ŠIFROVANIE, CERTIFIKÁTY, DIGITÁLNY PODPIS

ÚVOD

Toto je tretia metodika zo série troch metodík, ktoré sú venované problematike bezpečnosti IT. Táto metodika sa venuje ochrane zariadení, v bezpečnom používaní siete a v ochrane údajov. Obsahom metodiky je šifrovanie a vytváranie kľúčov. Žiaci budú aplikovať poznatky na vytváraní vlastných kľúčov pomocou online nástrojov, avšak učiteľ ukáže aj použitie softvéru **GoAnywhere PGP studio**[1], ktorý je potrebné nainštalovať na učiteľskom PC. Overia si používanie verejných a súkromných kľúčov. V prípade, že škola alebo učiteľ má k dispozícii cvičný digitálny podpis, žiaci budú digitálne podpisovať dokumenty Wordu a zošity Excelu.

Žiaci majú k dispozícii pracovný list, miesto na žiacke riešenie a miesto pre poznámky. Nakoľko v úlohách z pracovného listu bude potrebné kopírovanie údajov do online formulárov, je vhodné poskytnúť žiakom pracovné listy v elektronickej podobe.

PRIEBEH VÝUČBY

Osnova vyučovacej hodiny (podľa modelu 5E):

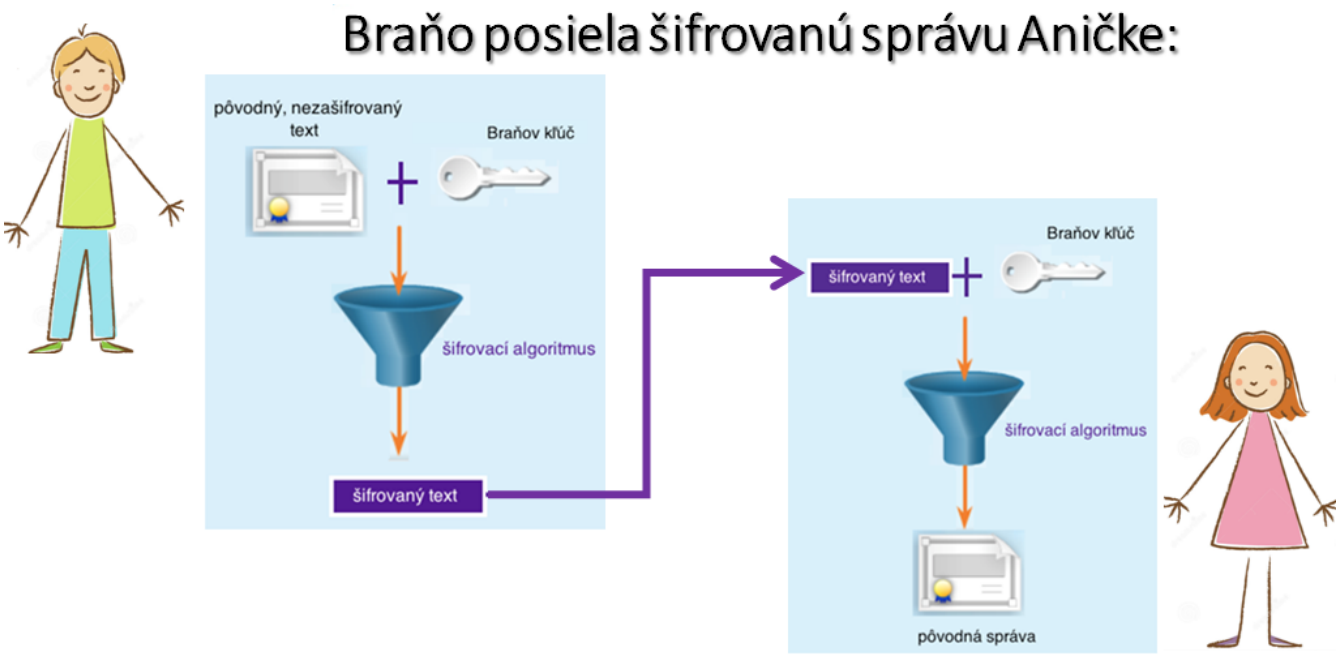
- **Zapojenie (5 minút)** – motivačný rozhovor so žiakmi na tému šifrovania
- **Skúmanie (8 minút)** – riešenie úloh z pracovného listu formou práce vo dvojiciach (úlohy 1 a 2)
- **Vysvetlenie (15 minút)** – zhrnutie výsledkov úlohy z pracovného listu, rozšírenie o asymetrické šifrovanie, digitálny podpis a certifikáty pomocou sprievodnej prezentácie a úlohy 3 z pracovného listu
- **Rozpracovanie (9minút)** – samostatná práca na PC s pracovným listom (úlohy 4 a 5)
- **Hodnotenie (3 minúty)** – sebahodnotiaci test

ZAPOJENIE (CCA 5 MIN.):

Hodinu začneme rozhovorom so žiakmi. Zopakujme so žiakmi 3 prvky zabezpečenej komunikácie – CIA – dôvernosť údajov, integrita údajov a autentifikácia pôvodu údajov. Položme im otázku, ako by sa mala podľa nich zabezpečiť dôvernosť údajov, t.j. aby sa neprezradilo to, čo je v správe napísane? Očakávame, že žiaci budú navrhovať rôzne spôsoby šifrovania. Môžeme sa spýtať, či poznajú niektoré

[1] voľne dostupný zo stránky https://www.goanywhere.com/openpgp-studio

spôsoby šifrovania (napr. Cézarovu šifru apod.). Následne sa opýtame, čo je potrebné poznať, aby sme mohli prečítať zašifrovanú správu, resp. získať jej pôvodný obsah. Žiaci by mali spomenúť pojem šifrovací kľúč. Vyzvime žiakov, aby navrhli postup ako by sa malo postupovať, ak by chcel Braňo poslať šifrovanú správu Aničke. Žiaci by sa mali pokúsiť tento proces vysvetliť vlastnými slovami, až následne im ho ukážeme pomocou sprievodnej prezentácie (snímka 2):



Keďže v praxi existuje veľké množstvo rôznych druhov šifrovacích nástrojov, pokúsime sa postupne pozrieť na niektoré druhy.

SKÚMANIE (CCA 8 MIN.):

Žiaci pracujú vo dvojiciach na počítačoch s pracovným listom (úloha 1 a 2). V tejto etape záznamy žiakov nevyhodnocujme ani nekomentujme.

Úloha 1 *Toto je ukážka zašifrovanej správy:*

B2234562A1255C944AF40E81221C0124A763CA9B2A89D2A22798133ABA7EE7DEE87E0AD2913AA9884072150574093B222A81208D03634449DC3BC94F41227AEBF996BB287AAAE86EA37BCFD8ACE3E2854D77593BBE34E49ABB36D322A9D4F473

Vo webovom prehliadači načítajte stránku https://www.devglan.com/online-tools/aes-encryption-decryption. *Pomocou nástroja na dešifrovanie (**AES Online Decryption**) zistite jej obsah – budete k tomu potrebovať tajný*

kľúč **narodeninyheleny** *. Nastavte aj správny vstupný formát (***Input Text Format***)* na **Hex** – viete, čo to znamená (pomocou akých znakov je Vaša šifrovaná správa zapísaná)? _____

Aby ste získali jej čitateľnú podobu, musíte najprv kliknúť na tlačidlo Decrypt *a potom ešte na tlačidlo* Decode to Plain Text *. Dešifrovaná správa znie:* _____

_____

Vyskúšajte vytvoriť vlastnú textovú správu, ktorú pomocou vlastného ***16-miestneho tajného kľúča*** *(použite mód* ***ECB*** *a* ***128-bitovú*** *dĺžku bloku, tzv.* ***Key Size****) zašifrujete pomocou tlačidla* Encrypt *. Formát výstupných dát môžete zvoliť* ***Base64*** *alebo* ***Hex*** *(vyskúšajte, porovnajte a zvoľte si). Odošlite svojmu spolužiakovi vo dvojici dva samostatné e-maily:*

1. *Najprv odošlite zašifrovanú správu (formát mu neprezraďte, mal by na to prísť sám)*
2. *Potom odošlite tajný kľúč, ktorým bude môcť správu dešifrovať*

Počkajte na e-maily od svojho spolužiaka a dešifrujte správu od neho.

Úloha 2 *Doplňte:*

Pokiaľ by sme použili kľúč dĺžky 1 bit, koľko rôznych možností by sme museli vyskúšať na jeho zistenie (tzv. kľúčový priestor)? _____

Pokiaľ by sme použili kľúč dĺžky 2 bity, potrebovali by sme vyskúšať _____ *možností.*

Pokiaľ by sme použili kľúč dĺžky 3 bity, potrebovali by sme vyskúšať _____ *možností.*

Pokiaľ by sme použili kľúč dĺžky ***n bitov****, potrebovali by sme vyskúšať* _____ *možností.*

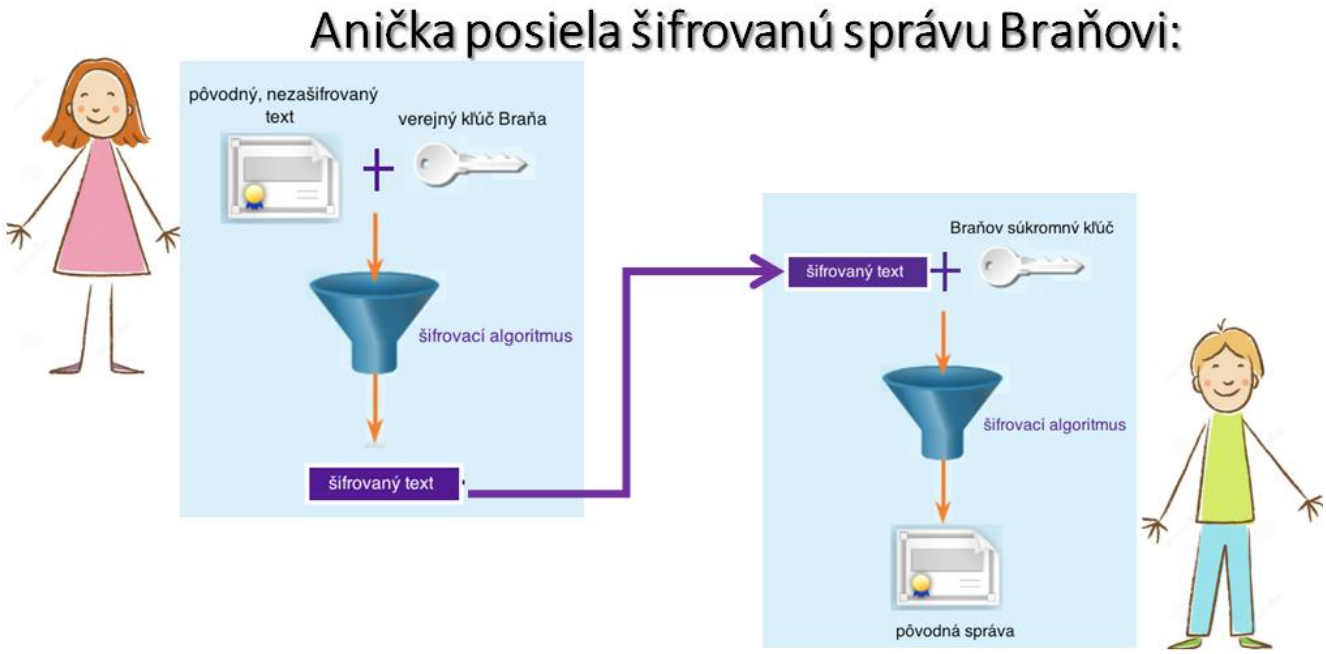
Zistite (na stránke z predošlej úlohy), koľko bitové sú kľúče, ktoré používa šifrovací algoritmus AES: _____

Aký veľký by bol ***kľúčový priestor*** *pre najdlhší kľúč algoritmu AES?* _____

VYSVETLENIE (CCA 15 MIN.):

Stručne spolu so žiakmi zhrnieme výsledky úlohy 1 a 2. Pri ich riešení sa dozvedeli o pojmoch **symetrický šifrovací algoritmus**, **dĺžka kľúča** a **kľúčový priestor**, pričom sme sa zamerali na **algoritmus AES** (***Advanced Encryption Standard***), ktorý predstavuje jeden z najbezpečnejších typov šifrovacích algoritmov používaných v moderných sieťach. Vrátime sa k obrázku na snímke 2 v sprievodnej prezentácii (*Braňo posiela šifrovanú správu Aničke*), na ktorom zdôrazníme, že sa jedná (aj v úlohe 1) o symetrické šifrovanie a že máme ten istý kľúč použitý na zašifrovanie aj odšifrovanie (podobne ako je to pri Cézarovej šifre). Čo bolo dôležité (a žiaci si to počas riešenia úlohy 1 pravdepodobne všimli) je, že tajný kľúč neposielali v tom istom e-maili ako samotnú zašifrovanú správu – spýtajme sa ich, prečo je to

dôležité. Očakávame odpovede, že je to bezpečnejšie, lebo pokiaľ by sa niekto iný dostal k správe, pri ktorej je aj samotný kľúč na jej dešifrovanie, tak by si ju vedel prečítať (bola by porušená požiadavka na dôvernosť údajov). Tu položíme žiakom otázku: pokiaľ by sa niekto iný počas šifrovanej komunikácie dostal ku kľúču, aké by to ešte mohlo mať následky? Je dôležité zdôrazniť, že tretia osoby by zároveň vedela pôvodnú správu od Braňa pozmeniť, nanovo zašifrovať a poslať pôvodnému adresátovi, teda Aničke, ktorá by vôbec netušila, že správa v tejto podobe nie je tá, ktorú jej pôvodne Braňo písal – došlo by teda aj k porušenie požiadavky na integritu údajov. Preto je potrebné si uvedomiť, že v dobe moderných technológií bezpečnosť šifrovania spočíva **v tajnosti kľúčov**, nie v algoritme. Existuje silnejšie šifrovanie, ktoré používa **asymetrickú šifru**[2], pri ktorej sa používa **dvojica kľúčov** - **verejný kľúč** a **súkromný kľúč**. Obidva kľúče sú schopné šifrovacieho procesu, ale na dešifrovanie je vždy potrebný doplnkový spárovaný kľúč. Dáta šifrované verejným kľúčom vyžadujú na dešifrovanie súkromný kľúč. Dĺžky kľúčov pri asymetrickom šifrovaní sú medzi 512 až 4 096 bitmi, pričom dĺžky väčšie alebo rovnajúce sa 1 024 bitom sa považujú za spoľahlivé. Princíp asymetrického šifrovania vysvetlíme žiakom pomocou obrázka v sprievodnej prezentácii (snímka 3):



Verejný kľúč sa používa na šifrovanie údajov, súkromný kľúč sa musí použiť na dešifrovanie údajov. Len jeden hostiteľ má privátny kľúč. Ak je súkromný kľúč prezradený, musí sa vygenerovať ďalší pár kľúčov, ktorý nahradí prezradený kľúč.

Podľa obrázka v prezentácii Anka požaduje a získa verejný kľúč od Braňa (on ho môže poskytnúť komukoľvek, preto sa tento kľúč nazýva verejný). Anka používa Braňov **verejný kľúč na zašifrovanie správy** pomocou dohodnutého algoritmu. Anka zašle šifrovanú správu Braňovi. Braňo potom používa svoj **súkromný kľúč na dešifrovanie správy** (on ako jediný má k dispozícii súkromný kľúč, teda iba on vie správu dešifrovať a prečítať, čím je splnená požiadavka na dôvernosť údajov). Súkromný kľúč sa

[2] v praxi existuje viacero protokolov, ktoré využívajú asymetrické šifrovanie (napr. IKE, SSL, SSH, PGP)

nikomu neposiela, verejne prístupný je len verejný kľúč – ak by tretia osoba mala Braňov verejný kľúč, môže mu síce zašifrovať vlastnú správu, ale pôvodnú správu, ktorú poslala Anička pre Braňa, pomocou neho nedešifruje a nezistí jej obsah. Ukážka práce s **asymetrickým algoritmom RSA** je v pracovnom liste v úlohe 3.

Poznámka:

Úlohu 3 môžeme nechať žiakov riešiť vo dvojiciach na hodine (pokiaľ máme dostatočný časový priestor, príp. šikovnejších žiakov), príp. ju môžu vypracovať ako domácu úlohu.

Úloha 3 *Vo webovom prehliadači načítajte stránku* https://www.devglan.com/online-tools/rsa-encryption-decryption.

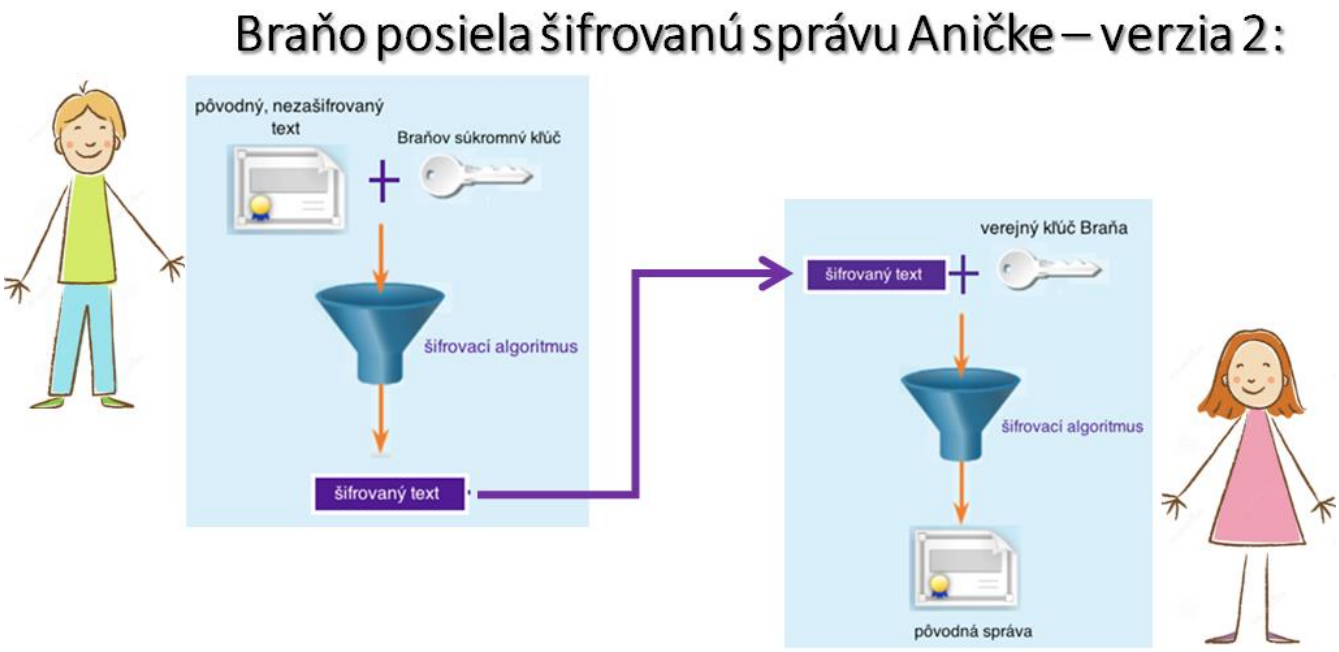
Riešte podľa pokynov učiteľa

1. *Najprv vygenerujte dvojicu kľúčov (**Public Key/Private Key**) kliknutím na tlačidlo* Generate RSA Key Pair *a vymeňte si so spolužiakom svoje verejné kľúče e-mailom (pošlite mu svoj verejný kľúč, on pošle Vám svoj).*
2. *Pomocou nástroja na zašifrovanie (**RSA encryption**) zašifrujte krátku správu pre svojho spolužiaka pomocou jeho verejného kľúča, ktorý Vám poslal. Správu zašifrujete kliknutím na tlačidlo* Encrypt .
3. *Zašifrovanú správu skopírujte a odošlite e-mailom spolužiakovi, ktorý ju odšifruje svojim súkromným kľúčom.*
4. *Počkajte na e-mail od spolužiaka s jeho zašifrovanou správou pre Vás a odšifrujte ju pomocou svojho súkromného kľúča nástrojom **RSA decryption** kliknutím na tlačidlo* Decrypt .

Správa, ktorú ste dostali od spolužiaka: _____

_____

Položme žiakom otázku, čo by sa stalo, keby sme pri asymetrickom šifrovaní vymenili verejný a súkromný kľúč, t.j. na zašifrovanie správy by sme použili náš súkromný kľúč a na jej dešifrovanie náš verejný kľúč (ktorý by bol prístupný pre kohokoľvek), čo znázorňuje v sprievodnej prezentácii snímka 4:



Napriek tomu, že sa tento postup zdá byť na prvý pohľad možno málo zmysluplný, pozrime sa na situáciu Braňa a Aničky. Tentokrát chce Braňo poslať správu Aničke a pomocou svojho súkromného kľúča (ktorý má len on ako jediný) zašifruje svoju správu pre Aničku. Anička správu dostane, nájde Braňov verejný kľúč a pomocou neho správu dešifruje. Je pravdou, že dešifrovať takúto správu by mohol pomocou verejne dostupného Braňovho kľúča prakticky ktokoľvek, teda o utajení je tu ťažké hovoriť, avšak tým, že jediný, kto mohol túto správu zašifrovať, bol Braňo (on jediný má súkromný kľúč), máme zaistené, že je to správa skutočne od Braňa (a nie od niekoho iného, kto sa za Braňa vydáva), čím sa Braňo autentifikoval, teda jedinečným spôsobom potvrdil svoju identitu, vytvoril svoj **digitálny podpis**.

Poznámka:

RSA algoritmus je príliš pomalý na šifrovanie celých dokumentov (týka sa to aj digitálneho podpisu), preto sa nešifruje celý dokument, ale iba **hash dokumentu**. Čiže digitálny podpis pracuje potom takto: Braňo vypočíta hash svojho dokumentu a hash zašifruje pomocou svojho súkromného kľúča a výsledok pripojí k dokumentu ako podpis a pošle Aničke. Anička vypočíta znovu hash dokumentu, dešifruje podpis a porovná so svojím hash. Ak sa zhodujú dokument je od Braňa.

Túto časť na vysvetlenie fungovania digitálneho podpisu odporúčame zaradiť v prípade, ak má učiteľ šikovnejších žiakov, napr. so záujmom o maturitu z informatiky; pre žiakov na odborných školách neinformatického zamerania nie je nevyhnutné sa jej venovať do detailov, teda postačí len základná zjednodušená predstava o digitálnom podpise.

Efektívny a šikovný nástroj na šifrovanú komunikáciu (napr. pre e-maily) vrátane podpisu predstavuje softvér **GoAnywhere PGP studio**[3], ktorý žiakom ukážeme frontálne pomocou dataprojektora z učiteľského počítača – na pripravených dokumentoch môžeme predviesť zašifrovanie a podpis, príp. dešifrovanie dokumentu.

Poznámka:

[3] krátke inštruktážne video pre učiteľa je na adrese https://www.youtube.com/watch?v=ZYyC-nM_db0

Opäť, len na rozšírenie pre triedy so šikovnejšími žiakmi, je možné spomenúť, že pri tomto programe (**PGP**, t.j. **Pretty Good Privacy**) je nepohodlné a časovo náročné pomocou asymetrickej šifry šifrovať celý dokument. Preto sa dokument zašifruje pomocou rýchlejšej symetrickej šifry a kľúč k symetrickej šifre sa zašifruje pomocou asymetrickej šifry.

Na území Slovenskej republiky upravuje používanie digitálneho podpisu **Zákon č. 215/2002 Z.z. o elektronickom podpise**, ktorý upravuje aj podmienky overovania verejného kľúča osôb, keďže jednoduchou možnosťou prelomenia podpisu je zameniť niekoho verejný kľúč za kľúč útočníka. Na overenie verejných kľúčov slúžia tzv. **certifikáty**, ktoré vydávajú dôveryhodné inštitúcie, tzv. **certifikačné autority**[4].

ROZPRACOVANIE (CCA 9 MIN.):

Žiaci pracujú samostatne na počítačoch s pracovnými listami – úloha 4 je určená na vyhľadanie digitálneho certifikátu webovej lokality, úloha 5 ukazuje, akým spôsobom je možné zašifrovať a digitálne podpísať dokumenty v prostredí MS Office.

Úloha 4 *V prehliadači Google Chrome načítajte niektorú zabezpečenú stránku (napr. stránku Vašej školy) a kliknutím pravým tlačidlom myši na ikonku uzavretej zámky*  *vľavo vedľa jej URL adresy získate okno, v ktorom nájdete informácie o platnosti digitálneho certifikátu pre túto stránku. Zistite a doplňte nasledovné informácie:*

a) Pre koho bol vydaný digitálny certifikát: _____
b) Kto je vydavateľom digitálneho certifikátu: _____
c) Aká je platnosť digitálneho certifikátu: _____

*V časti **Podrobnosti** nájdite typ algoritmu a dĺžku kľúča a nakopírujte sem verejný kľúč:*

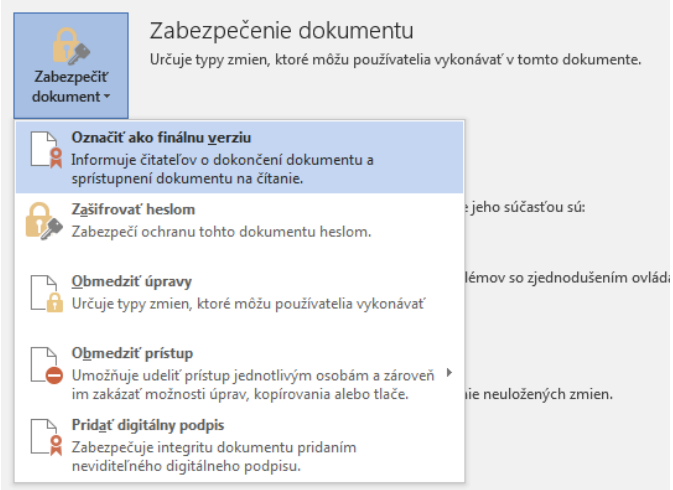
Poznámka:

Pokiaľ škola používa verzie MS Office, ktoré nepodporujú šifrovanie a podpisovanie dokumentov, tak túto úlohu na hodine riešiť nemusíme, avšak môžeme ju odporučiť žiakom na domácu úlohu (pre tých, ktorí na domácich počítačoch používajú novšie verzie tohto kancelárskeho balíka).

[4] zoznam certifikačných autorít, u ktorých je možné si overiť digitálne certifikáty, je možné nájsť napr. na stránke http://tlbrowser.tsl.website/tools/index.jsp, kde sú aj inštitúcie pôsobiace na Slovensku

Úloha 5 *Vyskúšajte nástroje na zabezpečenie bezpečnosti Vášho dokumentu v MS Word (napr. tohto pracovného listu)- cez tlačidlo Office v položke* ***Pripraviť*** *nájdete možnosti pre zabezpečenie dokumentu :*

Riešte podľa pokynov učiteľa



1. *Ak má váš počítač nainštalovaný digitálny certifikát na podpisovanie, tak dokument digitálne podpíšte*
2. *Zašifrujte dokument heslom*
3. *Označte ako finálnu verziu a odošlite e-mailom svojmu učiteľovi.*

HODNOTENIE (CCA 3 MIN.):

V krátkosti prediskutujeme so žiakmi výsledky predošlých úloh. Na evalváciu slúži sebahodnotiaci test v pracovnom liste, pomocou ktorého žiaci sami zhodnotia úroveň osvojenia vedomostí a zručností, ako aj splnenie cieľov hodiny. Zároveň sebahodnotiaci test slúži na zhrnutie základných poznatkov a zručností, ktoré si žiaci na hodine mali osvojiť. Výsledky testu môžeme spoločne so žiakmi skontrolovať pomocou sprievodnej prezentácie.

Poznámka:

Ak žiaci pracovali na hodine s elektronickou verziou pracovných listov, je dobré, ak na riešenie sebahodnotiaceho testu dostanú jeho vytlačenú verziu (postačí aj samostatná strana).

Sebahodnotiaci test

Do schém doplňte nasledujúce pojmy (niektoré sa môžu použiť aj viackrát):

VEREJNÝ KĽÚČ **TAJNÝ KĽÚČ** **SÚKROMNÝ KĽÚČ** **CERTIFIKÁT** **CERTIFIKAČNÁ AUTORITA**

Schéma 1:

Schéma 2:

Schéma 3: