Kriptografija

I–II (9–10) gimnazijos klasės

Užduotys

Mokytojas gali pasirinkti, kurias užduotis mokiniai atliks individualiai, o kurias – dirbdami grupėse, taip pat numatyti, kada bus atliekamos pasirinktos užduotys – pamokoje, mokantis savarankiškai, projektinėse veiklose ir kt.

1 užduotis (5 skaidrė):

Škotijos karalienės Marijos Stiuart likimas buvo ne pirmas kartas istorijoje, kai žmogaus gyvenimas ar visos valstybės likimas priklausė nuo susirašinėjimo ar informacijos šifro jėgos.

Pateikite savo sugalvotų ar jums žinomų pavyzdžių (situacijų) iš skaitytų knygų, straipsnių, pasakojimų, kai šifro rakto atskleidimas (neatskleidimas) galėtų turėti ar turėjo lemiamas pasekmes žmonių, šalies, Lietuvos kariuomenės, Lietuvos partizanų, ar rezistencinės (pasipriešinimo) kovos prieš okupaciją dalyvių likimams. Diskusijose su klasės draugais aptarkite, kaip buvo (būtų) galima išvengti šifro rakto atskleidimo ir jo pasekmių. Nepamirškite ir apie galimybę priešui pateikti silpnu raktu šifruotą klaidinantį pranešimą.

2 užduotis (7 skaidrė):

Užduotis pamąstymui ir diskusijai

Brangius daiktus, svarbią informaciją įstaigos, žmonės dažnai laiko seifuose. Kodėl, jūsų manymu, informacijos apsaugai nepakanka seifų, kodėl reikia sudėtingų kriptografinių sistemų (šifravimo)?

3 užduotis (21 skaidrė):

Laikinai pasijuskite Julijumi Cezariu ir, naudodami šį simetrinį šifravimo metodą, užšifruokite kokią nors jo mintį, pvz. iš https://www.c1.lt/zyme/gajus-julijus-cezaris/ ar kokią nors patarlę ir slaptai perduokite draugui(-ei) perskaityti. Aptarkite šį informacijos šifravimo metodą saugumo aspektu.

4 užduotis (22 skaidrė):

Žodžio „SUSITIKIME“ šifruotas žodis – „BUVUJŪJNJPF“. Nustatykite, kokį keičiamos raidės atstumą (postūmį) pasirinko vaikai. Pabandykite šiuo šifravimo metodu užšifruoti savo vardą ar trumpą tekstą. Šifruotais tekstais pasikeiskite su klasės draugais. Pabandykite gautą draugo tekstą iššifruoti.

5 užduotis (23 skaidrė):

Užduotis pamąstymui ir diskusijai

Ar garbingai pasielgė Žilvinas perskaitęs aptiktą pranešimą nors žinojo, kad tai Šarūno ir Živilės slaptas susirašinėjimas.

Kaip pasielgtumėte jūs?

6 užduotis (24 skaidrė):

Naudodami paprasto popieriaus lapo juosteles ir jums prieinamas skirtingo skersmens lazdeles užšifruokite trumpą pranešimą spartiečių stiliumi. Pasikeitus juostelėmis, bandykite perskaityti gautą užšifruotą tekstą. Jei kam pavyktų tai padaryti, aptarkite, ką buvo galima padaryti geriau, kad teksto atskleidimas būtų labiau apsunkintas.

7 užduotis (25 skaidrė):

Kritiškai įvertinkite šio simetrinio šifravimo metodo saugaus duomenų perdavimo galimybę. Kaip galima būtų patobulinti šį metodą?

Naudodami, pavyzdžiui, raktą „52143“ ar kitą, užšifruokite trumpą patarlę. Pateikite ją draugui, siūlydami iššifruoti.

8 užduotis (26 skaidrė):

Naudodami internete PDF formatu publikuojamą Vinco Mykolaičio Putino knygą „Altorių šešėly“ http://antologija.lt/files/pdf/vincas-mykolaitis-putinas-altoriu-sesely.pdf (žr. 2023-09-20), iššifruokite žinutę: „13-10-11 117-5-14 8-9-1 84-5-1 84-5-2“.

Pabandykite šiuo metodu užšifruoti mokytojo pateiktą ar savo žinutę. Duokite klasės draugui iššifruoti. Diskutuodami nustatykite šio šifravimo metodo silpnąsias ir stipriąsias puses.

9 užduotis (27 skaidrė):

Nustatykite, kurios iš pateiktų simetrinių šifravimo sistemų yra saugiausios. Pagrįskite tai argumentais diskutuodami su klasės draugais.

10 užduotis (28 skaidrė):

Užduotis (tema 29.3.3.). Klasė suskirstoma į kelias grupes po, pavyzdžiui, 3–5 mokinius.

Scenarijus. Yra numatytas klasės vakarėlis, kuriame dalyvaus ir mokytojai. Kiekviena mokinių grupė ruošia staigmeną vienam pasirinktam vakarėlio dalyviui iš kitos grupės arba mokytojui. Dirbant grupėje ir naudojant vieną iš nagrinėtų ar šioje skaidrėje pateiktose nuorodose aprašytų metodų arba šifravimo įrankį, reikia užšifruoti numatytos vakarėlio staigmenos trumpą aprašymą. Baigus šifravimą, grupės pasikeičia užšifruotais pranešimais (raktą laiko paslaptyje). Nutariama, iki kada mokiniai bandys iššifruoti pranešimus (gali tai daryti ir namuose). Nustatytu laiku grupės atstovai visai klasei praneša apie nustatytus šifravimo metodus, juos apibūdina, paskelbia dešifruotą pranešimą, pasako, kas buvo sunkiausia, išrenka saugiausią panaudotą šifravimo metodą.

11 užduotis (29–37 skaidrės):

Veikla, demonstruojanti, kaip vyksta asimetrinis šifravimas

Aprašomos veiklos esmė – parodyti, kad informacijai šifruoti asimetriniu šifravimu atliekami du skirtingi veiksmai: vienas, kuris atliekamas (prieš išsiunčiant) informacijai užrakinti (užšifruoti), ir kitas, kuris atliekamas (gavus siuntą) informacijai atrakinti (iššifruoti), ir kad šie veiksmai atliekami naudojant atitinkamus skirtingus raktus – viešąjį ir privatų.

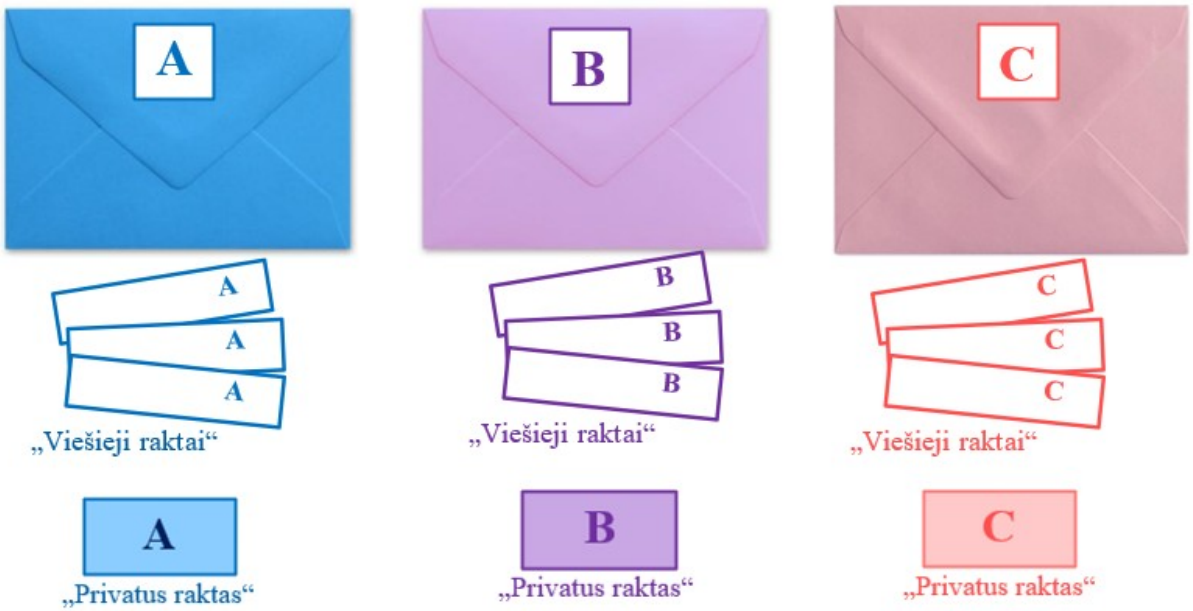
Aprašant šios užduoties veiklas, pateikiamas pranešimo užšifravimo bei iššifravimo realaus proceso žingsnių imitavimas.

Šis pavyzdys yra paprastas, bet jis leidžia suprasti asimetrinio šifravimo esmę: galimybę saugiai perduoti informaciją naudojant skirtingus raktus užšifravimui ir iššifravimui.

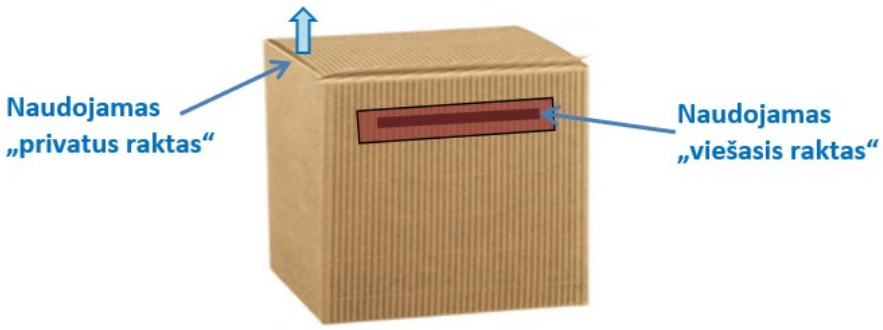
Priemonės:

- ✓ 3 dėžutės su dviem užraktais („viešuoju“ ir „privačiu“).
- ✓ 1 „privatus“ + 3 „viešieji“ raktai kiekvienai dėžutei.
- ✓ Etiketės, žymekliai arba kitos priemonės dėžučių ir raktų žymėjimui.
- ✓ Lapeliai užrašams, rašymo priemonės.

Patarimas. Neturint dėžučių, galima naudoti simbolines „dėžutes“ (tai gali būti vokai, kartoninės dėžutės arba sulenkti popieriaus lapai) ir simbolinius „raktus“ (pavyzdžiui, „viešieji raktai“ ir „privatūs raktai“ gali būti nedideli spalvoti ir (arba) atitinkamai pažymėti lapeliai):



Veiklai tinka ir kartoninės dėžutės:



Svarbu! Realaus proceso imitavimui naudojant simbolines „dėžutes“ ir simbolinius „raktus“, **būtini aiškus bendri susitarimai**, kada ir kaip turi būti naudojami „viešieji raktai“ bei kada ir kaip – „privatūs“.

Veikla:

Pasiruošimas:

- ✓ Sudaromos trys mokinių grupės, kiekviena grupė gali sugalvoti savo grupei pavadinimą. Mes paprastumo dėlei grupes pavadinome A, B ir C.
- ✓ Kiekviena iš trijų grupių gauna grupės vardu (A, arba B, arba C) pažymėtą dėžutę bei grupės vardu (A, arba B, arba C) pažymėtus raktus – „viešuosius“ ir vieną „privatų“ (jį reikia dar papildomai pažymėti, pavyzdžiui, grupės vardu 

arba įrašu „privatus“).

Raktų mainai:

- ✓ Grupė A perduoda grupėms B ir C po vieną savo „viešąjį“ raktą – šis raktas kitų grupių bus naudojamas tik tam, kad grupės B ir C į grupės A dėžutę įdėtų užrašytą „paslaptį“ („užšifruotų“ pranešimą). „Privatų“ raktą 

grupė A pasilieka sau.
- ✓ Tokius pat veiksmus atlieka ir grupės B bei C – perduoda savo „viešuosius“ raktus kitoms grupėms, sau palikdami „privatų“ raktą ir vieną „viešąjį“.

„Paslapčių“ įdėjimas ir užrakinimas (užšifravimas):

- ✓ Grupė A atidaro grupių B ir C dėžutes naudodamiesi atitinkamais tų grupių „viešaisiais“ raktais, įdeda „paslaptis“ (informaciją, kurią užšifruojama ir perduodama kitai grupei, pavyzdžiui, pranešimą **„Šį ketvirtadienį mokykloje vyks geografijos naktis. Renkamės 20 valandą sporto salėje. Nepamirškite pasiimti vandens ir maisto.“**) ir vėl užrakina („užšifruoja“).
- ✓ Taip pat elgiasi ir grupės B bei C.

„Paslapčių“ atrakinimas(iššifravimas):

- ✓ Grupė A naudoja savo „privatų“ raktą (raktą, kurio neatidavė kitoms grupėms, o pasiliko sau: 

), kad atrakintų savo dėžutę ir rastų kitų grupių įdėtas (atsiųstas) „paslaptis“ („iššifruoja“ perduotą pranešimą).

- ✓ Grupės B ir C daro tą patį.

Aptarimas

- ✓ Kiekviena grupė perskaito atsiustas „iššifruotas paslaptis“ ir visi kartu su mokytoju aptaria, kokie yra atliktos veiklos ir asimetrinio šifravimo žingsnių atitikimai (pavyzdžiui, vienu – *viešuoju* – raktu užrakiname (užšifruojame), kitu – *privačiu* – raktu atrakiname (iššifruojame)):

Realūs šifravimo veiksmai naudojant kompiuterius ir šifravimo raktus skaitmeninėje formoje bus atliekami informatikos pamokose 11–12 klasėse (III–IV gimnazijos klasėse).

Medžiagą parengė

Tatjana Balvočienė, informatikos mokytoja ekspertė, Šilutės Vydūno gimnazija

Antanas Balvočius, Kompetencijų aprašo, Bendrųjų programų (BP) įvado ir Informatikos BP bei rekomendacijų bendraautorius

2023 m. rugsėjis