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

Jeden z hlavních problémů (symetrické kryptografie / ~~kryptografie veřejného klíče~~) je proces výměny klíčů.

(Symetrická kryptografie / ~~Kryptografie veřejného klíče~~) (~~může~~ / nemůže) být užita k vytvoření digitálního podpisu.

(~~Symetrická kryptografie~~ / Kryptografie veřejného klíče) (může / ~~nemůže~~) být užita k vytvoření digitálního podpisu.

Při použití operace (ECB / ~~CBC~~) je vystavena strukturální informace holého textu.

Při použití druhu provozu CBC (je / ~~není~~) chyba šíření omezena.

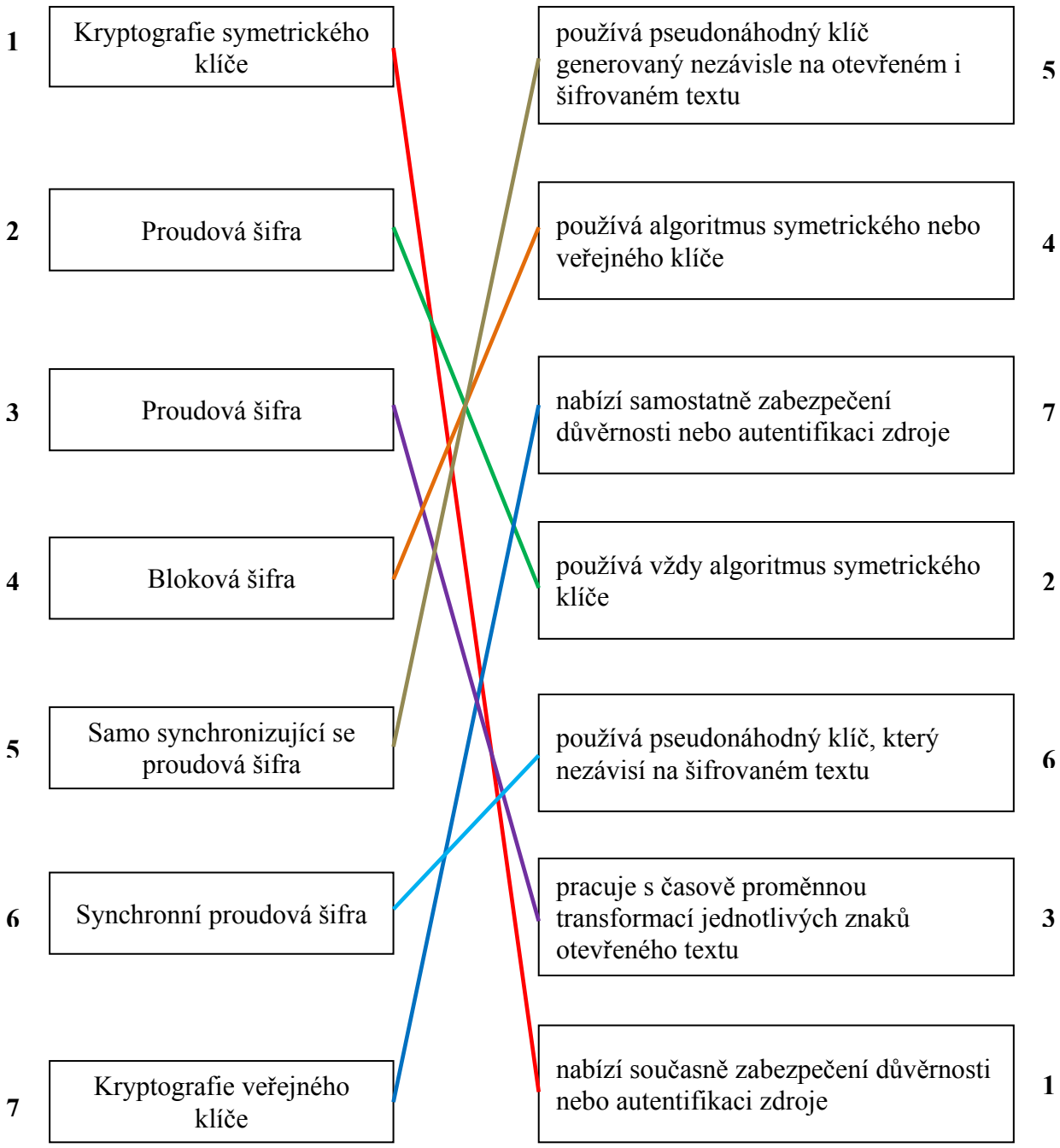
Nastane-li chyba v šifrovaném textu, tak při použití druhu provozu (CFB / ~~OFB~~ / ~~CTR~~) (jsou / ~~nejsou~~) tyto chyby propagovány i v obdrženém textu.

Nastane-li chyba v šifrovaném textu, tak při použití druhu provozu (~~CFB~~ / OFB / ~~CTR~~) (~~jsou~~ / nejsou) tyto chyby propagovány i v obdrženém textu.

Nastane-li chyba v šifrovaném textu, tak při použití druhu provozu (~~CFB~~ / ~~OFB~~ / CTR) (~~jsou~~ / nejsou) tyto chyby propagovány i v obdrženém textu.

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.

2. Přiřaď termíny z levého sloupce odpovídajícím definicím umístěným vpravo.



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. Označ pravdivá tvrzení.

☐ Digitální podpis závisí pouze na autorovi, nezávisí na zprávě.

X Digitální podpis musí použít nějaké jedinečné informace pro odesílatele, aby se předešlo padělání a odmítnutí.

X Výstup hash funkce má pevnou délku.

☐ Ze zprávy je jednoduché určit její hash a naopak.

X Je výpočetně neproveditelné nalézt dvě různé zprávy, jejichž otisk je stejný.

☐ Různé zprávy mají vždy různé hodnoty hash funkce.

---

4. Napiš následující typy útoků do tabulky jako aktivní nebo pasivní.

Eavesdropping, masquerade, analýza provozu, replay, denial of service, modifikace

Aktivní	**masquerade, replay, denial of service, modifikace**
Pasivní	**eavesdropping, analýza provozu**

---

5. Napiš čísla správných tvrzení.

2
4

1 – Digitální certifikát obsahuje tajný klíč subjektu nebo držitele certifikátu a zároveň identifikační data držitele certifikátu.

2 – Digitální certifikát je podepsán privátním klíčem certifikační autority (CA)..

3 – Tajný klíč certifikovaný certifikátem bude fungovat pouze s odpovídajícím veřejným klíčem vydaným entitou identifikovanou certifikátem.

4 – Digitální certifikát spojuje veřejný klíč s identitou..

5 – Digitální certifikát obsahuje veřejný klíč odpovídající certifikační autority (CA).

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.