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

Jeden z hlavných problémov kryptografie s (tajným kľúčom / verejným kľúčom) je distribúcia kľúčov na stranu adresáta.

(Symetrické / Asymetrické) šifrovanie (môže / nemôže) byť použité na vytvorenie digitálneho podpisu.

V prípade, že je použitý režim (ECB / CBC), informácia o štruktúre otvoreného textu je odkrytá.

Ak použijeme režim CBC, (dôjde / nedôjde) k obmedzeniu šírenia chýb.

Ak nastane chyba v zašifrovanom texte, pri aplikácii režimu (CFB / OFB / CTR) sa tieto chyby (šíria / nešíria) v dešifrovanom otvorenom texte.

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

2. Spojte termíny na ľavej strane s prislúchajúcimi definíciami vpravo.

Symetrické šifrovanie	používa pseudo-náhodnú postupnosť, ktorá závisí aj od zašifrovaného textu.
Prúdová šifra	môže mať symetrický, alebo asymetrický algoritmus.
Prúdová šifra	ponúka buď dôvernosť informácií alebo autentifikáciu zdroja.
Bloková šifra	používa výhradne symetrický kľúč na šifrovanie a dešifrovanie.
Prúdová šifra so spätnou väzbou	využíva pseudo-náhodnú postupnosť, vytvorenú nezávisle na otvorenom a zašifrovanom texte.
Synchrónna prúdová šifra	pracuje s časovo-premennou transformáciou otvoreného textu a transformuje každý prvok zvlášť.
Asymetrické šifrovanie	ponúka vždy zároveň dôvernosť a autentifikáciu.

Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

3. Označte pravdivé tvrdenia.

☐ Digitálny podpis je závislý iba na autorovi. Nezávisí na obsahu správy.

☐ Aby sa predišlo falšovaniu, digitálny podpis musí obsahovať nejakú informáciu o odosielateľovi informácie.

☐ Výstup hašovacej funkcie má fixnú dĺžku.

☐ Ak získame správu, je jednoduché nájsť jej hašovací kód a naopak.

☐ Odlišné správy majú vždy odlišný hašovací kód.

---

4. Rozdeľte nasledujúce útoky na aktívne a pasívne.

Odpočúvanie, maškaráda, analýza prenosu, opakovanie, odopretie služby, modifikácia

Aktívne	
Pasívne	

---

5. Do nasledujúcej tabuľky doplňte čísla správnych tvrdení týkajúcich sa digitálnych certifikátov.

1 – Digitálny certifikát obsahuje tajný kľúč subjektu alebo držiteľa certifikátu, podobne ako aj identifikačné údaje držiteľa certifikátu.

2 – Digitálne certifikáty sú podpísané súkromným kľúčom certifikačnej autority (CA).

3 – Iba tajný kľúč certifikovaný certifikátom bude fungovať so zodpovedajúcim verejným kľúčom, ktorý vlastní subjekt identifikovaný certifikátom.

4 – Digitálne certifikáty spájajú verejný kľúč s identitou.

5 – Digitálny certifikát obsahuje verejný kľúč zodpovedajúcej certifikačnej autority (CA).

Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).