Meno: ..... Trieda: ..... Dátum: ..... (verzia: 20200809)

ŠIFROVANIE, CERTIFIKÁTY, DIGITÁLNY PODPIS

PRACOVNÝ LIST

SKÚMANIE

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?* _____

Meno: ..... Trieda: ..... Dátum: ..... (verzia: 20200809)

VYSVETLENIE

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: _____

_____

ROZPRACOVANIE

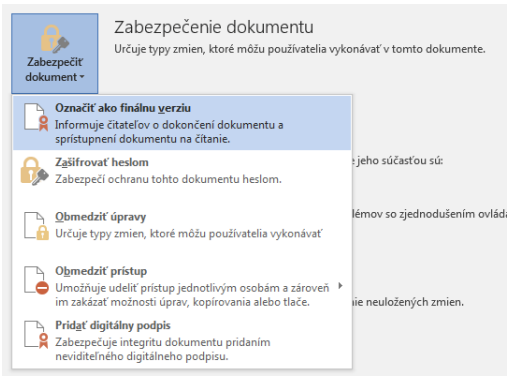
Úloha 4 *V prehliadači Google Chrome načítajte niektorú zabezpečenú stránku (napr. stránku Vašej školy) a kliknutím pravým tlačidlom myši na ikonku uzavretej zámky*  *vľavo vedľa jej URL adresy získate okno, v ktorom nájdete informácie o platnosti digitálneho certifikátu pre túto stránku. Zistite a doplňte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

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.*

Meno: ..... Trieda: ..... Dátum: ..... (verzia: 20200809)

HODNOTENIE

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: