

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

Ak použijeme kryptografiu s (~~tajným~~
verejným) kľúčom, odosielateľ a príjemca nepotrebujú zdieľať žiaden kľúč.

Na overenie digitálneho podpisu je potrebný (~~súkromný kľúč podpisujúceho sa~~
verejný kľúč podpisujúceho sa
~~súkromný kľúč príjemcu~~
verejný kľúč príjemcu).

Dĺžka kľúča v symetrických šifrách je (~~dlhšia~~
kratšia) ako v asymetrických šifrách (kryptografia s verejným kľúčom).

V symetrických šifrách je šifrovací proces (~~pomalší~~
rýchlejší) ako v asymetrických šifrách.

(**Symetrické**) šifry používajú (**rovnaký kľúč**) na šifrovanie a dešifrovanie.
(~~Asymetrické~~) (~~odlišné kľúče~~)

(~~Symetrické~~) (~~Asymetrické~~) šifry používajú (**rovnaký kľúč**) na šifrovanie a dešifrovanie.
(**odlišné kľúče**)

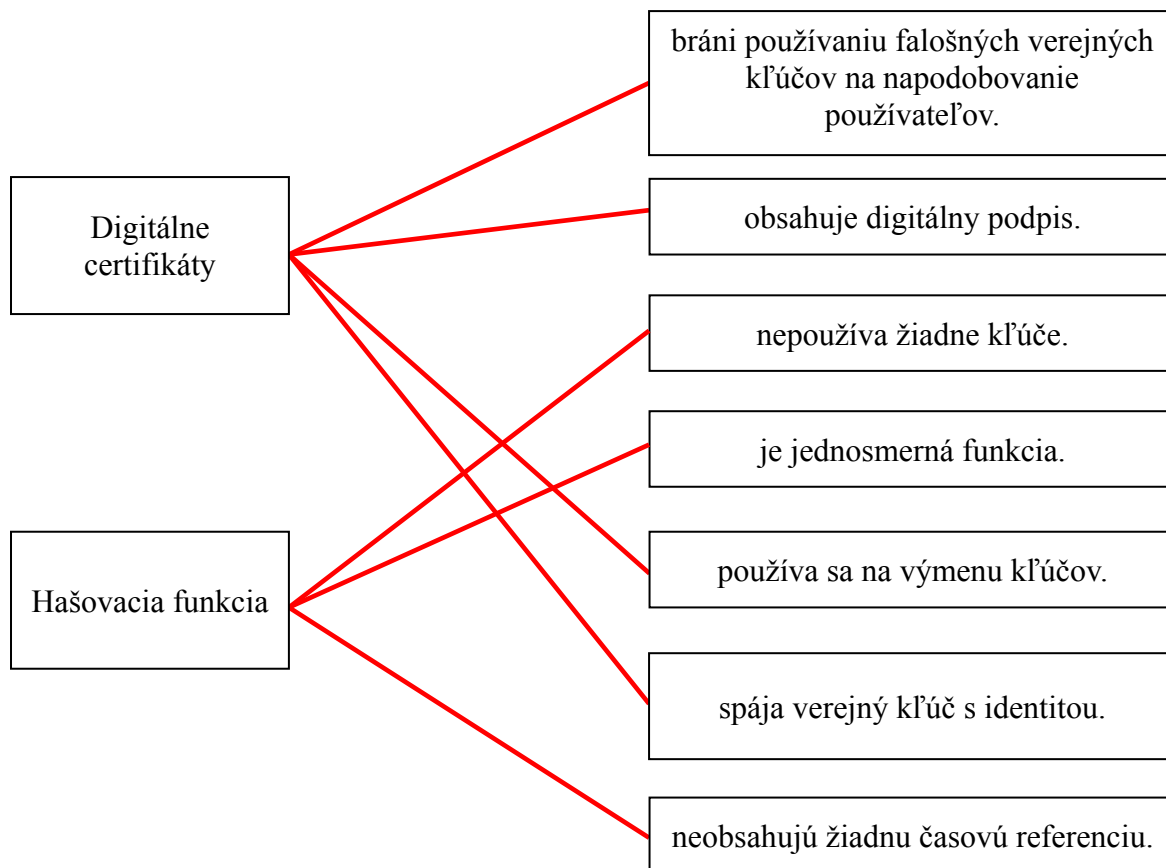
V hybridnom šifrovacom procese sú používateľské dáta šifrované pomocou algoritmov kryptografie s (~~tajným~~
verejným) kľúčom.

V hybridnom šifrovaní sa (~~tajným kľúčom odosielateľa~~
~~verejným kľúčom odosielateľa~~
~~tajným kľúčom príjemcu~~
verejným kľúčom príjemcu) šifrujú (~~používateľské dáta~~
kľúč relácie).

2. 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.



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

4. 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.

