Vilniaus universitetas

Metodinė medžiaga
Informacijos šifravimas

Mokyklos pedagogika

Metodinė medžiaga. Informacijos šifravimas

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“, skirta Mokyklos pedagogikos studijų programos moduliui „Informatikos didaktika". Tikslinė grupė – būsimi informatikos mokytojai. Šifravimas – tai informacijos kodavimas su tikslu tą informaciją įslaptinti. Šifravimas susijęs su informacijos užšifravimu ir iššifravimu. Priemonėje nagrinėjami populiarūs kvadratų, Cezario, Viženero, geležinkelio tvorelės šifrai; viešojo rakto kriptosistemos. Apibūdinamos kriptosistemos ir Duomenų šifravimo standartas. Nagrinėjami pavyzdžiai, užduotys pateikiamos su nurodymais ir sprendimais. Pateikiamas pagrindinių šaltinių sąrašas.

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

Redagavo: Viktoras Dagys

Iliustravo: Alvida Lozdienė

Projekto vykdytojas: Vilniaus universitetas.

2022, Vilnius

INFORMACIJOS ŠIFRAVIMAS

Žmonėms nuolat kyla poreikis apsaugoti svarbią informaciją: karo metu, kuriant naujas technologijas, produktus, meno kūrinius, saugant asmens tapatybę, saugant valstybines paslaptis ir daugybe kitų atvejų.

Dažnai informacijos kodavimas (atvirkščias veiksmas – dekodavimas) ir informacijos užšifravimas (atvirkščias veiksmas – iššifravimas) laikomi sinonimais.

Tačiau šifravimas nuo kodavimo truputį skiriasi.

Kodavimas – tai :

- informacijos apdorojimas, laikymas ir slėpimas naudojant sutartinių ženklų sistemą;
- atskiro objekto ar jo savybės žymėjimas skaičiumi arba tam tikros abėcėlės ženklais;
- programos užrašymas kompiuterine kalba, naudojant sutartų ženklų sistemą.

Šifravimas – tai informacijos kodavimas su tikslu tą informaciją įslaptinti. Šifravimas susijęs su informacijos užšifravimu ir iššifravimu.

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

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

Užšifruota informacija gali būti iššifruojama tik žinant raktą. Raktas – tai priemonė užšifruotiems duomenims iššifruoti.

Jeigu reikia duomenis kitaip pavaizduoti neturint tikslo jų užslaptinti, tai tikslingiau vartoti kodavimo sąvoką.

Nors ir kodavimas, ir šifravimas yra metodai, kurie transformuoja duomenis į skirtingus formatus, tikslai, kurių jais siekiama, yra skirtingi. Kodavimas atliekamas siekiant padidinti duomenų tinkamumą naudoti skirtingose sistemose ir sumažinti saugojimui reikalingą vietą, o šifravimas atliekamas siekiant išlaikyti duomenų paslaptį nuo trečiųjų šalių. Kodavimas atliekamas naudojant viešai prieinamus metodus ir jį galima lengvai pakeisti. Tačiau užšifruotų duomenų negalima lengvai iššifruoti. Tam reikia turėti specialią informaciją, vadinamą raktu.

Su šifravimu susijęs ir nuo praeito amžiaus labai sparčiai besivystantis mokslas vadinamas kriptologija. Kriptologija susideda iš kriptografijos ir kriptoanalizės.

Žodis kriptografija kilo iš dviejų graikiškų žodžių, reiškiančių „slaptas raštas“.

Kriptografija – tai mokslas, nagrinėjantis informacijos užšifravimo ir iššifravimo metodus. Kriptoanalizė – mokslas apie tai, kaip įveikti užšifruotus tekstus. Pagrindinis kriptografijos elementas yra kriptografinė sistema (kriptosistema) arba šifras.

Šiuolaikinė kriptografija – tai mokslo šaka, sprendžianti elektroninės informacijos saugos problemas. Kadangi kasmet vis daugiau informacijos siunčiama skaitmeninėmis ryšio priemonėmis, labai svarbu užtikrinti jos saugumą, nes skaitmeninė informacija dažniausiai perduodama nesaugiais kanalais, pavyzdžiui, interneto ryšiu, ir gali būti pasiekiama beveik visiems.

Užduotis. Diskusija

Pažvelkite į šias nuotraukas:

https://de.wikipedia.org/wiki/Kryptologen-Denkmal#/media/Datei:Polish_cryptologists_breaking_Enigma_ciphers_monument_01.jpg

https://en.wikipedia.org/wiki/Alan_Turing#/media/File:Turing-statue-Bletchley_14.jpg

Padiskutuokite, ką bendro turi šios dvi nuotraukos. Prieš diskusiją paieškokite populiarios informacijos apie informacijos šifravimą.

Užuomina. Pirmosios nuotraukos centre esantis objektas yra Poznanėje (Lenkija), o antrojoje – Milton Keinse (Didžioji Britanija).

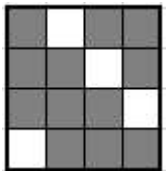
Kvadratų šifras

Norime saugiai perduoti pranešimą „SUSITINKAME RYTOJ“. Šis pranešimas sudarytas iš 16 raidžių.

Pranešimo užšifravimui pasirenkame 16 langelių kvadratą ir jame iškerpame 4 langelius.

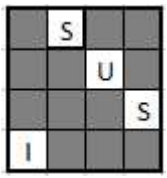
Žinoma, langeliai iškerpami specialiu būdu, kuris tuojau paaiškės.

Tarkime, kad pasirinkome tokį būdą:

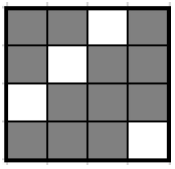


Specialiai parengtas 16 langelių kvadratas, kurio 4 balti langeliai yra kiauri.

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:

	S	T	A
M	I	U	
N	E		S
I		R	K

. Po trečio posūkio

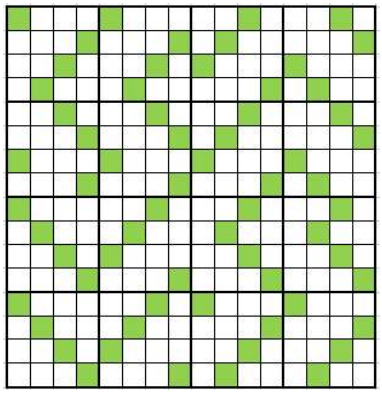
Y	S	T	A
M	I	U	T
N	E	O	S
I	J	R	K

bus užšifruotas visas pranešimas:

Siunčiamas toks pranešimo tekstas „YSTAMIUTNEOSIJRK“.

Gavėjas privalo turėti identišką kvadratą, kad galėtų iššifruoti tekstą.

Jei pranešimas yra ilgesnis, galima naudoti ir didesnį kvadratą. Kiekviename $4n^2$ langelių kvadrate galima išpjauti n^2 langelių, kad tris kartus pasukus 90 laipsnių kampu prieš laikrodžio rodyklę (arba kaip yra sutarta) galima būtų įrašyti pranešimą į visus mažus $4n^2$ langelius.



Paveiksle pavaizduotas $4 \times 8^2 = 256$ langelių kvadratas, jame žalia spalva pažymėti 64 langeliai, kurie turi būti kiauri. Tokį kvadratą su sutarta posūkio taisykle turi pranešimo siuntėjas ir gavėjas.

Užduotis

Parenkite kvadratų šifro 4 × 4 žaidimą mokiniams, sugalvokite kelis pranešimus, kurie nebūtų ilgesni nei 16 simbolių.

Cezario šifras

Cezario šifras yra gerai žinoma kriptosistema, kurią naudojant raidės pasislenka per kelias pozicijas abėcėlėje. Per kiek perstumti raides nustato šifro raktas. Tradiciškai su Cezario šifru siejamas kiekvienos raidės pakeitimas nutolusia nuo jos abėcėlėje trečiąja raide, einant per abėcėlę apskritimu.

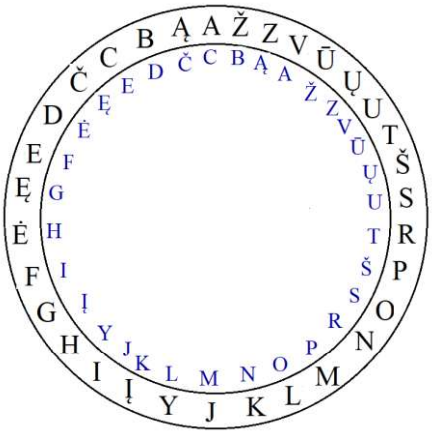
Pavyzdžiui, jei naudojama lietuviška abėcėlė

AĄBCČDEĘĖFGHIĮYJKLMNOPRSŠTUŲŪVZŽ

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

Žodis „ŠIFRAS“ užšifruojamas kaip „ĮJITCU“.

Dažnai Cezario šriftas vaizduojamas koncentriniais raidžių ratais, šifruotas pranešimas rašomas keičiant raides tokiomis raidėmis, kurios per tris pozicijas yra nutolusios. Vidiniame rate tos raidės jau yra pasuktos. Jei tokie ratai yra pagaminti ir vidinis ratas gali sukiotis, tai nebūtina naudoti šifro raktą lygų trims raidėms. Galima naudoti ir kitus raidžių poslinkius arba net kelis poslinkius.



Užduotys

1. Parinkite aforizmų ir juos užšifruokite naudodami įvairias Cezario raktų vertes.
2. Išsiaiškinkite, kodėl šis šifras pavadintas Gajaus Julijaus Cezario (100–44 pr. m. e) vardu.

Viženero šifras

Viženero šifrui (pranc. *Chiffre de Vigenère*) raktu naudojame pasirinktą žodį. Tarkime, kad raktas yra žodis KODAS ir norime užšifruoti žodį (pranešimą) AUTOSTEREOGRAMA (autostereograma – kompiuterio sukurtas paveikslas, kuris iš pirmo žvilgsnio atrodo abstraktaus dizaino, tačiau įsižiūrėjus jame išryškėja erdvinės figūros).

K	O	D	A	S	K	O	D	A	S	K	O	D	A	S
A	U	T	O	S	T	E	R	E	O	G	R	A	M	A

Kiekvieną rakto raidę naudojame kaip Cezario šifro poslinkį ir užšifruojame kiekvieną pranešimo raidę. Norėdami užšifruoti raidę A užšifruojame rakto raide K (poslinkis 16) ir gauname K (0 + 16). Tada toliau U raidei imama kodo O raidė, ji yra 20, todėl (26 + 20) mod 32 = 14 ir bus Y raidė.

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
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	26	27	28	29	30	31

Gaunamas kodas: K Y Z O Y F U Ų E H U G D M S.

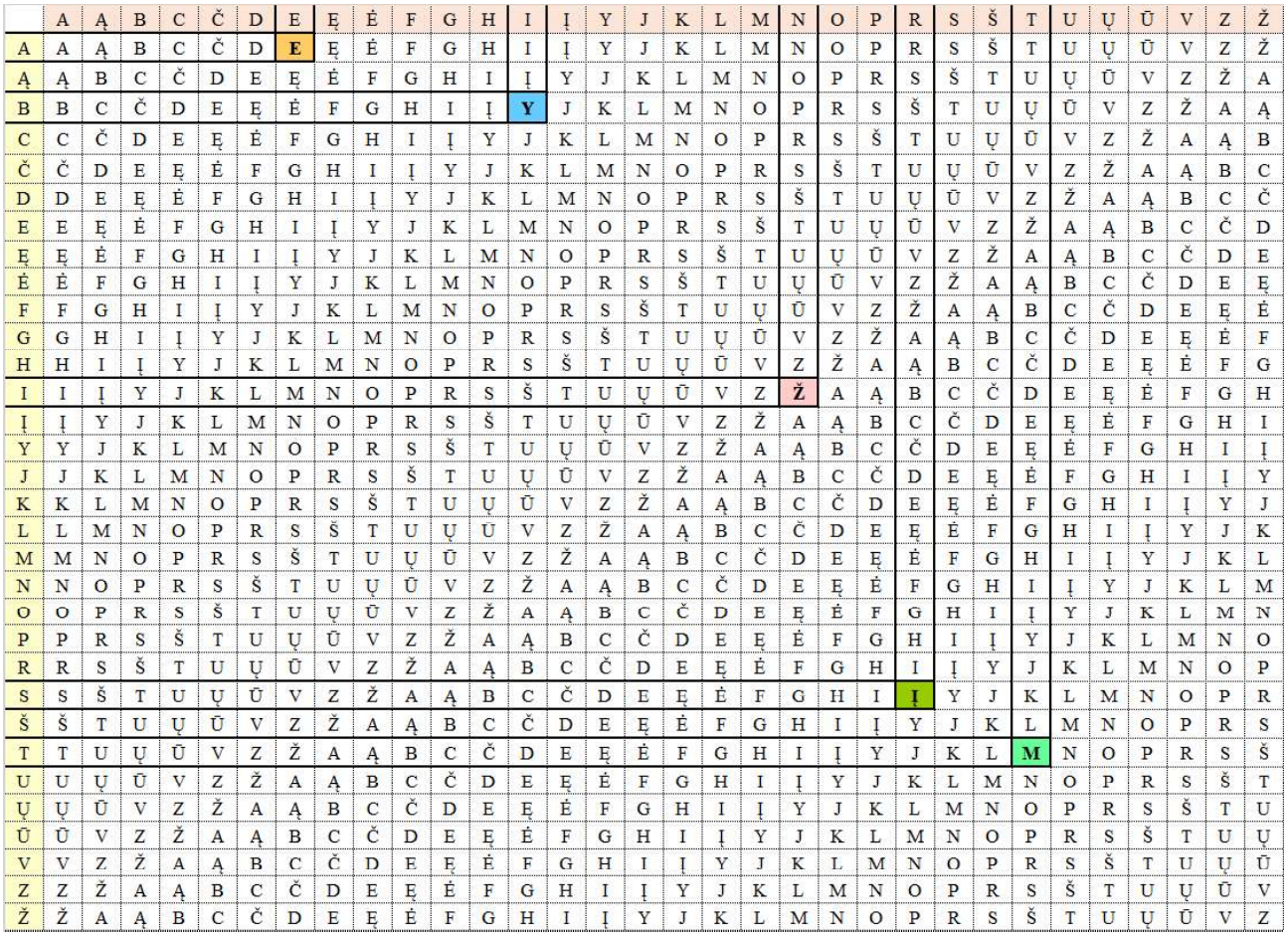
K	O	D	A	S	K	O	D	A	S	K	O	D	A	S
A	U	T	O	S	T	E	R	E	O	G	R	A	M	A
K	Y	Z	O	Y	F	U	Ų	E	H	U	G	D	M	S

Užšifravimui ir iššifravimui naudojamos abėcėlės lentelės, vadinamos *tabula recta* arba Viženero kvadratais (lentelėmis). Lietuviškos abėcėlės Viženero lentelę sudaro eilutės po 32 simbolius, o kiekviena eilutė pasislenka keliomis pozicijomis. Lentelėje pateikiami 32 skirtingi Cezario šifrai.

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

Kiekviename šifravimo etape naudojamos abėcėlės eilutės, pasirenkamos atsižvelgiant į raktinio žodžio raidę. Pavyzdžiui, tarkime, kad pirminis pranešimas yra INTERNETAS, o raktas BITAS.

Pirmoji raidė I užšifruojama rakto raide B. Rakto raidė B yra eilutėje B, kuriai susikirtus su I raidės stulpeliu gaunama Y raidė. Pranešimo N raidės stulpelis susikerta su eilute I ir gauname Ž raidę. Toliau T ir T susikerta ties raide M, E ir A – E, R ir S – Į, ir vel iš pradžių naudojama rakto pirma raidė B.



Užšifravus tokiu būdu visą žodį, jis atrodys taip:

B	I	T	A	S	B	I	T	A	S
I	N	T	E	R	N	E	T	A	S
Y	Ž	M	E	Į	P	M	M	A	Y

Ta pati Viženero lentelė naudojama ir iššifravimui. Jei norime tekstą iššifruoti, žiūrime į atitinkamą eilutę, kurioje yra kiekviena pasikartojančio rakto raidė, ir joje ieškome užšifruotos raidės. Rasta pirmoji stulpelio raidė yra iššifruota raidė.

Pavyzdžiui, raktas yra BETA, o gautas užšifruotas žodis BTĮNYŠTA.

Rakto pirmos raidės B eilutėje randame B raidę, jos stulpelio viršutinė raidė ir yra pirminio pranešimo raidė A. Toliau E eilutėje ieškome T ir stulpelio viršutinė raidė yra N, toliau T eilutėje randame Į, jos stulpelio viršutinė raidė O, ir toliau surandame likusias pirminio pranešimo raides. Tai ANONIMAS.

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

B	E	T	A	B	E	T	A
B	L	Į	N	Y	Š	T	S
A	N	O	N	I	M	A	S

Suprantama, kad Viženero raktas bus sunkiai surandamas, jei tai nebus prasmingas žodis. Čia buvo pateikti pavyzdžiai tik šio šifro greitesniam suvokimui. Šifruojant ilgesnius tekstus raktai naudojami irgi ilgi. Ilgiems raktams nereikia naudoti žinomų frazių, kurios lengvai nuspėjamos.

Užduotis

Pradinis pranešimas: S A U G U S I S E L E K T R O N I N I S P A R A Š A S

Užšifruotas pranešimas: R A H O E Į Š Y D L S U D I A G H N V Ą Ą R B S S A Ė

Pasinaudoję Viženero lentele surastkite raktą.

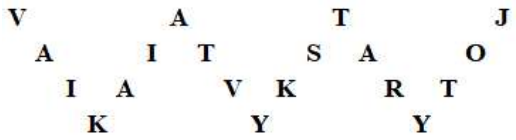
Atsakymas

ŽALGIRIS

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.



Skaitydami užšifruotą pranešimą eilutėmis, gauname „VATJAITSAOIAVKRTKYY“.

Tokiu 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“.

Užduotis

Pasinaudodami geležinkelio tvorelės šifru ir keliais jo raktais užšifruokite jums patinkantį trumpą aforizmą.

Viešojo rakto kriptosistemos

1976 metais Diffie ir Hellman pasiūlė naujo tipo kriptografiją, kurioje šifravimo ir dešifravimo raktai yra skirtingi. Vienas raktas yra viešai žinomas, kitas – saugomas slaptai.

Klasikinėje kriptografijoje siuntėjas ir gavėjas turi bendrą raktą. Viešojo rakto kriptografijoje – ne. Jei šifravimo raktas yra viešas, norint nusiųsti slaptą žinutę, tiesiog reikia užšifruoti ją su gavėjo viešuoju raktu. Gavėjas gali ją dešifruoti naudodamas savo privatųjį raktą.

RSA šifras

RSA (Rivest–Shamir–Adleman abreviatūra) – viešojo rakto kriptosistema, kurios algoritmą 1977 metais sukūrė Ronald Rivest, Adi Shamir ir Leonard Adleman.

RSA metodu šifruojami skaičiai, o ne tekstas. RSA yra kėlimo laipsniu šifras.

RSA metodo etapai:

1) pasirenkami du pakankamai dideli pirminiai skaičius p ir q;

2) skaičiuojamos tokios sandaugas: $n = p \times q$ ir $k = (p - 1) \times (q - 1)$;

3) pasirenkamas viešasis raktas (angl. *public key*) e, kuris neturi jokio bendro daugiklio, išskyrus 1 su skaičiumi k;

4) randamas toks privatusis raktas d (private key), kad $(d \times e) \bmod k = 1$. Šis raktas laikomas paslaptyje;

5) jei pasirenkame skaičių m, kurį norime užšifruoti, tai atliekamas toks veiksmas: skaičius keliamas k-uoju laipsniu ir skaičiuojama gauto skaičiaus liekana, kuri gaunama, tą skaičių operacija mod dalijant iš n: $c = m^e \bmod n$;

6) norint užšifruotą skaičių c iššifruoti, skaičius c keliamas laipsniu d ir liekana, gauta dalijant c^d iš n yra skaičius m: $c^d \bmod n = m$.

Pavyzdys

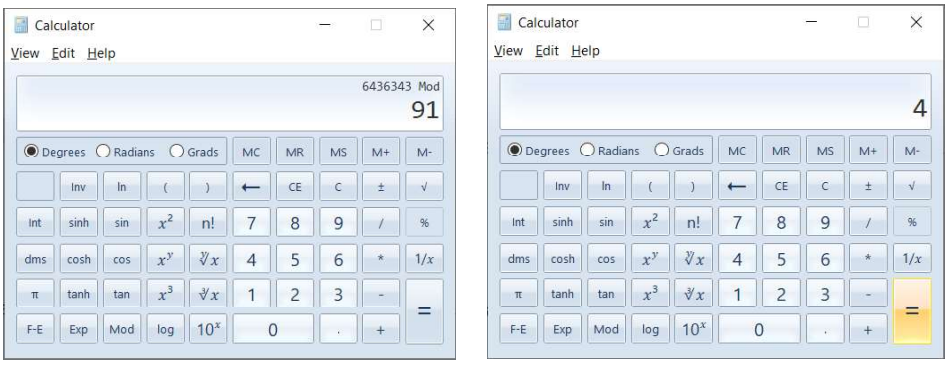
1) pasirenkame pirminius skaičius $p = 7$ ir $q = 13$. (Tikri RSA pirminiai skaičiai turi būti bent 512 bitų ilgio, taip gaunant bent 1024 bitų ilgio n);

2) randame sandaugas: $n = p \times q = 7 \times 13 = 91$ ir $k = (p - 1) \times (q - 1) = (7 - 1) \times (13 - 1) = 72$;

3) pasirenkame viešąjį raktą $e = 5$, kuris neturi jokio bendro daugiklio, išskyrus 1, su skaičiumi $k = 72$;

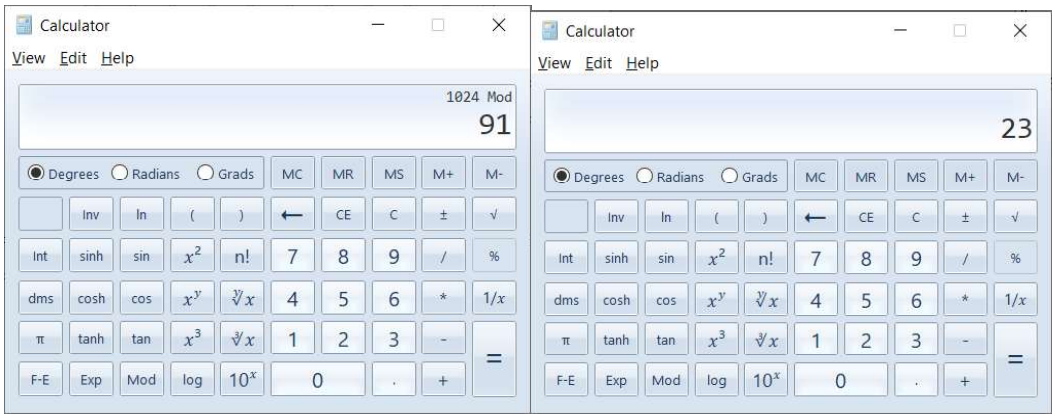
4) randame privatųjį raktą $d = 29$, kad $(d \times e) \bmod k = (29 \times 5) \bmod 72 = 145 \bmod 72 = 1$;

5) pasirenkame skaičių m = 23, kurį norime užšifruoti. Pasirinktą skaičių 23 dalijame operacija mod iš n: $c = m^e \bmod n = 23^5 \bmod 91$. Veiksmus atliekame pasinaudodami skaičiuotuvu: 6436343 mod 91 = 4.



Skaičių 23 užšifravome ir gavome 4.

6) iššifruokime skaičių c = 4 . Skaičius c = 4 keliamas laipsniu d = 5 ir liekana, gauta dalijant 4^5 iš 91 yra skaičius m = 23: $c^d \bmod n = 4^5 \bmod 91 = 1024 \bmod 91 = 23$.



Užduotis

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 užšfravote, jį iššifruodami.

Atsakymas

2

Teksto šifravimo RSA šifru pavyzdys

Lietuviškos abėcėlės raides pavaizduokime skaičiais, o tarpą skaičiumi 32:

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
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

Tarkime, kad $p = 7$, $q = 11$. Tada $n = 77$ ir $k = (7 - 1)(11 - 1) = 60$. Viešais raktas tegul bus $e = 17$, o privatų raktą galime apskaičiuoti, kad ir „Excel“ programa:

d	17d	17d mod 60
3	51	51
13	221	41
23	391	31
33	561	21
43	731	11
53	901	1
63	1071	51
73	1241	41
83	1411	31
93	1581	21
103	1751	11
113	1921	1
123	2091	51
133	2261	41
143	2431	31

Atlikus kelis skaičiavimus matome du tinkamus rezultatus. Kad būtų paprasčiau, pasirenkame mažesnį tinkamą raktą $d = 53$.

Siuntėjas siunčia tokį pranešimą: TEISINGUMO LENTELĖ

T	E	I	S	I	N	G	U	M	O		L	E	N	T	E	L	Ė
25	06	12	23	12	19	10	26	18	20	32	17	06	19	25	06	17	08

Panaudojus viešąjį raktą $e = 17$ kiekvienam raidės numeriui $c = m^{17} \bmod 77$, gaunamas toks užšifruotas tekstas: 09 41 45 67 45 24 54 38 72 48 65 19 41 24 09 41 19 57

T	E	I	S	I	N	G	U	M	O		L	E	N	T	E	L	Ė
25	06	12	23	12	19	10	26	18	20	32	17	06	19	25	06	17	08
09	41	45	67	45	24	54	38	72	48	65	19	41	24	09	41	19	57

Jei gavėjo privatus raktas $d = 53$, tai jis gautą užšifruotą pranešimą iššifruos taip: $m = c^{53} \bmod 77$

09	41	45	67	45	24	54	38	72	48	65	19	41	24	09	41	19	57
25	06	12	23	12	19	10	26	18	20	32	17	06	19	25	06	17	08
T	E	I	S	I	N	G	U	M	O		L	E	N	T	E	L	Ė

Jei norima patvirtinti ir slaptumą, ir autentiškumą, reikia užšifruoti naudojant siuntėjo privatųjį raktą ir gavėjo viešąjį raktą.

Tegul siuntėjo viešasis raktas yra 17, o privatus – 53. Gavėjo viešasis raktas yra 37, o privatus – 13.

Raidės T skaičius yra 25, todėl siuntėjas T raidę užšifruoja taip: $(25^{53} \bmod 77)^{37} \bmod 77 = 58$.

Gavėjas naudoja savo privatųjį raktą 13, kad iššifruotų pranešimą, ir siuntėjo viešąjį raktą 17, kad įsitikintų jo autentiškumu: $(58^{13} \bmod 77)^{17} \bmod 77 = 25$.

Vienkartinio rakto šifras

Vienkartinio rakto šifras (angl. *one-time pad*) yra šifras, kai prie atvirojo pranešimo bitų sekos panariui moduliu 2 pridedama rakto seka. Pavyzdžiui, jei pranešimas yra 00101, o raktas yra 10010, tai šifruotas tekstas yra $0 \oplus 1 \,||\, 0 \oplus 0 \,||\, 1 \oplus 0 \,||\, 0 \oplus 1 \,||\, 1 \oplus 0$, t. y. 10111, čia $\oplus$ yra suma moduliu 2 (loginė XOR operacija), o $||$ yra sąjunga (angl. *concatenation*). Rakto simbolių seka parenkama atsitiktinai, ir jos ilgis yra ne trumpesnis už pranešimo ilgį, todėl ji nesikartoja. Galima įrodyti, kad šio šifro neįmanoma įveikti.

Primename, kad loginės funkcijos XOR pavadinimas neturi trumpo lietuviško atitikmens. Lietuviškai ši funkcija vadinama taip: suma moduliu 2 arba loginis nelygiavertiškumas. Tai dviejų kintamųjų loginė funkcija, jos reikšmė lygi 1, jei tik vienas kintamasis lygus 1. Loginė operacija žymima simboliu $\oplus$.

Loginės operacijos XOR rezultatus galime užrašyti:

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

Išsamesnis kriptosistemų apibūdinimas

Kriptosistema yra rinkinys (E, D, M, K, C), čia M yra *atviruųjų (nešifruotų) pranešimų*)angl. *plaintext*) aibė, K yra *raktų* (angl. *key*) aibė, C yra *užšifruotų pranešimų*, (angl. *ciphertext*) aibė, E yra $M \times K \to C$ *užšifravimo funkcijų* (angl. *enciphering functions*) aibė ir D yra $C \times K \to M$ *iššifravimo funkcijų* (angl. *deciphering functions*) aibė.

Cezario šifras yra **kriptosistema**, kurią naudojant raidės perstumiamos per kelias pozicijas abėcėlėje. Per kiek pozicijų perstumti raides, nustato šifro raktas. Cezario šifras yra

kriptosistema (E, D, M, K, C), kurioje M = {visos lietuviškos abėcėlės raidės}; K = {i | i — sveikasis skaičius, $0 \le i \le 31$}; E = {E_k | $k \in K$ ir kiekvienam $m \in M$, $E_k(m) = (m + k) \bmod 32$}.

Jei kiekvienai raidei priskirtume jos eilės numerį abėcėlėje (pradedant nuo A, kurios eilės numeris bus 0), gautume, kad pranešimą CEZARIS atitinka seka 4, 7, 31, 1, 23, 13, 24. Jei k = 3, šifruoto pranešimo seka bus 7, 10, 2 (nes (31 + 3) mod 32 = 2), 4, 26, 16, 27 arba EFĄCTJU.

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
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

D = {D_k | $k \in K$ ir kiekvienam $c \in C$, $D_k(c) = (c - k) \bmod 32$} (kiekvienas D_k yra tiesiog atitinkamo E_k atvirkštinė funkcija);

C = M

Užduotis

Kokia bus iššifruoto pranešimo raidžių seka, kai užšifruotas pranešimas yra toks:

20, 26, 16, 25, 29, 24, 21, 24, 14, 16, 4, kai k = 3?

Atsakymas

KRIPTOLOGIJA

17, 23, 13, 22, 26, 21, 18, 21, 11, 13, 16, 1

Kriptografijos tikslas – išlaikyti užšifruotą informaciją paslaptyje. Tarkime, *priešininkas* (angl. *adversary*) nori iššifruoti užšifruotą tekstą. Kriptografijoje paprastai daroma prielaida, kad jis žino naudotą šifravimo algoritmą, bet nežino rakto (kitaip tariant, jis žino D ir E). Jis gali naudotis trijų tipų atakomis:

1. *Pavienio šifruoto teksto* (angl. *ciphertext only*) ataka: priešininkas turi tik užšifruotą tekstą. Jo tikslas – rasti atitinkamą atvirąjį tekstą. Jei įmanoma, jis gali pabandyti rasti ir raktą.

2. *Žinomo atvirojo teksto* (angl. *known plaintext*) ataka: priešininkas turi užšifruotą tekstą ir atitinkamą atvirąjį tekstą. Jo tikslas – rasti raktą, kuris buvo panaudotas šifruojant.

3. *Pasirinkto atvirojo teksto* (angl. *chosen plaintext*) ataka: priešininkas turi galimybę paprašyti užšifruoti bet kuriuos pasirinktus atviruosius tekstus. Jis gauna užšifruotus tekstus. Jo tikslas – rasti raktą, kuris buvo panaudotas šifruojant.

Gera kriptografinė sistema apsaugo nuo visų trijų tipų atakų.

Klasikinės kriptosistemos

Klasikinės kriptosistemos (dar vadinamos *slaptojo rakto*, arba *simetrinėmis*) yra tos, kurios naudoja tą patį raktą šifravimui ir dešifravimui. Joms galioja tokia savybė: visiems $E_k \in E$ ir $k \in K$ egzistuoja toks $D_k \in D$, kad $D_k = E_k^{-1}$

Jei Cezario šifro raktas 3, tai šifravimo funkcija yra E_3. Kad dešifruotume pranešimą, naudojome tą patį raktą su dešifravimo funkcija D_3. Cezario šifras yra klasikinė kriptosistema.

Yra du pagrindiniai klasikinių kriptosistemų tipai: *perstatų* šifras ir *keitinių* šifras.

Perstatų šifras (angl. *transposition cipher*) užšifruoja tekstą, sukeisdamas atvirojo teksto simbolius vietomis, patys simboliai nesikeičia. Tai jau aptartas geležinkelio tvorelių šifras.

Keitinių šifras (angl. *substitution cipher*) šifruoja pakeisdamas atvirojo teksto simbolius.

Cezario šifras naudojo raktą 3, kiekvieną atvirojo teksto raidę pakeisdamas raide, stovinčia abėcėlėje trimis pozicijomis toliau (jei reikia, cikliškai grįžtant į abėcėlės pradžią). Tai keitinių šifras.

Duomenų šifravimo standartas

Duomenų šifravimo standartas (angl. *Data Encryption Standard*, DES) buvo sukurtas šifruoti slaptus, bet nesusistemintus duomenis, kurie išreikšti bitais. Jis derina perstatas su keitiniais ir dėl to kartais vadinamas *sandaugos šifru* (angl. *product cipher*). Jo įvesties (angl. *input*), išvesties (angl. *output*) ir rakto ilgiai yra 64 bitai. 64 bitų sekos vadinamos *blokais*.

Šifrą sudaro 16 *ratų* (iteracijų arba ciklų; angl. *round*). Kiekviename rate naudojamas atskiras 48 bitų raktas. Tie *ratų raktai* sudaromi iš rakto bloko atmetus lyginumo bitus (taip sumažiname rakto dydį iki 56 bitų), perstatant bitus ir išrenkant 48 bitus. Vis kita 48 bitų seka išrenkama kiekviename iš 16 ratų. Jei ratų raktai naudojami atvirkščia tvarka, tai įvestis yra dešifruojama.

(Lyginumo bitas – bitas, papildantis baitą, kompiuterio žodį ar kitokią duomenų porciją taip, kad visų bitų, lygių vienetui, skaičius būtų lyginis.)

Pradinė perstata

Originalus pranešimas T (64 bitų blokas) konvertuojamas naudojant pradinę perstatą PP, kuri apibrėžta 1 lentelėje.

1 lentelė

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Pagal šią lentelę pirmieji 3 gauto bloko bitai po pradinės perstatos yra įvesties bloko bitai 58, 50, 42, o paskutiniai 3 bitai yra įvesties bloko bitai 23, 15, 7.

Pradinės perstatos bitai specialiu būdu padalinami po 32 bitus (pažymėkime L0 ir R0).

Duomenų šifravimo standarto pagrindas yra Feistelio funkcija, kuri žymima tiesiog *f* raide.

Feistelio funkcija *f* susideda iš 4 nuoseklių etapų: išplėtimo, raktų maišymo, pakeitimo ir perstatos.

Išplėtimas (angl. *expansion*): 32 bitų R0 išplečiamas iki 48 bitų, naudojant išplėtimo perstatą, schemoje pažymėtą E (žr. toliau), dubliuojant pusę bitų. Išvestį sudaro aštuonios 6 bitų (8 × 6 = 48 bitai) dalys, kurių kiekvienoje yra po keturias atitinkamų įvesties bitų kopijas ir po kaimyninio elemento iš kairės ir dešinės bito kopiją.

2 lentelė

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

2-oje lentelėje matome, kad bitai 1, 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24, 25, 28, 29, 32 kartojasi.

Raktų maišymas (angl. *key schedule*): rezultatas sujungiamas su daliniu raktu naudojant XOR operaciją. Šešiolika 48 bitų pagalbinių raktų – po vieną kiekvienam ratui – gaunami iš pagrindinio rakto naudojant raktų paskirstymą.

Pakeitimas (angl. *substitution*): sumaišius pagalbinį raktą, blokas padalijamas po 6 bitus į aštuonias dalis, kurias apdoroja pagrindinis raktų algoritmų komponentas – S dėžė. Kiekviena iš aštuonių S dėžių pakeičia šešis įvesties bitus keturiais išvesties bitais pagal netiesinę transformaciją, pateikiamą kaip paieškos lentelė. S dėžės yra Duomenų šifravimo standarto saugumo pagrindas – be jų šifras būtų tiesinis ir trivialiai nulaužiamas.

3 lentelė

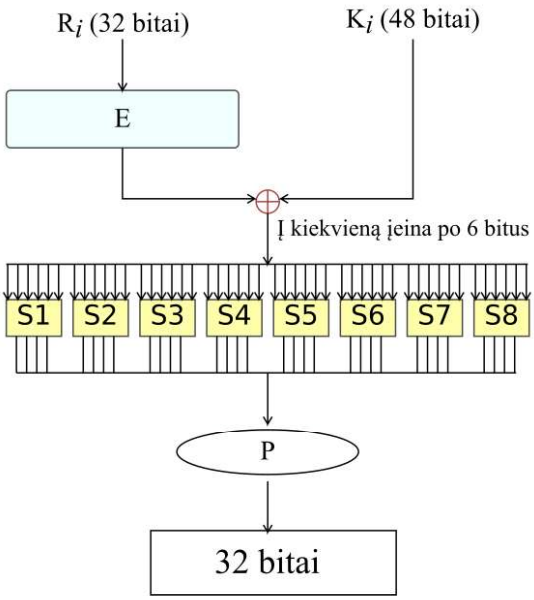
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	

3-ioje lentelėje pavaizduota pirmų trijų S dėžių transformacija. Tarkime, į S3 įeina 101111 ir tai reiškia, kad pirmos ir paskutinės skilties dvejetainiai skaičiai atitinka dešimtainį skaičių *a* uždarame intervale nuo 0 iki 3 (vertikalūs žalsvi langeliai), o keturi vidiniai – skaičių *b* uždarame intervale nuo 0 iki 15 (horizontalūs rusvi langeliai). Tai tiks bet kuriuo atveju.

Šiuo atveju $a = 11_2 = 3$, o $b = 0111_2 = 7$. Tad šių skaičių pora (susikirtimas) atitinka S3 dėžės skaičių 7 ir todėl iš S3 išeis dvejetainis 4 bitų kodas 0111 ($0111_2 = 7$).

Perstata (angl. *permutation*): 32 S dėžių išėjimai pertvarkomi P dėžėje. P dėžė sukurta taip, kad po perstatos bitai po kiekvieno rato iš S dėžės išėjimo būtų paskirstyti keturioms skirtingoms S dėžėms kitame rate.

Tokie etapai užtikrina „painiavą ir išsklaidymą“ (*angl.* confusion and diffusion) – šią sąvoką XX a. ketvirtajame dešimtmetyje Klodas Šenonas (*Claude Shannon*) įvardijo kaip būtiną saugaus, bet praktiško šifro sąlygą.



Funkcijos *f* schema

Duomenų šifravimo standartas yra **blokinis** šifras. Jis padalija pranešimą į 64 bitų blokus ir naudoja tą patį 56 bitų raktą kiekvienam blokui užšifruoti.

Duomenų šifravimo standartas yra viena iš svarbiausių klasikinių kriptosistemų kriptografijos istorijoje. Jis padėjo teorinius ir praktinius pamatus daugeliui kitų kriptografinių sistemų. Analizuodami jį, mokslininkai išplėtojo diferencinę ir tiesinę kriptoanalizę. Daugelis Duomenų šifravimo standarto ypatybių naudojamos kitose kriptosistemose.

2001 m. pabaigoje JAV Nacionalinis standartų ir technologijų institutas (angl. *The National Institute of Standards and Technology*) pranešė, kad Duomenų šifravimo standarto įpėdiniu pasirinktas Išplėstinis šifravimo standartas (angl. *Advanced Encryption Standard*, AES). Kaip ir Duomenų šifravimo standartas, Išplėstinis šifravimo standartas yra sandaugos šifras. Kitaip nei ankstesni, šis standartas gali naudoti 128, 192 ir 256 bitų ilgio raktus ir dirba su 128 bitų blokais. Jis buvo suprojektuotas taip, kad atlaikytų atakas, kurioms Duomenų šifravimo standartas pasiduodavo.

Sinchroniniai srautiniai šifrai

Kad imituotų atsitiktinį neriboto ilgio raktą, sinchroniniai srautiniai šifrai generuoja bitus iš kito šaltinio negu pranešimas. Paprasčiausias toks šifras paima bitus iš registro (kurio turinys nuolat keičiasi) ir naudoja kaip raktą.

Apibrėžimas

n pakopų tiesinis grįžtamojo ryšio postūmio registras (angl. *n-stage linear feedback shift register*, LFSR) sudarytas iš *n* bitų registro $r = r_0 \ldots r_{n-1}$ ir *n* bitų praleidimo sekos (angl. *tap sequence*) $t = t_0 \ldots t_{n-1}$. Bitas r_{n-1} naudojamas raktui, registras pastumiamas per vieną bitą į dešinę ir į registrą įterpiamas naujas bitas $r_0 t_0 \oplus \ldots \oplus r_{n-1}\, t_{n-1}$.

Pavyzdys

Tarkime, kad keturių pakopų tiesinis grįžtamojo ryšio postūmio registro praleidimo seka yra **1001**, o pradinė registro reikšmė yra **0010**. Tada rakto bitai ir registro reikšmės yra tokie, kaip parodyta 4-oje lentelėje. Raktas yra paskutinis esamo registro skaitmuo, o naujam registrui numetamas esamojo registro paskutinis skaitmuo, o iš dešinės pridedamas apskaičiuotas naujas bitas.

4 lentelė

	Esamasis registras	Raktas	Naujas bitas	Naujas registras
1.	**0010**	0	01 ⊕ 00 ⊕ 10 ⊕ 01 = 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0	**0001**
2.	0001	1	01 ⊕ 00 ⊕ 00 ⊕ 11 = 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1	1000
3.	1000	0	11 ⊕ 00 ⊕ 00 ⊕ 01 = 1 ⊕ 0 ⊕ 0 ⊕ 0 = 1	1100
4.	1100	0	11 ⊕ 10 ⊕ 00 ⊕ 01 = 1 ⊕ 0 ⊕ 0 ⊕ 0 = 1	1110
5.	1110	0	11 ⊕ 10 ⊕ 10 ⊕ 01 = 1 ⊕ 0 ⊕ 0 ⊕ 0 = 1	1111
6.	1111	1	11 ⊕ 10 ⊕ 10 ⊕ 11 = 1 ⊕ 0 ⊕ 0 ⊕ 1 = 0	0111
7.	0111	1	01 ⊕ 10 ⊕ 10 ⊕ 11 = 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1	1011
8.	1011	1	11 ⊕ 00 ⊕ 10 ⊕ 11 = 1 ⊕ 0 ⊕ 0 ⊕ 1 = 0	0101
9.	0101	1	01 ⊕ 10 ⊕ 00 ⊕ 11 = 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1	1010
10.	1010	0	11 ⊕ 00 ⊕ 10 ⊕ 01 = 1 ⊕ 0 ⊕ 0 ⊕ 0 = 1	1101
11.	1101	1	11 ⊕ 10 ⊕ 00 ⊕ 11 = 1 ⊕ 0 ⊕ 0 ⊕ 1 = 0	0110
12.	0110	0	01 ⊕ 10 ⊕ 10 ⊕ 01 = 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0	0011
13.	0011	1	01 ⊕ 00 ⊕ 10 ⊕ 11 = 0 ⊕ 0 ⊕ 0 ⊕ 1 = 1	1001
14.	1001	1	11 ⊕ 00 ⊕ 00 ⊕ 11 = 1 ⊕ 0 ⊕ 0 ⊕ 1 = 0	0100
15.	0100	0	01 ⊕ 10 ⊕ 00 ⊕ 01 = 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0	0010
16.	**0010**	0	01 ⊕ 00 ⊕ 10 ⊕ 01 = 0 ⊕ 0 ⊕ 0 ⊕ 0 = 0	**0001**

Tada ciklas vėl kartojasi. Rakto srauto, gaunamo iš šio tiesinio grįžtamojo ryšio postūmio registro, periodas yra 15 (pirma ir šešiolikta eilutės lentelėje sutampa) ir gaunamas toks raktas: 010001111010110.

Užduotis

Tarkime, kad tiesinio grįžtamojo ryšio postūmio registro praleidimo seka yra 1101, o pradinė registro reikšmė yra 0100. Užpildykite 4-ą lentelę naujomis reikšmėmis ir suraskite raktą.

Kriptografinės kontrolinės sumos

Siuntėjas nori nusiųsti gavėjui *n* bitų pranešimą. Jis norėtų, kad gavėjas galėtų patikrinti, ar pranešimas, kurį jis gavo, yra tas pats, kuris ir buvo išsiųstas. Todėl siuntėjas naudoja matematinę **maišos**, arba **kontrolinės sumos**, funkciją, kad gautų mažesnį skaičių *k* bitų iš pradinių *n*. Šis mažesnis bitų rinkinys vadinamas *kontroline suma* (angl. *checksum*) ar *pranešimo santrauka* (angl. *message digest*). Tada siuntėjas išsiunčia gavėjui ir pranešimą, ir kontrolinę sumą. Gavėjas, gavęs pranešimą, irgi apskaičiuoja kontrolinę sumą ir palygina ją su ta, kurią atsiuntė siuntėjas. Jei jos sutampa, jis nusprendžia, kad pranešimas nebuvo pakeistas.

Maiša pagrįstas pranešimo autentiškumo patvirtinimo kodas (angl. *Hash-based message authentication code*, HMAC) yra vienas iš informacijos vientisumo tikrinimo mechanizmų, kuriuo siekiama užtikrinti, kad nesaugioje aplinkoje perduotų ar saugomų duomenų nepakeistų pašaliniai asmenys. Maiša pagrįsto pranešimo autentiškumo patvirtinimo kodo algoritmas naudoja maišos funkciją be rakto ir kriptografinį raktą maišos funkcijai su raktu gauti.

Visos kriptosistemos paremtos keitiniais (kažkas pakeičiama kažkuo kitu) ir perstatomis (kažkas sumaišoma). Tobulėjant kriptoanalizės metodams, šifravimo metodų supratimas taip pat gilėja ir šifrai darosi sunkiau įveikiami. Tas pat tinka ir kriptografinėms kontrolinės sumos funkcijoms. Augant skaičiavimo pajėgumui, raktų ilgis irgi turi didėti.

Literatūra

1. Informacijos sauga. Parengė G. Skersys, Kauno technologijos universitetas, 2011, http://www.esparama.lt/documents/10157/490675/Informacijos_sauga.pdf, 2022-04-22.
2. Stakėnas, V. Kodai ir šifrai. Informacijos kodavimo ir kriptografijos pagrindai. – Vilnius, Vilniaus universitetas, 2007. – 352 p.
3. Stakėnas, V. Kodai ir šifrai, 2006, http://www.statistika.mif.vu.lt/wp-content/uploads/2014/08/kodai_sifrai_Stakenas.pdf, 2022-04-22.
4. Kriptografijos teorija. Parengė E. Sakalauskas, N. Listopadskis, G. S. Dosinas, Kauno technologijos universitetas, 2008, http://crypto.fmf.ktu.lt/lt/xdownload/Kriptografijos%20teorija.%20Mokomoji%20knyga.pdf, 2022-04-22
5. Cryptography Tutorial, https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm, 2022-04-22