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 stezískali jej čitateľnú podobu, musíte najprv kliknúť na tlačidlo a potom ešte na tlačidlo . 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 . 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

|  |  |
| --- | --- |
| **Úloha 3**  Riešte podľa pokynov učiteľa | Vo webovom prehliadači načítajte stránku <https://www.devglan.com/online-tools/rsa-encryption-decryption>.   1. Najprv vygenerujte dvojicu kľúčov (**Public Key**/**Private Key**) kliknutím na tlačidlo 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 . 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 .   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:   1. Pre koho bol vydaný digitálny certifikát: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2. Kto je vydavateľom digitálneho certifikátu: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 3. Aká je platnosť digitálneho certifikátu: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   V časti **Podrobnosti** nájdite typ algoritmu a dĺžku kľúča a nakopírujte sem verejný kľúč: |

|  |  |
| --- | --- |
| **Úloha 5**  Riešte podľa pokynov učiteľa | 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 :     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

Sebahodnotiaci test

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

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

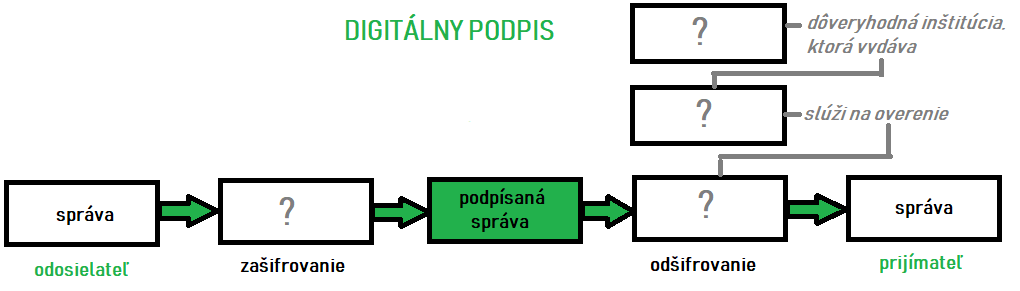
*Schéma 1:*

****

*Schéma 2:*

**

*Schéma 3:*

**