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

Při použití (~~symetrické kryptografie~~ / kryptografie veřejného klíče) nemusí odesílatel a příjemce sdílet tajný klíč.

Pro účely ověření digitálního podpisu je nutný (~~soukromý klíč odesílatele~~ / veřejný klíč odesílatele / ~~soukromý klíč příjemce~~ / ~~soukromý klíč příjemce~~).

Klíč u symetrického šifrování je (kratší / ~~delší~~) než klíč u šifrování veřejným klíčem.

Proces symetrického šifrování je (~~pomalejší~~ / rychlejší) než proces šifrování veřejným klíčem.

(Symetrická kryptografie / ~~Kryptografie veřejného klíče~~) používá (stejný klíč / ~~různé klíče~~) pro šifrování i dešifrování.

(~~Symetrická kryptografie~~ / Kryptografie veřejného klíče) používá (~~stejný klíč~~ / různé klíče) pro šifrování i dešifrování.

Při hybridní kryptografii uživatel data šifruje (symetrickým algoritmem / ~~algoritmem veřejného klíče~~).

Při hybridní kryptografii je (~~soukromý klíč odesílatele~~ / ~~veřejný klíč odesílatele~~ / ~~soukromý klíč příjemce~~ / soukromý klíč příjemce) použit pro šifrování (~~uživatelských dat~~ / klíče relace).

---

2. Označ pravdivá tvrzení.

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

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

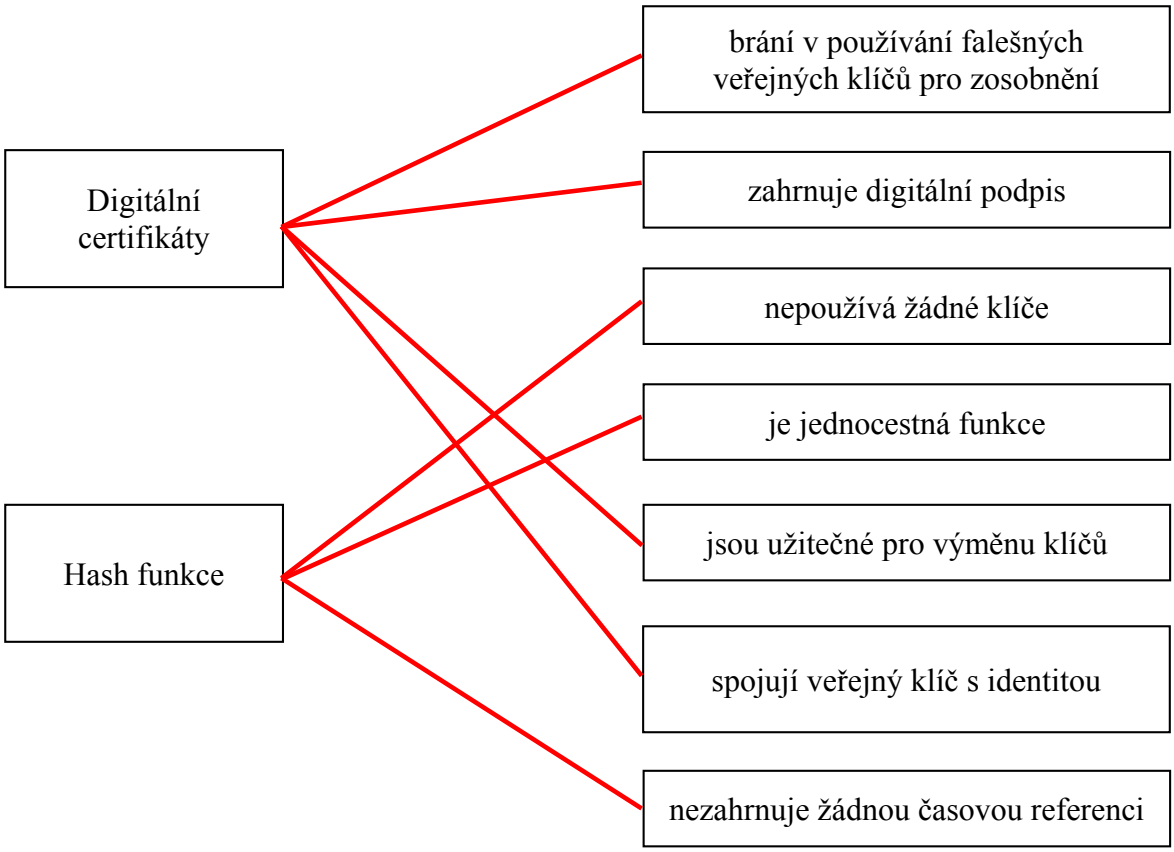
X Falšování digitálního podpisu musí být výpočetně neproveditelné. Falšováním se vytvoří buď nová zpráva pro existující digitální podpis, nebo falešný digitální podpis pro existující zprávu.

☐ Na základě digitálního podpisu je možné nalézt zprávu.

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

Erasmus+
Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

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



Erasmus+
Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

4. Napiš čísla správných tvrzení.

1
3
4

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.

Erasmus+
Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.