

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

Při použití $\left(\begin{array}{l} \text{symetrické kryptografie} \\ \text{kryptografie veřejného klíče} \end{array} \right)$ nemusí odesílatel a příjemce sdílet tajný klíč.

Pro účely ověření digitálního podpisu je nutný $\left(\begin{array}{l} \text{soukromý klíč odesílatele} \\ \text{veřejný klíč odesílatele} \\ \text{soukromý klíč příjemce} \\ \text{soukromý klíč příjemce} \end{array} \right)$.

Klíč u symetrického šifrování je $\left(\begin{array}{l} \text{kratší} \\ \text{delší} \end{array} \right)$ než klíč u šifrování veřejným klíčem.

Proces symetrického šifrování je $\left(\begin{array}{l} \text{pomalejší} \\ \text{rychlejší} \end{array} \right)$ než proces šifrování veřejným klíčem.

$\left(\begin{array}{l} \text{Symetrická kryptografie} \\ \text{Kryptografie veřejného klíče} \end{array} \right)$ používá $\left(\begin{array}{l} \text{stejný klíč} \\ \text{různé klíče} \end{array} \right)$ pro šifrování i dešifrování.

$\left(\begin{array}{l} \text{Symetrická kryptografie} \\ \text{Kryptografie veřejného klíče} \end{array} \right)$ používá $\left(\begin{array}{l} \text{stejný klíč} \\ \text{různé klíče} \end{array} \right)$ pro šifrování i dešifrování.

Při hybridní kryptografii uživatel data šifruje $\left(\begin{array}{l} \text{symetrickým algoritmem} \\ \text{algoritmem veřejného klíče} \end{array} \right)$.

Při hybridní kryptografii je $\left(\begin{array}{l} \text{soukromý klíč odesílatele} \\ \text{veřejný klíč odesílatele} \\ \text{soukromý klíč příjemce} \\ \text{soukromý klíč příjemce} \end{array} \right)$ použit pro šifrování $\left(\begin{array}{l} \text{uživatelských dat} \\ \text{klíče relace} \end{array} \right)$.

2. Označ pravdivá tvrzení.

- ☐ Podpis musí mít formu bitové postupnosti, která závisí na podepsované 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.



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

	brání v používání falešných veřejných klíčů pro zosobnění
Digitální certifikáty	zahrnuje digitální podpis
	nepoužívá žádné klíče
	je jednocestná funkce
Hash funkce	jsou užitečné pro výměnu klíčů
	spojují veřejný klíč s identitou
	nezahrnuje žádnou časovou referenci



4. 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 síť 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.

