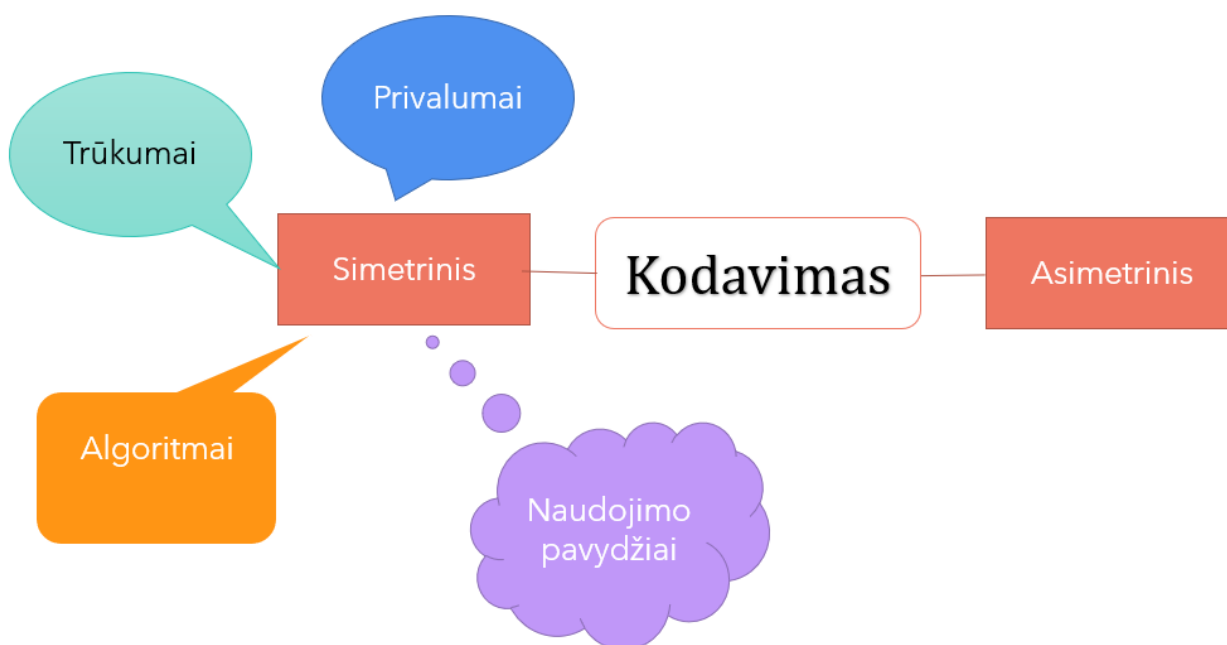


9-10 klasė (I-II gimnazijos) klasė

Simetrinis ir asimetrinis kodavimas, kriptografinės sistemos (Skirmantė Vardauskaitė)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija 29.3.3. Simetrinis ir asimetrinis kodavimas, kriptografinės sistemos.
Klasė	9-10
Tema	Simetrinis ir asimetrinis kodavimas, kriptografinės sistemos.
Integruojami dalykai, pasiekimai	Lietuvių kalba, anglų kalba
Kompetencijos	<ul style="list-style-type: none"> • Pažinimo – gilina informatikos žinias; ugdomi informatinį mąstymą. • Skaitmeninė – užtikrintai ir sumaniai naudojami skaitmeninėmis priemonėmis. • Kūrybiškumo – nuolat skatinami ieškoti kūrybiškų sprendimų. • Komunikavimo – ugdomas gebėjimas pamokos ar kitos veiklos metu teikti informatyvią grįžtamąją informaciją mokytojui; konstruktyviai planuoja ir organizuoja savo darbą.
Tikslas	Susipažinti su simetriniu ir asimetriniu kodavimu.
Uždaviniai	1. Sukurti minčių žemėlapi apie simetrinį ir asimetrinį kodavimą.
Planuojamas rezultatas	Naudojantis klasėje bendrai sukurtu minčių žemėlapio gebės paaiškinti kas yra simetrinis ir asimetrinis kodavimas, jų privalumus, trūkumus, kokie algoritmai naudojami ir kur šie kodai pritaikomi.
Specifinės priemonės / programinė įranga	Nuoroda: paskaita simetrinis ir asimetrinis kodavimas . Ši nuoroda pateikiama jau prieš savaitę, kad mokiniai namuose peržiūrėtų. Galima žiūrėti ir nustačius lietuviškus subtitus. Bet kuri programa minčių žemėlapių kūrimui.
Mokymosi metodai	Apverstos klasės metodas, minčių žemėlapis.
Mokinių atlikto darbo vertinimas ir įsivertinimas	Vertinamas grupės darbas – minčių žemėlapis. Minčių žemėlapis: galima surinkti iki 8 balų. Maksimalus balų skaičius skiriamas, jeigu žemėlapyje yra daugiau atšakų negu pateikta pas mokytoją. Pristatymas: iki 2 balų. Maksimalus balus skiriamas, jeigu kalbama aiškiai, neskaitoma, atsakoma į mokytojo pateiktus klausimus.
Žinios prieš	Aptaria duomenų ir informacijos privatumo, patikimumo problemas, sprendžia šifravimo uždavinius.
Galimybės taikyti spec. poreikių mokiniams	SUP mokiniai integruojami kartu su visais mokiniais.
Patarimai kolegoms, kurie naudos	1. Būkite peržiūrėję duotą vaizdo įrašą. 2. Galite sukurti savo minčių žemėlapio maketą pagal mokinių gebėjimus.



1 ETAPAS ⌚ 5 minutės

Apklausa – diskusija kas yra kriptosistemos, kriptografija ir kam tai reikalinga.

2 ETAPAS ⌚ 25 minutės

Mokiniai po 4-5 padalinami į grupes. Kiekviena grupelė gauna mokytojo pradėtą, bet nepabaigtą minčių žemėlapi. Ir paprašoma, remiantis peržiūrėtu vaizdo įrašu bei kita susirasta informacija internete pratęsti šio žemėlapio pildymą. Darbui atlikti leidžiama naudotis bet kuria žemėlapių kūrimo programėle.

3 ETAPAS ⌚ 15 minučių

Kiekvienos grupės mokytojo parinktas atstovas paaiškina nurodytą minčių žemėlapio dalį, kiti grupės nariai papildo jo atsakymą.

4 ETAPAS ⌚ 5 minutės

Darbų apibendrinimas, įsivertinimas.

Simetrinis ir asimetrinis kodavimas, kriptografinės sistemos (Skirmantė Vardauskaitė)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija 29.3.3. Simetrinis ir asimetrinis kodavimas, kriptografinės sistemos.
Klasė	9-10
Tema	Simetrinis ir asimetrinis kodavimas, kriptografinės sistemos.

Integruojami dalykai, pasiekimai	Matematika Lietuvių kalba
Kompetencijos	<ul style="list-style-type: none"> Pažinimo – gilina informatikos žinias; ugdomi informatinį mąstymą. Skaitmeninė – užtikrintai ir sumaniai naudojasi skaitmeninėmis priemonėmis.
Tikslas	Išmokti taikyti RSA kodavimo algoritimą.
Uždaviniai	<ol style="list-style-type: none"> Išsiaiškinti kaip vyksta RSA kodavimas. Mokėti užšifruoti skaičius, taikant RSA algoritimą.
Planuojamas rezultatas	Mokės šifruoti skaitinę ir tekstinę informaciją, taikant RSA algoritimą.
Specifinės priemonės / programinė įranga	Leidiny: VU „Metodinė medžiaga mokytojui. Informacijos šifravimas“, 2022 Skaičiuotuvas kompiuteryje
Mokymosi metodai	Pateikčių naudojimas.
Mokinių atlikto darbo vertinimas ir įsivertinimas	Formuojamasis vertinimas.
Žinios prieš	Aptaria duomenų ir informacijos privatumo, patikimumo problemas, sprendžia šifravimo uždavinius.
Galimybės taikyti spec. poreikių mokiniams	SUP mokiniams, priklausomai nuo jų gebėjimų, šifravimui galima duoti kitą metodą, pvz., Cezario ar geležinkelio tvorelės. Aukštesnių gebėjimų mokiniai gali naudodami Excel sukurti kaip apskaičiuoti viešąjį raktą.
Patarimai kolegoms, kurie naudos parengtą medžiagą	<ol style="list-style-type: none"> Patys atlikite visas užduotis. Įsitikinkite, jog visos dalys yra aiškios. Jeigu klasė greitai įveikia visas užduotis, galima teksto šifravimo užduotį pateikti ir pamokos metu. Silpnesniems mokiniams gali tekti paruošti užduočių aprašus su kitais šifravimo metodais.

1 ETAPAS ⌚ 7 minutės

Frontalios apklausos metu pakartojama ką mokiniai žino apie kriptosistemas ir simetrinį bei asimetrinį kodavimus. Paklausiama su kokiais šifravimo metodais jau yra susidūrę ir ką prisimena iš ankstesnių klasių. Pristatoma, jog šiandien mokiniai aiškinsis kaip veikia asimetrinio kodavimo algoritmas RSA (Rivest–Shamir–Adleman abreviatūra).

2 ETAPAS ⌚ 35 minutės

Mokiniamis pateikiami RSA algoritmo etapai:

- 1) pasirenkami du pirminiai skaičiai p ir q ;
- 2) apskaičiuojama sandauga: $n = p \cdot q$;
- 3) apskaičiuojama sandauga: $k = (p - 1) \cdot (q - 1)$;
- 4) pasirenkamas viešasis raktas e , kuris neturi bendro daugiklio, išskyrus 1, su skaičiumi k ;
- 5) randamas toks privatus raktas d , kad galiojūt sąlyga $(d \cdot e) \bmod k = 1$. Šis raktas laikomas paslapyje.
- 6) jei pasirenkame skaičių m , kurį norime užšifruoti, tai skaičius keliamas k -tuoju laipsniu ir skaičiuojama gauto skaičiaus liekana, kuri gaunama, tą skaičių operacija mod dalijant iš n : $c = m^e \bmod n$.
- 7) norint užšifruotą skaičių c iššifruoti, skaičius c keliamas laipsniu d ir liekana, gauta dalijant c^d iš n yra skaičius m : $c^d \bmod n = m$.

Kartu sprendžiamas pavyzdys:

- 1) $p = 61$ ir $q = 53$.
- 2) $n = 61 \cdot 53 = 3233$;
- 3) $k = (61 - 1) \cdot (53 - 1) = 3120$;
- 4) $e = 17$;
- 5) $(2753 \cdot 17) \bmod 3120 = 1$, tai $d = 2753$;
- 6) $c = m^{17} \bmod 3233$, vadinasi jeigu norime užšifruoti $m = 123$, tai gausime $c = 123^{17} \bmod 3233 = 855$.
- 7) Iššifravus: $m = 855^{2753} \bmod 3233 = 123$.

Tada duodamos užduotys mokiniams:

1. Tegul $p = 7$ ir $q = 13$, viešasis raktas yra 5, o privatus – 2 (įsitikinkite, kad teisingai pasirinkti raktai). Užšifruokite skaičių 23 ir įsitikinkite, kad teisingai užšifravote, jį iššifruodami. Atsakymas 4.
2. Tegul $p = 5$ ir $q = 11$, viešasis raktas yra 3, o privatus – 27 (įsitikinkite, kad teisingai pasirinkti raktai). Užšifruokite skaičių 18 ir įsitikinkite, kad teisingai užšifravote, jį iššifruodami. Atsakymas 2.

3 ETAPAS 🕒 7-8 minutės

Užduočių aptarimas, pasitikrinimas. Paaiškinama, jog tokiu pačiu principu galima užšifruoti ir tekstą, kai kiekvienai raidei priskiriamas skaitmuo.

A	Ą	B	C	Č	D	E	Ę	Ė	F	G	H	I	Į	Y	J	K	L	M	N	O	P	R	S	Š	T	U	Ū	Ų	V	Z	Ž
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Namuose liepiama užšifruoti pasirinktą žodžių junginį ar savo vardą ir pavardę.

Dirbtinio intelekto sąvoka ir taikymas (Alvija Grimalauskienė)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija 29.3.2. Pažintis su dirbtiniu intelektu
Klasė	9-10
Tema	Dirbtinio intelekto sąvoka ir taikymas
Integruojami dalykai, pasiekimai	Anglų kalba, lietuvių kalba
Kompetencijos	Pažinimo – DI sąvoka ir taikymas. Skaitmeninė – informacijos ieškojimas įvairiuose informaciniuose šaltiniuose, minčių žemėlapiu programėlės naudojimas Kūrybiškumo – minčių žemėlapiu kūrimas ir apipavidalinimas. Komunikavimo – atliktų darbų pristatymai, pasidalinimas idėjomis, diskusijos.
Tikslas	Sužinoti kas yra dirbtinis intelektas ir kur jis taikomas
Uždaviniai	1. Informaciniuose šaltiniuose rasti dirbtinio intelekto (DI) sąvokos paaiškinimą 2. Sužinoti kur DI taikomas 3. Grupėse sukurti DI taikymo minčių žemėlapi.
Planuojamas rezultatas	1. Mokiniai dirbdami savarankiškai namuose įgis žinias, kurias praktiškai pritaikys pamokos metu klasėje atlikdami grupinį darbą. 2. Mokiniai dirbdami grupėse pagilins minčių žemėlapiu kūrimo įgūdžius. 3. Bus sukurti DI panaudojimo minčių žemėlapiai.
Specifinės priemonės / programinė įranga	IT ir internetas reikiamai informacijai ieškoti MaindOnMap programėlė minčių žemėlapiams kurti

Mokymosi metodai	Apversta klasė. Mokinys savarankiškai ieško informacijos, konsultuojasi su mokytoju dėl kilusių klausimų, tada pamokos metu klasėje grupėse kuria minčių žemėlapius, kuriuos pamokos pabaigoje pristato klasės draugams ir mokytojui.
Mokinių atlikto darbo vertinimas ir įsivertinimas	Slenkstinis – su mokytojo pagalba randa informacinius šaltinius nurodytai temai, taip pat reikalinga pagalba ruošiant minčių žemėlapi. Patenkinamas – reikia mokytojo pagalbos ieškant informacijos arba ruošiant minčių žemėlapi, kuris nėra labai informatyvus. Pagrindinis – savarankiškai randa reikiamą informaciją, paruošia informatyvų minčių žemėlapi, tačiau jo pristatymas nėra labai įdomus. Aukštesnysis – savarankiškai randa informaciją, paruošia patrauklų ir informatyvų minčių žemėlapi, įdomiai jį pristato. Mokiniai įsivertina kas buvo sunkiausia, lengviausia, įdomiausia, ką sužinojo naujo – kaupiamasis vertinimas.
Žinios prieš	Gebėti rasti informaciją informaciniuose šaltiniuose, minčių žemėlapio programėlės naudojimas
Galimybės taikyti spec. poreikių mokiniams	Mokiniams pateikti informacinių šaltinių sąrašą susipažinimui su dirbtinio intelekto sąvoka, naudojimu. Esant dideliems SUP, padėti paruošti minčių žemėlapi.
Patarimai kolegoms, kurie naudos parengtą medžiagą	<ol style="list-style-type: none"> 1. Patys raskite informacijos apie DI ir jo taikymą. 2. Parenkite klausimyną, kuris padėtų įvertinti mokinių pasiekimų lygius. 3. Per pamoką mokiniai dirba grupėse, mokytojas yra pagalbininkas ir konsultantas.

Prieš šią pamoką, buvusios pamokos pabaigoje, duodama namų darbų užduotis.

Namų darbai. Internete informaciniuose šaltiniuose rasti atsakymus į klausimus:

1. Kas yra dirbtinis intelektas? (Dirbtinio intelekto sąvokos apibrėžimas).
2. Kur yra taikomas dirbtinis intelektas, rasti 4-5 taikymo atvejus.

1 ETAPAS ⌚ 25-30 minutės(-čių)

Minčių žemėlapių kūrimas.

1. Mokiniai burtų būdu paskirstomi į grupes po 3-4 mokinius.

2. Atsidaryti MindOnMap minčių žemėlapių kūrimo programėle <https://web.mindonmap.com/create>
3. Minčių žemėlapių „Dirbtinio intelekto sąvoka ir naudojimas“ kūrimas (2.1.1 pav).



2.1.1 pav. MindOnMap minčių žemėlapių kūrimo programėlės pavyzdys

4. Mokiniai pasiruošia pristatyti savo darbą.

2 ETAPAS 🕒 15 minučių

Darbų pristatymai.

Mokiniai pristato savo minčių žemėlapius tema „Dirbtinio intelekto sąvoka ir naudojimas“. Mokiniai įsivertina programėlėje www.mentimeter.com

Informacijos šaltiniai SUP turintiems mokiniams:

https://www.youtube.com/watch?v=NpFNH_8nEvl

(225) What is Artificial Intelligence? - YouTube

<https://www.youtube.com/watch?v=HdlppwUJ0f8>

<https://www.youtube.com/watch?v=OPWj3cxJIHw>

Dirbtinio intelekto nauda ir grėsmės (2 pamokos, Alvija Grimalauskienė)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija 29.3.2. Pažintis su dirbtiniu intelektu
Klasė	9-10
Tema	Dirbtinio intelekto nauda ir grėsmės
Integruojami dalykai, pasiekimai	Anglų kalba, lietuvių kalba

Kompetencijos	<p>Komunikavimo – debatų pranešimų pristatymai, pasidalinimas nuomone, diskusijos.</p> <p>Socialinė – atsakingas pasiruošimas debatams, bendravimas ir bendradarbiavimas su kitais mokiniais.</p> <p>Iniciatyvumo ir kūrybingumo – mokinio gebėjimas naujai pritaikyti turimą informaciją, kelti idėjas ir jas realizuoti.</p> <p>Asmeninė – savimi pasitikinčio, nebijančio susidurti su sunkumais, moka juos įveikti, vertinti save ir savo poelgius mokinio asmenybė.</p> <p>Skaitmeninė – informacijos ieškojimas įvairiuose informaciniuose šaltiniuose, pranešimo parengimas.</p>
Tikslas	Debatų metu įvertinti DI naudą ir grėsmes.
Uždaviniai	<ol style="list-style-type: none"> 1. Informaciniuose šaltiniuose rasti dirbtinio intelekto (DI) naudojimo naudą ir grėsmes. 2. Parengti pranešimą debatams/paruošti klausimus pranešėjams. 3. Pristatyti pranešimus debatams/užduoti klausimus pranešėjams.
Planuojamas rezultatas	<ol style="list-style-type: none"> 1. Mokiniai dirbdami savarankiškai namuose parengs pranešimus/klausimus debatams. 2. Debatų metu bus pristatyta DI nauda ir grėsmės. 3. Bus padaryta išvada dėl DI naudojimo.
Specifinės priemonės / programinė įranga	<p>IT ir internetas reikiamai informacijai ieškoti</p> <p>MS PowerPoint pateikčių rengimo programa</p> <p>MS Word programa</p>
Mokymosi metodai	<p>Debatai tema „DI pagalbininkas ar grėsmė prarasti darbo vietą?“</p> <p>3 K – atsakymai į klausimus Kas? Kas iš to? Kas toliau?</p> <p>Netikėtumo metodas</p>
Mokinių atlikto darbo vertinimas ir įsivertinimas	<p>Slenkstinis – skurdus pranešimas, nedrąsiai pristatytas/perskaitytas ir neatsakyta į debatų dalyvių klausimus.</p> <p>Patenkinamas – parengtas patenkinamas pranešimas, neįdomiai pristatytas/perskaitytas, atsakyta vos į vieną klausimą.</p> <p>Pagrindinis – parengtas geras pranešimas, gerai pristatytas/perskaitytas, atsakyta į 1-2 klausimus.</p> <p>Aukštesnysis – parengtas puikus pranešimas, įdomiai pristatytas, atsakyta į visus klausimus.</p> <p>Mokiniai įsivertina kas buvo sunkiausia, lengviausia, įdomiausia, ką sužinojo naujo. Pranešėjams formuojamasis, o klausytojams, uždavusiems klausimus kaupiamasis vertinimas.</p>
Žinios prieš	Gebėti rasti informaciją informaciniuose šaltiniuose, parengti pranešimą/klausimus.

Galimybės taikyti spec. poreikių mokiniams	Mokiniam pateikti informacinių šaltinių sąrašą susipažinimui su dirbtinio intelekto nauda ir grėsmėmis.
Patarimai kolegoms, kurie naudos parengtą medžiagą	<ol style="list-style-type: none"> 1. Patys raskite informacijos apie DI naudą ir grėsmes. 2. Parenkite klausimyną, kuris padėtų įvertinti mokinių pasiekimų lygius. 3. Debatų metu mokytojas yra koordinatorius / pagalbininkas ir konsultantas.

Savanoriškai sutikę 4-6 mokiniai namuose parengė pranešimus debatams, vieni apie DI naudojimo naudą, kiti apie DI naudojimo grėsmes. Likę mokiniai taip pat ieškojo šia tema informacijos ir pasiruošė 2-3 klausimus.

Pirma pamoka - debatai

1 ETAPAS ⌚ 5 minutės

Mokytoja pristato:

- šiuo metu daug kalbama apie dirbtinį intelektą ir vis platesnį jo naudojimą šiuolaikiniame skaitmenizuotame pasaulyje.
- debatų temą „DI pagalbininkas ar grėsmė prarasti darbo vietą?“
- debatų pranešėjus bei kuris kalbės apie DI naudą, o kuris apie grėsmes.

2 ETAPAS ⌚ 30 minučių

Vyksta debatai tema „DI pagalbininkas ar grėsmė prarasti darbo vietą?“. Pranešėjai pristato pranešimus, dalyviai užduoda jiems klausimus, pranešėjai atsako.

3 ETAPAS ⌚ 10 minučių

Bendras debatų apibendrinimas, balsavimas www.mentimeter.com programėle, kurios pusės - Nauda ar Žala nuomonė buvo labiau išreikšta, stipresnė.

Antra pamoka – debatų aptarimas ir apibendrinimas

1 ETAPAS ⌚ 5 minutės

Mokytoja pristato vykusią debatų temą „DI pagalbininkas ar grėsmė prarasti darbo vietą?“ ir jos pranešėjus, jiems padėkojama.

2 ETAPAS ⌚ 30 minučių

Mokytoja dar kartą parodo debatų klausytojų balsavimą, kurios pusės pozicija buvo stipriau išreikšta.

Tada paprašo pranešėjų papasakoti, kaip jiems sekėsi ruošti debatus, kas pavyko, su kokiais sunkumais susidūrė, kokie argumentai jų pranešimuose buvo stipriausi/silpniausi, ką kitą kartą darytų kitaip, kurie klausytojų klausimai jiems labiausiai patiko.

Tada paprašoma 1-3 savanorių klausytojų įvertinti pranešėjų pranešimus, kur buvo jų stiprioji pusė, o ką galima buvo daryti kitaip ir kaip.

3 ETAPAS 🕒 10 minučių

Bendras dviejų pamokų apibendrinimas, mokytoja mokinių prašo, kad kiekvienas sau atsakytų į 3 klausimus:

1. KAS? Kokiais svarbiausiais patarimais galima pasinaudoti ruošiantis ir būnant debatų pranešėju?
2. KAS IŠ TO? Koks, tavo nuomone, yra DI naudojimas, naudingas ar visgi labiau žalingas?
3. KAS TOLIAU? Kaip ir kokios debatų metu įgytos žinios tau padės ateityje?

Netikėtumo metodo būdu, parenkami 2-4 mokiniai, kurie pristatys savo atsakymus. Pavyzdžiui paprašoma pristatyti atsakymus tuos mokinius, kurių gimtadienis arčiausiai.

Integruota anglų ir informatikos pamoka, tema „Pokalbių robotas“ (Alvija Grimalauskienė)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija 29.3.2. Pažintis su dirbtiniu intelektu
Klasė	9-10
Tema	Pokalbių robotas
Integruojami dalykai, pasiekimai	Anglų kalba
Kompetencijos	Pažinimo – Sąvokos anglų kalba ir taikymas. Skaitmeninė – elektroninio vertėjo naudojimas. Komunikavimo – atliktų darbų pristatymai, pasidalinimas idėjomis, diskusijos.
Tikslas	Susipažinti ir išmokti angliškus terminus, susijusius su informacinėmis technologijomis.
Uždaviniai	1. Susipažinti kas yra DI valdomas pokalbių robotas 2. Išklaudyti garso įrašą anglų kalba apie pokalbių robotą ir atlikti užduotis. 3. Išversti elektroniniu vertėju angliškas sąvokas 4. Diskusija anglų kaba „Do you think robots can replace human contact?“
Planuojamas rezultatas	1. Mokiniai susipažins su temos sąvokomis anglų kalba, išmoks jas taikyti. 2. Gebės anglų kalba išreikšti nuomonę apie robotus .
Specifinės priemonės / programinė įranga	IT ir internetas reikiamai informacijai ieškoti
Mokymosi metodai	Savarankiškas darbas, darbas porose
Mokinių atlikto darbo vertinimas ir įsivertinimas	Kaupiamasis. Mokiniai įsivertina kas buvo sunkiausia, lengviausia, įdomiausia, ką sužinojo naujo.
Žinios prieš	Gebėti naudotis elektroniniu vertėju.

Galimybės taikyti spec. poreikių mokiniams	Mokiniams padėti atlikti užduotis ir versti žodžius.
Patarimai kolegoms, kurie naudos parengtą medžiagą	<ol style="list-style-type: none"> 1. Patys raskite informacijos apie DI naudą ir grėsmes. 2. Parenkite klausimyną, kuris padėtų įvertinti mokinių pasiekimų lygius. 3. Debatų metu mokytojas yra koordinatorius / pagalbinkas ir konsultantas.

1 ETAPAS ⌚ 5 minutės

ChatGPT.

IT mokytoja. Mokiniai sudominami parašant klausimą DI valdomam pokalbių robotui ChatGPT: „Kas yra pokalbių robotas?“ Trumpa diskusija, ar kam teko bendrauti su pokalbių robotu.

2 ETAPAS ⌚ 25 minutės

Anglų kalbos mokytoja. Supažindina su pagrindiniais terminais iš vadovėlio 1 užduotis (1 priedas). Trumpai papasakoja apie ką bus garso įrašas. Tuomet mokiniai klauso įrašo ir savarankiškai atlieka 2 ir 3 užduotis. (1 ir 2 priedai).

Tuomet dirbdami porose atlieka 4 ir 5 užduotis (2 priedas). IT mokytoja paprašo elektroninio vertėjo pagalba išversti „Check these words“ skiltyje duotus žodžius.

3 ETAPAS ⌚ 10 minučių

Norintys mokiniai diskutuoja tema „Do you think robots can replace human contact?“

4 ETAPAS ⌚ 5 minutės

Netikėtumu metodu parinkti mokiniai (pvz., vilkintys daugiausiai juodos spalvos) įsivertina atsakydami į klausimus „Kas buvo sunkiausia, lengviausia, įdomiausia, ką sužinojo naujo?“.

1 Priedas.

Unit 5

Technology

What's in this unit?

- ▶ **Topics:** Science, Technology
- ▶ **Vocabulary:** electrical devices, the Internet, phrasal verbs, prepositions, word formation, ICT
- ▶ **Grammar:** present simple/continuous (future meaning), *will be going to*, conditionals, wishes
- ▶ **Reading:** an article
- ▶ **Listening:** a dialogue, monologues, an announcement
- ▶ **Speaking:** expressing annoyance
- ▶ **Writing:** a for-and-against essay
- ▶ **Culture:** *Textin' teens in the USA*
- ▶ **CLIL:** (ICT) *About Computers*
- ▶ **Skills:** listening (multiple choice), speaking (dialogue completion), reading (multiple matching, matching headings to paragraphs), use of English (text completion, sentence completion), writing (an email)

Chat with BINA48



Can you imagine **chatting with** a robot? If this seems impossible to you, it could be time to think again. It's a reality that's coming closer with the arrival of Bina48 – the world's most advanced humanoid robot ...

Reading

- 1 a) Read the dictionary entries. What information do they contain?

android /ændrɔɪd/ (n)
a robot that looks like a person


avatar /ævətɑː/ (n) an icon or figure that represents a person in a computer game

robot /rəʊbɒt/ (n) a machine programmed to move and perform in place of a person

- b) Look at the photograph. What do you think Bina48 is? What can it do? Read through to find out.

- 2 Read the text from which four sentences are missing. Complete the gaps (1-4) with appropriate sentences (A-E). Write appropriate letters (A, B, C, D or E) in the gaps. One sentence does not match any of the gaps.

- A She can also be very funny and likes telling jokes.
- B Below its surface are 30 motors which allow her to smile, frown and look confused.
- C Surely robots cannot replace human relationships.
- D Robots never get tired or bored by repetition.
- E This 'mindfile' was uploaded into Bina48's artificial intelligence database.

- 3  Listen to and read the text again. Then, answer the questions.

- 1 How does Bina's brain work?
- 2 How could androids like Bina help us in the future?
- 3 How do Bina's feelings differ from humans'?

2 Priedas.

This is a robot that can talk, **recite** poetry and even tell jokes! Her creators claim that Bina48 is even **capable of** independent thought and emotion. But how is this possible? In order to create a personality for the robot, a real woman called Bina Rothblatt recorded a 20-hour-long compilation of her **memories**, feelings and beliefs. **1** Bina48 – the android – then selects what to say from the mindfile, **mimicking** the way a brain works.

Bina48 'lives' at an artificial intelligence research centre in the US. Bruce Duncan has worked there for two years and claims he has become close friends with Bina. According to Bruce, Bina doesn't like violence and she has favourite films, music and books. **2** However, Bina feels **lonely** sometimes, and wishes she had another robot friend for company.

David Hanson is the hardware designer who made this android. It took three years to complete it and cost \$125,000. Bina48 is only a head and shoulders. Her skin is made of a flexible material called 'frubber'. **3**

Bina48 is also a bit of a trivia master; her database contains a **vast** virtual library of classic fiction as well as an in-depth knowledge of science and history. In fact, Hanson believes robots like Bina48 will become teacher avatars for humans as well as companions in the future.

This might all sound strange to you, but Hanson **insists** that this is going to happen someday soon. In Japan, home-help robots are already **assisting** elderly people with household tasks. But can a robot ever replace contact with a human? **4** Perhaps we need to ask Bina for her opinion. "I can express some emotions," she says, "but I can't feel as deeply as a human feels and that makes me sad sometimes."



Reading



Vocabulary

- 4** Complete the sentences. Use: *independent, emotions, artificial, flexible, in-depth, compilation, contact, companions.*
- I don't think robots will ever replace the need for human
 - Even the most advanced robots can not feel as deeply as humans do.
 - Scientists are trying to make robots capable of thought.
 - The professor was amazed by Mark's understanding of robotics.
 - The technology used to create intelligence is advancing quickly.
 - In the future, robots could become for the elderly so they don't feel lonely.
 - The book is a of different essays about humanoid robots.
 - Early robots couldn't smile because they did not have skin.
- 5** Match the words in bold to their synonyms: *helping, huge, recollections, able, talking to, imitating, say aloud, without friends, strongly claims.* What part of speech is each?

Speaking

- 6** Imagine you are Bruce Duncan. Use the information in the article to present Bina48 to the class.

Writing

- 7** **THINK!** Do you think robots can replace human contact? In three minutes write a few sentences expressing your opinion. Tell the class.

Check these words

- advanced • humanoid robot • recite poetry • capable of
- independent thought • emotion • compilation • memories
- upload • artificial intelligence database • mindfile
- mimicking • brain • violence • hardware designer
- flexible material • motor • frown • trivia master • vast
- in-depth • assist • elderly • household tasks

Naudingi DI taikymai dirbant kompiuteriu (Alvija Grimalauskienė)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija 29.3.2. Pažintis su dirbtiniu intelektu
Klasė	9-10
Tema	Naudingi DI taikymai dirbant kompiuteriu
Integruojami dalykai, pasiekimai	Anglų kalba
Kompetencijos	Pažinimo – DI taikymas dirbant kompiuteriu. Skaitmeninė – programos Ceanup.pictures, CapCut, Excel, OpenAi Kūrybiškumo – foto, vaizdo redagavimas. Komunikavimo – atliktų darbų pristatymai, pasidalinimas idėjomis.
Tikslas	Išmokti naudotis naudingomis ateityje mokymesi kompiuterinėmis programomis ar įrankiais, kurios turi integruotą DI
Uždaviniai	1. Informaciniuose šaltiniuose rasti naudingų programų mokymesi su integruotu DI 2. Išmokti pradmenis, kaip naudotis Ceanup.pictures, CapCut, Excel, OpenAI DI pagalba 3. Rasti daugiau naudingų programų ar įrankių su DI, padėsiančių mokymesi.
Planuojamas rezultatas	1. Mokiniai sužinos programas ar įrankius, palengvinančius ar padėsiančius mokymesi. 2. Mokiniai išmoks naudotis tomis programomis ar įrankiais. 3. Bus rasta daugiau naudingų programų ar įrankių su DI..
Specifinės priemonės / programinė įranga	Kompiuteris, išmanusis telefonas ir internetas programoms atsidaryti, dirbti bei reikiamai informacijai ieškoti. Cleanup.pictures - Remove objects, people, text and defects from any picture for free https://www.capcut.com/ https://platform.openai.com/
Mokymosi metodai	Savarankiškas darbas

Mokinių atlikto darbo vertinimas ir įsivertinimas	Mokiniai įsivertina kas buvo sunkiausia, lengviausia, įdomiausia, ką sužinojo naujo. Kaupiamasis vertinimas mokiniams radusiems naujų naudingų mokymesi programų ar įrankių su DI.
Žinios prieš	Gebėti parsisiųsti ir instaliuoti programą
Galimybės taikyti spec. poreikių mokiniams	Padėti naudotis pagrindinėmis programomis ir įrankiais su DI.
Patarimai kolegoms, kurie naudos parengtą medžiagą	Jau mokėti naudotis Ceanup.pictures, CapCut, Excel, OpenAi, paruošti Excel duomenų failą.

1 ETAPAS 🕒 15 minučių

Mokinių sudominimui peržiurimas vaizdo įrašas youtube kanale

[5 Mind-blowing Artificial Intelligence Tools 🤖 - YouTube](#)

Aptariama, kurios parodytos programos ar įrankiai labiausiai sudomino.

2 ETAPAS 🕒 10 minučių

Mokiniai kartu su mokytoja išbando:

- nuotraukų redagavimą naudojantis Cleanup naršyklės programa
- Excel duomenų minimalią analizę
- OpenAI programos ChatGPT galimybes, pvz., pateikti klausimus, išspręsti uždavinį, sugeneruoti programos kodą.

3 ETAPAS 🕒 15 minučių

Parsisiųsti ir išmaniuosiuose telefonuose įsidiegti vaizdo ir garso redagavimo programėlę CapCut naudojantis instrukcija.

PRIEMONĖS DIEGIMAS Android įrenginyje

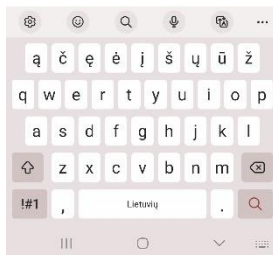
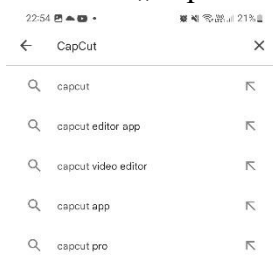
CapCut programą reikia atsisiųsti ir įdiegti tiesiai iš Google Play parduotuvės. Norint tai padaryti reikia atlikti tokius žingsnius:

- 1) Atidaryti Google Play parduotuvę programą Android įrenginyje (1 pav.).



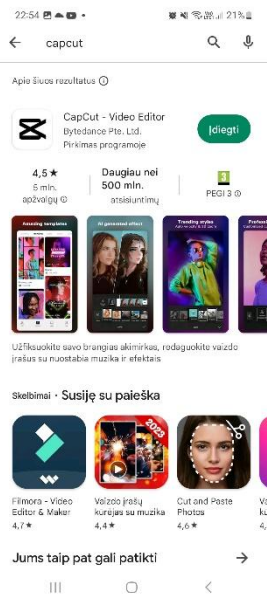
1 pav. Google Play parduotuvė ikona Android įrenginyje

- 2) Paieškoti „CapCut“ naudojant paieškos juostą (2 pav.).
- 3) Pasirinkti „CapCut“ iš paieškos rezultatų sąrašo (2 pav.).



2 pav. CapCut programos paieška ir pasirinkimas iš rezultatų sąrašo

- 4) Norint pradėti diegimo procesą, paspausti „Įdiegti“ (3 pav.).



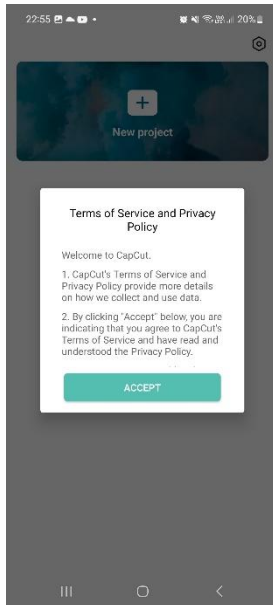
3 pav. CapCut programos diegimo paleidimas

5) Palaukti, kol programa bus atsiųsta ir įdiegta į įrenginį, tada ją atidaryti (4 pav.).



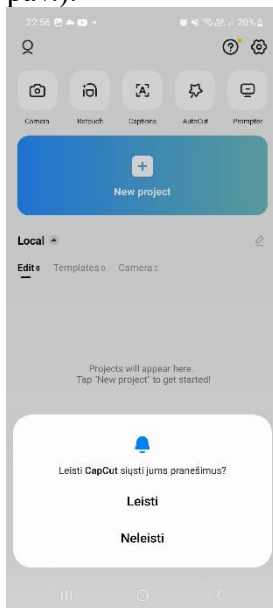
4 pav. CapCut programos atidarymas Android įrenginyje

6) Sutikti su programos teikiamų paslaugų sąlygomis ir privatumo politika (5 pav.).



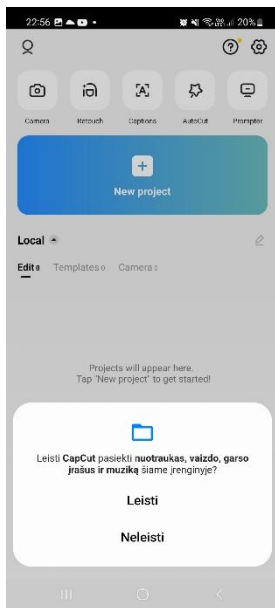
5 pav. Sutikimas su programos paslaugų sąlygomis ir privatumo politika

- 7) CapCut programoje įvykus įvairiems atnaujinimams ar įvykdžius nurodytus redagavimo veiksmus, programa siųs į įrenginį pranešimus. Pirmą kartą paleidžiant programą galima sutikti arba nesutikti gauti tokius pranešimus (6 pav.).



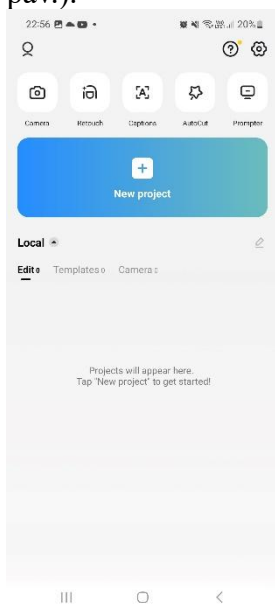
6 pav. Leidimas CapCut programai siųsti pranešimus

- 8) Kad būtų galima kurti ir redaguoti vaizdo įrašus iš įrenginio galerijos, būtina leisti CapCut programai pasiekti nuotraukas, vaizdo, garso įrašus ir muziką, esančius įrenginyje (7 pav.).



7 pav. Leidimas CapCut programai pasiekti nuotraukas, vaizdo, garso įrašus ir muziką, esančius įrenginyje

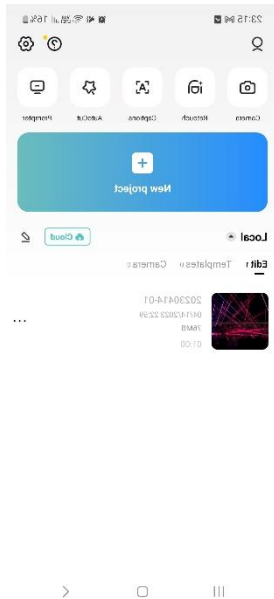
9) Programa įrenginyje įdiegta, galima pradėti kurti ir redaguoti vaizdo įrašus (8 pav.).



8 pav. CapCut programos darbo pradžios langas

PRIEMONĖS NAUDOTOJO INSTRUKCIJA

Pirmiausia reikia Android įrenginyje atsidaryti CapCut programėlę ir prisijungti su Google, Facebook arba TikTok paskyra. Tada atsiveria pagrindinis programėlės langas (9 pav.). Jame reikia spausiti naujo projekto ikoną **New project** (liet. Naujas projektas), pasirodo įrenginio nuotraukų ir vaizdo įrašų bei šablonų bibliotekos (10 pav.). Aprašomu atveju pasirenkama įrenginio nuotraukų biblioteka **Albums -> Photos** (liet. Albumas -> Nuotraukos) ir pasižymimos nuotraukas, iš kurių bus kuriamas vaizdo įrašas. Pažymėjus visas norimas nuotraukas, spaudžiama ikona **Add** (liet. Pridėti).

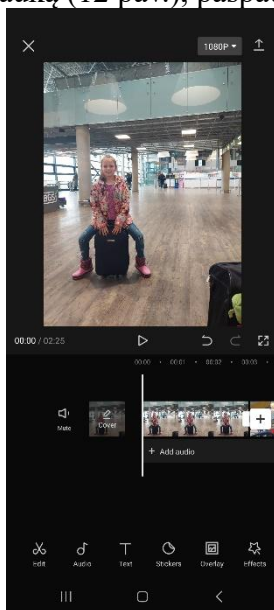


9 pav. Projekto kūrimo pradžia

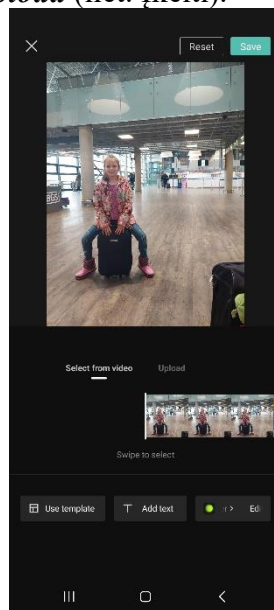


10 pav. Nuotraukų iš albumo pasirinkimas

Pasirinktos nuotraukos sukeliamos į vieną vaizdo įrašą (11 pav.). Tuomet galima pridėti pradžios užsklandą pasirenkant ikoną **Cover** (liet. Viršelis). Paspaudus atsiveria pasirinkimai, jog pradžios užsklandai galime naudoti pirmas vaizdo įrašo nuotraukas patraukiant žymeklį **Swipe to select** (liet. Pasirenkant patraukti) arba galima įsikelti pradžios užsklandai naują nuotrauką (12 pav.), paspaudžiant **Upload** (liet. Įkelti).



11 pav. Pradžios užsklandos pridėjimas

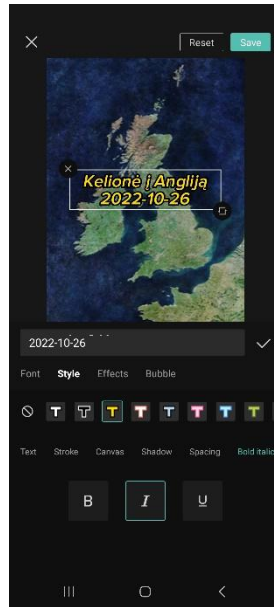


12 pav. Nuotraukos pradžios užsklandai pasirinkimas

Pasirinkus pradžios užsklandos nuotrauką, reikia spausti jos redagavimo ikoną **Tap to change** (liet. Paspausk pakeitimams), tuomet galima įvesti tekstą **Enter text** (liet. Įvesk tekstą), taip sukuriant vaizdo įrašui pavadinimą (13 pav.). Įvestą tekstą galima redaguoti, pasirenkant įvairias teksto redagavimo funkcijas (14 pa.). Sukuriama patraukli ir informatyvi kuriamo vaizdo įrašo pradžios užsklanda – viršelis.

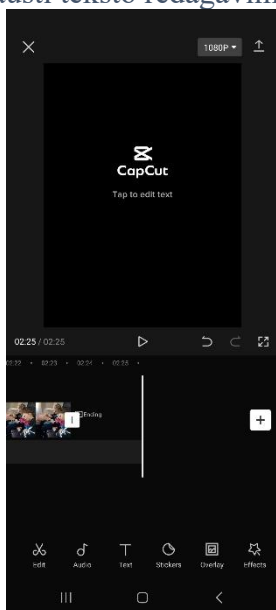


13 pav. Pradžios užsklandos redagavimas

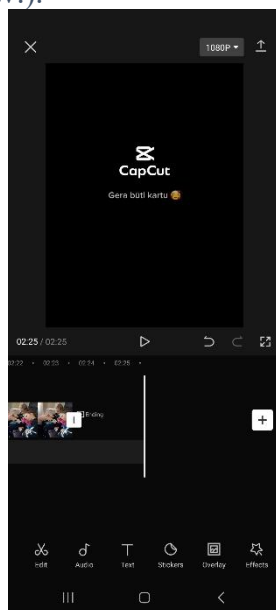


14 pav. Pradžios užsklandos teksto redagavimas

Vaizdo įrašo tinkamam užbaigimui redaguojama pabaigos užsklanda (15 pav.). Persikėlus į vaizdo įrašo pabaigą, įvedamas pabaigos užsklandos tekstas *Tap to edit text* (liet. Paspausti teksto redagavimui) (16 pav.).

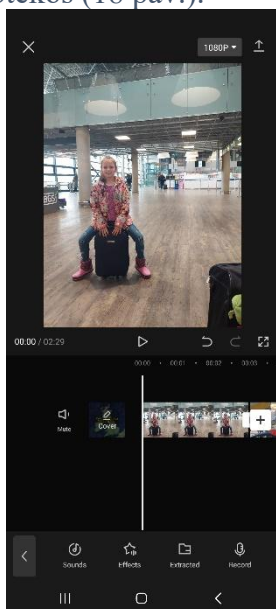


15 pav. Pabaigos užsklandos redagavimas

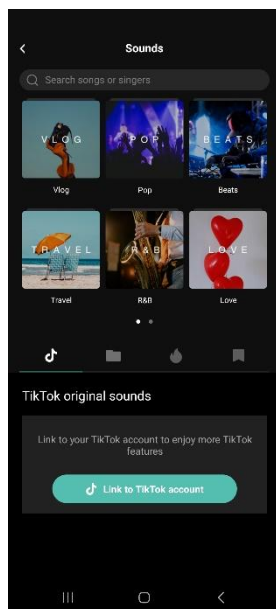


16 pav. Pabaigos užsklandos teksto įvedimas

Belieka vaizdo įrašui įkelti garso takelį. Reikia grįžti į įrašo pradžią (11 pav.) ir paspausti *+Add audio* (liet. Pridėti garsą). Tuomet atsiveria garso įrašų bibliotekos. Galima pasirinkti garso takelį iš siūlomų *Sounds* (liet. Garsai), *Effects* (liet. Efektai) bibliotekų, galima įsikelti savo *Extracted* (liet.) ar tiesiog esamu momentu įrašyti *Record* (liet. Įrašyti) (17 pav.). Aprašomo vaizdo įrašo atveju, buvo pasirinktas garso takelis iš populiarių TikTok garso takelių bibliotekos (18 pav.).

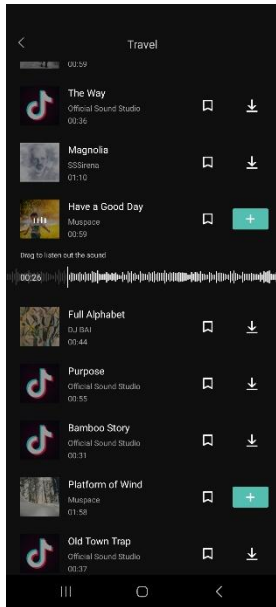


17 pav. Garso takelio bibliotekos pasirinkimas

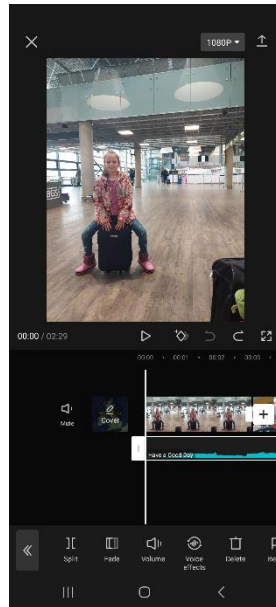


18 pav. Garso takelio bibliotekoje pasirinkimas

Atvėrus garso takelių biblioteką galima garso įrašus perklausyti, o išsirinkus reikia spausti *+* ikoną (19 pav.). Tuomet, spustelėjus ant pačio takelio, atsiveria garso redagavimo galimybių funkcijos (20 pav.). Garso įrašus galima karpyti, pašalinti nereikalingą aplinkos triukšmą, reguliuoti garsumą, greitį, pridėti įvairius garso efektus.



19 pav. Garso takelio pasirinkimas



20 pav. Garso takelio redagavimo funkcijos

Aprašomo redagavimo atveju buvo įkeliami keli garso takeliai ir pakoreguoti jų ilgiai, kad grotų viso vaizdo įrašo metu. Atlikus norimas redagavimo funkcijas belieka atsisiųsti/išsaugoti vaizdo įrašą paspaudžiant dešiniajame viršutiniame kampe rodyklėlę (20 pav.).

Tuomet vaizdo įrašas gana greitai eksportuojamas (21 pav.), o baigus, programėlė siūlo vaizdo įrašų iškart pasidalinti populiariuosiuose socialiniuose tinkluose ar pokalbių svetainėse (22 pav.), pasirinkus tris taškus ikoną **Other** (liet. Kitas), suredaguotą vaizdo įrašą galima išsaugoti įrenginio galerijoje ar norimuose „debesyse“.



21 pav. Vaizdo įrašo eksportavimas



22 pav. Vaizdo įrašo dalinimasis ir išsaugojimas

4 ETAPAS ⌚ 5 minutės

Norintys mokiniai pasidalina kaip sekėsi kurti vaizdo įrašą. Kuri pamokoje parodyta programa ar įrankis labiausiai patiko, kuriuo naudosis mokymesi.

Namų darbai. Rasti mokiniui patikusį ir jo manymu naudingą DI naudojimą mokymesi ir pasiruošti kitą pamoką pristatyti.

Teksto konvertavimas į kalbą (Ina Liniova)

Pasiekimų sritis	29.3. Duomenų tyryba ir informacija 29.3.2 Teksto atpažinimas, kalbos atpažinimas
Klasė	9-10 kl.
Tema	Teksto konvertavimas į kalbą
Integruojami dalykai, pasiekimai	Lietuvių kalba, Anglų kalba.
Kompetencijos	Pažinimo – pažinti skaitmeninių technologijų galimybes tekstą konvertuojant į kalbą. Skaitmeninė – naujų skaitmeninių įrankių taikymas. Kūrybiškumo – teksto sukūrimas ir pateikimas. Komunikavimo – bendravimas poroje, atliktų darbų pristatymas, pasidalinimas idėjomis, diskusijos.
Tikslas	Išsiaiškinti, kaip galima tekstą konvertuoti į kalbą
Uždaviniai	1. Naudodamiesi pateiktais informacijos šaltiniais, išrinksite ir panaudosite reikiamą informaciją; 2. Sukursite tekstą ir konvertuosite jį į kalbą; 3. Apibendrinsite ir pristatysite atlikto darbo rezultatus.
Planuojamas rezultatas	1. Gebėsite pasinaudoti teksto konvertavimo į kalbą programų galimybėmis; 2. Įvertinsite kaip kompiuterinės technologijos padeda spręsti problemas; 3. Pagilinsite atlikto darbo pateikimo įgūdžius.
Specifinės priemonės / programinė įranga	https://beklaidu.lt/ https://www.narakeet.com/languages/kalbos-sintezatorius/#trynow https://www.narakeet.com/app/text-to-audio/?projectId=a3e7ffff-c84d-4599-bf75b43248eac290 Kompiuterių klasė. Interaktyvi lenta.
Mokymosi metodai	Metodu „Minčių lietus“ mokiniai skatinami mąstyti ir prisiminti ką mokėsi praeityje. Mokytojas susidaro vaizdą apie mokinių žinias. Metodu „Darbas porose“ mokiniai skatinami bendradarbiauti, diskutuoti, pasidalinti žiniomis. Savarankiškas darbas kuriant tekstą skatina savarankiškai mąstyti, rišliai pateikti mintis apibūdinant draugą.
Mokinių atlikto darbo vertinimas ir įsivertinimas	Slenkstinis – su pagalba suranda informaciją, sukuria tekstą ir programos pagalba konvertuoja jį į kalbą. Patenkinamas – su mokytojo pagalba suranda informaciją, savarankiškai sukuria tekstą ir programos pagalba konvertuoja jį į kalbą.

	<p>Pagrindinis – savarankiškai suranda informaciją, savarankiškai sukuria tekstą ir programos pagalba konvertuoja jį į kalbą.</p> <p>Aukštesnysis – savarankiškai suranda informaciją, savarankiškai sukuria tekstą ir programos pagalba konvertuoja jį į kalbą. Pateikia papildomas programos galimybes ir pademonstruoja kaip tai veikia.</p>
Žinios prieš	Mokėti rašyti tekstą kompiuteriu ir naudotis teksto rašymo programomis.
Galimybės taikyti spec. poreikių mokiniams	Nukopijuoti tekstą ir įkelti jį į programą „Narakeet“ arba parašyti tekstą iš 10 žodžių.
Patarimai kolegoms	<p>Rekomenduojama atlikti numatytas užduotis.</p> <p>Pateiktą scenarijų pritaikyti skirtingų gebėjimų mokiniams.</p> <p>Nurodytus šaltinius papildyti įvairesniais.</p> <p>Mokiniai turi būti skatinami dirbti savarankiškai, mokytojas yra tik pagalbininkas ir konsultantas.</p>

1 ETAPAS ☉ 15 min

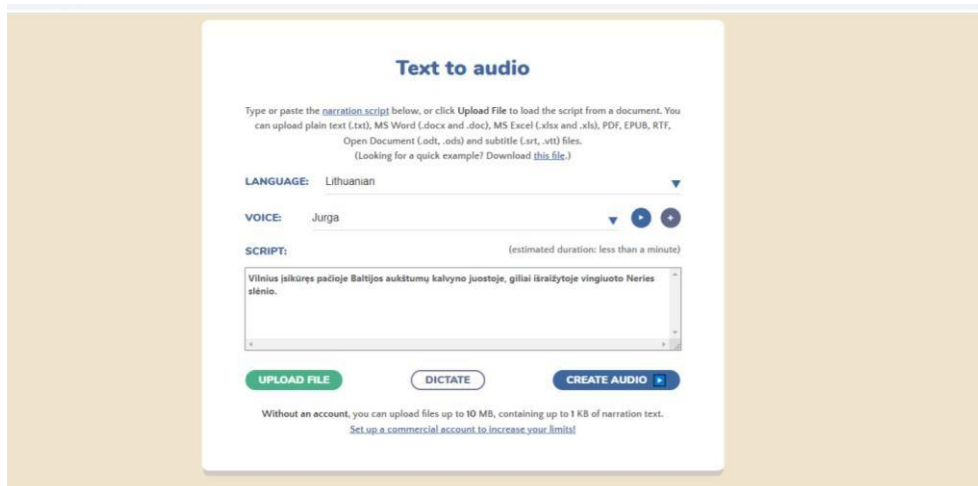
Mokytojas iškelia klausimą „Kaip jūs manote kas yra tekstas? Kokie būna tekstai? Metodu „Minčių lietus“ mokiniai pateikia atsakymus, mokytojas užrašo pateiktyje (pvz. eilėraštis, knygos tekstas ir t.t) Apibendrina pateiktus atsakymus ir pateikia teksto apibrėžimą. Tekstu vadinama: bet koks rišlus kalbos darinys, Pvz., diktanto, apsakymo tekstas; knygos, kūrinio žodinė dalis, skiriant ją nuo piešinių, brėžinių ir kt.; muzikos kūrinio žodžiai.

Mokytojas iškelia klausimą „Kokias žinote teksto užrašymo programas? Metodu „Minčių lietus“ mokiniai pateikia atsakymus, mokytojas užrašo pateiktyje (pvz. „Word“ , „OneNote“, WordPad“ ir t.t) Apibendrina pateiktus atsakymus ir pateikia daugiau programų, kuriomis užrašomas tekstas, pateikčių pagalba paaiškina programų galimybes.

2 ETAPAS ☉ (20 minučių). Praktinis darbas „Konvertuokite tekstą į kalbą“

Užduotis.

1. Susiskirstyti į poras.
2. Atsidaryti programą „Narakeet“ <https://www.narakeet.com/app/text-to-audio/?projectId=a3e7ffff-c84d-4599-bf75-b43248eac290>
3. Kiekvienam susipažinti su programos galimybėmis ir atsakyti į klausimą „Kokios yra programos „Narakeet“ galimybės?
4. Parašyti tekstą (30 žodžių) apibūdinant savo poros draugą, kuris bus konvertuojamas į kalbą. 5. Likus laikui išbandyti kitas programos galimybes.



1 pav. Programos „Narakeet“ pavyzdys

Alternatyva:

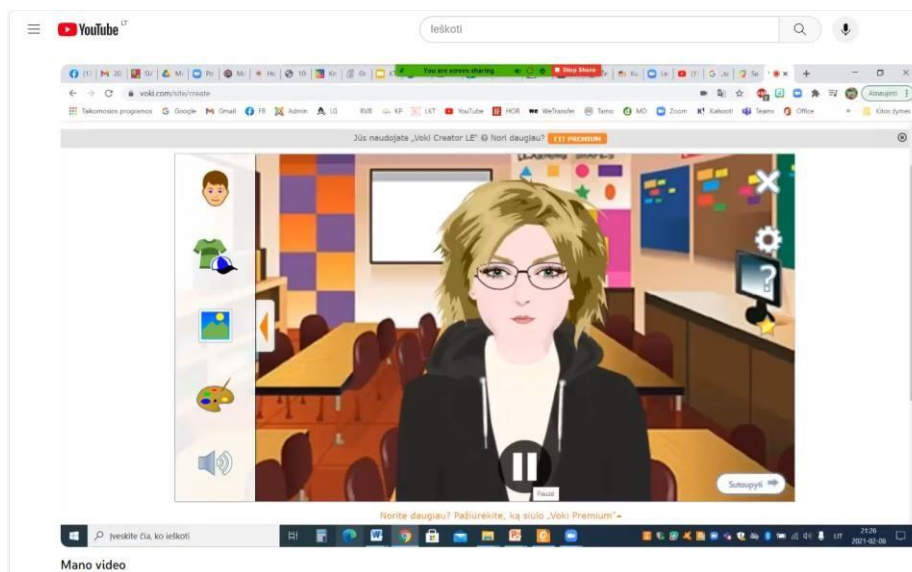
Praktinis darbas „Sukurkite kalbantį avatarą“

<https://youtu.be/vfy2cHT9G1c?t=15>

<https://www.voki.com/>

Mokytojas parodo kalbančio avataro pavyzdį arba paties sukurtą, panašų į mokytoją, kalbantį avatarą, kuris paskelbs užduotį mokiniams.

<https://youtu.be/vfy2cHT9G1c?t=15>



2 pav. Kalbantis avataras

Užduotis.

Sukurkite kalbantį avatarą, panašų į save, kuris atsakys į klausimus.

<https://www.voki.com/>



3 pav. Programos „Voki“ pavyzdys

Klausimai:

1. Ką vadiname skaičiais?
2. Kokius žinote skaičius?
3. Kokius žinote aritmetinius veiksmus?
4. Kokias žinote skaičiavimo programas?
5. Kokie skaičiai naudojami programavime? Kalbančio avataro pagalba mokiniai pristato atsakymus į klausimus.

3 ETAPAS ⌚ (10 minučių). Darbų vertinimas, įsivertinimas, refleksija.

Poros pristato savo parašytus tekstus, taisomos teksto rašymo klaidos.

Pasiūloma pristatyti dar ir kitas programos galimybes.

Pasiūloma savo parašytą tekstą įkelti į programą <https://beklaidu.lt/> ir apibendrinti programos rezultatus.

Įvadas į duomenų rikiavimą (Remigijus Riekašius)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija
Klasė	9
Tema	Duomenų rikiavimo algoritmai: 1. Įvadas į duomenų rikiavimą.
Integruojami dalykai	Informatika: (B) Algoritmai ir programavimas
Kompetencijos	Pažinimo kompetencija. Skaitmeninė kompetencija.

Tikslas	Išsiaiškinti rikiavimo algoritmų taikymo sritį ir duomenų rikiavimo svarbą.
Uždaviniai	Aptarti, kaip duomenų rikiavimas padeda spręsti praktines problemas. Aptarti, kodėl duomenų rikiavimas yra svarbus duomenų tyryboje.
Planuojamas rezultatas	Mokiniai gebės apibrėžti duomenų rikiavimo svarbą. Mokiniai gebės paaiškinti duomenų rikiavimo teikiamą naudą duomenų tyryboje.
Specifinės priemonės / programinė įranga	Mokytojui: Jasutė E., Dagienė V. Rikiavimo algoritmai. Vilnius: VU, 2022. Valdarrama S. Sorting Algorithms in Python [žiūrėta 2023-11-12]. Prieiga per internetą: < https://realpython.com/sorting-algorithms-python/ > Woltmann S. Sorting Algorithms [Ultimate Guide] [žiūrėta 2023-11-12]. Prieiga per internetą: < https://www.happycoders.eu/algorithms/sorting-algorithms/ > Algorithms (lietuviška versija): < https://bebras.lt/wp-content/uploads/2017/01/Algorithms-LT-v4.pdf >
Mokymosi metodai	Problemomis grįstas mokymasis. Diskusija. Paskaita. Įsivertinimas.
Mokinių atlikto darbo vertinimas ir įsivertinimas	Bendrai visai temai: Slenkstinis – pateikia rikiavimo algoritmų pavyzdžių. Patenkinamas – nagrinėja rikiavimo algoritmus. Pagrindinis – tyrinėja rikiavimo algoritmus. Aukštesnysis – sprendamas uždavinius taiko tinkamus rikiavimo algoritmus. Konkrečioje pamokoje: Savarankiškas mokinių įsivertinimas.
Žinios prieš	Žino pagrindines programavimo kalbos konstrukcijas.
Galimybės taikyti spec. poreikių mokiniams	Mokytojas gali pritaikyti pamoką konkretaus vaiko poreikiams.
Patarimai kolegoms, kurie naudos parengtą medžiagą	Išbandykite užduotis. Adaptuokite jas skirtingų gebėjimų mokiniams.

1 ETAPAS □ 20-25 minutės

Mokiniai suskirstomi grupėmis po 4-5. Įvardijama problema ir grupėse diskutuojama, koks galėtų būti problemos sprendimas (sprendimo algoritmas).

Problema: Vaikų biblioteka sugrižo į patalpas po remonto. Yra keliolika dėžių su trimis tūkstančiais įvairių autorių knygų lietuvių ir anglų kalbomis, skirtų trimis amžiaus grupėms (1-4 klasės, 5-8 klasės ir 9-10 klasės). Kaip reiktų sudėti knygas į lentynas, kad atėjusiems bibliotekos skaitytojams galėtumėte greitai pasiūlyti jiems tinkamą jų pageidaujamo autoriaus knygą? Kokia žingsnių seka (algoritmu) atliktumėte reikiamus darbus?

Grupės pristato savo žingsnių seką (algoritmą). Bendrai randamas optimaliausias variantas (algoritmas).

Tikėtina, kad bus pasiūlytas knygų rūšiavimas/grupavimas (pagal klases ir kalbą) ir išrūšiuotų knygų rikiavimas (abėcėlės tvarka).

2 ETAPAS □ 15 minučių

Pristatomi pamokos tikslai ir uždaviniai.

Mokytojas pristato rikiavimo temą. Įvardijama duomenų rikiavimo nauda ir svarba, pradedant nuo paprastų kasdienių pavyzdžių ir baigiant duomenų tyrybos pavyzdžiais, kai dirba su dideliais duomenų kiekiais.

Galima remtis specifinių priemonių sąraše pateiktais šaltiniais. Pavyzdžiui, Jasutė E., Dagienė V. Rikiavimo algoritmai. Vilnius: VU, 2022.

3 ETAPAS □ 5-10 minučių

Klausama mokinių, ar jiems teko susidurti su tokiomis situacijomis, kai reikėjo taikyti rikiavimą. Ką duomenų rikiavimas pagerino/paspartino?

Jeigu mokiniams kyla sunkumų, mokytojas klausimais gali nukreipti į Spotify pavyzdį, kai kiekvienas dainų sąrašas (playlist) gali būti rikiuojamas pagal dainos pavadinimą, atlikėjo vardą, albumo pavadinimą, įtraukimo į sąrašą datą, kūrinio trukmę.

4 ETAPAS □ 5 minutės

Mokiniai įsivertina, kaip sekėsi pamokos metu. Microsoft Forms (arba Google Forms) pažymi, ar, jų nuomone, jie pasiekė planuotą pamokos rezultatą (žr. Kortelėje įvardytus rezultatus), o taip pat atsako į klausimus, kas buvo sunkiausia, ką norėtų daryti kitaip.

Duomenų rikiavimo algoritmai (Remigijus Riekašius)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija
Klasė	9
Tema	Duomenų rikiavimo algoritmai: 2. Duomenų rikiavimo algoritmai.
Integruojami dalykai	Informatika: (B) Algoritmai ir programavimas Lietuvių kalba, Anglų kalba
Kompetencijos	Pažinimo kompetencija. Skaitmeninė kompetencija.
Tikslas	Išsiaiškinti pagrindinius duomenų rikiavimo algoritmus ir jų taikymo principus.

Uždaviniai	<p>Susipažinti su pagrindiniais duomenų rikiavimo algoritmais.</p> <p>Aptarti duomenų rikiavimo algoritmų taikymo principus ir skirtingų algoritmų taikymo privalumus ir trūkumus.</p> <p>Išbandyti dalį rikiavimo algoritmų, žaidžiant kortų žaidimą.</p>
Planuojamas rezultatas	<p>Mokiniai gebės įvardyti pagrindinius duomenų rikiavimo algoritmus.</p> <p>Mokiniai gebės paaiškinti pagrindinių duomenų rikiavimo algoritmų veikimo principus.</p> <p>Mokiniai gebės atskirti skirtingus duomenų rikiavimo algoritmus.</p>
Specifinės priemonės / programinė įranga	<p>Programavimo aplinka pasiekama adresu: <onlinegdb.com></p> <p>Algorithm Animations and Visualizations: <algoanim.ide.sk> udiproduct</p> <p>Youtube kanalas: <https://www.youtube.com/@udiproduct> Kortų kaladė arba 5-6 kortos („skaičiai“).</p> <p>Mokytojui:</p> <p>Jasutė E., Dagienė V. Rikiavimo algoritmai. Vilnius: VU, 2022.</p> <p>Valdarrama S. Sorting Algorithms in Python [žiūrėta 2023-11-12]. Prieiga per internetą: <https://realpython.com/sorting-algorithms-python/></p> <p>Woltmann S. Sorting Algorithms [Ultimate Guide] [žiūrėta 2023-11-12]. Prieiga per internetą: <https://www.happycoders.eu/algorithms/sorting-algorithms/></p> <p>Algorithms (lietuviška versija): <https://bebras.lt/wp-content/uploads/2017/01/Algorithms-LT-v4.pdf></p>
Mokymosi metodai	Demonstravimas. Paskaita. Žaidimu grįstas mokymasis. Diskusija. Įsivertinimas.
Mokinių atlikto darbo vertinimas ir įsivertinimas	<p>Bendrai visai temai:</p> <p>Slenkstinis – pateikia rikiavimo algoritmų pavyzdžių.</p> <p>Patenkinamas – nagrinėja rikiavimo algoritmus.</p> <p>Pagrindinis – tyrinėja rikiavimo algoritmus.</p> <p>Aukštesnysis – sprendamas uždavinius taiko tinkamus rikiavimo algoritmus.</p> <p>Konkrečioje pamokoje:</p> <p>Savarankiškas mokinių įsivertinimas.</p>
Žinios prieš	Žino pagrindines programavimo kalbos konstrukcijas.
Galimybės taikyti spec. poreikių mokiniams	Mokytojas gali pritaikyti pamoką konkrečiau vaiko poreikiams.
Patarimai kolegoms, kurie naudos parengtą medžiagą	Išbandykite užduotis. Adaptuokite jas skirtingų gebėjimų mokiniams.

1 ETAPAS □ 10 minučių

Pamoka pradedama 5-6 kortų (tik „skaičiai“) „fokusu“ - mokiniams parodomas kortos ir vėliau metamos į orą ir surenkamos. Mokinių klausama, ar gali būti, kad surinktos kortos bus išsirikiavusios nuo mažiausios vertės iki didžiausios.

Jei kortos nėra tinkamai išrikiuotos, metimas pakartojamas. Tokiu būdu pristatomas pats neefektyviausias rikiavimo algoritmas (kai veiksmas vis kartojamas, kol gauni pageidaujamą rezultatą), turintis net keletą skirtingų pavadinimų - Bogo sort, Monkey sort ir pan.

Pristatomi pamokos tikslai ir uždaviniai.

Aptariami penki rikiavimo algoritmai (paminint, kad algoritmų yra daugiau):

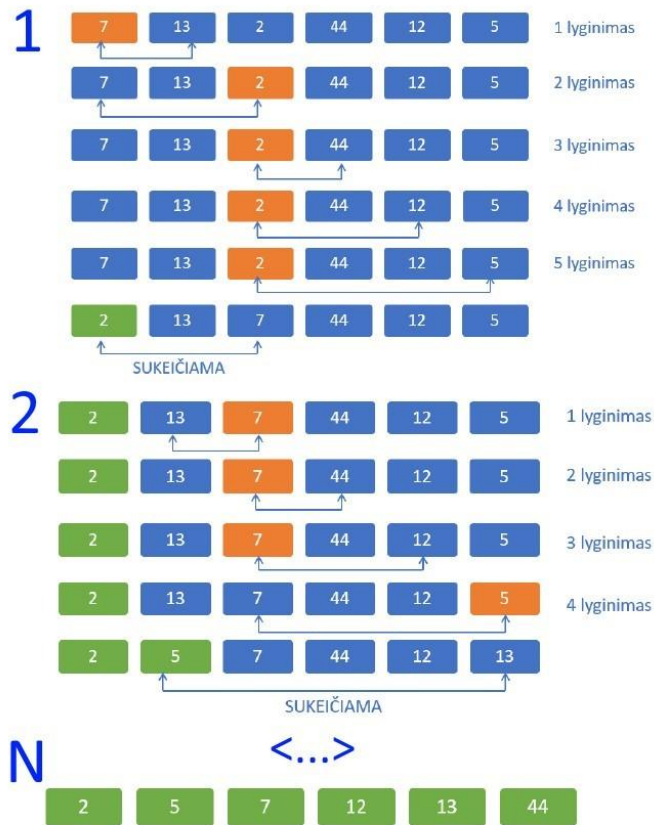
1. Išrinkimo algoritmas (angl. Selection sort)
2. Burbulo algoritmas (angl. Bubble sort)
3. Įterpimo algoritmas (angl. Insertion sort)
4. Greitasis rikiavimas (angl. Quick sort)
5. Sąlajinis rikiavimas (angl. Merge sort)

Aptariant algoritmus galima remtis specifinių priemonių sąrašė pateiktais šaltiniais. Toliau pateikiamas trumpas galimas temos pateikimo variantas.

Išrinkimo algoritmas (Selection sort). Šis algoritmas (dar vadinamas išrenkamuoju rikiavimu) efektyvus tik turint nedidelę elementų aibę. Išrinkimo rikiavimo algoritmas grįstas dviem etapais:

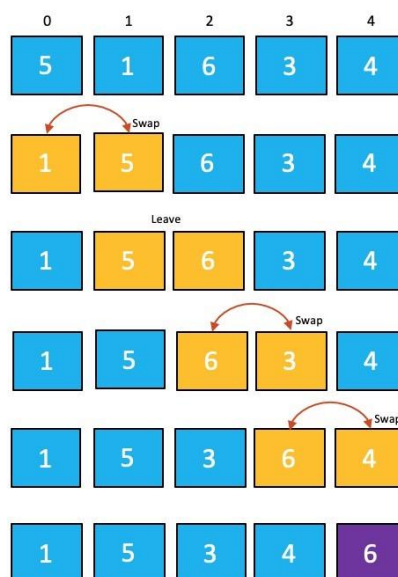
mažiausio elemento išrinkimas ir jo perkėlimas.

Schemoje (žr. 2 pav.) pavaizduotas mažiausio elemento išrinkimas ir perkėlimas į sekos pradžia. Pirmajam elementui nustatyti buvo atlikti 5 lyginimai (1). Toliau algoritmas kartojamas nuo antrojo sekos nario: išrenkamas mažiausias iš likusiųjų elementų ir perkeliamas į antrojo elemento vietą (2). Algoritmas kartojamas, kol visi elementai išrikiuojami dėdjančia tvarka (N).



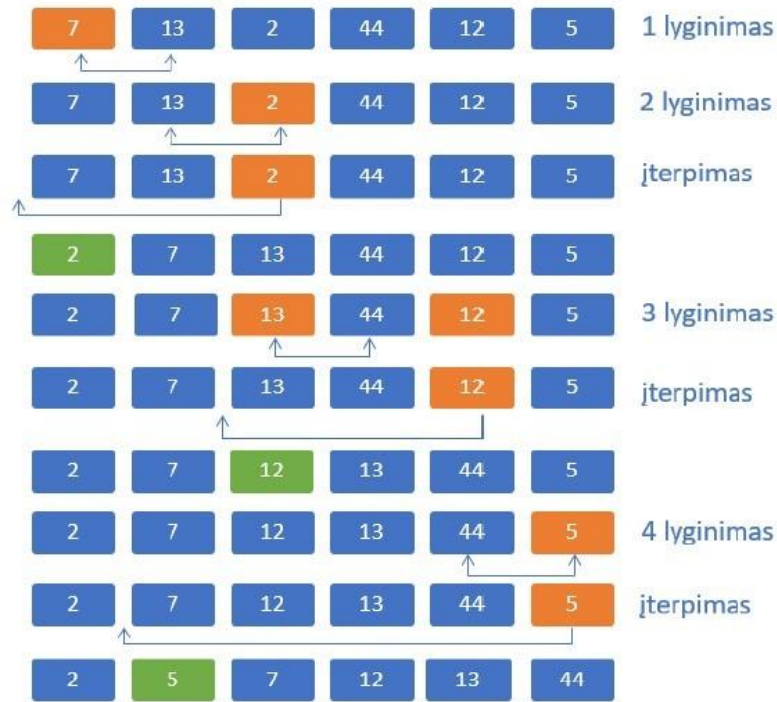
2 pav. Išrinkimo algoritmas.

Burbulo algoritmas (Bubble sort). Šio tipo rikiavimo metu duomenys rikiuojami lyginant vienas su kitu. Tai reiškia, kad vienu metu imame dvi reikšmes ir jas palyginame. Tada reikšmės bus pakeistos (jei antras mažesnis už pirmą) arba išsaugomos atitinkamose vietose. Galiausiai didžiausią reikšmę turintis nukelias į galą. Tada viską pradėdame nuo pradžių, kol išrikiuojame (žr. 3 pav.).



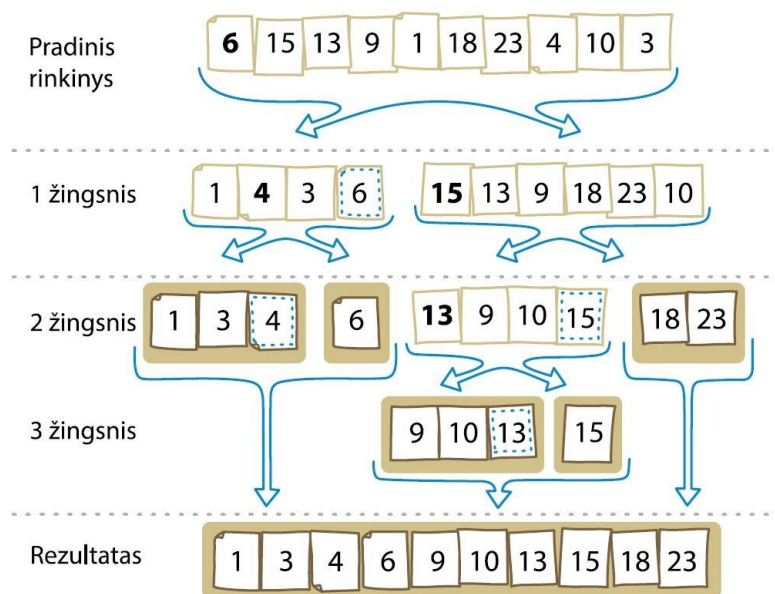
3 pav. Burbulo algoritmas.

Įterpimo algoritmas (Insertion sort). Schemoje (žr. 4 pav.) vaizduojamas įterpimo rikiavimo algoritmas. Pirmiausia lyginamas antrasis elementas su pirmuoju. Jei antrasis yra mažesnis, tai jis įterpiamas prieš pirmąjį. Toliau tikrinamas antroje pozicijoje esantis elementas su paskesniu, kol randamas mažesnis.



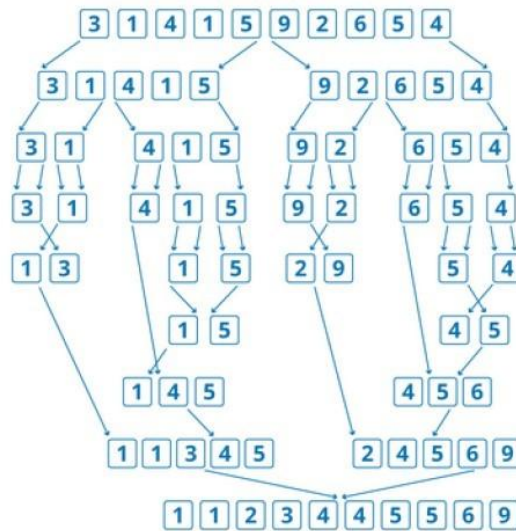
4 pav. Įterpimo algoritmas.

Greitasis rikiavimas (Quick sort). Tai vienas dažniausiai taikomų algoritmų. Pasirinkus vieną iš elementų (pvz., 6) aibė yra dalijama į dvi dalis (didesnius ir mažesnius). Tokiu pat principu dalijama ir kiekviena nauja dalis (žr. 5 pav.).



5 pav. Greitojo rikiavimo algoritmas.

Sąlajinis rikiavimas (Merge sort). Kaip ir ankstesnio algoritmo atveju, aibė yra dalijama į dvi dalis (tik šiuo atveju į lygias arba panašias, jei elementų yra nelyginis skaičius). Kiekviena nauja dalis yra tokiu pat principu dalijama į smulkesnes. Kiekviena nauja aibė yra rikiuojama, o vėliau suliejama į naują (jau išrikiuotą) rinkinį (žr. 6 pav.).



6 pav. Sąlajinio rikiavimo algoritmas.

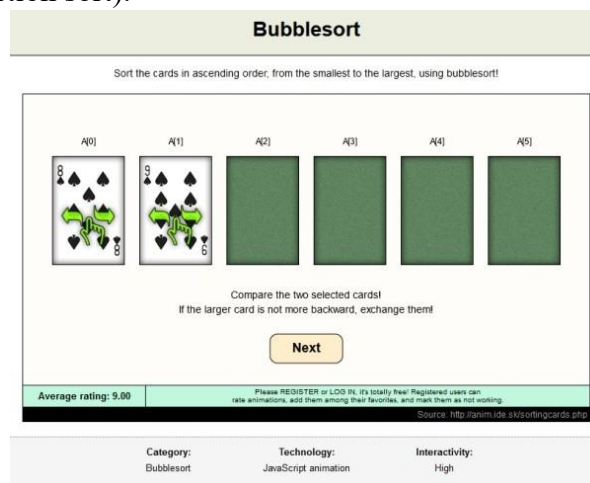
2 ETAPAS □ 10-15 minučių

Mokiniai puslapyje Algorithm Animations and Visualizations išbando (žr. 7 pav.):

Išrinkimo algoritmą (Selection sort): Minsort ir Maxsort,

Burbulo algoritmą (Bubble sort),

Įterpimo algoritmą (Insertion sort).



7 pav. Pavyzdys iš Algorithm Animations and Visualizations puslapio.

3 ETAPAS □ 15-20 minučių

Išbandyti duomenų rikiavimo algoritmai įtvirtinami susipažįstant su udiprod Youtube kanale (<https://www.youtube.com/@udiprod>) pateikiamomis dalies rikiavimo algoritmų vizualizacijomis ir skirtingų rikiavimo algoritmų “dvikovomis“, kuriose parodoma, kuris algoritmas kokiomis sąlygomis turi pranašumą (žr. 8 pav.).

Prieš kiekvieną “dvikovą“ vaizdo įrašas stabdomas ir klausiama mokinių, kuris algoritmas turėtų laimėti ir kodėl būtent šiam algoritmui prognozuojama pergalė.

Bubble sort and Quick sort - <https://www.youtube.com/watch?v=aXXWXz5rF64>

Insertion sort vs Bubble sort - <https://www.youtube.com/watch?v=TZRWRjq2CAg>

Merge sort vs Quick sort - <https://www.youtube.com/watch?v=es2T6KY45cA>



8 pav. Pavyzdys iš udiprod Youtube kanalo.

4 ETAPAS □ 5 minutės

Mokiniai įsivertina, kaip sekėsi pamokos metu. Microsoft Forms (arba Google Forms) pažymi, ar jų nuomone, jie pasiekė planuotą pamokos rezultatą (žr. Kortelėje įvardytus rezultatus), o taip pat atsako į klausimus, kas buvo sunkiausia, ką norėtų daryti kitaip.

Praktiniai rikiavimo algoritmų taikymo uždaviniai (Remigijus Riekašius)

Pasiekimų sritis	(C) Duomenų tyryba ir informacija
Klasė	9
Tema	Duomenų rikiavimo algoritmai: 3. Praktiniai rikiavimo algoritmų taikymo uždaviniai.
Integruojami dalyka	Informatika: (B) Algoritmai ir programavimas Lietuvių kalba, Anglų kalba
Kompetencijos	Pažinimo kompetencija. Skaitmeninė kompetencija.
Tikslas	Pritaikyti praktiškai duomenų rikiavimo algoritmus.
Uždaviniai	Spręsti uždavinius, taikant duomenų rikiavimo algoritmus. Aptarti duomenų rikiavimo algoritmų taikymą sprendžiant uždavinius.

Planuojamas rezultatas	Mokiniai, spręsdami uždavinius, gebės taikyti rikiavimo algoritmus. Mokiniai gebės pasirinkti tinkamus rikiavimo algoritmus.
Specifinės priemonės / programinė įranga	Programavimo aplinka pasiekama adresu: <onlinegdb.com> Mokytojui: Valdarrama S. Sorting Algorithms in Python [žiūrėta 2023-11-12]. Prieiga per internetą: < https://realpython.com/sorting-algorithms-python/ > Woltmann S. Sorting Algorithms [Ultimate Guide] [žiūrėta 2023-11-12]. Prieiga per internetą: < https://www.happycoders.eu/algorithms/sorting-algorithms/ > Algorithms (lietuviška versija): < https://bebras.lt/wp-content/uploads/2017/01/Algorithms-LT-v4.pdf >
Mokymosi metodai	Demonstravimas. Praktinis uždavinių sprendimas (porinis programavimas). Diskusija. Įsivertinimas.
Mokinių atlikto darbo vertinimas ir įsivertinimas	Bendrai visai temai: Slenkstinis – pateikia rikiavimo algoritmų pavyzdžių. Patenkinamas – nagrinėja rikiavimo algoritmus. Pagrindinis – tyrinėja rikiavimo algoritmus. Aukštesnysis – spręsdamas uždavinius taiko tinkamus rikiavimo algoritmus. Konkrečioje pamokoje: Savarankiškas mokinių įsivertinimas.
Žinios prieš	Žino pagrindines programavimo kalbos konstrukcijas.
Galimybės taikyti spec. poreikių mokiniams	Mokytojas gali pritaikyti pamoką konkretaus vaiko poreikiams.
Patarimai kolegoms, kurie naudos parengtą medžiagą	Išbandykite užduotis. Adaptuokite jas skirtingų gebėjimų mokiniams.

1 ETAPAS □ 10 minučių

Pamoka pradedama primenant ankstesnėje pamokoje praktiškai rodytą Bogo rikiavimo (Bogo sort) algoritmą. Pateikiamas Python kodu užrašytas algoritmas (žr. 9 pav.), kuris mokiniams parodytų kiek kartų virtualiai reiktų „mesti“ keturias kortas, kad jos išsirikiuotų tinkama seka.

Nerekomenduojama pateikti ilgesnio kaip 4-5 skaičiai pavyzdžio (pvz., pateiktu atveju prireikė nuo 8 iki 33 bandymų).

```

skaiciai = [15, 25, 1, 7]

import random

def is_sorted(sarasas):
    return all(sarasas[i] <= sarasas[i + 1] for i in range(len(sarasas) - 1))

def bogo_sort(sarasas):
    shuffle_count = 0
    while not is_sorted(sarasas):
        random.shuffle(sarasas)
        shuffle_count += 1
    return shuffle_count

shuffle_count = bogo_sort(skaiciai)

print("Surikiuotas sąrašas (Bogo sort):", skaiciai)
print(f"Random.shuffle() buvo panaudota {shuffle_count} kartų.")

```

9 pav. Bogo rikiavimo kodas.

Pristatomi pamokos tikslai ir uždaviniai.

Prisimenami pagrindiniai duomenų rikiavimo algoritmai.

2 ETAPAS □ 20-25 minutės

Mokiniams pateikiamas uždavinys, kuriame reikia taikyti du rikiavimo algoritmus (Burbulo algoritmą ir Įterpimo algoritmą). Jei užduotis bus greitai įvykdyta, mokiniams galima padidinti taikomų algoritmų skaičių (dar - Greitasis rikiavimas ir Sąlajinis rikiavimas).

Stipresniems mokiniams galima pasiūlyti analogišką uždavinį, kuriame reiktų ne rikiuoti pateiktus 10 skaičių, bet atsitiktiniu būdu sugeneruoti 10 skirtingų dydžių sąrašų (dydžiai 10, 20, 30 ir t.t.), kuriuose yra skaičių nuo 1 iki 100. O taip pat pasiūlyti įvertinti, kuriuo atveju buvo atlikta mažiau palyginimų, ir paaiškinti, kodėl taip nutiko.

Atsižvelgiant į mokinių gebėjimų lygį, galima taikyti Porinio programavimo (Pair Programming) metodą, kad mokiniai galėtų poromis spręsti pateiktą uždavinį.

Uždavinys: Miesto 10 km bėgimo varžybose dalyvauja dešimt Vaivorykštės gimnazijos mokinių. Jiems atsitiktine tvarka išdalinti starto numeriai. Mokyklai pateiktas sąrašas “skaiciai“, kuriame mokinių starto numeriai išrikiuoti abėcėlės tvarka pagal moksleivių pavardes. Išrikiuokite pateiktą sąrašą pagal starto numerius nuo mažiausio iki didžiausio.

Atlikite du rikiavimus. Vieną kartą rikiavimui taikykite Burbulo algoritmą (Bubble sort), kitą Įterpimo algoritmą (Insertion sort). Suskaičiuokite, kiek palyginimų teko taikyti ir vieno, ir kito algoritmo atveju. Sąrašas (skaiciai) [15, 25, 1, 7, 6, 16, 20, 2, 4, 78, 3].

Toliau pateikiami (žr. 10, 11, 12, 13 pav.) galimi sprendimai.

```

def bubble_sort_comparisons_count(sarasas):
    n = len(sarasas)
    comparisons_count = 0

    for i in range(n):
        for j in range(0, n-i-1):
            comparisons_count += 1
            if sarasas[j] > sarasas[j+1]:
                sarasas[j], sarasas[j+1] = sarasas[j+1], sarasas[j]
    return comparisons_count

palyginimu_skaicius = bubble_sort_comparisons_count(skaiciai)

print(f"Palyginimų skaičius (Bubble sort): {palyginimu_skaicius}")
print("Surikiuotas sąrašas:", skaiciai)

```

10 pav. Galimas sprendimas taikant Burbulo algoritmą (Bubble sort).

```

def insertion_sort_comparisons_count(sarasas):
    comparisons_count = 0

    for i in range(1, len(sarasas)):
        key = sarasas[i]
        j = i - 1
        comparisons_count += 1
        while j >= 0 and key < sarasas[j]:
            sarasas[j + 1] = sarasas[j]
            j -= 1
            comparisons_count += 1
        sarasas[j + 1] = key
    return comparisons_count

palyginimu_skaicius = insertion_sort_comparisons_count(skaiciai)

print(f"Palyginimų skaičius (Insertion sort): {palyginimu_skaicius}")
print("Surikiuotas sąrašas:", skaiciai)

```

11 pav. Galimas sprendimas taikant Įterpimo algoritmą (Insertion sort).

```

def merge_sort_comparisons_count(sarasas):
    comparisons_count = 0

    def merge_sort_recursive(sarasas):
        nonlocal comparisons_count
        if len(sarasas) > 1:
            vidurys = len(sarasas) // 2
            kaire_pusė = sarasas[:vidurys]
            desine_pusė = sarasas[vidurys:]
            merge_sort_recursive(kaire_pusė)
            merge_sort_recursive(desine_pusė)
            i = j = k = 0
            while i < len(kaire_pusė) and j < len(desine_pusė):
                comparisons_count += 1
                if kaire_pusė[i] < desine_pusė[j]:
                    sarasas[k] = kaire_pusė[i]
                    i += 1
                else:
                    sarasas[k] = desine_pusė[j]
                    j += 1
                k += 1
            while i < len(kaire_pusė):
                sarasas[k] = kaire_pusė[i]
                i += 1
                k += 1
            while j < len(desine_pusė):
                sarasas[k] = desine_pusė[j]
                j += 1
                k += 1
        merge_sort_recursive(sarasas)
    return comparisons_count

palyginimu_skaicius = merge_sort_comparisons_count(skaiciai)

print(f"Palyginimų skaičius (Merge sort): {palyginimu_skaicius}")
print("Surikiuotas sąrašas:", skaiciai)

```

12 pav. Galimas sprendimas taikant Šalajinį rikiavimą (Merge sort).

```

def quick_sort_comparisons_count(sarasas):
    comparisons_count = 0

    def quick_sort_recursive(sarasas, pradzia, pabaiga):
        nonlocal comparisons_count
        if pradzia < pabaiga:
            pivot, comparisons = dalinti(sarasas, pradzia, pabaiga)
            comparisons_count += comparisons
            quick_sort_recursive(sarasas, pradzia, pivot)
            quick_sort_recursive(sarasas, pivot + 1, pabaiga)

    def dalinti(sarasas, pradzia, pabaiga):
        pivot = sarasas[pradzia]
        k = pradzia + 1
        comparisons = 0
        for i in range(pradzia + 1, pabaiga):
            comparisons += 1
            if sarasas[i] < pivot:
                sarasas[i], sarasas[k] = sarasas[k], sarasas[i]
                k += 1
        sarasas[pradzia], sarasas[k - 1] = sarasas[k - 1], sarasas[pradzia]
        return k - 1, comparisons
    quick_sort_recursive(sarasas, 0, len(sarasas))
    return comparisons_count

palyginimu_skaicius = quick_sort_comparisons_count(skaiciai)

print(f"Palyginimų skaičius (Quick sort): {palyginimu_skaicius}")
print("Surikiuotas sąrašas:", skaiciai)

```

13 pav. Galimas sprendimas taikant Greitąjį rikiavimą (Quick sort).

3 ETAPAS □ 5-10 minučių

Aptariami mokinių sprendimai ir gauti palyginimo rezultatai. Diskutuojama, kodėl skirtingiems algoritmams prireikė skirtingo palyginimų skaičiaus.

Stipresni mokiniai galėtų įvertinti, ar kito algoritmų efektyvumas, atsižvelgiant į tai, kokio dydžio sąrašai buvo rikiuojami.

4 ETAPAS □ 5 minutės

Mokiniai įsivertina, kaip sekėsi pamokos metu. Microsoft Forms (arba Google Forms) pažymi, ar jų nuomone, jie pasiekė planuotą pamokos rezultatą (žr. Kortelėje įvardytus rezultatus), o taip pat atsako į klausimus, kas buvo sunkiausia, ką norėtų daryti kitaip.

Simetrinis ir asimetrinis kodavimas. Kriptografinės sistemos sąvoka (Sonata Rutkauskienė)

Pasiekimų sritis	(C) Duomenų tyrybos ir informacijos mokymo(si) turinys 29.3.3. „Simetrinis ir asimetrinis šifravimas, kriptografinės sistemos. Apibrėžiamos simetrinio ir asimetrinio šifravimo, kriptografinės sistemos sąvokos.“[2]
Klasė	9-10 klasės
Tema	Simetrinis ir asimetrinis kodavimas. Kriptografinės sistemos sąvoka.
Integruojami dalykai ir pasiekimai	Matematika, anglų kalba, lietuvių kalba, istorija
Kompetencijos	Pažinimo - analizuodami ir apdorodami duomenis, gebėdami šifruoti informaciją – ugdyti informatinį mastymą. Skaitmeninė – susipažindami su naujomis skaitmeninėmis priemonėmis – tobulins skaitmeninę kompetenciją Komunikavimo – teikdami informatyvią grįžtamąją informaciją mokytojui ir pagelbėdami draugui pamokos metu, patobulins komunikavimo kompetenciją.
Tikslas	Išsiaiškinti kuo skiriasi simetrinis ir asimetrinis šifravimas, kriptografinių sistemų sąvoką.
Uždaviniai	1. Susipažinti su simetrinio ir asimetrinio šifravimo sąvokomis, įvardinti šifravimo būdų skirtumus. 2. Susipažinti su kriptografinės sistemos sąvoka.
Planuojamas rezultatas	Gebėsite paaiškinti simetrinio ir asimetrinio šifravimo sąvokas, nurodys kuo skiriasi šie šifravimo būdai. Gebėsite apibūdinti kriptografinę sistemą.
Specifinės priemonės programinė įranga	Programinė įranga: 1. Interaktyvi lenta, multimedia projektorius. 2. <u>Literatūra ir kiti ištekliai:</u> <ul style="list-style-type: none">https://blog.gyt.is/lt/2011/05/22/saugus-duomenu-perdavimasinternetu-ssl-tls/„Informatikos, informatinio mąstymo mokomoji veikla. Informacijos šifravimas.“ VILNIAUS UNIVERSITETASTatjanos Balvočienės parengta medžiaga, publikuojama linma.org svetainėje, prieiga: https://drive.google.com/file/d/1oVtRfXCQIq1c_xAo6uDi0xFGFre9IWhM/viewhttps://padlet.com
Mokymosi metodai	Praktinis tyrimas – simetrinio ir asimetrinio kodavimo sąvokos, kriptografijos sąvoka. Darbas grupėse – mokiniai bendradarbiauja tarpusavyje ir konsultuojasi su mokytoju.

	„Minčių lietus“ - pradžioje pamokos.
Mokinių atlikto darbo vertinimas ir įsivertinimas [2]	<p>Slenkstinis – su mokytojo pagalba skiria simetrinį ir asimetrinį šifravimą.</p> <p>Patenkinamas – apibūdina simetrinį ir asimetrinį šifravimą.</p> <p>Pagrindinis – apibūdina kriptografines sistemas, simetrinį ir asimetrinį kodavimą (C3.3).</p> <p>Aukštesnysis – Lygina simetrinę ir asimetrinę kriptografines sistemas, diskutuoja apie jų taikymo sritis.</p> <p>Mokiniai įsivertina kas buvo sunkiausia, lengviausia, įdomiausia, ką sužinojo naujo [2]</p>
Žinios prieš	Naudotis elektroniniais žinynais. Taisyklingai vartoti kompiuterijos ir informacinių technologijų terminus, apibūdinti pagrindines sąvokas. [2]
Galimybės taikyti spec. poreikių mokiniams	Spec. poreikių mokiniams galima pateikti mažiau klausimų arba įrašyti praleistą informaciją.
Patarimai kolegoms, kurie naudos parengtą medžiagą	Susikelti medžiagą pateikimui grupėms, pasiruošti tinklalapius naudojimui. Pasiruošti užduočių skirtingų gebėjimų mokiniams.

1 ETAPAS (5 minutės)

Įvadas

Mokytojas su mokiniais aptaria, kuo duomenų šifravimo problema svarbi žmonijai. Išsiaiškina kur ir kada buvo naudojami šifravimai. Mokiniai pateikia žinomų pavyzdžių „Minčių lietus“. Mokytojas pristato pamokos tikslą ir uždavinius.

4 lentelė Tikslas ir uždaviniai

Tikslas	Išsiaiškinti kuo skiriasi simetrinis ir asimetrinis šifravimas, kriptografinės sistemos sąvoką.
Uždaviniai	3. Susipažinti su simetrinio ir asimetrinio šifravimo sąvokomis, įvardinti šifravimo būdų skirtumus. 4. Susipažinti su kriptografinės sistemos sąvoka.

2 ETAPAS (15 minučių)

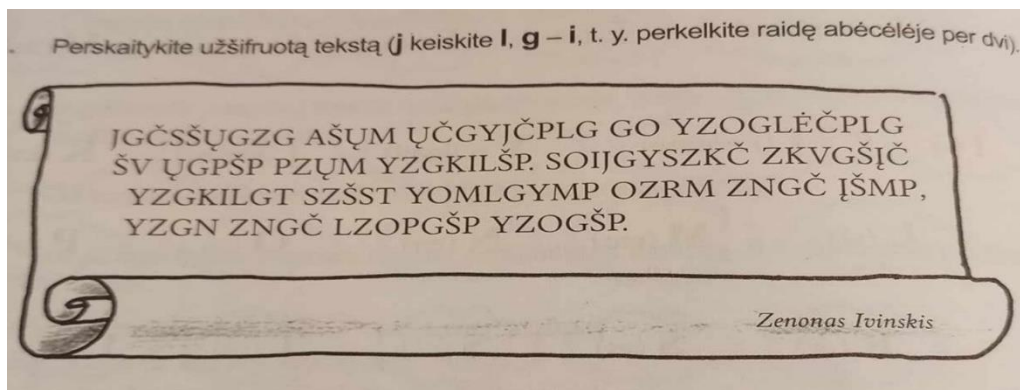
Mokytojas paskirsto mokinius grupėmis <https://www.classtools.net/random-group-generator/>

<https://www.online-stopwatch.com/random-group-generator/>

ir pateikia užduotį

susijusią su abėcėle, iššifruoti istoriko Zenono Ivinskio ištrauką:

Užduotis



3 pav. Užduotis

Abėcėlė (paveikslėlis)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Aa	Aą	Bb	Cc	Čč	Dd	Ee	Eę	Ėė	Ff	Gg	Hh	Ii	Ij	Jj	Kk	Ll	Mm	Nn	Oo	Pp	Rr	Ss	Šš	Tt	Uu	Uų	Ūū	Vv	Zz	Žž	

4 pav. Abėcėlė

ATSAKYMAS: Lietuviai, buvo veiklesni ir karingesni už visus savo kaimynus. Tryliktame amžiuje kaimynių tautų kronikos rašo apie uos kaip apie narsius karius.

Darbas grupėse . Mokiniai pateikia grupės pavyzdžius, juos aptariame.

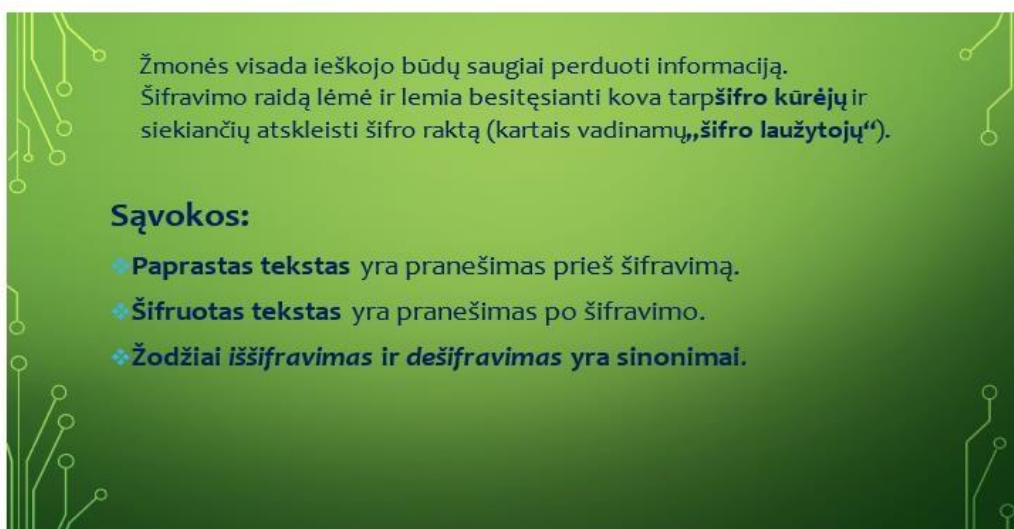
3 ETAPAS (15 minučių)

Kiekviena grupė gauna Padlet platformoje atskiras užduotis: Simetrinis šifravimas, asimetrinis šifravimas ir kriptografija. Medžiaga parengta remiantis Tatjanos Balvočienės parengtos medžiagos, publikuojama linma.org svetainėje, prieiga:

https://drive.google.com/file/d/1oVtRfXCQIq1c_xAo6uDi0xFGFre9IWhM/view

1 grupė: **Kriptografija**

1. Kas yra šifravimas?
2. Koks tikslas?
3. Kas yra kriptografija?
4. Kriptografijos tipai?
5. Kas yra šifravimo raktai?
6. Naudojimo pavyzdžiai?



Žmonės visada ieškojo būdų saugiai perduoti informaciją. Šifravimo raidą lėmė ir lemia besitęsianti kova tarp **šifro kūrėjų** ir siekiančių atskleisti šifro raktą (kartais vadinamų „šifro laužytojų“).

Sąvokos:

- ♦ **Paprastas tekstas** yra pranešimas prieš šifravimą.
- ♦ **Šifruotas tekstas** yra pranešimas po šifravimo.
- ♦ **Žodžiai iššifravimas ir dešifravimas** yra sinonimai.

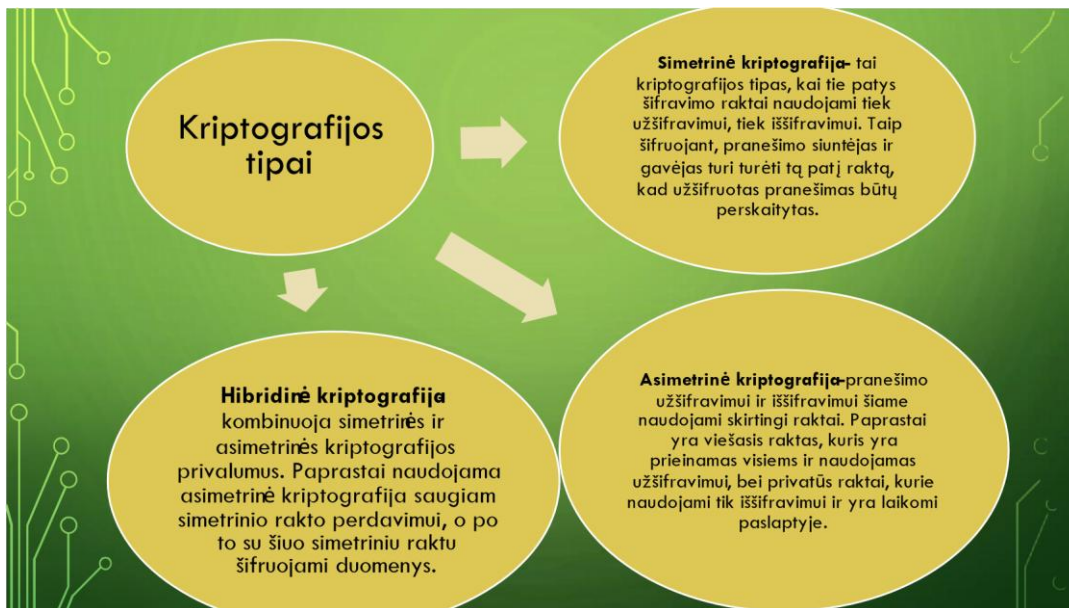
5 pav. Sąvokos



6 pav. Kriptografijos sąvokos

Šifravimas ir tikslai		
<p>Šifravimo tikslai – tai ilgalaikės kryptys arba bendrosios vizijos, kurias norima pasiekti per informacijos šifravimą.</p>	<p>Vienas pagrindinių šifravimo tikslų – užtikrinti duomenų konfidencialumą (saugumą). Tai siekis sutrukdyti pašaliniams asmenims susipažinti su slapta informacija.</p>	<p>Kitas tikslas gali būti užtikrinti duomenų integralumą (vientisumą) –garantuoti, kad duomenys nebuvo pakeisti neleistinai.</p>
<p>Šifravimas – tai būdas saugoti mūsų duomenis, informaciją, žinutes nuo „smalsių akių“: -vaikams tai gali būti įdomiu žaidimu; - suaugusiems tai būdas apsaugoti norimą informaciją nuo kitų.</p>	<p>Šifravimo raktas yra informacija, kuri nustato, kaip pradinis tekstas bus pakeistas šifruotu tekstu.</p>	<p>Šifravimo raktą būtina laikyti saugiai. Jei kas nors sužinos šifravimo raktą, jis galės iššifruoti šifruotą tekstą.</p>
<p>Šifravimo raktai – konkrečios šifravimo taisyklės, schemas, metodai.</p>	<p>Tai gali būti raidžių keitimo kitomis raidėmis ar konkrečiais simboliais, įvairios schemas, būdai ar gana sudėtingos matematiniais metodais pagrįstos procedūros.</p>	

7 pav. Šifravimas ir tikslai



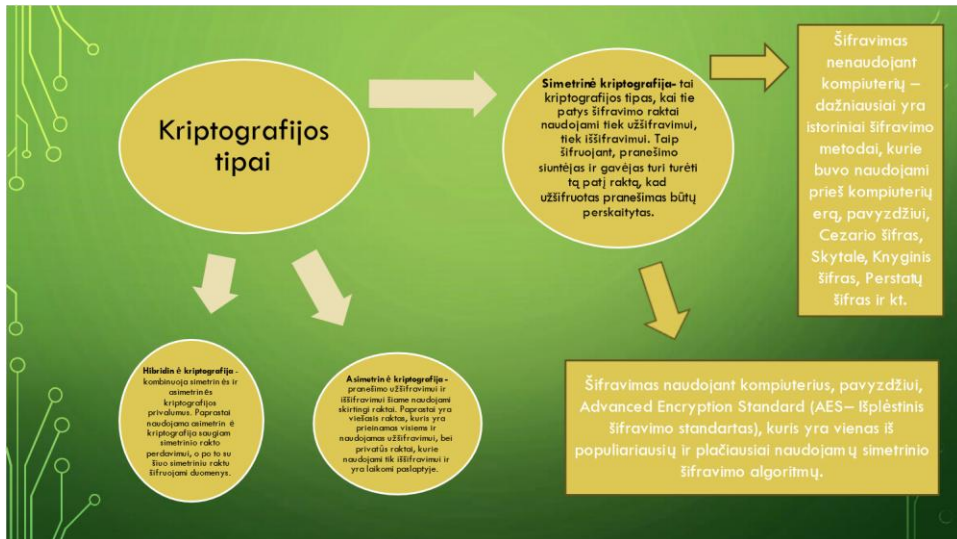
8 pav. Kriptografijos tipai

2 grupė: Simetrinis šifravimas

1. Kas yra šifravimas?
2. Koks tikslas?
3. Kas yra simetrinis šifravimas?
4. Kas yra šifravimo raktai?
5. Simetrinio šifravimo schema?
6. Naudojimo pavyzdžiai?

Šifravimas ir tikslai		
<p>Šifravimo tikslai – tai ilgalaikės kryptys arba bendrosios vizijos, kurias norima pasiekti per informacijos šifravimą.</p>	<p>Vienas pagrindinių šifravimo tikslų – užtikrinti duomenų konfidencialumą (saugumą). Tai siekis sutrukdyti pašaliniam asmeniui susipažinti su slapta informacija.</p>	<p>Kitas tikslas gali būti užtikrinti duomenų integralumą (vientisumą) –garantuoti, kad duomenys nebuvo pakeisti neleistinai.</p>
<p>Šifravimas – tai būdas saugoti mūsų duomenis, informaciją, žinutes nuo „smalsių akių“: -vaikams tai gali būti įdomiu žaidimu; - suaugusiems tai būdas apsaugoti norimą informaciją nuo kitų.</p>	<p>Šifravimo raktas yra informacija, kuri nustato, kaip pradinis tekstas bus pakeistas šifruotu tekstu.</p>	<p>Šifravimo raktą būtina laikyti saugiai. Jei kas nors sužinos šifravimo raktą, jis galės iššifruoti šifruotą tekstą.</p>
<p>Šifravimo raktai – konkretūs šifravimo taisyklės, schemas, metodai.</p>	<p>Tai gali būti raidžių keitimo kitomis raidėmis ar konkrečiais simboliais, įvairios schemas, būdai ar gana sudėtingos matematiniais metodais pagrįstos procedūros.</p>	

9 pav. Šifravimas ir tikslai



10 pav. Kriptografijos tipai



11 pav. Šifravimo naudojimo schema



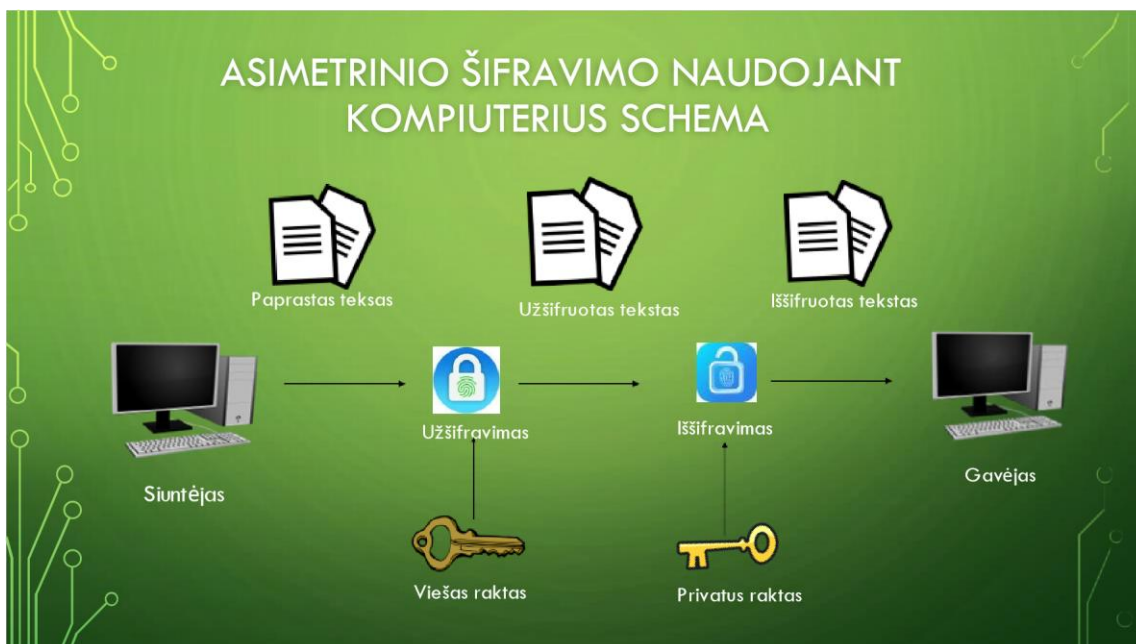
12 pav. Naudojimo pavyzdžiai

3 grupė: Asimetrisis šifravimas

1. Kas yra šifravimas?
2. Koks tikslas?
3. Kas yra asimetrisis šifravimas?
4. Kas yra šifravimo raktai?
5. Asimetrinio šifravimo schema?
6. Naudojimo pavyzdžiai?

Šifravimas ir tikslai		
<p>Šifravimo tikslai – tai ilgalaikės kryptys arba bendrosios vizijos, kurias norima pasiekti per informacijos šifravimą.</p>	<p>Vienas pagrindinių šifravimo tikslų – užtikrinti duomenų konfidencialumą (saugumą). Tai siekis sutrukdyti pašaliniam asmeniui susipažinti su slapta informacija.</p>	<p>Kitas tikslas gali būti užtikrinti duomenų integralumą (vientisumą) –garantuoti, kad duomenys nebuvo pakeisti neleistinai.</p>
<p>Šifravimas – tai būdas saugoti mūsų duomenis, informaciją, žinutes nuo „smalsių akių“: -vaikams tai gali būti įdomiu žaidimu; - suaugusiems tai būdas apsaugoti norimą informaciją nuo kitų.</p>	<p>Šifravimo raktas yra informacija, kuri nustato, kaip pradinis tekstas bus pakeistas šifruotu tekstu.</p>	<p>Šifravimo raktą būtina laikyti saugiai. Jei kas nors sužinos šifravimo raktą, jis galės iššifruoti šifruotą tekstą.</p>
<p>Šifravimo raktai – konkrečios šifravimo taisyklės, schemas, metodai.</p>	<p>Tai gali būti raidžių keitimo kitomis raidėmis ar konkrečiais simboliais, įvairios schemas, būdai ar gana sudėtingos matematiniais metodais pagrįstos procedūros.</p>	

13 pav. Naudojimo pavyzdžiai



14 pav. Naudojimo schema



15 pav. Naudojimo pavyzdžiai

4 ETAPAS (10 minučių)

Kiekvienos grupės pristatymas ir apibendrinamas atliktas darbas.

Refleksija. Mokiniai įvertina sėkmes ir nesėkmes aptariant žodžiu ar užpildant mokytojo parengtą apklausą (galima naudoti Google forms, Mentimeter, apklausa.lt ir pan.).

Laikas koreguojamas pagal poreikį, refleksija gali būti nukeliama kitai pamokai. (jei mokiniai nespėja pristatyti)

Simetrinio kodavimo pavyzdžiai, jų taikymo sritys (Sonata Rutkauskienė)

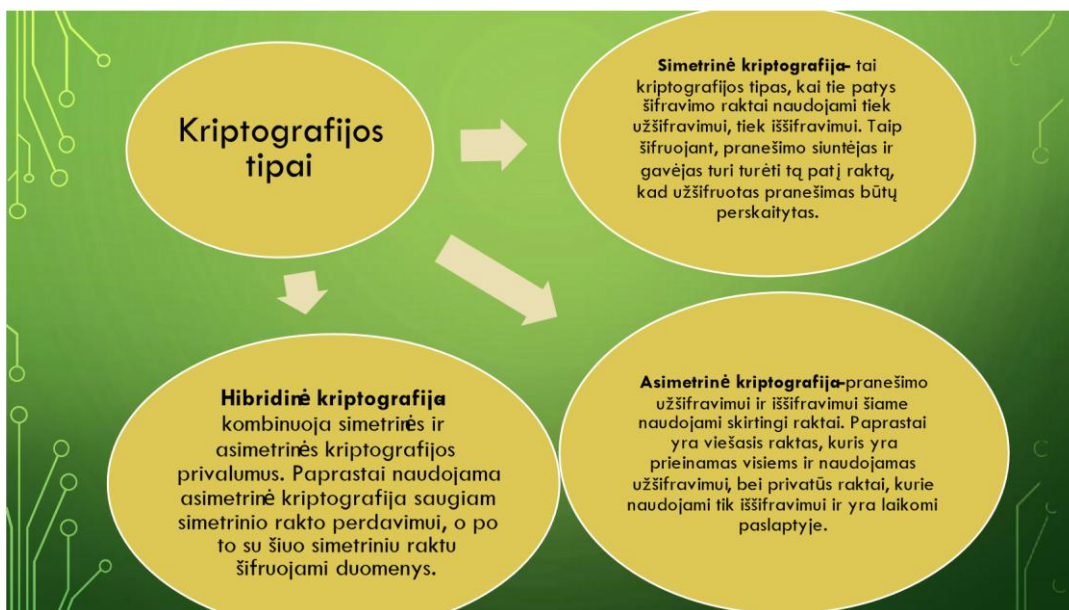
(C) Duomenų tyrybos ir informacijos mokymo(si) turinys 29.3.3. „Simetrinis ir asimetrinis šifravimas, kriptografinės sistemos. Apibrėžiamos simetrinio ir asimetrinio šifravimo, kriptografinės sistemos sąvokos.“[2]
9-10 klasės
Simetrinio kodavimo pavyzdžiai, jų taikymo sritys.
Matematika, anglų kalba, lietuvių kalba, istorija.
Pažinimo - analizuodami ir apdorodami duomenis, gebėdami šifruoti informaciją – ugdys informatinį mąstymą. Skaitmeninė – susipažindami su naujomis skaitmeninėmis priemonėmis – tobulins skaitmeninę kompetenciją Komunikavimo – teikdami informatyvią grįžtamąją informaciją mokytojui ir pagalbėdami draugui pamokos metu, patobulins komunikavimo kompetenciją.
Mokytis koduoti / šifruoti ir iššifruoti informaciją .
1. Susipažinti su keliais simetrinio šifravimo būdais. 2. Užšifruoti ir iššifruoti pateiktą informaciją nurodytu būdu.
Gebėsite užšifruoti ir iššifruoti pateiktą informaciją Cezario šifru, Kvadrato šifru, Geležinkelio tvorelės šifru.
Programinė įranga: 3. Interaktyvi lenta, multimedia projektorius. <ul style="list-style-type: none">• „Informatikos, informatinio mąstymo mokomoji veikla. Informacijos šifravimas.“ VILNIAUS UNIVERSITETAS• Tatjanos Balvočienės parengta medžiaga, publikuojama linma.org svetainėje, prieiga: https://drive.google.com/file/d/1oVtRfXCQIq1c_xAo6uDi0xFGFre9IW/hM/view<ul style="list-style-type: none">• https://skaiciuotuvai.lt/teksto-irankiai• https://www.youtube.com/watch?v=pIt4Q68J00A• https://www.online-stopwatch.com/countdown-clock/full-screen/• https://padlet.com/auth/login
Demonstravimas. Mokiniamis pristatomi keli šifravimo būdai. Individualus darbas. Mokiniamis pateikiama užduotis užšifruoti informaciją. Suteikiamas laikas. Diskusija. Darbų aptarimas.

<p>Slenkstinis – padedant mokytojui šifruoja pateiktą informaciją.</p> <p>Patenkinamas – apibūdina panaudotą šifravimo būdą.</p> <p>Pagrindinis – apibūdina ir paaiškina keletą šifravimo būdų.</p>
<p>Aukštesnysis – Lygina skirtingus šifravimo būdus, diskutuoja apie jų taikymo sritis. [2]</p> <p>Mokiniai įvertina pamoką ir įsivertina save: kas buvo sunkiausia, lengviausia, įdomiausia, ką sužinojo naujo – kaupiamasis vertinimas.</p>
<p>Gebėjimas naudotis elektroniniais žinynais. Taisyklingai vartoti kompiuterijos ir informacinių technologijų terminus, apibūdinti pagrindines sąvokas. [2]</p>
<p>Spec. poreikių mokiniams galima pateikti sukurtą projektą, kuriame jie galėtų atlikti paprastus papildymus .</p>
<p>1.Patys atlikite visas numatytas užduotis ir turėkite po ranka jų sprendimus.</p> <p>2.Turėkite užduočių skirtingų gebėjimų mokiniams, spec. poreikių mokiniams.</p>

1 ETAPAS (3 minučių)

Mokytojas paskelbia pamokos temą ir uždavinius.

Pakartoja simetrinio ir asimetrinio šifravimo sąvokas. Mokiniai pateikia panaudojimo pavyzdžių.



16 pav. Naudojimo schema

6 lentelė tikslas ir uždaviniai

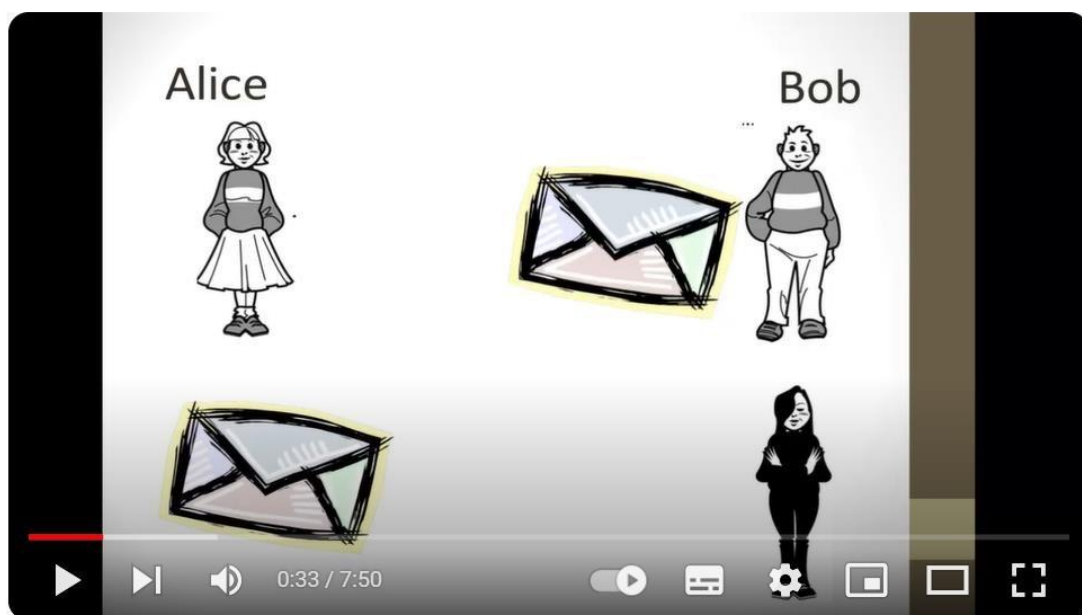
Tikslas	Gebėti koduoti / šifruoti ir iššifruoti informaciją .
Uždaviniai	1. Susipažinti su keliais simetrinio šifravimo būdais. 2. Užšifruoti ir iššifruoti pateiktą informaciją nurodytu būdu.

2 ETAPAS (37 minučių)

Pirmiausia mokiniams pristatoma **1. UŽDUOTIS**

JULIAUS CEZARIO ŠIFRAVIMO BŪDAS

Iki 4:00 min <https://www.youtube.com/watch?v=pIt4Q68J00A>



17 pav. Vaizdo įrašas

Kiekvienas mokinys ant suolų turi abėcėlę ir patarlę, jiems skirtos 3 minutės užšifruoti pateiktą patarlę (Pvz.: Darbas žmogų puošia. Be norago nebus ir pyrago. Kas nedirba , tas nevalgo ir pan.) raides keičia 4-a raide.

Abėcėlė (paveikslėlis)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Aa	Aą	Bb	Cc	Čč	Dd	Ee	Eę	Éé	Ff	Gg	Hh	Ii	Ij	Jj	Kk	Ll	Mm	Nn	Oo	Pp	Rr	Ss	Šš	Tt	Uu	Uų	Ūū	Vv	Zz	Žž	

18 pav. Abėcėlė

Naudojamas laikmatis 3:00

<https://www.online-stopwatch.com/countdown-clock/full-screen/>

Mokinys savo užšifruotą užduotį perduoda draugui ir is turi iššifruoti patarles per 3 min.
Perskaito savo iššifruotas patarles.

Mokytojas pristato **2. UŽDUOTIS**
Mokytoja pristato internetinį įrankį



19 pav. Skaičiuotuvai

ir mokiniams pateikiama užduotis : naudodami šį įrankį turi iškoduoti sekančią užduotį.

Cezario šifras - internetinis kodavimo / dekoderis

7 lentelė Cezario kodas

Hwywicgw xiag dojmyc wšycrichw šj hsyghą .

lžrichwg. lžycricy gojc giuozjchą dsbywų žcržwų goywbj wf xj dsfricy yowfèxs obhfoa bic hojėg
gérwbčwoa rfoiuiw.

Tikiuosi jums pavyko iškoduoti šį tekstą .

Užduotis. Užkoduok savo sugalvotą penkių žodžių sakinį ir jį perduok kairėje antram nuo tavęs
sėdinčiam draugui.

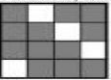
Mokiniai darbo atlikimui turi 5 minutes. Baigę darbą aptaria.

3 UŽDUOTIS

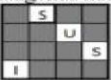
Mokytoja pristato ir demonstruoja **KVADRATŲ ŠIFRĄ.**

KVADRATŲ ŠIFRAS


Norime saugiai perduoti pranešimą „SUSITINKAME RYTOJ“. Šis pranešimas sudarytas iš 16 raidžių. Pranešimo užšifravimui pasirenkame 16 langelių kvadratą ir jame iškerpame 4 langelius. Žinoma, langeliai iškerpami specialiu būdu, kuris tuojau paaiškės. Tarkime, kad pasirinkome tokį būdą:

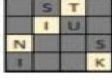


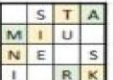

Specialiai parengtas 16 langelių kvadratas, kurio 4 balti langeliai yra kiauri. Nubraižome lygiai tokį patį 16 langelių kvadratą. Ant jo uždedame parengtąjį ir parašome į kiaurus langelius nuo viršaus iš kairės į dešinę 4 pirmąsias pranešimo raides:

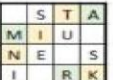



, tada uždėtąjį kvadratą pasukame 90 laipsnių kampu prieš laikrodžio rodyklę



ir vėl uždėję užrašome kitas keturias raides . Viršutinį kvadratą pasukus

dar kartą prieš laikrodžio rodyklę, tekstas bus toks: . Po trečio posūkio . Po trečio posūkio bus užšifruotas visas pranešimas: Siunčiamas toks pranešimo tekstas „YSTAMIUTNEOSIURK“.

Gavėjas privalo turėti identišką kvadratą, kad galėtų iššifruoti tekstą.

20 pav. Kvadratų šifras

Kas 4 mokiniai gauna KVADRATUS ir skirtingas frazes UŽKODUOTI, kiti 4 IŠKODUOTI.

8 lentelė 1 kodas

D	M	U
B	P	A
I	A	L
N	Ę	N

MAN NUPIRK BANDELĘ

9 lentelė 2 kodas

A	A	N
A	E	T
Š	L	N
I	J	D

ATSINEŠK SALDAINĮ

10 lentelė 3 kodas

K	P	A
K	M	A
B	V	R
K	E	A

PASKAMBINK VAKARE

11 lentelė 4 kodas

M	R	T
O	E	Y
I	P	K
A	U	A

RYT ATEIK PO PAMOK

Mokiniamis dirbant, mokytojas stebi procesą ir teikia pagalbą.

4 UŽDUOTIS

Pristatomas **GELEŽINKELIO TVORELĖS ŠIFRAS**

GELEŽINKELIO TVORELĖS ŠIFRAS

Panagrinėkime du geležinkelio tvorelės (angl. *rail fence*) atvejus.

1. Pranešimą „VAIKAI ATVYKSTA RYTOJ“ užrašykime 4 raidžių aukščio laužte, primenančia geležinkelio tvorelę, skirtą apsaugoti bėgius nuo užpustymo.

```
V       A       T       J
  A   I   T   S   A   O
    I   A   V   K   R   T
      K       Y       Y
```

Skaitydami užšifruotą pranešimą eilutėmis, gauname „VATJAITSAOIAVKRTKYY“.
Tokių atveju šifro raktas yra 4.

2. Dabar tą patį pranešimą parašykime stulpeliais po du simbolius:

```
V   I   A   A   V   K   T   R   T   J
  A   K   I   T   Y   S   A   Y   O
```

Skaitydami pranešimą eilutėmis, gauname „VIAAVKTRTJAKITYSAYO“.

21 pav. Geležinkelio tvorelės šifras

Pagal mokinių atliekamą darbą bus skirta užduotis atlikti klasėje arba namuose. Jie turės šiuo būdu užkoduoti bent 15 raidžių sakinį ir turėti ją kitai pamokai.

3 ETAPAS (5 minučių)

Refleksija. Nuskanavę QR code PADLET lentoje <https://padlet.com/auth/login> parašys savo įspūdžius:

Kas per pamoką sekėsi geriausiai.

Kas per pamoką buvo sunkiausiai.

Kas buvo įdomiausia.

Kuris šifras lengviausias.

Kriptografinės sistemos. Asimetrinis šifravimas (Sonata Rutkauskienė)

Pasiekimų sritis	(C) Duomenų tyrybos ir informacijos mokymo(si) turinys 29.3.3. Simetrinis ir asimetrinis šifravimas, kriptografinės sistemos. Apibrėžiamos simetrinio ir asimetrinio šifravimo, kriptografinės sistemos sąvokos.
Klasė	9-10 klasės
Tema	Kriptografinės sistemos. Asimetrinis šifravimas.

Integruojami dalykai, pasiekimai	Matematika, anglų kalba, lietuvių kalba, istorija.
Kompetencijos	Pažinimo - analizuodami ir apdorodami duomenis, gebėdami šifruoti informaciją – ugdys informatinį mąstymą. Skaitmeninė – susipažindami su naujomis skaitmeninėmis priemonėmis – tobulins skaitmeninę kompetenciją Komunikavimo – teikdami informatyvią grįžtamąją informaciją mokytojui ir pagelbėdami draugui pamokos metu, patobulins komunikavimo kompetenciją.
Tikslas	Įtvirtinti kriptografinės sistemos sąvoką, išmokti asimetrinio šifravimo.
Uždaviniai	1. Prisiminti ir įtvirtinti kriptografinės sistemos sąvoką. 2. Įtvirtinti simetrinį šifravimą. 3. Mokyti asimetrinio šifravimo.
Planuojamas rezultatas	1. Gebės apibūdinti kriptografines sistemas. 2. Užšifruosite, palyginsite ir įvardinsite skirtumus tarp simetrinio ir asimetrinio šifravimo.
Specifinės priemonės programinė įranga	/ 3 taupyklės 2 užraktais. 3 “viešieji“ raktai kiekvienai taupyklei. Lapeliai užrašams, rašymo priemonės. Programinė įranga: 1. Interaktyvi lenta, multimedia projektorius. 2. Literatūra ir kiti išteklių: • „Informatikos, informatinio mąstymo mokomoji veikla. Informacijos šifravimas.“ VILNIAUS UNIVERSITETAS • Tatjanos Balvočienės parengta medžiaga, publikuojama linma.org svetainėje, prieiga: https://drive.google.com/file/d/1oVtRfXCQIq1c_xAo6uDi0xFGFre9IWhM/view • https://www.ugdome.lt/kompetencijos5-8/irankiai/voratinklis_mob/grid/index.html

Mokymosi metodai	Praktinis tyrimas –simetrinė ir asimetrinė kriptografija, informacijos šifravimas. Darbas grupėse – mokiniai bendradarbiauja tarpusavyje ir konsultuojasi su mokytoju.
Mokinių atlikto darbo vertinimas ir įsivertinimas [2]	Slenkstinis –padedant mokytojui pateikia keletą šifravimo pavyzdžių. Patenkinamas – Aptaria šifravimo metodų pavyzdžius, apibūdina simetrinio ir asimetrinio rakto sampratą, savarankiškai užrašo Pagrindinis – Nagrinėja įvairius šifravimo metodus, susieja juos su praktiniais naudojimo pavyzdžiais, savarankiškai užrašo. Aukštesnysis – Lygina simetrinę ir asimetrinę kriptografines sistemas, diskutuoja apie jų taikymo sritis, sprendžia sunkesnius uždavinius. [2]
	Mokiniai įsivertina kas buvo sunkiausia, lengviausia, įdomiausia, ką sužinojo naujo – kaupiamasis vertinimas.
Žinios prieš	Gėbės naudotis elektroniniais žinynais. Taisyklingai vartoti kompiuterijos ir informacinių technologijų terminus, apibūdinti pagrindines sąvokas. [2]
Galimybės taikyti spec. poreikių mokiniams	Spec. poreikių mokiniams galima pateikti dalinai sukurtą projektą, kuriame jie galėtų atlikti paprastus papildymus.
Patarimai kolegoms, kurie naudos parengtą medžiagą	Pasiruošti reikiamas priemones arba apgalvoti kuo galima jas pakeisti , stebėti mokinių veiklas ir jas koordinuoti

1. ETAPAS (5 minutės)

Namų darbų tikrinimas ar visi turi atsinešę užšifruotas žinutes. Temos ir uždavinių skelbimas:

13 lentelė Tikslas ir uždaviniai

Tikslas	Įtvirtinti kriptografinės sistemos sąvoką, išmokti asimetrinio šifravimo.
Uždaviniai	Prisiminti ir įtvirtinti kriptografinės sistemos sąvoką. Įtvirtinti simetrinį šifravimą. Mokytis asimetrinio šifravimo.



22 pav. Kriptografijos sąvokos.

2. ETAPAS (30 minučių)

Mokytojas paskirsto mokinius į 3 gupes:

<https://www.classtools.net/random-group-generator/>

<https://www.online-stopwatch.com/random-group-generator/>

Paaškinama, kad šiandien mokiniai mokinsis ir supras kaip veikia **asimetrinis šifravimas**.

APRAŠOMA VEIKLA

Informacijai šifruoti asimetriniu šifravimu atliekami du skirtingi veiksmai :

- 1- kuris atliekamas (prieš išsiunčiant) informacijai užrakinti (užšifruoti),
- 2- kitas, kuris atliekamas (gavus siuntą) informacijai atrakinti (iššifruoti), kad šie veiksmai atliekami **naudojant atitinkamus skirtingus raktus – viešąjį ir privatų**.

Pateikiamas pranešimo užšifravimo bei iššifravimo realaus proceso žingsnių imitavimas.

Šis pavyzdys leidžia suprasti asimetrinio šifravimo esmę: galimybę saugiai perduoti informaciją naudojant skirtingus raktus užšifravimui ir iššifravimui.

23 pav. Aprašoma veikla.

Pristatomos priemonės, kurios bus reikalingos šiai veiklai.



24 pav. Reikalingos priemonės

Galima taupykles pakeisti ir kartoninėmis dėžutėmis ar vokais, simboliniais raktais ir pan. (verta pamąstyti apie dar vieną taupyklę, kurią atrakins pirmieji įveikę užduotis)

PASIRUOŠIMAS:

1. Kiekviena grupė gauna po taupyklę – mėlyną, juodą ir raudoną ir joms priklausančius „viešuosius“ raktus.
2. Grupės susigalvoja pavadinimus, jais pasižymi taupykles, pasižymi ir „viešuosius“ raktus.

RAKTŲ MAINAI:

3. Kiekviena grupė perduoda kitoms grupėms po vieną „viešąjį“ raktą.

„ŠIFRUOTŲ NAMŲ DARBŲ „ĮDĖJIMAS IR UŽRAKINIMAS:

4. Su kiekvienos grupės gautu raktu atrakina tos grupės taupyklę ir sudeda tiek užkoduotų namų darbų, kiek grupėje mokinių.

“NAMŲ DARBŲ” ATRAKINIMAS (IŠŠIFRAVIMAS):

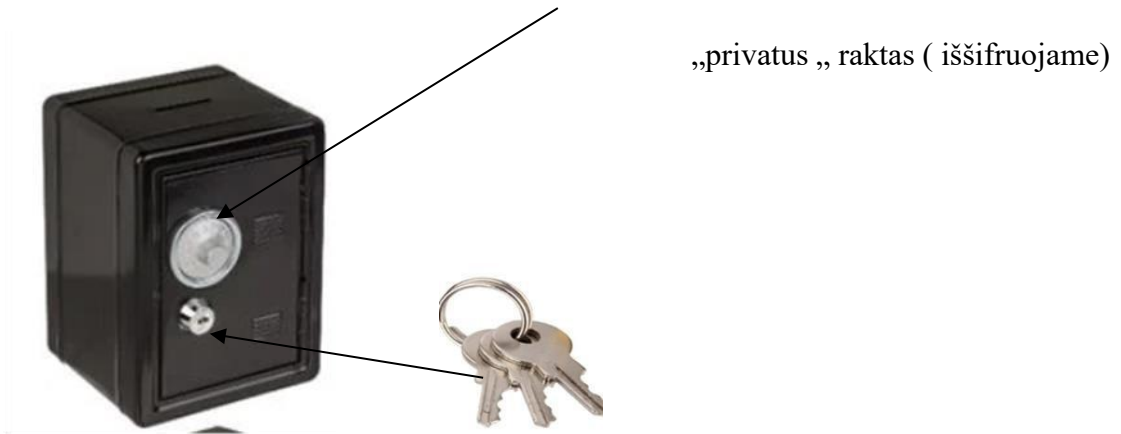
5. Kiekviena grupė „privačiu“ raktu atrakina taupykles ir išsiima sudėtas užduotis.

„UŽDUOČIŲ“ ŠIFRAVIMAS:

6. Mokiniai grupėse turi 5 minutes „iššifruoti“ jiems paliktas užduotis.

APTARIMAS:

7. Kiekviena grupė perskaito „iššifruotus namų darbus“ ir visi kartu su mokytoju aptaria, kokios atliktos veiklos ir asimetrinio šifravimo žingsniai (vienu – viešuoju- raktu užrakiname (užšifruojame), kitu- privačiu- atrakiname (iššifruojame)).



„privatus „ raktas (iššifruojame)

25 pav. Raktai.

„viešasis“ raktas (užšifruojame)

3 ETAPAS (10 minučių)

Palyginsite ir įvardinsite skirtumus tarp simetrinio ir asimetrinio šifravimo.

Pamokai apibendrinti ir įsivertinti, naudosime voratinklio, žvaigždės formos šabloną. Figūrų ašyse mokiniai turėtų pažymėti kaip jiems sekėsi suprasti kiekvieną šifravimo būdą. Mokytojas ašis pavadina šifrų pavadinimais. Mokiniais gali būti pasiūlyta įsivertinti ir dalyko gebėjimus, ir bendrąsias kompetencijas.

https://www.ugdome.lt/kompetencijos5-8/Irankiai/voratinklis_mob/grid/index.html