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)? ***v šestnástkovom kóde***

Aby ste získali jej čitateľnú podobu, musíte najprv kliknúť na tlačidlo Decrypt *a potom ešte na tlačidlo* Decode to Plain Text. *Dešifrovaná správa znie:* ***Prave ste vyskusali desifrovat spravu pomocou symetrickeho sifrovacieho algoritmu AES.***

*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)? ***2***

Pokiaľ by sme použili kľúč dĺžky 2 bity, potrebovali by sme vyskúšať ***4*** *možností.*

Pokiaľ by sme použili kľúč dĺžky 3 bity, potrebovali by sme vyskúšať ***8*** *možností.*

*Pokiaľ by sme použili kľúč dĺžky **n bitov**, potrebovali by sme vyskúšať* 2^n *možností.*

Zistite (na stránke z predošlej úlohy), koľko bitové sú kľúče, ktoré používa šifrovací algoritmus AES: ***128/192/256***

*Aký veľký by bol **kľúčový priestor** pre najdlhší kľúč algoritmu AES?* 2^{256}, *t.j.* $1{,}1579209 \times 10^{77}$

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

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: napr.* ****.edupage.org***
b) *Kto je vydavateľom digitálneho certifikátu: napr.* ***Sectigo RSA Domain Validation Secure Server CA***
c) *Aká je platnosť digitálneho certifikátu: napr.* ***od 15.08.2019 do 27.08.2020***

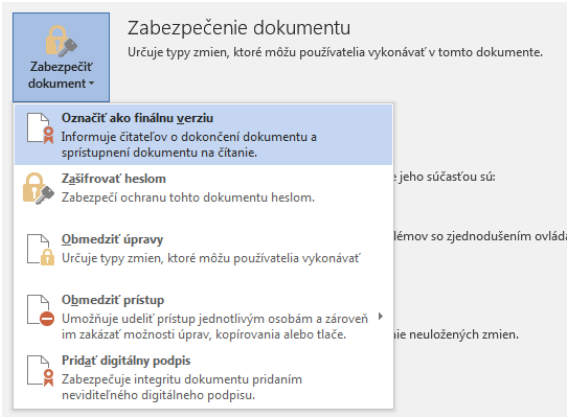
V časti ***Podrobnosti*** *nájdite typ algoritmu a dĺžku kľúča a nakopírujte sem verejný kľúč:*

RSA (2048 bitov)

```
30 82 01 0a 02 82 01 01 00 9c 41 c3 03 31 44 14 23 38 79 ff bb f2 62 68 3b 92 87 28 de 92 06
45 16 68 50 00 23 4d 99 68 78 71 6b f4 ef f6 fb 27 e5 67 58 81 f9 26 bf 4f df 96 63 64 9a 6f
33 88 79 90 25 91 69 75 bb a1 6c fa f7 94 d3 86 ed 09 b7 bd e1 1f 6d 35 e3 d0 26 5a e5 80 2e
05 e6 fc 6f 18 93 e9 ec fa 2b e1 f1 d6 34 a1 ab 45 d5 e1 a2 3d d7 04 8d e3 92 e7 b6 b1 36 48
7f 39 05 fe b7 59 87 a5 db 9a a4 37 69 2a 58 2f 60 1b bb 75 44 87 31 3c 21 02 82 27 0b 05 e3
7c c7 3b 73 ad 4e 56 98 46 76 44 88 58 8c 4d 6a 33 94 13 91 dc 3a 17 7f a0 72 6a 97 2a c2 f5
b2 c1 fc 4c 51 3f de 1b 4d 7d 49 c9 7d fd bb 5e 41 bd de da 8d e0 6e 93 33 e4 d2 b5 58 32 68
8d bc b8 89 d2 e8 4c 4c 65 4c a6 e4 98 5b 23 c4 31 b3 51 1e a7 cc fb bf 38 a2 37 4e 5b 9f 00
27 cf 14 9b 54 9a 8b 8f 81 8c 94 be 20 e4 ce 35 d1 02 03 01 00 01
```

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: