Vilniaus universitetas

Metodinė medžiaga Informacijos šifravimas pradiniam ugdymui

Vaikystės pedagogika

Kuriame
Lietuvos ateitį
2014–2020 metų
Europos Sąjungos
fondų investicijų
veiksmų programa

Metodinė medžiaga. Informacijos šifravimas pradiniam ugdymui

Informatikos ir informatinio mąstymo veiklos, metodinė medžiaga sukurta įgyvendinant projektą „Aukštųjų mokyklų tinklo optimizavimas ir studijų kokybės gerinimas Šiaulių universitetą prijungiant prie Vilniaus universiteto“, projekto Nr. 09.3.1-ESFA-V-738-03-0001, vykdomą pagal 2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programos 9 prioriteto ,,Visuomenės švietimas ir žmogiškųjų išteklių potencialo didinimas“ 09.3.1-ESFA-V-738 įgyvendinimo priemonę ,,Aukštųjų mokyklų tinklo tobulinimas“, finansuojamą Europos Sąjungos fondų ir Lietuvos Respublikos valstybės biudžeto lėšomis.

Metodinė medžiaga „Informacijos šifravimas pradiniam ugdymui“, skirta Vaikystės pedagogikos studijų programos moduliui „Matematinio ir informatinio raštingumo ugdymas: Informatinio mąstymo didaktika“. Tikslinė grupė – būsimi pradinio ugdymo mokytojai. Medžiaga siejasi su informatikos ir matematikos Bendrosiomis programomis, pateikiamas teorinis temos pagrindimas mokytojui, aptariamos pagrindinės srities sąvokos. Šifravimas arba kriptografija – tai informacijos kodavimas siekiant informaciją įslaptinti. Šifravimas yra abipusis procesas, t. y. susijęs su informacijos užšifravimu ir iššifravimu. Priemonėje nagrinėjami paprasti, pradinių klasių mokiniams suprantami šifrai: raidžių keitimas skaičiais, Cezario, stačiakampis, tinklelio, geležinkelio tvorelės šifrai. Nagrinėjami pavyzdžiai, užduotys pateikiamos su nurodymais ir sprendimais. Nurodomas pagrindinių šaltinių sąrašas.

Šios veiklos autoriai: Alvida Lozdienė ir prof. dr. Valentina Dagienė

Redagavo: Viktoras Dagys

Projekto vykdytojas: Vilniaus universitetas

Vilnius, 2022

TEMA: INFORMACIJOS ŠIFRAVIMAS PRADINIAM UGDYMUI

Ryšys su bendrosiomis programomis

3–4 kl.

25.3. Duomenų tyrybos ir informacijos mokymosi turinys:

25.3.6. Duomenų šifravimas. Sprendžiami šifravimo uždaviniai ir pristatoma duomenų šifravimo sąvoka. Mokomasi, kaip duomenis užšifruoti taikant paprastus būdus ir juos iššifruoti (pavyzdžiui, postūmį per kelias abėcėlės raides, raidžių keitimą kuriais nors simboliais ir pan.)

3. Duomenų tyryba ir informacija (C)

Nurodo keletą duomenų ir informacijos saugumo problemų, aptaria šifravimo pavyzdžius (C3.2.)

INFORMACIJOS ŠIFRAVIMAS

Kriptografija (sudėtinė kriptologijos mokslo dalis) dažnai vadinama šifravimu. Šifravimas – tai mokslas, tyrinėjantis informacijos saugojimo ir perdavimo slaptumą ir saugumą. Šiuolaikinis šifravimas susijęs su matematika, informatika ir elektrotechnika. Šifravimas naudojamas bankomatų (bankų) kortelėse, kompiuterių slaptažodžiuose, internetinėje prekyboje.

Kriptologija (gr. *kryptós* – paslėptas ir *logos* – elgesys) – mokslas apie slaptumą, šifravimą, pranešimų slėpimą (kriptografija) ir užšifruotų duomenų atskleidimą (kriptoanalizė). Kriptologija – tai kriptografijos ir kriptoanalizės mokslas.

Kai pranešimas siunčiamas naudojant šifravimą, prieš siunčiant jis pakeičiamas (užšifruojamas). Teksto keitimo metodas vadinamas „šifru“. Pakeistas tekstas vadinamas šifruotuoju tekstu. Dėl pakeitimo gautą pranešimą tampa sunku perskaityti. Norintysis jį perskaityti, turi iššifruoti. Kaip pranešimą iššifruoti yra paslaptis. Tiek pranešimą siunčiantis, tiek jį gaunantis asmuo turi žinoti paslaptį (būdą, kaip tekstas buvo pakeistas), tačiau kiti žmonės to neturėtų žinoti. Šifrogramos teksto tyrimas siekiant sužinoti užšifruotą pranešimą vadinamas „kriptoanalize“.

Užšifravimas – tai specialus informacijos kodavimo būdas siekiant ją įslaptinti (paslepiama informacijos prasmė).

Iššifravimas – tai procesas, kurio metu grąžinama pradinė užšifruotų duomenų forma.

Skirtingų rūšių užšifravimas gali būti paprastesnis arba sudėtingesnis. Šifruose naudojamas „raktas“, kuris yra slaptas. Užšifravimo būdas (metodas) nebūtinai turi būti slaptas. Įvairūs žmonės gali naudoti tą patį metodą, bet skirtingus raktus, todėl jie negali perskaityti vienas kito pranešimų. Pavyzdžiui, Cezario šifras turi tik tiek raktų, kiek naudojamoje abėcėlėje yra raidžių. Išbandžius visus raktus užšifruotą pranešimą lengva iššifruoti ir nežinant rakto. Šifrai, kurie leidžia naudoti milijardus raktų, iššifruojami (nulaužiami) sudėtingesniais metodais.

Nuo Cezario laikų buvo sukurta įvairių šifrų. Kai kuriuose buvo pasitelkta gudri matematika, kad kriptoanalizės procesas būtų labai sudėtingas. XX a. kompiuteriai tapo pagrindine pranešimų šifravimo priemone.

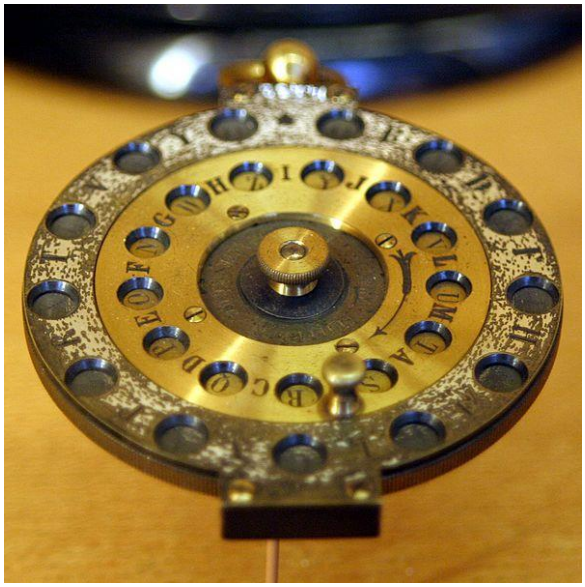
Šifravimui naudojant simetrinio rakto algoritmą, tiek siuntėjas, tiek gavėjas dalijasi raktu. Siuntėjas raktą naudoja pranešimui paslėpti. Gavėjas tą patį raktą naudoja atvirkščiu būdu, kad perskaitytų pranešimą. Šimtmečius didžioji dalis kriptografijos buvo simetrinė.

Asimetrinį šifravimą naudoti sunkiau. Kiekvienas asmuo, norintis naudoti asimetrinį šifravimo būdą, naudoja slaptą skaičių (privatų raktą), kuriuo nesidalijama, ir kitą skaičių (viešąjį raktą), kurį gali pasakyti visiems. Jei kas nors kitas norės šiam asmeniui nusiųsti pranešimą, jis pasinaudos jam pasakytu skaičiumi, kad paslėptų pranešimą. Pranešimo gavėjas, naudodamasis savo slaptuoju (privačiuoju) raktu, gali lengvai perskaityti pranešimą. Niekam kitam nereikia žinoti slaptojo rakto.

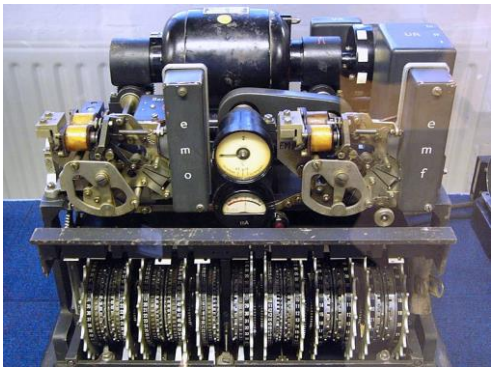
Asimetrinė kriptografija paprastai užima daugiau laiko ir reikalauja galingų kompiuterių, todėl mažiau naudojama. Ji dažnai taikoma skaitmeniniams parašams, kai kompiuteris turi žinoti, kad tam tikrus duomenis (pvz., failą ar svetainę) atsiuntė tam tikras siuntėjas. Pavyzdžiui, kompiuterių programinės įrangos bendrovės, kurios išleidžia savo programinės įrangos naujinimus, gali juos pasirašyti, kad įrodytų, jog naujinimą atliko jos – taip apsisaugoma nuo įsilaužėlių, kurie gali sumanyti sukurti savo naujinimų, darančius žalą. Saityno HTTPS protokolą naudojančios interneto svetainės naudoja populiarų viešojo rakto sistemos RSA algoritmą, kad sukurtų sertifikatus, kurie įrodo, kad svetainė priklauso joms ir kad ji yra saugi.

Kompiuteriai gali generuoti labai saugų šifravimą ir XXI a. toks dažniausiai ir naudojamas. Šifravimo ir dešifravimo užduotys ugdo mokinių informatinį mąstymą.

Pateikiamos iliustracijos, kurias mokytojas gali pademonstruoti ir mokiniams.



XX a. pradžios šifravimo ratas (https://kids.kiddle.co/Image:CNAM-IMG_0558.jpg)



Vokiečių Lorenco šifravimo mašina, naudota Antrojo pasaulinio karo metais labai aukšto lygio generalinio štabo pranešimams šifruoti (https://kids.kiddle.co/Image:Lorenz-SZ42-2.jpg)

XVI a. knygos formos prancūziškas šifravimo aparatas

(https://kids.kiddle.co/Image:16th_century_French_cypher_machine_in_the_shape_of_a_book_with_arms_of_Henri_II.jpg)

Nacionalinės saugumo agentūros centrinė būstinė, Fort Meade, Merilandas, JAV

(https://kids.kiddle.co/Image:National_Security_Agency_headquarters,_Fort_Meade,_Maryland.jpg)

MOKINIAMS

Kodas – tai simbolių, raidžių, žodžių ar signalų sistema, naudojama vietoj įprastų žodžių ir skaičių pranešimams siųsti ar informacijai saugoti. Kodas naudojamas siekiant, kad pranešimas būtų trumpas.

Šifrai yra slaptos bendravimo formos. Kodas pakeičia žodžius, frazes ar sakinius raidžių ar skaičių grupėmis, o šifras pertvarko raides arba naudoja kitus būdus, kad paslėptų pranešimą nuo nepageidaujamų asmenų.

Siunčiant įslaptintą pranešimą, jis užšifruojamas, o tokį pranešimą perskaitant, jis iššifruojamas.

Mokslas, tiriantis tokį slaptą bendravimą, vadinamas kriptografija.

Slaptas raštas atsirado su paties rašto sukūrimu. Istorijoje buvo naudojami šifrai, kai žmonės norėjo išsaugoti pranešimų slaptumą. Kriptografiją jau seniai taiko vyriausybės, kariuomenė, įmonės ir organizacijos, kad apsaugotų savo pranešimus. Šiandien šifravimas naudojamas duomenims ir sandoriams apsaugoti.

Senovėje, kai pranešimai buvo nešami pėsčiomis daugybę kilometrų, karaliai ir valdovai šifruodavo laiškus, kuriuos siųsdavo sąjungininkams. Tai padėdavo apsaugoti pranešimų slaptumą tuo atveju, jei jie būdavo perimami (atimami, pavagiami).

Šiandien žmonės šifruoja įvairius dokumentus, el. pašto žinutes, kad apsaugotų savo pranešimų slaptumą nuo pašalinių žmonių. Nauji šifravimo būdai yra labai sudėtingi, bet visada naudinga nagrinėti senovinius šifravimo metodus.

Šifravimo būdai

Žodžių rašymas atbulai

Tai pats paprasčiausias šifravimo būdas.

Pavyzdys

Antuano de Sent Egziuperi pasakos pavadinimas MAŽASIS PRINCAS užšifruotas, parašius kiekvieną žodį atbulai, skaitomas taip:

SISAŽAM SACNIRP

Jei pranešimo gavėjas žino „paslaptį“, kad šis užrašas parašytas atbulai, tai labai paprasta iššifruoti.

Užduotys

Perskaitykite žinutę

SITYKOM ADAKEIN ULĖVEN

Atsakymas

MOKYTIS NIEKADA NEVĖLU

Užšifruokite jums patinkančią frazę. Paprašykite klasės draugo perskaityti (iššifruoti) užšifruotą frazę.

Pusiau apversta abėcėlė

Standartinės lietuvių kalbos abėcėlę sudaro 32 raidės. (Svetimvardžiams užrašyti gali būti vartojamos likusios trys lotynų abėcėlės raidės: Q, W, X, taip pat ir raidės su diakritiniais ženklais.) Jos surašomos į dvi eilutes ir atitinkamos kiekvieno stulpelio raidės sukeičiamos.

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	Ų	Ū	V	Z	Ž

Pavyzdžiui, B raidė keičiama į M, R raidė – į E, Į – į V.

Pavyzdys

P	E	P	Ė		I	L	G	A	K	O	J	I	N	Ė
D	R	D	Š		Ū	Ą	U	K	A	Č	Ž	Ū	C	Š

Užduotys

Užšifruokite pusiau apverstos abėcėlės būdu Salomėjos Nėries eiliuotos pasakos „Eglė žalčių karalienė“ pavadinimą.

Padiskutuokite klasėje, kuris šifras – žodžių rašymo atbulai ar pusiau apverstos abėcėlės – yra sunkiau „nulaužiamas“. Jei norite užšifruoti savo slaptažodį, kurį būdą rinktumėtės? Kodėl?

Užšifruokite pusiau apverstos abėcėlės būdu savo šeimos narių vardus į lapelius. Namuose lapelius išdalinkite šeimos nariams ir paprašykite kiekvieno jų iššifruoti visus vardus. Kokiu būdu užšifravote iš karto nesakykite.

Stačiakampis šifras

Pirmiausia tekstas užrašomas vienodo ilgio eilutėmis, o užšifruojant atskirais žodžiais surašomi stulpeliai.

Pavyzdžiui, amerikiečių poeto Carlo Sandburgo frazę „Niekas nevyksta, kol neatsiranda svajonė“, galima užrašyti trimis eilutėmis.

N	I	E	K	A	S	N	E	V	Y	K	S
T	A	,	K	O	L	N	E	A	T	S	I
R	A	N	D	A	S	V	A	J	O	N	Ė

Perrašome frazę surašydami kaip atskirus žodžius stulpelius ir užšifruota frazė atrodo taip:

NTR IAA E,N KKD AOA SLS NNV EEA VAJ YTO KSN SIĖ

Galima surašyti ir 4 eilutėmis:

N	I	E	K	A	S	N	E	V
Y	K	S	T	A	,	K	O	L
N	E	A	T	S	I	R	A	N
D	A	S	V	A	J	O	N	Ė

Keturiomis eilutėmis užšifruota frazė atrodys taip:

NYND IKEA ESAS KTTV AASA S,IJ NKRO EOAN VLNĖ

Užduotys

Užšifruokite stačiakampiu šifru lietuvių liaudies patarlę „Genys margas, pasaulis – dar margesnis“ trimis eilutėmis.

Užšifruokite pasirinktą lietuvių liaudies patarlę ir paprašykite draugo ją iššifruoti.

Geležinkelio tvorelės šifras

Kartais šis šifras dar vadinamas zigzago šifru.

Pranešimo žodžiai rašomi ne vertikaliai, o įstrižai. Įstrižainės ilgis priklauso nuo pasirinkto būdo. Žodžiai atskiriami tarpais.

Pavyzdys

LIETUVOS SOSTINĖ VILNIUS

Užšifruokime, kai įstrižainė lygi dviem.

L		E		U		O				O		T		N				I		N		U	
	I		T		V		S		S		S		I		Ė		V		L		I		S

Užšifruotas tekstas: LEUO OTN INUITVSSSIĖVLIS

Tą patį tekstą užšifruokime, kai įstrižainė lygi 3:

L				U									T								N		
	I		T		V		S		S			S		I		Ė		V		L		I		S
		E				O				O					N				I				U	

Užšifruotas tekstas: LU T NITVSSSIĖVLISEOONIU

Tą patį tekstą užšifruokime, kai įstrižainė lygi 4:

L						O						T						I					
	I				V		S				S		I				V		L				S
		E		U						O				N						N		U	
			T						S						Ė						I		

Užšifruotas tekstas: LOTIIVSSIVLSEU ON NUTSĖI

Užduotis

Iššifruoti tekstą, kai įstrižainė lygi 3.

TĄA I AJIR RUĄPŽNINLIĖEKDGASEM

Atsakymas

Tikrą draugą pažinsi nelaimėje

T				Ą				A								I								A				J	
	I		R				R		U		Ą		P		Ž		N		I		N		L		I		Ė		E
		K				D				G				A				S				E				M			

Raidžių keitimas skaičiais

Surašome standartines lietuvių kalbos abėcėlės raides eilute, o po jomis iš eilės surašome skaičius.

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	Ų	Ū	V	Z	Ž
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

Kiekvieną teksto raidę keičiame atitinkamu skaičiumi. Pavyzdžiui, raidę A keičiame 1, raidę N – 20.

Pavyzdys

Užšifruokime frazę SUSITINKAME RYTOJ.

24 27 24 13 26 13 20 17 1 19 7 23 15 26 21 16

Užduotys

Užšifruokite tekstą MOKYKLOS SPORTO ŠVENTĖ

Atlikite veiksmus ir naudodami raidžių pakeitimo skaičiais iššifravimą, užrašykite užšifruotus žodžius.

10 + 14	1	21 + 6	6 + 12	4 + 5

Atsakymas SAULĖ

30 – 11	12 – 3	25 – 5	30 – 3	25 – 7	15 – 2	25 – 1

Atsakymas MĖNULIS

4 × 8	21 : 3	38 : 2	3 × 3

Atsakymas ŽEMĖ

Tinklelio šifras

Nubraižome tinklelį iš 5 eilučių ir 9 stulpelių. Pirmoji eilutė yra antraštinė, joje surašome skaičius nuo 1 iki 8.

Pirmajame stulpelyje surašome raides A, B, C ir D. Į likusius tinklelio langelius surašome standartines lietuviškos abėcėlės raides. Teksto raides užšifruojame parašydami raidės eilutės raidę ir stulpelio skaičių. Pavyzdžiui, raidė P bus užšifruojama C6, o raidė T – D2.

	1	2	3	4	5	6	7	8
A	A	Ą	B	C	Č	D	E	Ę
B	Ė	F	G	H	I	Į	Y	J
C	K	L	M	N	O	P	R	S
D	Š	T	U	Ų	Ū	V	Z	Ž

Pavyzdys

Užšifruotas Maironio poezijos knygos pavadinimas PAVASARIO BALSAI:

C6A1D6A1C8A1C7B5C5 A3A1C2A1B5

Užduotys

Naudodami tinklelio šifrą iššifruokite šį poemos pavadinimą:

A1C4B7C1D1A5B5D4 D1B5C2A7C2B5C8

Atsakymas ANYKŠČIŲ ŠILELIS

Naudodami tinklelio šifrą užšifruokite patarlę
MOKSLO ŠAKNYS KARČIOS, BET VAISIAI SALDŪS.

Cezario šriftas

Cezario šifras yra vienas iš seniausių šifrų ir atsirado gerokai anksčiau, nei jis buvo taip pavadintas. Romos imperatorius Julijus Cezaris naudojo šį šifrą paslinkdamas kiekvieną raidę per 3 raides, taip užšifruodamas karinius pranešimus savo vadams. Nužudžius Cezarį jo sūnėnas Augustas toliau naudojo dėdės šifrą savo korespondencijai apsaugoti. Nepaisant to, kad egzistavo sudėtingesnių kodų, valdovai greičiausiai pirmenybę teikė šiam šifrui dėl jo paprastumo.

Tradiciškai su Cezario šifru siejamas kiekvienos raidės pakeitimas nutolusia nuo jos abėcėlėje trečiąja raide, einant per abėcėlę apskritimu.

Pavyzdžiui, jei naudojama lietuviška abėcėlė

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 Ų Ū V Z Ž

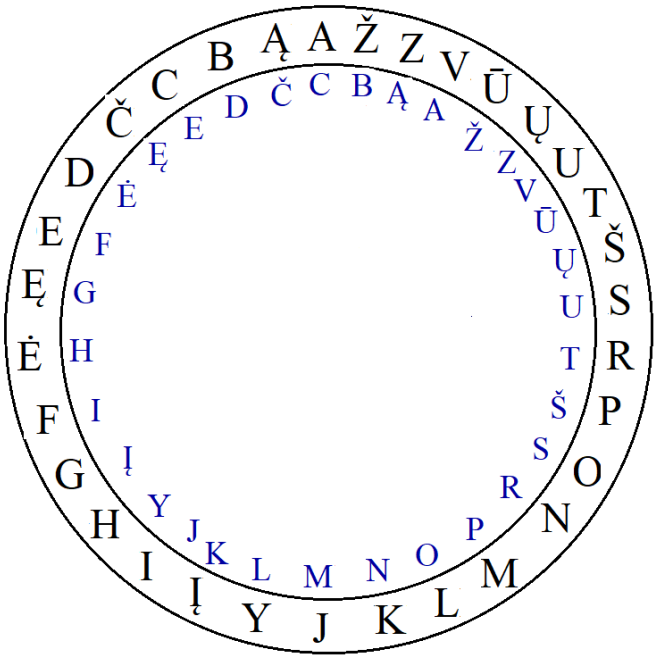
ir raktas yra 3, tai raidė A tampa C, Ą tampa Č ir t. t., o raidė Ž tampa B.

Žodis ŠIFRAS užšifruojamas taip: ŲJITCU.

Galima Cezario šifrui naudoti paprastą lentelę, kurioje raidės pakeičiamos trečiąja raide. Galima naudoti ir kitokį raidžių keitimą.

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	Ų	Ū	V	Z	Ž
C	Č	D	E	Ę	Ė	F	G	H	I	Į	Y	J	K	L	M	N	O	P	R	S	Š	T	U	Ų	Ū	V	Z	Ž	A	Ą	B

Dažnai Cezario šriftas vaizduojamas raidžių ratais, o šifruotas pranešimas rašomas keičiant raides tokiomis raidėmis, kurios yra nutolusios per tris pozicijas nuo kiekvienos nešifruoto pranešimo raidės. Vidiniame rate tos raidės jau yra pasuktos.

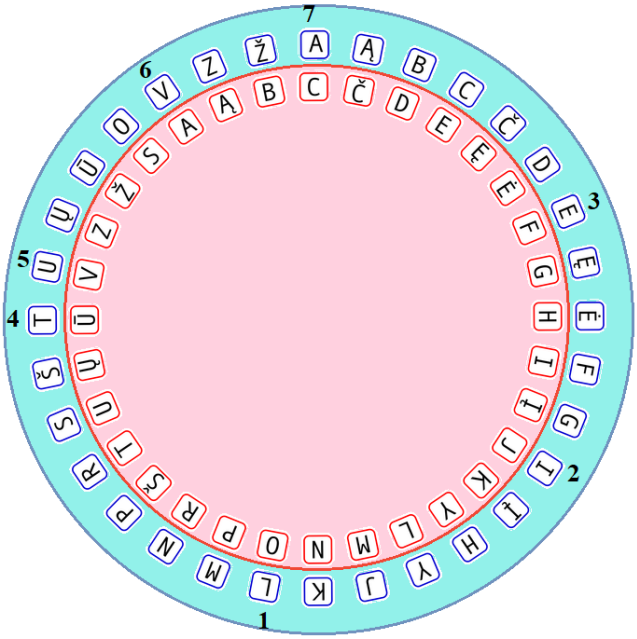


Jei bent vienas ratas gali sukiotis apie centre esančią ašį, galima prikurti įvairių šifrų, paslenkant norimą skaičių raidžių.

Pavyzdys

Užšifruoti žodį LIETUVA, kai raidės paslenkamos per tris raides.

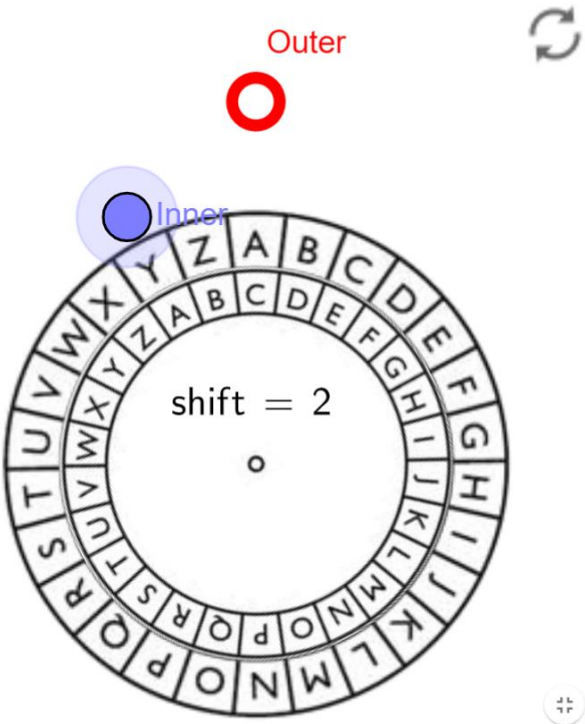
Skaičiais pažymėta kiekviena žodžio LIETUVA raidė. Matome, kad užšifruotas žodis LIETUVA atrodo taip: OJFŪVAC



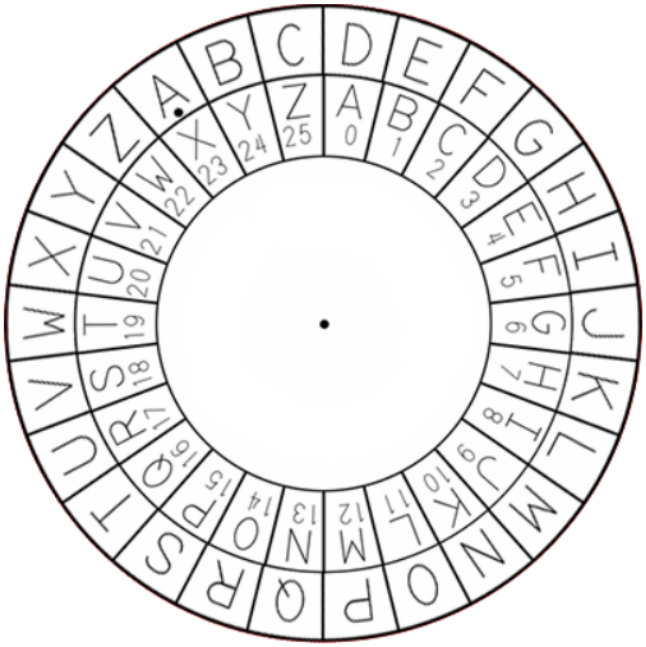
Interaktyvūs pavyzdžiai

Panagrinėkime Cezario šifrą, kai naudojamos 26 angliškos abėcėlės raidės:

Atvėrę nuorodą https://www.geogebra.org/m/SRdYhZ2J , galime sukti vidinį (pele sukamas mėlynas skrituliukas) ar išorinį ratą (pele sukamas raudonas žiedas). Pasirinkus norimą raidžių keitimą, galima užšifruoti įvairias frazes. Žaisdami su draugais turite nepamiršti, per kiek raidžių buvo pasuktas ratas.



Atvėrę šią nuorodą http://inventwithpython.com/cipherwheel/ , galite sukti tik išorinį ratą. Tačiau čia yra galimybė matyti ir horizontaliai išdėstytas atitinkamas raides.



D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

Užduotys

Panagrinėkite šią Cezario šrifto lentelę.

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	Ų	Ū	V	Z	Ž
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	Ų	Ū	V	Z	Ž	A	Ą

ĄŽBYIĄĘG – koks žodis užšifruotas, remiantis pateikta šifravimo lentele?

Atsakymas: ŽVAIGŽDĖ

Kaip sudaryta Cezario šrifto lentelė, jei užšifravus žodį MOKYKLA jis užrašytas taip: RŠOMOPČ

Atsakymas

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	Ų	Ū	V	Z	Ž
Č	D	E	Ę	Ė	F	G	H	I	Į	Y	J	K	L	M	N	O	P	R	S	Š	T	U	Ų	Ū	V	Z	Ž	A	Ą	B	C

Šaltiniai

1. Stakėnas, V. Kodai ir šifrai, 2006, http://www.statistika.mif.vu.lt/wp-content/uploads/2014/08/kodai_sifrai_Stakenas.pdf (2022-07-05).
2. Stakėnas, V. Kriptografija: menas, pavirtęs mokslu. Alfa ir omega, 2003, 1, p. 20-33. http://web.vu.lt/mif/v.stakenas/a+o/2003-1/2003-1-20-33.pdf (2022-07-05)

Žemiau pateiktuose šaltiniuose šifruojama naudojantis anglų kalbos abėcėle.

3. Šifravimo pavyzdžiai. Secret Codes for Cubs and Scouts. https://sites.google.com/site/codesforscouts/welcome, 2022-06-16
4. Kriptologija vaikams. Cryptology for Kids. https://www.cerias.purdue.edu/education/k-12/teaching_resources/lessons_presentations/cryptology.html, 2022-06-16
5. Kriptografijos faktai vaikams. Cryptography facts for kids. https://kids.kiddle.co/Cryptography, 2022-06-16