17 veikla

Dalijimasis paslaptimis. Informacijos slėpimo protokolai

Santrauka

Kriptografijos metodai leidžia dalytis informacija su kitais žmonėmis ir kartu išlaikyti itin aukštą privatumo lygį. Šiame skyriuje aptariama, kaip galima dalytis neatskleista informacija: mokinių grupė skaičiuoja savo grupės amžiaus vidurkį, nors nežino tikslaus grupės narių amžiaus.

Ryšiai su ugdymo programomis

- ✓ Matematika: sudėtis ir vidurkis

Gebėjimai

- ✓ Vidurkio skaičiavimo
- ✓ Bendradarbiavimo

Amžius

- ✓ Nuo 7 metų

Priemonės

Kiekvienai mokinių grupei reikės:

- ✓ Užrašų knygelės ar sąsiuvinio
- ✓ Rašiklio

Dalijimasis paslaptimis

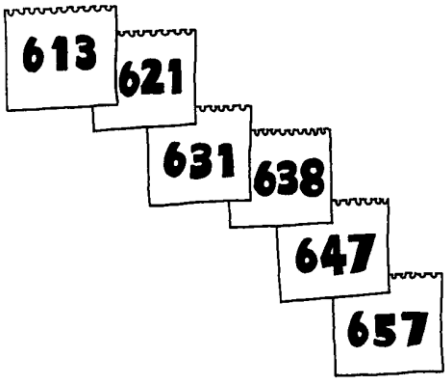
Įvadas

Atlikdami šią veiklą mokiniai skaičiuoja savo grupės amžiaus vidurkį, nors nežino tikslaus kiekvieno grupės mokinio amžiaus. Lygiagrečiai kitos grupės gali skaičiuoti grupės gaunamų dienpinigių vidurkį. Šių statistinių duomenų skaičiavimas ypač tinkamas suaugusiesiems – juk jiems labiau rūpi informacija apie amžių ir pajamas.

Grupėse turi būti bent po 3 mokinius.

Diskusija

1. Paaiškinama, kad grupių mokiniai vieni kitiems negali pasakyti savo tikslaus amžiaus (ar dienpinigių sumos). Jie turi suskaičiuoti amžiaus (dienpinigių) vidurkį nežinodami vienas kito amžiaus (dienpinigių sumos). Mokinių paklausiama, ar jie tiki, kad tai įmanoma padaryti, ir kaip tai būtų galima padaryti.
2. Pasirenkama 6–10 mokinių. Pirmajam mokiniui duodama užrašų knygelė ir rašiklis ir paprašoma užrašyti bet kokį triženklį skaičių. Pavyzdyje dešinėje atsitiktinai parinktas skaičius 613.
3. Pirmasis mokinys išplėšia lapą su užrašytu atsitiktiniu skaičiumi. Jis prideda savo amžių prie pirmojo skaičiaus ir užrašo gautą rezultatą antrajame lape. Pavyzdyje pirmojo mokinio amžius yra 8, todėl antrasis triženklis skaičius yra 621. Išplėštas lapas nerodomas kitiems mokiniams.



4. Užrašų knygelė perduodama antrajam mokiniui. Jis išplėšia lapą, prideda savo amžių prie užrašyto lape skaičiaus ir užrašo gautą rezultatą trečiajame lape. Pavyzdyje antrojo mokinio amžius yra 10 metų, todėl užrašoma 631.
5. Tai tęsiama, kol visi mokiniai užrašo skaičius.

6. Užrašų knygelė grąžinama pirmajam mokiniui. Mokinys atima savo sugalvotą skaičių iš užrašyto paskutinio skaičiaus. Pavyzdyje užrašų knygelė perėjo per penkių mokinių rankas, paskutinis užrašytas skaičius – 657. Iš 657 atimamas sugalvotas skaičius 613. Gaunama 44. Tai visų mokinių amžiaus suma. Šią sumą padalijus iš 5 gaunamas grupės mokinių amžiaus vidurkis – 8,8.
7. Pabrėžiama, kad nė vieno mokinio amžius nebus žinomas, kol nebus parodyti išplėštieji lapai su skaičiais.

Gudručiams

Ši sistema gali būti taikoma slaptai balsuojant, kai kiekvienas balsuojantysis prideda vienetą, jei balsuoja „taip“, arba 0, jei balsuoja „ne“. Žinoma, jei kas nors prideda daugiau kaip vieną (arba mažiau kaip 0), balsavimas yra neteisingas. Taip pat rizikuojama sukelti įtarimų, jei visi balsuoja „taip“, nes balsų „taip“ skaičius būna didesnis užbalsavusių žmonių skaičių.

Apie ką visa tai?

Kompiuteriuose saugoma labai daug mūsų asmeninės informacijos: banko sąskaitų likučiai, socialinių tinklų informacija, kiek mokame mokesčių, kiek galioja turimas vairuotojo pažymėjimas, kokie mūsų egzaminų rezultatai, medicininiai įrašai ir pan. Šios informacijos privatumas labai svarbus, tačiau kai kuria informacija mums reikia dalytis su kitais. Pavyzdžiui, parduotuvėje mokant už prekes banko kortele, pardavėjui reikia įsitikinti, kad pirkėjas turi lėšų savo banko sąskaitoje.

Dažnai pateikiama daugiau informacijos, negu iš tikrųjų reikia. Pavyzdžiui, kai atliekamas elektroninis mokėjimas, pardavėjas gauna pirkėjo banko pavadinimą, sąskaitos numerį, vardą ir pavardę. Be to, bankui perduodama, kur asmuo perka. Iš banko gaunamų privačių kliento duomenų būtų galima sukurti to kliento profilį: kur perkami degalai, kur bakalėjos prekės, kiek ir kur išleidžiama per dieną. Mokant grynaisiais pinigais šios informacijos nebūtų galima sužinoti. Dauguma žmonių nekreipia dėmesio į savo asmens duomenų dalijimą, tačiau visada yra tikimybė, kad privačiais duomenimis gali būti piktnaudžiaujama: jie gali būti naudojami tikslinei rinkodarai (pavyzdžiui, siunčiama kelionių reklama žmonėms, daug išleidžiantiems kelionių bilietams), jais disponuojant galima diskriminacija (pavyzdžiui, geresnių paslaugų siūlymas pasiturintiems bankų klientams) ar šantažas(pavyzdžiui, grasinimai paviešinti abejotiną sandorį). Visada galima pakeisti pirkimo būdą, jei manoma, kad perkančiojo privačiais duomenimis kas nors neteisėtai pasinaudos.

Nors nurodyti privatumo pažeidimai priimtini daugumai žmonių, jau esama kriptografijos protokolų, kurie leidžia elektronines finansines operacijas atlikti tokiu pačiu privatumo lygiu, kaip mokant grynaisiais. Sunku patikėti, kad pinigai gali būti pervedami iš jūsų banko sąskaitos į parduotuvės sąskaitą niekam nežinant, iš kurios sąskaitos ir į kurią jie pervedami. Ši veikla leidžia įsitikinti, kad tokia operacija įmanoma: abiejose situacijose ribojamas informacijos dalijimasis, o tai įmanoma pasiekti „protingu“ protokolu.

Daugiau informacijos

Davido Chaumo straipsnyje „Security without identification: transaction systems to make Big Brother obsolete“ pateikiama paprastų informacijos slėpimo protokolų pavyzdžių, kaip gali būti atliekamos visiškai privačios elektroninės finansinės operacijos. Straipsnis išspausdintas 1985 m. žurnale „Communication softhe ACM“.