III gimnazijos klasė. Kriptografinės sistemos, viešasis ir privatusis raktas
30.3.4. Kriptografinės sistemos, viešasis ir privatusis raktas. Prisimenamos kriptografinės sistemos, simetrinis ir asimetrinis šifravimas. Apibrėžiamos viešojo ir privačiojo rakto, sertifikato sąvokos. Išbandomi kriptografinių sistemų pavyzdžiai (pavyzdžiui, OpenPGP). Diskutuojama apie sertifikato patikimumo požymius.

Ugdomos kompetencijos: Pažinimo, skaitmeninė

Pasiekimų lygiai
Slenkstinis: Apibrėžia kriptografinės sistemos, viešojo rakto, sertifikato sąvokas (C3.1).
Patenkinamas: Aptaria kriptografinės sistemos, viešojo rakto, sertifikato patikimumą (C3.2).
Pagrindinis: Vertina kriptografinės sistemos, viešojo rakto, sertifikato patikimumą (C3.3).
Aukštesnysis: Vertina kriptografinės sistemos, viešojo rakto, sertifikato patikimumą (C3.4).

Testas „Kriptografija“

Nr.	**Klausimas**	**Atsakymas**	**Vertinimas**
1	Kaip vadinasi mokslas, nagrinėjantis informacijos užšifravimo ir iššifravimo metodus?	Kriptografija	**1 taškas**
2	Apibrėžkite, kas yra duomenų šifravimo sertifikatas?	Sertifikatas yra dokumentas, patvirtinantis raktų autentiškumą.	**1 taškas**
3	Kai tas pats raktas naudojamas pranešimams užšifruoti ir iššifruoti, turime: A. Šifruotą tekstą B. Paprastą tekstą C. Asimetrinį šifravimą D. Simetrinį šifravimą	D	**1 taškas**
4	Naudodamas asimetrinį šifravimą asmuo X nori pasirašyti ir	Jei klausime būtų kalbama tik **apie šifravimą**, tai	**1 taškas**

	išsiųsti šifruotą pranešimą asmeniui Y. Kurį raktą asmuo X naudoja pranešimui užšifruoti? A. Y privatųjį raktą B. Y viešąjį raktą C. X privatųjį raktą D. X viešąjį raktą	teisingas atsakymas B. Šį kartą klausiama klausiama **apie pranešimo pasirašymą**, tai teisingas dar ir C atvejis.	
5	Kodėl sertifikatai laikomi patikimu viešojo rakto autentiškumo patvirtinimu?	Sertifikatai patvirtina viešojo rakto autentiškumą, nes juos išduoda patikimos sertifikavimo institucijos, kurios patvirtina rakto savininko tapatybę.	**1 taškas**
6	Nurodykite du simetrinio šifravimo trūkumus lyginant su asimetriniu šifravimu?	Galimi atsakymai: ● **Simetrinis šifravimas** reikalauja, kad abi šalys (siuntėjas ir gavėjas) turėtų tą patį raktą, kad galėtų užšifruoti ir iššifruoti pranešimus.Raktų perdavimas gali būti nesaugus, nes jei kas nors sužino raktą, jis galės pasiekti visus šifruotus pranešimus. Tai gali būti pavojinga, jei raktas perduodamas nepatikimu kanalu (pvz., per internetą). ● **Simetrinio šifravimo raktų valdymas** tampa sudėtingas, kai naudojama daug šifruotų pranešimų tarp daugelio dalyvių, nes kiekvienam poros dalyviui reikalingas atskiras raktas.Tad reikia keistis daugeliu raktų, tai tampa sunku valdyti, saugoti ir užtikrinti jų paslaptį. Tai rimtas iššūkis didelėse sistemose. ● **Simetrinio šifravimo raktas** turi būti saugomas saugiai. Jei raktas prarandamas	**2 taškai**

		arba pavagiamas, visi šifruoti duomenys tampa pažeidžiami.Norint užtikrinti šifruotų duomenų saugumą, raktai turi būti apsaugoti ir valdomi itin atsargiai. ● **Simetrinis šifravimas** negali natūraliai užtikrinti žinutės autentiškumo (kas ją siuntė), nes jis neturi mechanizmo, leidžiančio patikrinti siuntėjo tapatybę. Jei tikslas yra užtikrinti ir šifravimą, ir autentifikavimą, tai simetrinis šifravimas tam nėra pakankamai saugus be papildomų priemonių (pvz., skaitmeninio parašo). ● **Simetrinis šifravimas** paprastai yra greitesnis nei asimetrinis šifravimas, tačiau siekiant užtikrinti didelį saugumą, šifravimo algoritmai gali tapti sudėtingesni ir lėtesni, nes tenka naudoti labai ilgus raktus. ● **Simetrinis šifravimas** veikia gerai, kai yra tik keletas dalyvių ir tikslingai valdomi raktai, tačiau esant dideliam skaičiui dalyvių, raktų valdymas ir apsauga gali tapti neįmanomi arba labai sudėtingi.	
7	Kokia yra kriptoanalizės paskirtis? Kokiais atvejais ji naudojama?	Pagrindinė kriptoanalizės paskirtis yra analizuoti, ar šifravimo metodas yra saugus. Dažniausiai naudojama šifravimo stiprumui išbandyti.	**2 taškai** 1 taškas už tinkamai nurodytą kriptoanalizės paskirtį, 1 taškas

			už tinkamai nurodytus naudojimo atvejus.
8	Paaiškinkite, kuo skiriasi viešasis raktas ir privatusis raktas asimetriniame šifravime.	Viešasis raktas naudojamas duomenų šifravimui ir yra prieinamas visiems, o privatusis raktas yra laikomas paslaptyje ir naudojamas dešifravimui. Tik žinant privatųjį raktą, galima iššifruoti viešuoju raktu užšifruotus duomenis.	**2 taškai** 1 taškas už viešojo rakto, 1 taškas už privačiojo paskirties apibūdinimą.
9	Nurodykite du atvejus, kada tikslinga naudoti simetrinį šifravimą.	**Reikia greito šifravimo dideliems duomenų kiekiams**: Simetrinis šifravimas yra itin greitas, todėl jis puikiai tinka apsaugoti didelius duomenų srautus, pavyzdžiui, kai reikia šifruoti failus, diskus ar komunikaciją realiu laiku. **Duomenis saugoti reikia vietoje, o ne perduoti**: Kai duomenys saugomi viename įrenginyje, galima saugiai naudoti simetrinį šifravimą, nes nėra būtina perduoti raktą tinklu. **Galima saugiai perduoti šifravimo raktą**: Simetrinis šifravimas yra naudingas, jei abiem pusėms (pvz., siuntėjui ir gavėjui) įmanoma saugiai perduoti raktą asmeniškai arba naudojant saugius kanalus. **Reikalinga greita ir efektyvi apsauga tinklo ryšiuose**: Simetrinis šifravimas dažnai naudojamas šifruotam ryšiui užtikrinti VPN ar HTTPS ryšiuose, nes jis leidžia užtikrinti saugų ryšį, neapkraunant sistemos.	**2 taškai** Po 1 tašką už kiekvieną atvejį.

10	Nurodykite du atvejus, kada tikslinga naudoti asimetrinį šifravimą.	**Reikia saugiai perduoti raktus nesaugiu kanalu**: Asimetrinis šifravimas yra idealiai tinkamas, kai raktai turi būti perduodami internetu arba kitu nesaugiu kanalu. Viešojo rakto metodas leidžia siuntėjui šifruoti duomenis, naudojant gavėjo viešąjį raktą, o tik gavėjas gali dešifruoti juos savo privačiuoju raktu. **Autentifikacija ir tapatybės patvirtinimas**: Asimetrinis šifravimas naudojamas siekiant užtikrinti, kad duomenys siunčiami ar pasirašomi patikimo šaltinio. Skaitmeniniai parašai naudoja privatųjį raktą, kad užtikrintų, jog duomenys siunčiami autentiško siuntėjo ir kad jų turinys yra nepažeistas. **Saugumas komunikacijoje su daug vartotojų**: Asimetrinis šifravimas tinkamas, kai būtina apsikeisti raktų informacija tarp daugelio vartotojų, nes kiekvienas vartotojas turi savo viešąjį raktą, prieinamą visiems, ir privatųjį raktą, laikomą paslaptyje. **Skaitmeninių sertifikatų ir saugių ryšių užmezgimas**: Viešojo rakto infrastruktūra, kuri remiasi asimetriniu šifravimu, leidžia kurti skaitmeninius sertifikatus, kurie patvirtina tapatybę ir užtikrina saugų internetinį ryšį (pvz., SSL/TLS sertifikatai).	**2 taškai** Po 1 tašką už kiekvieną teisingą atsakymą.
11	Kaip skaitmeniniai sertifikatai užtikrina, kad prieigą prie informacijos turi tik autentiški vartotojai? A. Naudodami viešojo ir privataus rakto porą. B. Tikrindami slaptažodį. C. Analizuodami naudotojo naršymo istoriją.	A Skaitmeniniai sertifikatai remiasi viešojo ir privataus rakto poros naudojimu, kad užtikrintų, jog prieigą prie informacijos turi tik autentiški	**1 taškas**

	D. Patikrindami geografinę vietą.	vartotojai. Viešasis raktas naudojamas šifruoti informaciją, o privatus – ją dešifruoti.	
12	Koks pagrindinis skaitmeninio sertifikato vaidmuo užtikrinant saugumą? A. Patvirtinti ryšio kanalo greitį. B. Patvirtinti viešojo rakto priklausymą konkrečiam subjektui. C. Valdyti privatųjį raktą. D. Pakeisti slaptažodžius kas 30 dienų.	B Skaitmeninis sertifikatas patvirtina, kad viešasis raktas priklauso konkrečiam subjektui (pvz., asmeniui, organizacijai, serveriui), taip užtikrindamas saugų ir patikimą duomenų perdavimą.	**1 taškas**
13	Kodėl svarbu, kad skaitmeninį sertifikatą išduotų patikima sertifikavimo institucija? A. Užtikrinti, kad sertifikatas atitiktų tarptautinius standartus. B. Suteikti sertifikatui garantiją ir pratęsti jo galiojimo laiką. C. Užtikrinti, kad sertifikatas yra išduotas patikimo šaltinio, kuris patikrino subjekto tapatybę. D. Užtikrinti, kad sertifikatas veiktų tik tam tikrose šalyse.	C Patikima sertifikavimo institucija patikrina subjekto tapatybę ir užtikrina, kad viešasis raktas priklauso patikimam šaltiniui, taip sumažindama sukčiavimo riziką.	**1 taškas**
14	Koks yra pagrindinis simetrinio šifravimo trūkumas? A. Sunkiai įgyvendinamas didelėse sistemose. B. Reikia saugiai perduoti raktą gavėjui. C. Lėtas duomenų apdorojimas. D. Nepalaiko didelio duomenų kiekio šifravimo.	B Pagrindinis simetrinio šifravimo trūkumas yra raktų perdavimo problema – raktas turi būti perduotas saugiu kanalu, nes jo praradimas leistų bet kam dešifruoti duomenis.	**1 taškas**
15	Kuriame iš šių atvejų simetrinis šifravimas yra ypač naudingas?	B	**1 taškas**

	A. Kai reikia saugiai perduoti raktus per nesaugų kanalą. B. Kai duomenis reikia šifruoti dideliu greičiu. C. Kai duomenis reikia laikyti ilgą laiką. D. Kai reikia autentifikuoti pranešimo siuntėją.	Simetrinis šifravimas yra naudingas, kai reikia greitai šifruoti didelius duomenų kiekius, nes šis metodas veikia efektyviau nei asimetrinis šifravimas.	
16	Kaip simetrinis šifravimas apsaugo duomenis, saugomus diske? A. Jis automatiškai keičia raktus kas savaitę. B. Jis šifruoja duomenis naudojant tą patį raktą, kuris vėliau naudojamas duomenims iššifruoti. C. Jis šifruoja duomenis naudodamas viešojo rakto metodą. D. Jis saugo duomenis serveriuose, užtikrinant jų pasiekiamumą.	B Naudojant simetrinį šifravimą, tas pats raktas naudojamas tiek duomenų šifravimui, tiek jų iššifravimui. Šis metodas užtikrina duomenų saugumą diske.	**1 taškas**
17	Kuri simetrinio šifravimo metodo ypatybė gali sukelti saugumo problemų? A. Vienas raktas naudojamas šifravimui ir dešifravimui. B. Raktą reikia perduoti viešu kanalu. C. Jis per lėtas greitai informacijai apdoroti. D. Naudojamas tik tekstinių failų apsaugai.	A Simetrinio šifravimo saugumo problema kyla dėl to, kad tas pats raktas naudojamas tiek šifruojant, tiek dešifruojant duomenis. Jei raktas pasisavinamas, visas užšifruotas turinys tampa pažeidžiamas.	**1 taškas**
18	Koks yra pagrindinis asimetrinio šifravimo privalumas? A. Jis yra greitesnis nei simetrinis šifravimas. B. Jame galima saugiai perduoti raktus nesaugiu kanalu. C. Naudojamas vienas bendras raktas, todėl paprasta valdyti. D. Gali būti naudojamas tik vietiniam failų šifravimui.	B Asimetrinis šifravimas leidžia saugiai perduoti raktus nesaugiu kanalu, nes viešasis raktas gali būti laisvai dalijamas, o privatusis lieka tik gavėjo žinioje.	**1 taškas**
19	Kokiais atvejais paprastai naudojamas asimetrinis	B	**1 taškas**

	šifravimas? . Didelių duomenų kiekių greitam šifravimui. A. Siekiant autentifikuoti vartotoją ir patikrinti jo tapatybę. B. Duomenų saugojimui vietiniuose įrenginiuose. C. Realiojo laiko duomenų šifravimui dideliu greičiu.	Asimetrinis šifravimas dažnai naudojamas autentifikacijai, siekiant patvirtinti vartotojo ar serverio tapatybę, pvz., naudojant skaitmeninius parašus ir sertifikatus.	