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

Při použití nemusí odesílatel a příjemce sdílet tajný klíč.

Pro účely ověření digitálního podpisu je nutný .

Klíč u symetrického šifrování je než klíč u šifrování veřejným klíčem.

Proces symetrického šifrování je než proces šifrování veřejným klíčem.

používá pro šifrování i dešifrování.

používá pro šifrování i dešifrování.

Při hybridní kryptografii uživatel data šifruje .

Při hybridní kryptografii je použit pro šifrování .

1. Označ pravdivá tvrzení.

□ Podpis musí mít formu bitové postupnosti, která závisí na podepisované zprávě.

□ Realizace a implementace digitálního podpisu musí být relativně jednoduchá bez soukromého klíče.

□ Falšování digitálního podpisu musí být výpočetně neproveditelné. Falšováním se vytvoří buď nová zpráva pro existující digitální podpis, nebo falešný digitální podpis pro existující zprávu.

□ Na základě digitálního podpisu je možné nalézt zprávu.

□ Veřejný klíč osoby, která se hodlá podepsat, je vyžadován k verifikaci jejího podpisu.

1. Přiřaď termíny z levého sloupce odpovídajícím definicím umístěným vpravo (jeden či více).

brání v používání falešných veřejných klíčů pro zosobnění

Digitální certifikáty

Hash funkce

zahrnuje digitální podpis

nepoužívá žádné klíče

je jednocestná funkce

jsou užitečné pro výměnu klíčů

spojují veřejný klíč s identitou

nezahrnuje žádnou časovou referenci

1. Napiš čísla správných tvrzení.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

**1** – Analýza provozu označuje proces odposlouchávání a analýzy zpráv za účelem získání jakýchkoli informací o komunikaci.

**2** – Hostitelské útoky označují všechny typy útoků, jejichž cílem je pozměnit počítače nebo sítě tak, že oprávněný uživatel počítače nebo sítě jej nebude moci použít.

**3** – Útoky na protokoly využívají známé (nebo dosud neznámé) slabé stránky síťových služeb.

**4** – Při útoku typu MitM (Man in the Middle) útočník zachytí komunikaci mezi dvěma stranami, obvykle mezi uživatelem a web serverem.

**5** – Útoky typu DoS (Denial of Service) využívají zranitelnosti operačních systémů počítačů oběti nebo toho, jak je systém nastaven a spravován.