1. Pozměň následující text tak, aby tvrzení byla pravdivá.

Jeden z hlavních problémů je proces výměny klíčů.

být užita k vytvoření digitálního podpisu.

být užita k vytvoření digitálního podpisu.

Při použití operace je vystavena strukturální informace holého textu.

Při použití druhu provozu CBC chyba šíření omezena.

Nastane-li chyba v šifrovaném textu, tak při použití druhu provozu tyto chyby propagovány i v obdrženém textu.

Nastane-li chyba v šifrovaném textu, tak při použití druhu provozu tyto chyby propagovány i v obdrženém textu.

Nastane-li chyba v šifrovaném textu, tak při použití druhu provozu tyto chyby propagovány i v obdrženém textu.

1. Přiřaď termíny z levého sloupce odpovídajícím definicím umístěným vpravo.

**7**

**6**

**5**

**4**

**3**

**2**

**1**

používá pseudonáhodný klíč generovaný nezávisle na otevřeném i šifrovaném textu

Kryptografie symetrického klíče

používá algoritmus symetrického nebo veřejného klíče

Proudová šifra

Proudová šifra

nabízí samostatně zabezpečení důvěrnosti nebo autentifikaci zdroje

používá vždy algoritmus symetrického klíče

používá pseudonáhodný klíč, který nezávisí na šifrovaném textu

pracuje s časově proměnnou transformací jednotlivých znaků otevřeného textu

Bloková šifra

Samo synchronizující se proudová šifra

Kryptografie veřejného klíče

nabízí současně zabezpečení důvěrnosti nebo autentifikaci zdroje

**5**

**4**

**7**

**2**

**6**

**3**

**1**

Synchronní proudová šifra

1. Označ pravdivá tvrzení.

□ Digitální podpis závisí pouze na autorovi, nezávisí na zprávě.

**x** Digitální podpis musí použít nějaké jedinečné informace pro odesílatele, aby se předešlo padělání a odmítnutí.

**x** Výstup hash funkce má pevnou délku.

□ Ze zprávy je jednoduché určit její hash a naopak.

**x** Je výpočetně neproveditelné nalézt dvě různé zprávy, jejichž otisk je stejný.

□ Různé zprávy mají vždy různé hodnoty hash funkce.

1. Napiš následující typy útoků do tabulky jako aktivní nebo pasivní.

Eavesdropping, masquerade, analýza provozu, replay, denial of service, modifikace

|  |  |
| --- | --- |
| Aktivní | **masquerade, replay, denial of service, modifikace** |
| Pasivní | **eavesdropping, analýza provozu** |

1. Napiš čísla správných tvrzení.

|  |
| --- |
| **2** |
| **4** |
|  |
|  |
|  |

**1** – Digitální certifikát obsahuje tajný klíč subjektu nebo držitele certifikátu a zároveň identifikační data držitele certifikátu.

**2** – Digitální certifikát je podepsán privátním klíčem certifikační autority (CA)..

**3** – Tajný klíč certifikovaný certifikátem bude fungovat pouze s odpovídajícím veřejným klíčem vydaným entitou identifikovanou certifikátem.

**4** – Digitální certifikát spojuje veřejný klíč s identitou..

**5** – Digitální certifikát obsahuje veřejný klíč odpovídající certifikační autority (CA).