06 CHRÁŇME SVOJE SÚKROMIE

Tematický celok / Téma	*Stupeň školy / Odporúčaný ročník / Rozsah*
Informačná spoločnosť – bezpečnosť a riziká	SŠ / 1. ročník / 1 vyučovacia hodina

Požiadavky na vstupné vedomosti a zručnosti

- Informácia, kódovanie informácie

Ciele

Žiakom osvojované vedomosti a zručnosti	*Žiakom rozvíjané spôsobilosti*
Informačná spoločnosť – bezpečnosť a riziká **Výkonový štandard** • diskutovať o rizikách na internete, • zhodnotiť, ktoré informácie musia byť chránené pred zneužitím, • aplikovať pravidlá pre zabezpečenie prístupu do e-mailu, do komunity, do počítača a proti neoprávnenému použitiu, • posúdiť riziká práce na počítači so škodlivým softvérom. **Obsahový štandard** Vlastnosti a vzťahy: vírus ako škodlivý softvér, riziká na internete a sociálnych sieťach Procesy: šírenie počítačových vírusov, bezpečné a etické správanie sa na internete, činnosť hekerov	**Informatické myslenie:** Logika • (LOG4) vyvodzovať (logicky zdôvodňovať) závery z pozorovaní a experimentov (aj myšlienkových – práca s textom) Algoritmy • (ALG1) rozpoznať či postup/návod je algoritmom (algoritmus – zrozumiteľné/jednoznačné pravidlá/kroky/inštrukcie poskytujúce výsledky v konečnom čase, napr. princíp použitia verejného a súkromného kľúča) Hľadanie vzorov • (VZO5) preniesť/použiť vzory/myšlienky/riešenia z jedného problému na druhý problému (použitie stratégie riešenia problému)

Riešený didaktický problém

Žiaci často krát používajú najnovšie technológie bez poznania rizík, ktoré so sebou prinášajú. Formálne o nich vedia, neuvedomujú si však ich dopad na ľudskú spoločnosť, mieru ich škodlivosti a rizika.

Dominantné vyučovacie metódy a formy	*Príprava učiteľa a pomôcky*
• Bádateľská metóda (model 5E), • frontálna a individuálna forma.	pre učiteľa • **I_SS_59_Kody_sifry_kompresia_M.pdf** metodika vyučovania vo formáte pdf • **I_SS_59_Kody_sifry_kompresia_pracovne_texty.docx** pracovné texty pre skupiny žiakov • **I_SS_59_Kody_sifry_kompresia_PL.docx** pracovný list pre žiaka • **I_SS_59_Kody_sifry_kompresia_PL.pdf** pracovný list Použitie digitálnych nástrojov: NUTNÉ

Diagnostika splnenia vzdelávacích cieľov

Karta 3-2-1 v pracovnom zošite.

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
it akadémia
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

ÚVOD

Vo vzdelávacej oblasti Matematika a práca s informáciami inovovaného ŠVP pre gymnáziá so štvorročným a päťročným vzdelávacím programom nenájdeme samostatný pojem šifrovanie. Môžeme ho však včleniť pod tému Informačná spoločnosť – bezpečnosť a riziká (v zmysle vyššie uvedených štandardov).

Cieľom tejto metodiky je preto poukázať na potrebu chrániť údaje, napríklad šifrovaním informácií (či už ide o súbory alebo elektronickú komunikáciu), ale aj zálohovaním údajov s využitím ich kompresie.

S kompresiou grafických súborov (napr. stratová kompresia jpg alebo bezstratová kompresia png) a zvukových súborov (napr. stratová kompresia mp3 alebo bezstratová kompresia flac) sa žiaci mohli stretnúť v rámci vyučovacích hodín, ktorými mohli byť rozšírené základné hodiny pokryté metodikami (kódovanie grafickej a zvukovej informácie). Výhody kompresie grafických, zvukových, ale aj video súborov, využívajú dennodenne. Priamu, vedomú skúsenosť so šifrovaním zatiaľ nemajú (maximálne s protokolom https).

Žiaci majú k dispozícii pracovný list, ktorý obsahuje zadania úloh, miesto na žiacke riešenie a miesto pre poznámky. Odporúčame, aby učiteľ žiakom pri každej fáze vyučovania uviedol zoznam úloh z pracovného listu, ktoré budú aktuálne riešiť. Poslednou časťou je karta 3-2-1 (lístok pri odchode) ako nástroj formatívneho hodnotenia.

Poznámka:

Pracovný list je jedným z výstupov žiaka. Odporúčame, aby si žiaci jednotlivé vypracované pracovné listy odkladali. Neskôr ich môžu využiť pri opakovaní učiva.

PRIEBEH VÝUČBY

Osnova vyučovacej hodiny (podľa modelu 5E):

- **Zapojenie (8 minút)** – práca s textom, diskusia (úloha 1 z pracovného listu)
- **Skúmanie (8 minút)** – význam šifrovania (otázky 1 a 2 z pracovného listu)
- **Vysvetlenie (10 minút)** – vysvetlenie riešenia predchádzajúcich otázok (princíp asymetrického šifrovania) (úloha 2 z pracovného listu)
- **Rozpracovanie (10 minút)** – riešenie náročnejších úloh (úlohy 3, 4 a 5 z pracovného listu)
- **Vyhodnotenie (4 minúty)** – vyplnenie karty 3-2-1

ZAPOJENIE (CCA 8 MIN)

Na prvej vyučovacej hodine z tejto série metodík sa žiaci dozvedeli, čo je to kódovanie informácií. Kompresia a šifrovanie dát tu boli predstavené ako podmnožiny samotného kódovania, s ohľadom na cieľ takéhoto špeciálneho kódovania informácií (kompresia – úspora dátového priestoru, šifrovanie – utajenie informácií).

S kódovaním a šifrovaním informácií sa žiaci mohli stretnúť už na 2. stupni základnej školy. Tejto problematike sa venujú štyri metodiky série ZŠ - kódy, šifry, kompresia z 1. kola overovania metodík IT Akadémie. Ak sa žiaci tejto téme na základnej škole nevenovali, môžeme siahnuť práve po spomínaných metodikách a hravou formou žiakov do nej uviesť.

V úvodnej aktivite budú žiaci pracovať textami popisujúcimi skutočné udalosti a fakty. K dispozícii máme štyri sady pracovné texty (každý v rozsahu jednej strany A4) – žiakov rozdelíme do dvoj až trojčlenných skupín. Každej skupine dáme jeden z pracovných textov, s ktorým bude pracovať. Texty rozdelíme pokiaľ možno rovnomerne. Žiaci si texty prečítajú a zapíšu svoje odpovede na dané otázky.

Úloha 1	*Prečítajte si pozorne pridelený text. Zapíšte si odpovede na nasledujúce otázky:* *a) Opísané útoky sa týkajú najmä takých cieľov, ktoré môžu prísť o cenné údaje. Ak by sa podobný útok odohral vo Vašom počítači, ktoré súbory by boli pre Vás nenahraditeľné?* *b) Je podľa Vás riešením tejto situácie zaplatenie výkupného?* *c) Ako sa do počítača môže dostať takýto škodlivý kód?* *d) Ako je možné chrániť sa pred popísaným spôsobom počítačovej kriminality?*

Po ukončení práce žiaci prezentujú svoje odpovede na dané otázky, diskutujú.

V otázke a) je dôležité, aby si žiaci uvedomili hodnotu informácií. Tá je samozrejme relatívna, pre nich môže mať vysokú hodnotu rozpracovaný referát z biológie, ktorý je potrebné odovzdať čo najskôr, no jeho hodnota klesá, ak si uvedomia, že takto môžu byť zasiahnuté súbory napr. so zdravotnou dokumentáciou.

V otázke b) majú odborníci jednotný názor – výkupné neplatiť. Ak ho totiž zaplatíme, nemáme istotu, že proces vydierania skončí, ani to, že naše dáta budú spätne dešifrované. Tu sa možno objaví otázka, ako sa teda k svojim dátam dostať. Existujú návody ako sa správať v prípade takéhoto útoku – napr. okamžite vypnúť počítač a obrátiť sa na odborníkov, ktorí pri troche šťastia zachránia ešte nezašifrované dáta. Očakávať odšifrovanie súborov je však nereálne – aj vzhľadom na výpočtovú silu dnešných technológií sa na to určite nemôžeme spoliehať, najmä ak ide o dáta, ktoré potrebujeme hneď.

Spôsoby infiltrácie sú rôzne – využitie nesprávneho návrhu počítačovej siete, nedodržiavanie bezpečnostných pravidiel a podobne. Niekedy stačí otvoriť prílohu elektronickej správy, a tým sme otvorili dvere škodlivému softvéru.

Základom je však prevencia – práve o nej môžeme diskutovať pri otázke d). Používanie aktualizovaného operačného systému, antimalvérového softvéru, ostražité dodržiavanie bezpečnostných pravidiel a zálohovanie dát je ideálnou kombináciou, ktorá nám pomôže ak nie priamo predísť takémuto útoku, tak aspoň minimalizovať straty. Je dôležité školiť a následne preškoľovať zamestnancov v oblasti bezpečnostných postupov.

Poznámka:

Ak žiakov problematika ransomwaru zaujala, viac informácií nájdu napr. na stránke https://www.eset.com/sk/ransomware/.

V oblasti prevencie sa môžeme inšpirovať stránkou https://www.eset.com/sk/firemna-it-bezpecnost/bezpecnostne-sluzby/services/riadenie-it-bezpecnosti/skolenia/.

SKÚMANIE (CCA 8 MIN)

Každá minca má dve strany – samotná myšlienka šifrovania vznikla pôvodne s cieľom utajiť informácie pred „nepovolanými“. V histórii ľudstva asi ani nenájdeme vynález, ktorý by nebol zneužitý práve proti človeku. Ale pozrieme sa aj na pozitívny prínos šifrovania.

Otázka 1 *Prečo nie je reálne súbory zasiahnuté útokom ransomwarom odšifrovať?*

Necháme priestor pre argumenty žiakov. Následne ich doplníme.

Dávno sú už preč časy tzv. symetrických šifier – teda takých, kde obe komunikujúce strany mali k dispozícii ten istý kľúč, pomocou ktorého dokázali zašifrovať aj odšifrovať informácie. Spomeňme Cézarovu šifru, kedy stačilo poznať číslo určujúce posun v abecede, či rôzne substitučné šifry, na prelomenie ktorých stačila frekvenčná analýza. Samozrejme, postupy šifrovania sa postupne zdokonaľovali a stávali sa stále náročnejšími na prelomenie. Spomeňme napríklad elektromechnický šifrovací stroj Enigma, ktorého šifru považovali Nemci za neprelomiteľnú. Ako z histórie vieme, aj táto šifra bola prelomená (ale napr. na dešifrovanie nemeckého rozkazu bol potrebný jeden až dva dni, teda získaná informácia už nemusela byť aktuálna).

Poznámka:

Viac informácií o šifrovacom stroji Enigma: https://sk.wikipedia.org/wiki/Enigma_(%C5%A1ifrovac%C3%AD_stroj)

Prierez témou šifrovania: https://www.khanacademy.org/computing/computer-science/cryptography

Intenzívny rozvoj v oblasti šifrovania nastal najmä s príchodom počítačových sietí, ktoré umožňujú zdieľať informácie. A práve vtedy sa problematika „utajenia“ stala blízkou každému človeku využívajúcemu služby počítačových sietí.

Otázka 2	*Odpovedzte na nasledujúce otázky, svoje odpovede zdôvodnite:* *a) Môžeme si byť istí, že správu naozaj odoslal uvedený odosielateľ?* *b) Môžeme si byť istí, že sa správa nedostane do rúk nepovolaným osobám?* *c) Môžeme si byť istí, že správa nebola upravená?*

Ponecháme priestor na názory a skúsenosti žiakov. Pre žiakov bude možno novou informáciou, že ani v jednom z uvedených prípadov nemáme stopercentnú istotu. Napr. pomocou programovacieho jazyka PHP je možné falšovať identitu odosielateľa. Pomocou nezabezpečenej verejnej siete (napr. wifi v kaviarni) je možné správu zachytiť, prečítať si ju, zmeniť ju, prípadne znemožniť jej doručenie. Aj keď sa spoliehame na zabezpečený hypertextový prenosový protokol https, ktorý nám zaručuje, že komunikácia medzi nami a príslušným serverom prebieha šifrovane, nevieme, kto má prístup k údajom na danom serveri. Napr. do sociálnej siete Facebook pristupujeme práve cez protokol https, napriek tomu stále čítame správy o úniku osobných údajov z tejto siete.

Poznámka:

Aktuálna správa https://zive.aktuality.sk/clanok/151936/unik-z-facebooku-na-webe-su-telefonne-cisla-e-maily-aj-dalsie-data-pol-miliardy-ludi/?utm_source=aktuality.sk&utm_medium=zona-hp&utm_content=box-crosspromo-hp-new&utm_campaign=cross&_ga=2.237234944.1803832997.1617015711-2112944521.1606683139.

Pojmy ako „https“, „súkromná správa“ a podobne v nás vzbudzujú klamlivý pocit bezpečia. Ako teda komunikovať tak, aby sme mohli so stopercentnou istotou odpovedať kladne na každú otázku v časti Otázka 2? Jedným riešením by bolo nekomunikovať prostredníctvom počítačových sietí, ale toto riešenie asi nie je reálne.

VYSVETLENIE (CCA 10 MIN)

Riešením je asymetrické šifrovanie, ktoré používa odlišný kľúč na zašifrovanie a odlišný kľúč na odšifrovanie informácie. Táto metóda vznikla v polovici 70. rokov minulého storočia a zaistila dôvernosť a autenticitu komunikácie.

Ak chceme komunikovať s využitím asymetrického šifrovania, budú nám vygenerované dva „kľúče“: súkromný (privátny) a verejný. Ako už naznačujú prídavné mená, privátny kľúč si budeme chrániť, aby sa k nemu nikdy nikto nedostal; verejný kľúč zverejníme – môžeme ho bezpečne doručiť každému, s kým chceme takto komunikovať (neskôr si uvedieme aj inú metódu takéhoto sprístupnenia verejného kľúča). Osoba, s ktorou chceme takto komunikovať – nazvime ju Adam, má teda istotu, že tento verejný kľúč patrí nám. Ak si takúto dvojicu kľúčov dá vygenerovať aj Adam, môžeme si vziať jeho verejný kľúč.

Naša komunikácia s Adamom bude potom prebiehať nasledovne:

- Napíšem správu pre Adama.
  - Aby si Adam bol istý, že som odosielateľom správy skutočne ja, podpíšem ju svojím súkromným kľúčom. Som jeho jediným vlastníkom, teda nikto iný nemohol správu pomocou neho podpísať. Tým je zaručená autenticita správy.

  - Aby správu nemohol nikto prečítať či pozmeniť, použijem Adamov verejný kľúč – správa sa zašifrujte a odšifrovať ju môže len Adam pomocou svojho súkromného kľúča. Tým je zaručená dôvernosť správy.
- Správu odošlem. Ak ju niekto aj odchytí, nedokáže ju prečítať, pretože nemá Adamov súkromný kľúč. Ak aj správu (náhodne) pozmení, Adam to zistí pri pokuse dešifrovať správu pomocou svojho súkromného kľúča.
- Adam správu prijme. Pomocou svojho súkromného kľúča správu dešifruje. Pomocou môjho verejného kľúča overí správnosť môjho podpisu.

Úloha 2	*Naša kamarátka Katka nemá vygenerovanú svoju dvojicu kľúčov. Má pre ňu význam mať môj verejný kľúč?*

Katka môže použiť môj verejný kľúč na to, aby si overila, že som danú správu naozaj odoslala ja. Nemáme však istotu, že správu nikto iný nečítal alebo ju nepozmenil.

Čo je to vlastne ten kľúč? Prestavme si pod týmto pojmom reťazec náhodných čísel. Súkromný a verejný kľúč sú matematicky príbuzní – teda vznikli istým matematickým výpočtom s využitím veľkých prvočísel. Na ich generovanie sa používajú rôzne algoritmy, napr. ECC, DSA alebo RSA (princíp tohto algoritmu- „výpočet“ súkromného a verejného kľúča) si môžete pozrieť na https://cs.wikipedia.org/wiki/RSA).

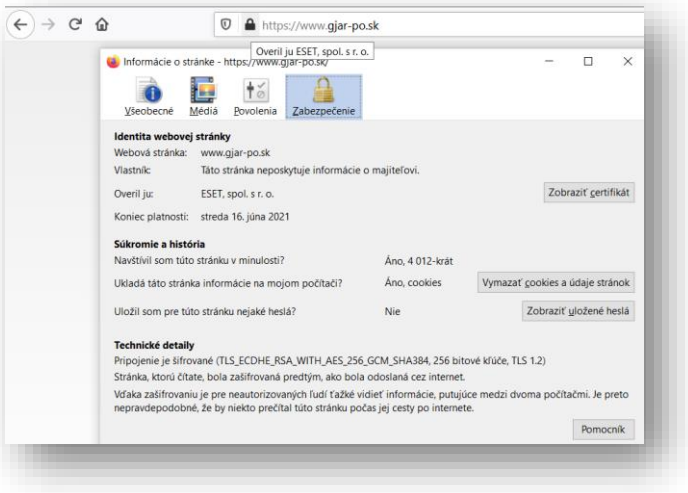
Niektorí odborníci však varujú, že s rastúcim výkonom počítačov a s príchodom kvantových počítačov nám hrozí „kryptokalypsa“ (náhle zneplatnenie digitálnych podpisov, digitálnych mien či odtajnenie dokumentov spôsobené prelomením spomenutých algoritmov). Preto sa pozornosť zameriava na algoritmy s takou matematicky dokázanou bezpečnosťou, aby ich neprelomil ani kvantový počítač (post-quantum cryptography). Vidíme, že táto oblasť bude v nasledujúcom období prechádzať obrovskými zmenami a pokrokmi.

ROZPRACOVANIE (CCA 10 MIN)

Samozrejme, tento princíp sa nevyužíva len pri osobnej elektronickej komunikácii. Uplatnenie našiel aj pri zabezpečení webových serverov (protokoly SSL a TLS), ide o zabezpečené pripojenie HTTPS k prehliadačom či digitálnom podpisovaní dokumentov.

Ako ale zverejniť svoj verejný kľúč tak, aby druhá strana mala istotu, že je môj a nie je podvrhom? Ako si máme byť istí, že verejný kľúč nejakej inštitúcie je naozaj kľúčom danej inštitúcie a nie podvrhom?

Na to slúžia tzv. certifikačné autority (CA). Informácie o certifikačnej autorite k danému webovému sídlu získate kliknutím na symbol zámku vedľa adresy sídla, napr.:



Po kliknutí na tlačidlo Zobraziť certifikát zistíme podrobnejšie informácie o danom certifikáte.

Úloha 3	*Zistite, aký algoritmus generovania verejného kľúča používa webové sídlo www.facebook.com.*

Uvedená sociálna sieť používa algoritmus ECC.

Úloha 4	*„Od 2. decembra 2013 sa vydáva nový typ občianskeho preukazu s elektronickým kontaktným čipom – tzv. elektronická identifikačná karta (eID).* *eID má na zadnej strane elektronický kontaktný čip. Na čipe sú uložené údaje uvedené na občianskom preukaze: meno, priezvisko, adresa, dátum narodenia a údaje o platnosti dokladu. V prípade záujmu si môže občan zvoliť, či má čip obsahovať aj iné údaje, napr. údaje potrebné pre vytváranie kvalifikovaného elektronického podpisu (KEP). Ten je v elektronickej komunikácii občana s úradmi alebo komerčnými inštitúciami rovnocennou náhradou vlastnoručného podpisu.“ (www.slovensko.sk)* *a) Požiadali ste pri vydaní vášho eID o vydanie kvalifikovaného certifikátu pre vytvorenie KEP?* *b) Zistite, ktoré elektronické služby verejnej správy prostredníctvom internetu môže využívať občas s eID.*

Pri hľadaní odpovedí na túto úlohu využijeme stránku https://www.slovensko.sk, v pravej časti položku Vybrané služby, resp. Nájsť službu.

Dôležité je žiakov upozorniť na existenciu Elektronických schránok a tiež na možnosť využiť eID s elektronickým čipom eID alebo s KEP pri komunikácii s Finančnou správou.

Úloha 5	*O dáta na zariadeniach môžeme prísť rôznymi spôsobmi – chyba zariadenia, krádež zariadenia, nechcené vymazanie, kybernetický útok (napríklad spomínaný ransomware). Je preto dôležité dáta pravidelne zálohovať.* *Akým spôsobom zálohujete svoje dáta?*

Žiaci svoje dáta väčšinou nezálohujú, niektorí možno využívajú cloudové služby, iní USB či externý disk. Diskutujme so žiakmi o výhodách a nevýhodách jednotlivých riešení, ktoré budú prezentovať. Venujeme sa faktorom ako pravidelnosť, typ zariadenia použitého na zálohovanie (jeho

životnosť, bezpečnosť, kapacita, umiestnenie...). Dôležité je, aby si žiaci uvedomili dôležitosť zálohovania, ale tiež zraniteľnosť jednotlivých spôsobov zálohovania

Operačné systémy už majú inštalovaný softvér na zálohovanie dát (napr. MS Windows 10 ponúka možnosť zálohovať dáta na OneDrive prípadne na inú jednotku).

VYHODNOTENIE (CCA 4 MIN)

V záverečnej časti hodiny požiadame žiakov, aby vyplnili kartu 3-2-1. Odporúčame žiakom vysvetliť a zdôrazniť, že cieľom je zistiť čo a ako si žiak z obsahu hodiny zapamätal a nie klasifikácia známkou. Pre učiteľa a žiaka zvlášť, je cenná pravdivá informácia o úrovni osvojených poznatkov než umelo vylepšená.. Odporúčame, aby učiteľ tieto karty pozbieral a využil ich na nasledujúcej vyučovacej hodine (vysvetlenie prípadných miskoncepcií, hľadanie odpovedí na nové otázky a podobne).

3-2-1 KARTA

3 veci, ktoré som sa dnes naučil(a):	
2 fakty, ktoré ma zaujali:	
1 otázka, ktorú ešte stále mám:	