1. Vyberte jednu možnosť v zátvorkách tak, aby tvrdenia boli pravdivé.

Jeden z hlavných problémov kryptografie s je distribúcia kľúčov

na stranu adresáta.

šifrovanie byť použité na vytvorenie digitálneho podpisu.

šifrovanie byť použité na vytvorenie digitálneho podpisu.

V prípade, že je použitý režim , informácia o štruktúre otvoreného textu je odkrytá.

Ak použijeme režim CBC, k obmedzeniu šírenia chýb.

Ak nastane chyba v zašifrovanom texte, pri aplikácii režimu sa tieto chyby v dešifrovanom otvorenom texte.

Ak nastane chyba v zašifrovanom texte, pri aplikácii režimu sa tieto chyby v dešifrovanom otvorenom texte.

Ak nastane chyba v zašifrovanom texte, pri aplikácii režimu sa tieto chyby v dešifrovanom otvorenom texte.

1. Spojte termíny na ľavej strane s prislúchajúcimi definíciami vpravo.

**7**

**6**

**5**

**4**

**3**

**2**

**1**

používa pseudo-náhodnú postupnosť, ktorá závisí aj od zašifrovaného textu.

Symetrické šifrovanie

môže mať symetrický, alebo asymetrický algoritmus.

Prúdová šifra

Prúdová šifra

ponúka buď dôvernosť informácií alebo autentifikáciu zdroja.

používa výhradne symetrický kľúč

na šifrovanie a dešifrovanie.

využíva pseudo-náhodnú postupnosť, vytvorenú nezávisle na otvorenom

a zašifrovanom texte.

pracuje s časovo-premennou transformáciou otvoreného textu

a transformuje každý prvok zvlášť.

Bloková šifra

Prúdová šifra so spätnou väzbou

Asymetrické šifrovanie

ponúka vždy zároveň dôvernosť

a autentifikáciu.

**5**

**4**

**7**

**2**

**6**

**3**

**1**

Synchrónna prúdová šifra

1. Označte pravdivé tvrdenia.

□ Digitálny podpis je závislý iba na autorovi. Nezávisí na obsahu správy.

x Aby sa predišlo falšovaniu, digitálny podpis musí obsahovať nejakú informáciu o odosielateľovi informácie.

x Výstup hašovacej funkcie má fixnú dĺžku.

□ Ak získame správu, je jednoduché nájsť jej hašovací kód a naopak.

□ Odlišné správy majú vždy odlišný hašovací kód.

1. Rozdeľte nasledujúce útoky na aktívne a pasívne.

Odpočúvanie, maškaráda, analýza prenosu, opakovanie, odopretie služby, modifikácia

|  |  |
| --- | --- |
| Aktívne | maškaráda, opakovanie, odopretie služby, modifikácia |
| Pasívne | odpočúvanie, analýza prenosu |

1. Do nasledujúcej tabuľky doplňte čísla správnych tvrdení týkajúcich sa digitálnych certifikátov.

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

**1** – Digitálny certifikát obsahuje tajný kľúč subjektu alebo držiteľa certifikátu, podobne ako aj identifikačné údaje držiteľa certifikátu.

**2** – Digitálne certifikáty sú podpísané súkromným kľúčom certifikačnej autority (CA).

**3** – Iba tajný kľúč certifikovaný certifikátom bude fungovať so zodpovedajúcim verejným kľúčom, ktorý vlastní subjekt identifikovaný certifikátom.

**4** – Digitálne certifikáty spájajú verejný kľúč s identitou.

**5** – Digitálny certifikát obsahuje verejný kľúč zodpovedajúcej certifikačnej autority (CA).