rozmezí může být různé od pár hodin až po několik dní. Během této doby učitel zastává spíše roli průvodce než roli řídící.

Projektová výuka se zaměřuje na dané téma nebo oblast které se věnuje. Online materiál od Zormanové (2012), vytvořený za účelem informování čtenářů o základním principu projektové výuky v tomto kontextu uvádí, že: „Charakteristickým znakem projektové výuky je cíl, který je představován určitým konkrétním výstupem, tj. výrobkem, praktickým řešením problému, ...“ Jedná se o složitý pracovní úkol, na kterém se mají žáci společně podílet a vyřešit otázky tématu. Důraz se klade na vlastní iniciativu a zájem o téma. Tento přístup je založen na předpokladu, že vlastním zkoumáním problému a bádáním nad řešením se totiž učivo mnohem lépe uchytí v paměti. Projekt má smysl, pokud splňuje dvě kritéria. Za prvé, studenti musí vnímat svou práci jako osobně významnou, jako úkol, na kterém jim záleží a který chtějí vykonat dobře. Za druhé, smysluplný projekt naplňuje vzdělávací účel. Dobře navržené a správně realizované projektové vyučování je smysluplné v obou těchto ohledech (Larmer & Mergendoller, 2010).

Hlavním přínosem projektové výuky je zvýšená motivace žáků. Témata se proto volí s ohledem na cílovou skupinu žáků nebo společně se žáky samotnými. Se zvýšeným zájmem se výuka stává zábavnější a zvyšuje se tak i míra informací, které si cílová skupina odnese. Dalšími přínosy je například rozvíjení samostatnosti žáka, případně spolupráce v týmu, rozvíjení kreativity, kritického myšlení nebo organizační dovednosti. „Projektová výuka také napomáhá k začleňování mezipředmětových vazeb a průřezových témat do výuky.“ (Zormanová, 2012)

Projektová výuka má i několik nevýhod. Řešení projektů je pro žáky časově náročné a mnohdy nemají potřebné kompetence. Stejně tak pro učitele je příprava projektu velmi

časově náročná. Je totiž potřeba důkladně prozkoumat dané téma a zmapovat spoustu aspektů jeho obsahu. Důležité je myslet na to, že projektová výuka nenahrazuje normální výuku. Žáci totiž nemají dostatek prostředků na zvládnutí projektové výuky v celé šířce vzdělávání. Z tohoto důvodu by projektová výuka měla sloužit spíše jako doplněk tradiční výuky.

3 Materiály k projektové výuce

3.1 Hesla a náročnost jejich prolomení

Snad každý se již setkal s vymyšlením hesla. Nakonec každý chytrý mobilní telefon s přístupem na internet si požaduje propojení s vlastním účtem, který je chráněn heslem. Sociální sítě, internetové bankovníctví i samotná zařízení vyžadují nějaký způsob uzamčení. Člověk se v průměru přihlašuje 40krát až 110krát za dva týdny (Hayashi & Hong, 2011). Z těchto dat lze hrubě odhadnout, že přibližný počet přihlašování za jeden den, se pohybuje někde mezi pěti a šesti přihlášeními. Je možné, že na některé účty máme uložená hesla a když je zapínáme, automaticky jsme přihlášení bez nutnosti zadávat heslo. I tak ale je účet zabezpečen heslem a je nutné se přihlašovat. „Hesla představují první linii ochrany před neoprávněným přístupem k online účtům, zařízením a souborům.“ (Microsoft, n. d.)

V následujících podkapitolách je vysvětlen postup pro tvorbu dostatečně silného hesla, jsou uvedeny a specifikovány některé kybernetické útoky společně s tipy, jak se proti nim chránit. Dále je vysvětleno, jak funguje ochrana hesel na internetových serverech pomocí šifrování. Následují praktické podklady pro projektovou výuku matematiky, zaměřené na téma hesel. Pomocí kombinatoriky je ukázáno, jak důležité je používat složitější hesla k zabezpečení zařízení a účtů.

3.2 Tvorba bezpečného hesla

Mnohé stránky a aplikace si již v dnešní době většinou žádají dostatečně silné heslo, a pokud zadané heslo nesplňuje požadavky, stránka nám neumožní registraci. Častým požadavkem je mít v heslu nějaké malé a velké písmeno, číslici a speciální znak. Má to ale své opodstatnění? S každou přidanou znakovou sadou přibývá počet možných kombinací. Snaha prolomit heslo hrubou silou se při omezeném počtu možných zadání hesla pak stává prakticky nemožná. Jedná se o náhodné, či systematické zkoušení všech možných hesel popořadě, dokud se nenarazí na to správné. Pokud použijeme všechny výše vyjmenované sady na pětimístné heslo, počet kombinací je několik miliard. Uhádnutí takového hesla se pak značně komplikuje.

Zviran a Haga (1999) ve své studii využili dotazník ohledně tvorby a charakteristiky hesel. Dotazník vyplnilo téměř tisíc jedinců. Ukázalo se, že téměř polovina dotazovaných využívá hesla v délce pět a šest znaků. Dále pak téměř osmdesát procent svá hesla nikdy nemění, méně než jedno procento uživatelů používá ve svém heslu speciální znaky a téměř osmdesát procent v hesle využívá nějaká osobní data významná pro daného uživatele. Výsledky dotazníku se pochopitelně s větším nástupem digitálních technologií do běžného života mění. Dle výzkumu po sedmi letech se situace místy o něco zlepšila. Shannon (2006) uvádí dotazník pro tři sta patnáct respondentů. Heslo si nikdy nemění skoro padesát tři procent a speciální znaky využívá téměř třicet procent uživatelů. Významné údaje stále využívá přibližně sedmdesát tři procent, což moc velké zlepšení není. S rostoucími požadavky na hesla však také roste obtížnost jejich zapamatování si. Proto si spousta uživatelů usnadňuje zapamatování hesel pomocí významných údajů, nebo si hesla někam napíší.

Je opravdu důležité vytvářet silná hesla. Při využití slabého hesla necháváme své údaje téměř nechráněné. Ačkoliv to může být lákavé, použití jednoduchého hesla za možné následky nestojí. Záleží také na účtu, který chráníme. Pokud máme účet například pro odebrání novin z nějakého oboru, nezáleží nám na jeho bezpečnosti tak moc, jako když vytváříme heslo k bankovnímu účtu. Další rizikový faktor je zadávání stejných hesel do více různých aplikací. Lidé mají totiž často tendenci opakovat určitá hesla, aby si usnadnili jejich zapamatování. Po odhalení jednoho hesla může získat útočník přístup k mnoha dalším aplikacím a napáchat tak mnohonásobně víc škody. Mezi jednoduchá, často používaná a snadno prolomitelná hesla patří dle webu Weakpass (n. d.) například následující: 123456; password; qwerty; 111111; dragon; football; letmein.

Dobrým příkladem toho, jaký obrovský dopad může mít jednoduché heslo je případ z dubna roku 1994. Útočníkem byl šestnáctiletý mladík z Velké Británie, který se naboural do Pentagonu, ústřední budovy ministerstva obrany Spojených států amerických. Mladík nejdříve získal nízko-úrovňový přístup k počítači laboratoře, pomocí výchozího hesla pro návštěvy. Když byl uvnitř systému stáhnul si zabezpečený soubor s hesly do počítače. Poté na něj pustil program, který jej bombardoval padesáti tisíci slovy za sekundu. Tento útok by zmařilo, kdyby všichni s přístupem k počítači dodržovali předpisy a využívali silná hesla. Jeden z poručíků však použil jako heslo jméno své fretky Carmen. Právě toto heslo bylo

programem odhaleno a útočník tak získal plný přístup k vysoce tajným a důvěrným dokumentům. Útočník se poté naboural do systému více než sto padesátkrát. Během jednoho svého pátrání v systému se pokusil dostat k informacím o jaderných zařízeních v Koreji. Mladík byl později odhalen, vystopován a zatknut (Ungoed-Thomas, 1998). V tomto případě selhalo zabezpečení heslem hned dvakrát. Nejdříve bylo odhaleno jednoduché výchozí, nejspíše i často používané heslo s nízkým zabezpečením. Důsledkem toho ale došlo k možnosti odhalení již vysoce důležitého hesla. Jelikož ale i toto heslo bylo velmi slabé, útočník k němu získal přístup. Důsledky tohoto nedostatečného zabezpečení mohly být skutečně katastrofické v globálním měřítku. Běžný člověk se ale v současné době s takto promyšlenými útoky téměř nesetká. Výjimkou mohou být třeba útoky v souvislosti na bankovní služby.

V současné době se již více hledí na správné zabezpečení. Mnohé weby jako například Google, Steam nebo Paypal se nespolehlí pouze na svědomitost svých uživatelů. Umožňují možnost vícefázového ověřování nebo jiné kontroly osoby, která se přihlašuje. Zabezpečení spočívá v tom, že po přihlášení je třeba odlišným způsobem dokázat, že se přihlašuje skutečně vlastník účtu. Častým ověřením je zaslání přístupového kódu prostřednictvím e-mailu, SMS zprávy nebo potvrzení přímo v mobilní aplikaci. Navíc k tomu ještě některé společnosti zasílají informační zprávu o přihlášení se z nového, dosud neznámého místa. Další způsob, který využívají například mobilní telefony nebo platební karty je zablokování účtu po určitém počtu nesprávných pokusů o přihlášení nebo zadání PIN kódu. V takovém případě je poté potřeba navázat kontakt, někdy i osobní, se společností a požádat o odblokování a resetování přihlašovacích údajů.

Jaké jsou tedy základní pravidla pro udržení si bezpečného hesla? Nejdříve vytvoříme heslo dostatečné délky (alespoň 8 znaků), na které použijeme velká a malá písmena, číslice a speciální znaky. Dobré je použití neexistujícího slova nebo kombinace písmen. Pro každý účet používáme ideálně unikátní heslo. Za žádných okolností NIKDY nikomu své heslo nesdělujeme. Pro další ochranu můžeme hesla čas od času měnit. Jsme ostražití vůči podezřelým zprávám a chování na internetu, jelikož nikdy nevíme, kdy se můžeme stát cílem kybernetického útoku.

3.3 Kybernetické útoky na účty chráněné heslem

V předchozí části byl zmíněn pouze okrajově útok hrubou silou. Konark (2013) uvádí, že se jedná o útok principu pokus omyl. Útočník si může nasbírat nějaké informace o uživateli jako je například jméno, číslo auta, číslo pokoje, jména dětí atd. Tyto údaje pak náhodně zkouší v různých kombinacích a úpravách zadávat jako hesla k uživatelskému účtu své oběti. Takováto snaha může trvat hodiny, dny, měsíce nebo i roky. Tuto práci značně usnadňují počítačové programy, které dokážou vyzkoušet obrovské množství možností během krátkého času. Jedním ze způsobů ochrany je limitovaný počet nesprávných pokusů. Po vypotřebování se účet uzamkne buď na nějakou určitou dobu, nebo dokud jej neodblokuje administrátor. Dalším způsobem je využívání bezpečnostního systému CAPTCHA. Jedná se o akronym z anglického: Completely Automated Public Turing test to tell Computers and Humans Apart. V překladu jde o plně automatizovaný veřejný Turingův test k odlišení počítačů a lidí. Jedná se o program, který se spustí po určitém počtu neplatných pokusů o přihlášení. Před každým dalším pokusem je zapotřebí správně vyřešit daný úkol. Tento úkol je relativně jednoduchý na splnění pro člověka, ale složitý pro počítačový program (Konark, 2013). CAPTCHA typů je mnoho. Asi nejčastěji je využíván textový, ve kterém je za úkol zadat krátký zobrazený text. Tento text je nějakým způsobem znetvořen, aby byl hůře čitelný. Po každém nesprávném pokusu se text vygeneruje nový, a proto je třeba jej zadat správně na první pokus. Dalším hojně používaným úkolem je výběr obrázků nebo jeho částí dle požadovaných parametrů. Již méně využívané jsou videa, audio záznamy nebo skládačky (Kiranjot & Sunny, 2014). Počítačové programy musí mít tedy navíc nějakým způsobem ošetřenou zpětnou vazbu k této ochraně. Tím se značně komplikují jejich funkce a složitost daného programu. Hlavní ochrana proti tomuto útoku je ale stále na straně uživatele, který si zvolí dostatečně dlouhé heslo s využitím vícero znakových sad.

Variací útoku hrubou silou je takzvaný slovníkový útok. „Tyto útoky se snaží prolomit heslo zadáním každého slova ve slovníku, používáním odvozenin těchto slov s nahrazováním znaků a alfanumerických znaků a používáním uniklých hesel a klíčových frází.“ (Microsoft, n. d.) Slovníkový útok lze odvrátit využíváním neexistujících slov a kombinací písmen v heslech. Dále na něj platí výše zmíněné opatření, stejně jako u útoku hrubou silou.

Složitě heslo je velmi problematické prolomit hrubou silou, a tak se útočníci soustředí na získání hesla jiným způsobem. Nejčastějším způsobem je phishing. „Phishing se jedna z technik kybernetických podvodů sociálního inženýrství, jejímž cílem je získat od uživatelů jejich důvěrné, nejčastěji přihlašovací, údaje.“ (Digitální a informační agentura, 2025) Útočníci se proto vydávají za legitimní společnosti a snaží se tak vyvolat v uživateli důvěru. Buď požadují přímo údaje, nebo nabádají k rozkliknutí odkazu. Ten může vést na přesnou kopii internetové stránky společnosti za kterou se vydávají, z té pak získají údaje poté, co se uživatel pokusí přihlásit. Druhá možnost je, že se z odkazu přímo stáhne virus, který dané údaje odcizí. Základ obrany proti metodám phishingu tvoří zdravý selský rozum. Uživatel by si měl vždy v duchu odpovědět na prostou otázku: „Opravdu by mi banka (nebo jiná podobná instituce) posílala nešifrovaný e-mail a chtěla po mně takovéto důvěrné údaje?“ (NÚKIB, 2015) Samotný selský rozum je však skutečně pouze základem ochrany. Mezi podezřelé znaky se řadí krkolomná čeština, zvláštní otázky nebo požadavky, nepřesná URL adresa, ve které je chyba, co vypadá jako překlep nebo webové stránce chybí bezpečnostní certifikát.

Dalším často využívaným způsobem je malware virus. Jedná se o škodlivý software, který ohrožuje uživatele internetu. Po aktivaci se šíří internetem a způsobuje závady v operačních systémech, které mohou mít za cíl odcizení údajů. Malware virus využívá zranitelností v počítačových aplikacích a systémech ke zneužití dat pomocí škodlivého kódu (Razak et al., 2016) Virus lze získat mnoha způsoby. Rozkliknutím neznámých podvodných odkazů, zapojováním nalezených USB disků do zařízení, skenováním neověřených QR kódů a spoustou dalších. Prevencí je tedy být ostražitý vůči podezřelým odkazům a zprávám, jako je například: Ahoj, nejsi to ty na tomto videu? Pro ochranu existují antivirové programy, které slouží k detekci hrozeb, již získaných virů a jejich následné vymazání.

Kybernetických útoku je mnoho. Výše zmíněným příkladům se lze z naší strany chránit. Existují ale útoky, které my nemůžeme ovlivnit ani jim zabránit. Jsou to útoky na webové stránky, kam své údaje zadáváme.

3.4 Ochrana hesel a šifrování

Po online registraci účtu se naše přihlašovací jméno a heslo zpravidla uloží na server společnosti, ke které jsme si vytvořili účet. Pokud se hackeři dostanou do databáze, mají možnost se podívat na uložená hesla. Uvidí však pouze zašifrované kódy. Na ochranu hesel existuje takzvaná hashovací funkce. Ta slouží k zašifrování textového řetězce do kódovaného řetězce, kterému se říká hash. „Kryptografická hashovací funkce se využívá především pro autentizaci dat, integritu nebo při použití digitálních podpisů.“ (Ošťádal, 2012, s. 1)

Hashovací funkce má řadu výhod oproti jiným způsobům šifrování. K některým typům šifrování je potřeba konkrétní klíč. Informace se s pomocí tohoto klíče zakóduje a následně ji lze s využitím (stejného nebo jiného) klíče také rozkódovat.

Například šifrování RSA³, které je hojně používáno na internetových stránkách nebo v bankovníctví, využívá veřejného a soukromého klíče. Veřejný klíč je volně dostupný a slouží k zašifrování. Soukromý klíč pak zprávu dešifruje. RSA šifra funguje na základě součinu prvočísel. Vynásobit dvě velká prvočísla je jednoduché. Přijít ale na to, ze kterých prvočísel se součin skládá je velmi časově náročné a prakticky téměř nemožné. „K zašifrování zprávy stačí znalost součinu, zatímco k jejímu dešifrování je potřebná znalost jednotlivých prvočísel.“ (Zajíčková et al., n. d., s. 1) Právě jednotlivá prvočísla slouží k vytvoření dešifrovacího soukromého klíče. Ve skutečnosti se využívá číslo délky alespoň 2048 bitů (Barker, 2020). Takové číslo je dlouhé 617 cifer. Odhadování dvou prvočísel, ze kterých je takto dlouhé číslo složené je tedy skutečně až příliš časově náročné. Potenciální útočník nezná původní prvočísla. Nedokáže si tak vytvořit dešifrovací klíč pomocí kterého by získal citlivé údaje.

Na rozdíl od RSA, hashovací funkce žádný takový klíč nemá. Pro hashovací funkci proto také prakticky neexistuje způsob, jak se vrátit od neznámého hashe k původnímu zakódovanému textu. Hashování je totiž jednosměrná funkce, tedy neexistuje inverzní funkce. To znamená, že se dá zpráva zakódovat, avšak již není způsob, jak jí rozluštit nazpět.

³ RSA je pojmenováno podle svých autorů Rivest, Shamir a Adleman, kteří jej zveřejnili v roce 1977.

Jedním z důvodů je to, že při hashování se ztrácí informace o původním kódovaném řetězci. Příkladem jsou například kolize, o kterých je něco málo napsáno níže.

Hashování má několik pravidel. Dva totožné řetězce se zakódují do stejného hashe. Řetězec libovolné délky se zašifruje do hashe pevně dané délky. Z této podmínky však vyplívá problém hashovacích funkcí. Jelikož se různé řetězce libovolných délek vždy kódují do řetězce pevné délky, nutně musí dojít ke kolizím. Nelze totiž nekonečné množství řetězců nacpat všechny do konečného počtu hashů. Jednou z hashovacích funkcí známou svými kolizemi je MD5. Jedná se o hashovací funkci z rodiny MD (Message Digest), jejímž autorem je R. Rivest z RSA Data Security Inc. (Lianhua & Xingquan, 2017). Nalezení kolizí hashovací funkce MD5 se věnoval i český projekt. Klíma (2005) ukázal, že k hledání kolizí lze využívat i domácí počítač již v roce 2005. Ačkoliv jsou kolize při běžném používání extrémně vzácné, stále se vyvíjejí nové funkce, u kterých je pravděpodobnost kolize ještě nižší. Jednou z možností je například prodlužování výsledného hashe.

Při kódování pomocí hashovacích funkcí se využívá ještě další stupeň ochrany, kterým je salting, jedná se o přidání dodatečného řetězce. Přidání náhodného dodatečného řetězce, dodá k heslu prvek náhodnosti. To probíhá tak, že při vytvoření hesla se k němu přiřadí náhodně generovaný řetězec znaků a teprve potom se heslo zahashuje. To zaručuje, že v případě dvou stejných hesel jsou jejich hashe rozdílné. Toto zabezpečení chrání hesla před potenciálními útočníky. Útočníci si totiž můžou předem připravit tabulku hashů známých a často používaných hesel a jejich upravených variant. Tyto tabulkové hashe by pak již pouze stačilo porovnat s databází hashů na serveru, kam pronikli. Když najdou shodu, odhalí heslo pro daný účet, jelikož budou mít stejný hash. Díky přidaným řetězcům však tyto útoky nejsou úspěšné, jelikož ke každému heslu je přiřazen onen náhodný prvek. Dodatečné řetězce se ukládají spolu s heslem. Útočník by tedy pro prolomení musel každé své připravené heslo doplnit o řetězec, zahashovat a porovnat. Takto by musel vyzkoušet všechna svá připravená hesla což je opět velmi časově náročné.

Existuje řada hashovacích funkcí jako například již zmíněná MD5, dále pak Argon2 nebo SHA-256. Pro příklad si vyzkoušíme vytvořit vlastní zvolený hash pomocí online

dostupného generátoru (<https://www.sordum.org/hashgenerator/>). Využijeme algoritmus kódování MD5.

Zadaný řetězec: Matematika

MD5 Hash: **65a6a6ccc5c136d3a123a5d6049cfb65**

V praxi by se však k heslu nejdřív přidal dodatečný řetězec a teprve potom proběhlo hashování. Na ukázkou přidáme vlastní řetězec, například: 4Ever. Zahashování s přidaným řetězcem proběhne následovně.

MD5 Hash s dodatečným řetězcem: **aed8b4e20e095c416d69d00478c09b9a**

Pod tímto hashem bude uloženo naše heslo společně se použitým dodatečným řetězcem. Když se pak pokusíme přihlásit, server k našemu heslu Matematika přidá řetězec 4Ever a zahashuje. Výsledný hash porovná s uloženým a pokud jsou totožné, udělí nám přístup. V případě tabulkového útoku na server by útočník sice viděl zakódované heslo, nedokázal by si jej však díky přidanému řetězci spojit s originálem. V realitě se jedná o značně komplexnější řetězec znaků, jelikož je delší a náhodně vygenerovaný.

3.5 Osnova projektové výuky

V této části je popsána projektová výuka do hodiny matematiky. Časový odhad pro celou výuku je přibližně 270 minut, tedy 6 vyučovacích hodin, což odpovídá přibližně jednomu projektovému dni.

3.5.1 Motivační aktivity

Tento blok je zaměřen na motivační úvod. Časový odhad je 45 až 60 minut. K výuce je zapotřebí přinést nějaké fyzické zámky na kód, například zámek na kolo, zámek ke skřínce nebo starý mobilní telefon s nastaveným heslem, který je možné půjčit žákům. Alespoň tři zámky se stejným kódem jsou potřeba. Aktivita zde popsaná počítá se zámky na čtyřmístný kód.

Určete, kolik možných kombinací existuje pro standardní zámek na kufru. Tj. třímístný kód skládající se z cifer {0; 1; 2; 3; 4; 5; 6; 7; 8; 9}.

Úloha je jednoduchá a výsledek lze odhadnout. Žáci pracují samostatně. Časový odhad je maximálně 5 minut. Předpokládá se, že žáci se někdy s takovým zámekem již setkali a úloha proto pro ně nepředstavuje problém. Zadat se dají třiciferná čísla od [0; 0; 0] do [9; 9; 9]. V součtu je správný výsledek 1000 kombinací. Může se stát, že někdo zapomene připočíst kombinaci [0; 0; 0] a uvede výsledek o 1 nižší. Cílem úlohy je ukázat žákům, že princip hesla lze uplatnit i jinde než na internetové účty.

Aktivita na hádání hesla

Časový odhad pro společnou aktivitu je přibližně 20 minut. Cílem aktivity je, aby si žáci vyzkoušeli, jak těžké může být uhádnutí hesla člověkem i za velmi slabého hesla. Je tedy ukázáno, jak je pro člověka náročné snažit se prolomit hesla hrubou silou. Zároveň je tím do výuky zařazen formát soutěže, který může žáky povzbudit a zvýšit atraktivitu aktivity.

Učitel si myslí jeden libovolný znak na klávesnici. Jelikož hesla rozlišují mezi malými a velkými písmeny tak je budeme i zde rozlišovat. Může se tedy jednat o jakékoliv malé nebo velké písmeno, číslici nebo jiný znak jako například procento (%), stříšku (^) nebo třeba zpětné lomítko (\). Pro věrohodnost jej může napsat na papírek a ten například připnout magnetem k tabuli tak, aby nešel přečíst. Žáci utvoří frontu a popořadě budou psát znaky na tabuli a budou se snažit uhádnout ten znak, který je na papírku. Psaní na tabuli zaručí minimum opakujících se tipů a také částečně simuluje odezvu programu a čas potřebný k zadání hesla na klávesnici. Žáci se opakovaně střídají, dokud nenajdou správný znak. Hledání specifického znaku může být velmi náročné, zvláště když učitel zvolí málo známý symbol. Když budou potom žákům docházet nápady, mohou se povolit telefony, které jim pomohou s hledáním správného znaku. Nakonec se zaznamená čas potřebný k uhádnutí a počet nesprávných tipů. Tímto způsobem se může odehrát pár kol dle potřeby. Role se mohou libovolně prohazovat, například může znak zadávat jeden z žáků nebo naopak žáci zadají znak a učitel bude sám hádat.

Následně se zprůměrují naměřená data. Zjistíme, kolik jsme průměrně stihli pokusů za daný čas. Žáci nyní odpoví na pár otázek:

- Za jak dlouho bychom naším tempem prověřili 50 000 kombinací?
- Jak dlouho by nám nanejvýše trvalo naším tempem prolomit heslo složené ze čtyř znaků, když by byly použity všechny znakové sady? Tedy malá a velká písmena, číslice a speciální znaky (přibližně 32 znaků).

Aktivita s fyzickými zámky

Časový odhad pro společnou aktivitu je 20 až 30 minut. Cílem aktivity je procvičit se žáky nějaké základní pravidla dělitelností a snižování počtu kombinací čtyřmístných kódů zábavným způsobem.

Učitel vybere tři dobrovolníky z řad žáků. Ti dostanou každý jeden fyzický zámek, který budou mít za úkol otevřít. Standartní zámky na kolo bývají zamčené čtyřmístným kódem. Kód lze libovolně nastavit. Pro tento případ budou zámky nastavené na hodnotu 1860. Není nutností, aby žáci zámky sami odemknuli. Na začátek necháme pár minut, kdy mohou vybraní žáci diskutovat se třídou taktiku, kterou si zvolí pro zkoušení náhodných kombinací. Během toho, co budou vybraní žáci zkoušet náhodné možnosti, se učitel dotazuje třídy na doplňující otázky. Tyto otázky všechny souvisí s kódem, který žáci hledají. Učitel to však nijak nenaznačuje a bude vidět, zda někoho napadne dané otázky rovnou aplikovat na hledaný kód.

1. Kolik možností bychom vyřadili z celkového množství kombinací, když bychom uvedli, že číslo je menší než 3000?
2. Kolik možností bychom vyřadili z celkového množství kombinací, když bychom uvedli, že číslo je dělitelné pěti?
3. Kolik možností bychom vyřadili z celkového množství kombinací, když bychom uvedli, že druhá cifra je 8?
4. Kolik možností bychom vyřadili z celkového množství kombinací, když bychom uvedli, že kód je dělitelný čtyřmi.
5. Kolik možností zbude, pokud aplikujeme všechny více zmíněné podmínky?

Po zodpovězení otázek se učitel zeptá, jak na tom jsou žáci s odemykáním. Pokud se nikdo ještě nedostal ke správnému kódu, učitel vyzve třídu, aby jim prozradili, kolik možností musí

vyzkoušet podle páté otázky. Očekává se, že v tento moment již někoho ze třídy napadne aplikovat dříve zmíněné podmínky. Pokud se tak nestane, napoví sám učitel. Na vyzkoušení poté zbývá třicet možností, což už tři žáci dokáží projít poměrně rychle.

3.5.2 Kybernetické útoky

Tento blok projektové výuky je zaměřen na kybernetické útoky. Proveden je formou vzájemné diskuse mezi učitelem a žáky. Časový odhad je přibližně 20 minut. Učitel se nejdříve zeptá třídy, jaké kybernetické útoky znají a zda se s některými již setkali. Útoky se vypisují na tabuli. Učitel dopíše a nějak stručně vysvětlí některé následující, pokud ještě nebyly zmíněny a zmíní způsob ochrany proti daným útokům. Dále následuje diskuse o skutečných kybernetických útocích z historie.

Útok hrubou silou: Systematické zkoušení všech možných kombinací hesla popořadě. Pro člověka je velmi časově náročné, avšak počítače dokážou prověřovat sta tisíce kombinací za sekundu. Základní ochranou je tvorba dostatečně silného hesla. Silné heslo by mělo být alespoň osm znaků dlouhé a mělo by se skládat ze všech čtyř dostupných sad, tedy z číslic, malých a velkých písmen abecedy a speciálních znaků.

Slovníkový útok: Podobný útoku hrubou silou. Útočník zkouší všechna slova ze slovníku, společně s jejich odvozeninami. Princip ochrany je opět dostatečně silné heslo, složené například z neexistujícího slova nebo náhodné kombinace znaků.

Phishing: Jedná se o pokus oklamat uživatele ke sdělení vlastních přihlašovacích nebo jiných osobních údajů. Útočníci se vydávají za legitimní společnosti a snaží se tak v obětech vyvolat důvěru. Ochranou proti těmto útokům je všeobecná opatrnost ohledně neočekávaných e-mailů, SMS zpráv a telefonátů. Útočníci mohou také vyzývat k rozkliknutí odkazů, které přímo stáhnou nebezpečný virus do počítače, nebo vedou na kopii skutečných stránek. Podezřelým znakem jsou lámaná a nespisovná čeština, žádosti o sdělování neobvyklých údajů nebo neznalost některých vašich údajů, které by například banka měla znát.

Malware virus: Virus je škodlivý a nežádoucí program v zařízení, který má za úkol odcizit osobní informace. Lze získat klikáním na neznámé odkazy, navštěvováním nelegálních

pirátských stránek, připojováním se k neznámým zařízením jako jsou USB disky nebo wifi sítě, skenováním neznámých QR kódů a podobně. Prevencí je tedy vyvarovat se těmto rizikovým chováním. Hlavní ochranou je využívání služeb antivirových programů, které mají za úkol hledat a odstraňovat takovéto hrozby.

Až se projdou vypsane útoky, učitel se zeptá třídy, zda znají nějaký skutečný útok z historie. Za zmínku stojí příběh detailně popsany v kapitole 3.2, kdy se mladík z Velké Británie mnohokrát naboural do Pentagonu, díky slabému heslu jednoho z důstojníků. Tento útok se velmi přiblížil k rozpoutání války mezi Spojenými státy a Koreou. Na příběhu je krásně vidět, jak snadno lze prolomit slabé heslo a jaký dopad to někdy může mít.

3.5.3 Šifrování a prolamování jednoduchých šifer

V tomto bloku se žáci seznámí s šifrováním. Časový odhad pro výuku je přibližně 90 minut. Nejsou potřeba žádné speciální pomůcky pro tuto aktivitu. Žáci nejdříve popíšu své zkušenosti s šifrováním. Následně jim bude vysvětleno několik jednoduchých substitučních šifer. V druhé části pak žáci zkusí zašifrovat pomocí vlastní šifry heslo MATEMATIKA a vzájemně se budou snažit najít způsob jakým šifrovali ostatní.

Seznámení se s různými typy šifer

První část aktivity proběhne formou diskuse. Časový odhad je 30 minut. Učitel se zeptá třídy, jaké šifry znají nebo se kterými se setkali. Následuje debata ohledně šifer, když žák přijde s nějakou známou šifrou, stručně jí vysvětlí zbytku třídy. Tento úsek potrvá zhruba 10 až 15 minut, záleží na vlastním zapojení žáků. Poté budou krátce představeny některé jednoduché šifry, které dosud nebyly zmíněny.

Substituční šifry jsou takové šifry, které zaměňují znaky šifrované zprávy za jiné. Jedná se o typově nejjednodušší šifry, které se v kryptografii využívají (Carter & Magoc, 2007). Jejich komplikovanost záleží na klíči a pravidle, dle kterého jsou zašifrované. Následuje krátký popis vybraných substitučních šifer.

Caesarova šifra: Princip Caesarovy šifry spočívá v posouvání písmen zprávy o určitý, pevně daný počet písmen v abecedě. Například když budeme posouvat o 7 znaků, písmeno M se změní na písmeno T. Pokud dojdeme na konec abecedy, vracíme se opět na začátek a

pokračujeme v posunu. Heslo MATEMATIKA se proto při posunu třeba o 11 změní na XLEPXLETVL.

Atbašova šifra: Tato šifra funguje na principu převrácení abecedy. To znamená že z A se stane Z, z B se stane Y a třeba z W se stane D. Heslo MATEMATIKA by se tedy zašifrovalo jako NZGVNZGRPZ.

Vigenèrova šifra: Princip této šifry je podobný jako v Caesarově šifře, až na to že délka posunu není pevně daná. Zvolí se nějaké klíčové slovo z používané abecedy. Čím delší je toto klíčové slovo, tím náročnější je prolomení šifry. Šifrování probíhá dle posunuté abecedy. Vytvoří se tabulka V jejímž záhlaví bude vypsána celá abeceda v řádku i sloupci. Vznikne tak tabulka 26x26. První řádek se vyplní abecedou od začátku až do konce. Druhý řádek se vyplní obdobně akorát se celá abeceda posune o jeden znak, to znamená že z A se stane B. Třetí řádek se abeceda posune o dva znaky. Další řádky již pokračují obdobným způsobem (Carter & Magoc, 2007). Vznikne nám tak tabulka znaků symetrická podle hlavní diagonály viz níže Tabulka 1. Této tabulce se říká Vigenèrův čtverec. Šifrování pak probíhá následovně. Každý znak kódovaného textu se spojí se znakem šifrovacího klíče. V tabulce se pak najde příslušné políčko pro kódovaný znak a jeho klíčový obraz. Písmeno zapsané v políčku je poté zašifrovaný původní znak.

Tabulka 1: Vigenèrův čtverec

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Z matematického pohledu lze tuto šifru interpretovat dalším, možná o něco jednodušším způsobem. Není totiž zapotřebí využívat Vigenèrova čtverce. Písmena abecedy si postupně očíslováme od nuly, to znamená že $A = 0$; $B = 1 \dots$ Poté už pouze sečteme hodnoty kódovaného znaku a příslušného znaku z klíčového slova. Zbytek po dělení tohoto čísla 26 pak udává číslo zakódovaného znaku. Na ukázkou si opět zakódujeme slovo MATEMATIKA. Klíč si zvolíme libovolný, například PES. Po zašifrování nám vznikne kódované heslo BELTQSIMCP.

Dalším typem hojně využívané šifry je RSA šifra. Tato šifra se již neřadí mezi substituční šifry. Je to takzvaná asymetrická šifra. Využívá dva klíče, jeden je veřejný a druhý soukromý. K rozšifrování je zapotřebí znalost soukromého klíče, které je však velmi obtížné získat z veřejného klíče. Funguje na principu násobení vysokých prvočísel v řádu stovek cifer. Proces šifrování a dešifrování využívá modulování, tedy zbytky po dělení.

Zajímavým způsobem šifrování, které také stojí během výuky za zmínku jsou hashovací funkce. Zajímavé jsou tím, že se používají jako ochrana hesel na internetu. Jedná se o jednosměrné šifrování, jelikož není způsob, jakým by se jednou zašifrovaná zpráva dala rozšifrovat. Libovolně dlouhé řetězce se zašifrují do otisku neboli hashe pevně dané délky. Tato délka závisí na typu využívané hashovací funkce. Pravidlem je, že totožné řetězce se vždy zašifrují na totožné výstupní hashe. Se třídou je možné diskutovat, zda existují dva rozdílné řetězce, které mají stejný hash. Jelikož funkce kóduje libovolně dlouhé řetězce do řetězců pevné délky, nutně musí dojít ke kolizím. Nelze totiž dostat téměř neomezený počet řetězců do striktně omezeného počtu zakódovaných otisků. V praxi se ještě přidává k heslům dodatečný soubor znaků a teprve poté se celé heslo zahashuje. Následně učitel ukáže některé online hash generátory a společně se třídou si vyzkouší, jak vypadají konkrétní zahashovaná hesla.

Princip RSA šifrování a hashovacích funkcí je detailně popsán v kapitole 3.4.

Aktivita na vytváření vlastní šifry

Časový odhad této aktivity je 45 až 60 minut. Žáci dostanou za úkol samostatně nebo ve dvojicích vymyslet nějakou vlastní matematickou šifru. Podmínkou bude využívat klíče ve formě tabulky. Inspirací jim můžou být šifry zmíněné v předchozím bloku. Dle této vlastní šifry následně zakódují vlastní heslo délky maximálně deset znaků. Na tuto část mají 10 minut. Po uplynutí času, nebo pokud již mají všichni hotovo tak dříve, si šifry prohodí s jiným žákem nebo dvojicí. Následujícím úkolem bude rozluštit, jakým způsobem je heslo zašifrováno a co se pod ním skrývá. Jelikož mají žáci k dispozici šifrovací tabulku, mohou se k zašifrovanému řetězci dostat. Na hledání původního hesla je 15 minut. Během této doby učitel prochází po třídě a nahlíží na různé výtvary nebo poskytuje odpovědi na otázky. Po

uplynutí časového limitu se společně celá třída podívá na některé vytvořené šifry, které byly velmi zdařilé nebo ještě nebyly rozluštěny.

3.5.4 Závěrečná hra – Útěk z hackerského doupěte

Poslední blok projektové výuky si pokládá za úkol procvičit témata vyučovaná během celé projektové výuky. Závěrečné procvičování je uvedeno formou hry. Časový odhad je přibližně 60 až 90 minut. K výuce je zapotřebí speciálně upravený QR kód. Žáci mají za úkol zjistit heslo schované v QR kódu. Ten však není kompletní. Počítáním úloh budou žáci postupně získávat informace o tom, která políčka mají vybarvit. Po vypočítání všech úloh a vybarvení chybějících políček žáci následně oskenují kompletní QR kód. V QR kódu je uložený text s heslem na dokončení hry. Na úvod se žáci rozdělí do skupin po čtyřech. V případě výrazně nižšího nebo naopak vyššího počtu žáků je možné skupiny zmenšit či zvětšit. Úloh je více, čím větší tedy skupiny budou, tím rychleji se přes ně žáci propočítají. Po rozdělení do skupin uvede učitel úvod pro vtažení do příběhu.

Úvodní příběh

Právě jste se probrali v neznámé místnosti s černým pytlek přes hlavu. Skrz látku matně rozpoznáváte rozměry pokoje, ve kterém se nacházíte. Co ale s jistotou poznáte jsou hlasy vašich přátel, kteří jsou hned někde vedle vás. Společnými silami dokážete rozvázat pouta a konečně si sundat pytle z hlavy. Když se rozkoukáte, můžete prozkoumat své okolí. Vidíte pouze jedny vstupní dveře, pochopitelně jsou zamčené. K otevření zámku je potřeba nějaké desetimístné heslo. Zkusíte základní kombinaci 0123456789 ale nefunguje. Rozhlížíte se tedy dál. Vypadá to, že se nacházíte v hackerském doupěti. Zajímavé však je to, že po stěnách jsou všude možně načmárané šifry a rozvěšené papíry s podivnými kódy a příklady. Jeden z vás našel instrukce k odemčení zámku spolu s nápovědou. Pro osvobození se, musíte vyřešit úlohy, které jsou rozvěšené kolem. Výsledky vám řeknou, která písmena z tabulky máte do hesla dosadit. Následně je pak zapotřebí heslo rozšifrovat pomocí Atbašovy šifry. Společně jste tedy shromáždili všechny úlohy, které budete muset vyřešit. Po rozšifrování hesla se můžete osvobodit.

Po úvodním příběhu se učitel ujistí, že všichni pochopili princip hry. Dále žáky upozorní, že je zapotřebí vyřešit všechny úlohy a pokusy o uhádnutí hesla z částečně sestavených znaků

se nepočítá jako úspěšné dokončení hry. Po seznámení žáků s příběhem a pravidly, rozdá učitel každé skupině pracovní list s nevyplněným heslem a sadou úloh. Následně prochází třídou a sleduje, jak se žákům daří. Případně může poskytovat malé rady s ohledem na férovost hry.

Heslo a jeho řešení

1		2		3		4		5	
13	K	22	A	875	P	323	H	314	M
351	O	448	O	840	G	636	Z	3 333	K
886	Q	71	B	705	K	47	S	756	C
12 450	D	540	Y	1 128	E	441	N	9	I
292	G	218	F	187	X	4 600	A	232	Z

6		7		8		9		10	
40	T	8	J	10	I	808	G	49	Y
81	P	14	D	9 500	V	56	U	80	H
42	L	95	Y	70	W	2 048	S	35	O
11 001	B	10 000	L	957	B	64	M	226	T
150	V	99	T	100	K	43	Z	20 450	J

Obrázek 2: Náповěda k heslu

Každá skupina obdrží list s nápovědou k heslu, viz Obrázek 2. Výsledky úloh korespondují s právě jedním písmenem v nápovědě. Po vyřešení všech úloh se žáci dostanou k heslu KBGSZTLIZH. Toto heslo se pak pomocí Atbašovy šifry rozluští. Atbašova šifra přiřadí k abecedě tu samou abecedu akorát čtenou odzadu. A se změní na Z, B na Y a tak dále. Po rozšifrování vznikne heslo PYTHAGORAS. Toto je správné heslo pro útěk z doupěte a úspěšné dokončení hry. Učitel by skutečně měl dohlížet na vyřešení všech úloh, jelikož je

možné, že někteří žáci se přeci jen pokusí o odhadnutí hesla již z částečně rozluštěných znaků.

Jednotlivé úlohy a jejich rozbor

V této části jsou popsány všechny úlohy, které budou žáci v rámci závěrečné hry řešit. Ke každé je napsán stručný postup řešení a správný výsledek. Úlohy jsou sestavené tak, že počítat lze s kalkulačkou dostupnou v mobilních telefonech, týmy s vědeckou kalkulačkou proto nemají výhodu, naopak týmy bez vědecké kalkulačky se mohou dopočítat ke všem řešením. Možná by bylo dobré mít kopie QR kódů, pro případ že nějaký tým by vybarvil špatná políčka.

Úloha 1: Určete, kolik existuje různých PIN kódů na platebních kartách?

Žáci si musí nejdříve uvědomit jaké podmínky platí pro daný problém. Jedná se o čtyřciferné číslo, tudíž se dosazují číslice od 0 do 9 na čtyři pozice. Na každou ze čtyř pozic lze tedy dosadit 10 cifer. Z toho vyplývá výsledek 10000 možností.

Úloha 2: Počítač dokáže hrubou silou překontrolovat 250 000 kombinací za sekundu. Kolik hodin by mu trvalo prověřit všechna hesla délky osm znaků složené pouze z malých písmen? Výsledek zaokrouhlete na celé hodiny.

V této úloze musejí žáci nejdříve spočítat, kolik existuje hesel dle daných požadavků. Písmen abecedy je 26 a dosazujeme na osm pozic, to znamená že takových různých hesel existuje 26^8 . Tento počet všech hesel vydělíme 250 000, což je počet prozkoumaných hesel za sekundu. Dostaneme se k číslu zaokrouhleném na 835 308. Tento výsledek je doba, za jakou projde počítač všechna hesla v sekundách. Úloha si však žádá výsledek v hodinách. Pouze proto vydělíme toto číslo 3600, což je převod ze sekund na hodiny. Finální výsledek, který úloha hledá je 232 hodin.

Úloha 3: Pomocí Vigenèrovy šifry rozluštěte zašifrovaný text CYUVIULK LO XIPNCMX. Klíč k rozluštění je HACKER.

Z předchozích bloků žáci vědí, jak se Vigenèrova šifra generuje. Sami však musí dojít ke zpětnému algoritmu rozšifrování. U této úlohy možná bude potřeba žákům připomenout, o kterou šifru se přesně jednalo. Zpětný algoritmus funguje následovně. Najdu si příslušné

písmeno z klíče. V tabulce Vigenèrova čtverce jedu po řádku (nebo sloupci) tohoto písmene, dokud nenarazím na příslušné zašifrované písmeno. Poté pokračuji ve sloupci (nebo řádku) zpět k záhlaví tabulky, kde najdu rozšifrované písmeno. Například první písmeno klíče je H. Jedu tedy po řádku H, dokud nenarazím na písmeno C, které přísluší mému písmenu z klíče. Když poté vyjedu po sloupci nahoru tak zjistím, že po rozšifrování se jedná o písmeno V. Úloha není počítačového charakteru, proto je možné ve skupině zapojení i žáků, kteří si nejsou v počítání tak jistí. Po rozšifrování celého řetězce nám vznikne VYSLEDEK JE TRINACT, tedy výsledek je třináct. Žáci proto vyberou v QR kódu políčko s číslem 13.

Úloha 4: Určete kolik možností existuje pro čtyřmístný číselný kód dle následujících podmínek:

- a) Číslo je sudé, druhá cifra je 5, číslo je menší než 2 000, třetí cifra je dělitelná třemi**
- b) Číslo je větší než 4 000, poslední cifra je nižší než 7, druhá cifra je dělitelná 5**
- c) První cifra je dělitelná 3, druhá cifra je 4 nebo 7, celé číslo je dělitelné 6**

V této úloze si žáci procvičí vyřazování nežádoucích hesel podle vypsanych podmínek. První dvě varianty jsou rychle vypočitatelné. Nejvýraznější způsob je přiřazování kolik čísel mohou dát na jednotlivé pozice a následné vynásobení. Třetí varianta je složitější kvůli dělitelnosti šesti. Dají se snadno určit varianty pro první dvě cifry. Poslední dvě cifry již musí žák určovat jako dvojčíslí, jelikož jedinou informací, kterou má, je dělitelnost šesti. Proto je třeba brát ohled na ciferný součet. Výsledky jednotlivých variant jsou po řadě: a) 40; b) 840; c) 80.

Úloha 5: Podařilo se vám odchytnout zprávu, zakódovanou pomocí stejného principu, na kterém funguje RSA šifrování. Podařilo se vám dohledat, že klíč obsahuje číslo 2021. Pro rozšifrování zprávy je potřeba znát z jakých prvočísel je číslo složeno. Nalezněte tato dvě prvočísla.

V této úloze si mohou žáci vyzkoušet, jak obtížné je prolomit RSA šifrování. Tento příklad je velmi zjednodušená verze. Na vyřešení úlohy není jiný způsob než systematické zkoušení prvočísel. Když budou žáci postupně zkoušet všechna prvočísla od nejmenšího, po třinácti chybných pokusech dojdou k řešení. Číslo 2021 je složeno z prvočísel 43 a 47. K vyřešení úlohy stačí znalost prvočísel a kalkulačka.

Úloha 6: Nabourali jste se do databáze přísně střežených dokumentů. Potřebujete odhalit přístupové heslo abyste mohli pokračovat. Bohužel jste v databázi našli pouze hash s dodatečným řetězcem JeHeslo. Využijte hashovací funkci MD5 a zašifrujte připravená hesla poté co k nim přidáte dodatečný řetězec (bez mezer). Výsledek pak porovnejte se zachyceným hashem dokud nenarazíte na správné heslo.

Zachycený hash: 1a6e4eb375f089d7e9db6e3248a09ed5

Připravená hesla: 10a11; 27a92; 89a28; 4a11; 27a39; 15a71; 89a92; 10a71; 15a39; 4a28

S touto úlohou budou nejspíše žáci potřebovat pomoc. K vyřešení je zapotřebí mobilní telefon s přístupem na internet. Žáci si musejí najít příslušný MD5 hash generátor (učitel jim může konkrétní doporučit). Poté budou postupně zadávat připravená hesla a doplní je o dodatečný řetězec JeHeslo. Nutné je zadat je bez mezer a dbát na přesné opsání, jelikož i drobná změna vygeneruje unikátní kód. Bude to vypadat například takto: 89a28JeHeslo. Následně jej zahashují a výsledný hash porovnají se zachyceným. Správný výsledek je 10a71. Žáci proto vyberou políčka 10 a 71. Při vytváření úlohy byl využíván online dostupný generátor <https://www.md5hashgenerator.com>.

Shrnutí projektové výuky

Celé téma si pokládá za úkol seznámit žáky se základy kybernetické bezpečnosti. Jelikož je téma široké, projektová výuka je zaměřena na hesla a šifrování. Schopnost vytvářet silná hesla slouží jako prevence proti odcizení osobních údajů. S pomocí úloh a aktivit se odhaluje matematika na pozadí ochrany osobních údajů. Celá výuka je tvořena ve snaze udělat výuku pro žáky atraktivní a zábavnou, proto je upřednostňován formát aktivit a her. Závěrečná hra slouží jako procvičení a zopakování si nově získaných vědomostí.

Na konci projektové výuky, budou žáci:

- obeznámeni s pravidly pro vytvoření dostatečně silného hesla
- získají základní povědomí o kybernetických útocích a způsobech, jak se proti nim bránit
- seznámí se s některými typy substitučních šifrování, RSA šifrování a hashovací funkce

- získají vědomostní podklady pro budoucí správu a ochranu osobních dat
- budou schopni problematiku zjednodušeně vysvětlit dalšímu člověku

Závěr

Práce se zaměřovala na vytvoření podkladů pro projektovou výuku matematiky. Tématem byla ochrana osobních údajů na internetu pomocí hesel.

První kapitola obsahuje popis digitálních kompetencí, jejich rozdělení a propojení s předmětem matematika.

Ve druhé kapitole je stručně charakterizována projektová výuka, její přínosy, výhody a nevýhody.

Třetí kapitola popisuje principy tvorby dostatečně silného hesla a rizika využívání slabého hesla. Dále jsou zmíněné některé kybernetické útoky se způsoby, jak se proti nim chránit, Nakonec jsou popsány principy ochrany údajů na serverech pomocí šifrování. Následuje praktická část, která obsahuje detailní osnovu projektové výuky s úlohami, aktivitami a jejich rozbořem.

Cílem práce bylo připravit materiály, které mohou být využity na středních školách v rámci matematiky k zapojení digitálních klíčových kompetencí do výuky. Cíle bylo úspěšně dosaženo. Jako úskalí vidím náročnost některých témat, jak na požadovanou úroveň vědomostí, tak na časový rozsah. Témata šifrování nelze popsat do detailu jejich fungování, protože žáci středních škol nemají obecně potřebné znalosti a v rámci projektové výuky, jak jí mám nastavenou, není čas se všemu věnovat úplně od základů.

Práce je vhodná zejména pro učitele předmětu matematika na středních školách. Na práci lze navázat vyzkoušením zde vybudovaných principů v praxi a následným vyhodnocením didaktických cílů. Dále je možné rozšířit téma o další prvky digitální bezpečnosti jako je například digitální stopa.

Seznam použitých informačních zdrojů

- Altmanová, J. (2010). *Gramotnosti ve vzdělávání* (J. Faltýn, K. Nemčíková, & E. Zelendová, Ed.; 1. vyd.). Výzkumný ústav pedagogický. https://archiv-nuv.npi.cz/uploads/Publikace/vup/Gramotnosti_ve_vzdelavani11.pdf
- Barker, E. (2020). *Recommendation for Key Management: Part 1 – General*. National Institute of Standards and Technology. <https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final>
- Bawden, D., & Robinson, L. (2009). The dark side of information: Overload, anxiety and other paradoxes and pathologies. *Journal of Information Science*, 35(2), 180–191. <https://doi.org/10.1177/0165551508095781>
- Bendl, V. (2023). *Využití digitálních technologií ve výuce matematiky na gymnáziích*. Metodický portál: Články [online]. <https://clanky.rvp.cz/clanek/23440/VYUZITI-DIGITALNICH-TECHNOLOGII-VE-VYUCE-MATEMATIKY-NA-GYMNAZIICH.html>
- Carter, B., & Magoc, T. (2007). *Classical Ciphers and Cryptanalysis*. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4ef5260b4709a8f8427e5af24724878780b5e39a>
- Černý, M. (2023). *DigCompEdu: Digitální kompetence učitelů od teorie k praxi* (1. vyd.). Národní pedagogický institut České republiky. <https://digitalizace.rvp.cz/files/digcompedu.pdf>
- Digitální a informační agentura. (2025). *Návod, jak poznat phishingové útoky*. Portál veřejné správy [online]. <https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phishingove-utoky>
- Ferrari, A., Punie, Y., & Brečko, B. (2013). *DIGCOMP – A framework for developing and understanding digital competence in Europe* (Y. Punie & B. Brečko, Ed.). Publications Office of the European Union. <https://doi.org/10.2788/52966>

- Gilbert, S. (2017). Information literacy skills in the workplace: Examining early career advertising professionals. *Journal of Business & Finance Librarianship*, 22(2), 111–134. <https://doi.org/10.1080/08963568.2016.1258938>
- Hayashi, E., & Hong, J. I. (2011). *A Diary Study of Password Usage in Daily Life*. Carnegie Mellon University. <https://dl.acm.org/doi/pdf/10.1145/1978942.1979326>
- K. Gary. (2015). Project-Based Learning. *Computer*, 48(9), 98–100. <https://doi.org/10.1109/MC.2015.268>
- Kiranjot, K., & Sunny, B. (2014). Captcha and Its Techniques: A Review. *International Journal of Computer Science and Information Technologies*, 5(5). https://www.researchgate.net/profile/Sunny-Behal/publication/285110169_Captcha_and_Its_Techniques_A_Review/links/565bede108ae4988a7bb0d0c/Captcha-and-Its-Techniques-A-Review.pdf
- Klíma, V. (2005). *Nalézání kolizí MD5—Hračka pro notebook*. https://cryptophy.hyperlink.cz/md5/MD5_kolize.pdf
- Konark, D. T. (2013). Brute-force Attack “Seeking but Distressing”. *International Journal of Innovations in Engineering and Technology*, 2(3). <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=02449b7b97662ef7cd48b880a701f416084d8c31>
- Larmer, J., & Mergendoller, J. R. (2010). Seven essentials for project-based learning. *Educational leadership*, 68(1), 34–37.
- Lianhua, C., & Xingquan, Z. (2017). Hashing Techniques: A Survey and Taxonomy. *Association for Computing Machinery*, 50(1). <https://doi.org/10.1145/3047307>
- Microsoft. (n. d.). *Co je ochrana heslem?* Microsoft [online]. <https://www.microsoft.com/cs-cz/security/business/security-101/what-is-password-protection>

Ministerstvo školství, mládeže a tělovýchovy. (2023). *Digitální kompetence v uzlových bodech vzdělávání*. Národní pedagogický institut České republiky - revize rámcových vzdělávacích programů [online]. <https://digitalizace.rvp.cz/digikompetence-uzlove-body>

Ministerstvo školství, mládeže a tělovýchovy. (2021a). *Rámcový vzdělávací program pro gymnázia*. https://www.edu.cz/wp-content/uploads/2021/09/001_RVP_GYM_-_vyznacene_zmeny.pdf

Ministerstvo školství, mládeže a tělovýchovy. (2021b). *Rámcový vzdělávací program pro základní vzdělávání*. <https://www.edu.cz/wp-content/uploads/2021/07/RVP-ZV-2021.pdf>

Národní pedagogický institut České republiky. (2021). *Infografika RVP ZV 2021*. <https://digitalizace.rvp.cz/files/infografika-rvp-zv-2021-web.pdf>

Národní úřad pro kybernetickou a informační bezpečnost. (2015). *Phishing—Stále aktuální hrozba*. Národní úřad pro kybernetickou a informační bezpečnost [online]. <https://nukib.gov.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/>

Ošťádal, R. (2012). *Teoretický základ a přehled kryptografických hashovacích funkcí*. https://is.muni.cz/www/ostadal/hash_overview.pdf

Razak, M. F. A., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of “malware”: Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, 75, 58–76. <https://doi.org/10.1016/j.jnca.2016.08.022>

Růžicková, D., Fanfulová, E., & Maněnová, M. (2020). *Digitální gramotnost v uzlových bodech vzdělávání*. Národní pedagogický institut České republiky. <https://digitalizace.rvp.cz/files/digitalni-gramotnost-ocekavane-vysledky-uceni.pdf>

Shannon, R. (2006). Password Security: What Users Know and What They Actually Do. *Usability news*, 8(1). <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6f920ba7e350d1f3523894ee604e41df9faab0bd>

- Ungoed-Thomas, J. (1998). The schoolboy spy. *Sunday Times*. <https://www.kujimedia.com/the-schoolboy-spy-sunday-times/>
- Weakpass. (n. d.). *10_million_password_list_top_10000*. Weakpass [online]. https://weakpass.com/wordlists/10_million_password_list_top_10000.txt
- Zajíčková, J., Žák, M., & Fuksa, M. (n. d.). *Teorie čísel a šifrování*. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0923f18940ed2029c3ee98cb975c6479c9abd8e7>
- Zormanová, L. (2012). *Projektová výuka*. Metodický portál: Články [online]. <https://clanky.rvp.cz/clanek/c/s/14983/PROJEKTOVA-VYUKA.html>
- Zviran, M., & Haga, W. J. (1999). Password Security: An Empirical Study. *Journal of Management Information Systems*, 15(4), 161–185. <https://doi.org/10.1080/07421222.1999.11518226>

Vyjádření k využití nástrojů umělé inteligence

Nástroje umělé inteligence nebyly pro tuto práci využívány.