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

Ak použijeme kryptografiu s kľúčom, odosielateľ a príjemca nepotrebujú zdieľať žiaden kľúč.

Na overenie digitálneho podpisu je potrebný .

Dĺžka kľúča v symetrických šifrách je ako v asymetrických šifrách (kryptografia

s verejným kľúčom).

V symetrických šifrách je šifrovací proces ako v asymetrických šifrách.

šifry používajú na šifrovanie a dešifrovanie.

šifry používajú na šifrovanie a dešifrovanie.

V hybridnom šifrovacom procese sú používateľské dáta šifrované pomocou algoritmov kryptografie s kľúčom.

V hybridnom šifrovaní sa šifrujú .

1. Označte pravdivé tvrdenia.

**X** Digitálny podpis musí byť postupnosť bitov, ktorá závisí na danej podpisovanej správe.

□ Realizácia a implementácia digitálneho podpisu musí byť relatívne ľahká bez tajného kľúča podpisujúcej sa osoby.

**X** Falšovanie digitálneho podpisu musí byť výpočtovo nemožné, či už vytvorením novej správy pre existujúci podpis alebo vytvorením falošného digitálneho podpisu pre danú správu.

□ Daným digitálnym podpisom možno získať príslušnú správu.

**X** Na potvrdenie digitálneho podpisu je požadovaný verejný kľúč podpisujúceho sa.

1. Spojte termíny na ľavej strane s prislúchajúcimi definíciami vpravo (jeden a viac).

bráni používaniu falošných verejných kľúčov na napodobovanie používateľov.

Digitálne certifikáty

Hašovacia funkcia

obsahuje digitálny podpis.

nepoužíva žiadne kľúče.

je jednosmerná funkcia.

používa sa na výmenu kľúčov.

spája verejný kľúč s identitou.

neobsahujú žiadnu časovú referenciu.

1. Do nasledujúcej tabuľky doplňte čísla správnych tvrdení, ktoré sa týkajú mechanizmov útokov.

|  |
| --- |
| **1** |
| **3** |
| **4** |
|  |
|  |

**1** – Analýza prevádzky sa vzťahuje na proces zachytenia a skúmania správ tak, aby bolo možné zistiť konkrétnu informáciu zo zachytenej komunikácie.

**2** – Hostiteľské útoky sú všetky typy útokov, ktoré majú prelomiť ochranu počítača alebo siete takým spôsobom, že zamedzia konkrétnym používateľom obsluhu daného zariadenia alebo siete.

**3** – Útoky na úrovni protokolov využívajú výhody známych (alebo menej známych) slabín v sieťových službách.

**4** – V útokoch „Man in the Middle“ (človek uprostred, MitM), útočník sleduje komunikáciu medzi dvoma stranami, zvyčajne medzi koncovým používateľom a web stránkou.

**5** – Útok „výpadok služby“ využíva zraniteľnosť operačných systémov obetí alebo to, ako je systém nastavený a spravovaný.