Kriptoskiltis

Kriptologija (gr. *kryptos* – paslėptas) yra mokslas apie slaptaraščių (šifrų) sudarymą ir skaitymą. Iki pastarųjų dešimtmečių informacijos šifravimu daugiausia domėjosi karyba, žvalgyba ir diplomatija. Tačiau laikai pasikeitė ir daugeliui žmonių dabar tenka rūpintis savo asmeninio gyvenimo paslapčių saugojimu. Išties ar jūs esate tikri, kad Jaunesnioji sesutė neskaito jūsų asmeninio dienoraščio kompiuterio failuose? Arba Vyresnysis Brolis – elektroniniu paštu siunčiamų laiškų?

Daugelį matematikos klasikų, vertinamų už jų grynosios matematikos rezultatus gerbė ir amžininkai karalių bei didžiūnų dvaruose – už jų sumanumą sudarant ir skaitant šifrus. Džirolamo Kardano (*Girolamo Cardano,* 1501-1576), kurį minime, kaip darbo apie kubinės lygties sprendinius autorių, dirbo Romos popiežiaus kriptografijos tarnyboje, šiuolaikinės algebros pradininkas Fransua Vietas (*François Viète,* 1540-1603) padėjo Prancūzijos karaliui Henrikui IV iššifruoti slaptą ispanų korespondenciją. Jam taip gerai sekėsi, kad ispanai apskundė jį popiežiui už tariamą sąjungą su velniu ir pareikalavo inkvizicijos teismo. Vienas iš integralinio skaičiavimo pradininkų Džonas Valis (*John Wallis,* 1616-1703) tapo Oksfordo universiteto profesorium už ypatingus nuopelnus kriptologijos srityje. Kriptologija teko užsiiimti ir G. V. Leibnicui (*G. V. Leibniz,* 1646-1716) ir L. Oileriui (*L. Euler,* 1707-1783). Genialaus matematiko Alano Tiuringo (*Alan Turing,* 1912-1954) veikla II pasaulinio karo metais iššifruojant slaptus vokiečių šifrus – atskiro straipsnio verta tema. Tuo labiau – dabartinės matematikos ir kriptologijos ryšiai (žr., pvz., Jonas Kubilius, Pirminiai skaičiai ir kriptografija, Alfa plius omega, 1996, 1, 65–70.) Kriptologijos kursai dėstomi universitetų matematikos fakultetuose. Kriptologija dėstoma ir Vilniaus universiteto informatikos specialybės studentams.

Kvadratai ir šifrai

Polibijaus kvadratai

Jei autorius, rašydamas apie ką nors, negali pasakyti, ką šiuo klausimu manė antikos graikai, akivaizdu, kad jam trūksta žinių.

Tad kaip gi šifruodavo savo pranešimus antikos graikai?

Istorikas ir rašytojas Polibijus (apie 208 m. pr. Kr.) aprašo šifrų sudarymo būdą naudojant kvadratus. Į 5×5 dydžio kvadrato langelius atsitiktinai surašomos 24 graikiškos abėcėlės raidės. Kadangi lietuvių kalbos abėcėlėje yra 32 raidės, tai prireiks 6×6 dydžio kvadrato. Neužpildytuose langeliuose įrašysime specialius simbolius (žr. 1 pav.).

• • • $\alpha + \omega$ • • •

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

1 pav.

Kiekvieną raidę šifruosime to paties stulpelio aukščiau stovinčia raide, pavyzdžiui, L keisime raide Ū, V – H. Pirmosios eilutės raides keisime paskutinės eilutės simboliais: Ę – raide M, B – Z ir taip toliau. Taigi pagal šį būdą (1 pav. kvadratas yra šio šifro raktas) žodis MATEMATIKA šifruojamas žodžiu ŽTBUŽTBŠLT.

Polibijus taip pat aprašė, kaip galima perduoti taip užšifruotą pranešimą, naudojant ugnies kodą. Tarkime, dviejose aukšto kalno vietose stovi du žmonės su degančiais fakelais. Kadangi raidė H yra trečioje kvadrato eilutėje ir ketvirtame stulpelyje, tai ši raidė bus perduota tolimam stebėtojui, jei pirmasis žmogus iškels aukštyn tris, o antrasis – 4 uždegtus deglus.

Magiškieji kvadratai

Viduramžių žmonės domėjosi magiškaisiais kvadratais ir manė juos turint ypatingos galios. Tad tikėta, kad šifrai, sudaryti naudojantis tais kvadratais, bus ypač patikimi. Primename, kad magiškuoju vadiname $n \times n$ dydžio kvadratą, kurio langeliuose surašyti natūralieji skaičiai nuo 1 iki n^2, ir kiekvienos eilutės, stulpelio, įstrižainės skaičių suma yra ta pati. Pavyzdys parodytas 2 pav.

5	10	16	3
15	4	6	9
2	13	11	8
12	7	1	14

2 pav.

Kaip buvo šifruojama naudojant kvadratus, skaitytojas supras, iš tokio pavyzdžio. Nešifruotas tekstas: SLAPTIEJI RAŠTAI. Kaip sudaromas šifras parodyta 3 pav.

5	10	16	3
15	4	6	9
2	13	11	8
12	7	1	14

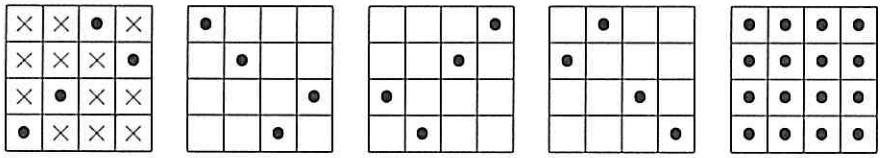
T		I	A
A	P	I	I
L	Š	R	J
A	E	S	T

3 pav.

Šifras: T IAAPIILŠRJAEST.

Džirolamo Kardano kvadratai

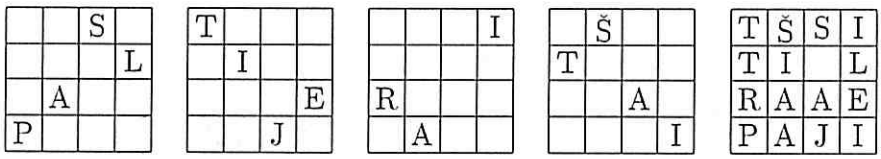
D. Kardano, nagrinėdamas magiškuosius kvadratus, sugalvojo dar vieną šifrų rūšį. Paaiškinsime jo idėją nagrinėdami 4×4 dydžio kvadratą. Nusibrėžkime tokį kvadratą, iškirpkime jo kopiją, o joje – išpjaukime keturis langelius, neišpjautieji pažymėti ženklu „$\times$“ (žr. 4 pav.).



4 pav.

Gautą trafaretą uždėkime ant pradinio kvadrato ir pažymėkime „$\bullet$“ atidengtus pradinio kvadrato langelius. Pasukime trafaretą 90° kampu pagal laikrodžio rodyklę ir vėl pažymėkime neuždengtus langelius. Pasukime trafaretą tuo pačiu kampu dar ir dar. Ketvirtą kartą pažymėję neuždengtus pradinio kvadrato langelius, pamatysime, kad visi langeliai jau pažymėti (žr. 4 pav.).

Dabar naudodami trafaretą užšifruokime tekstą SLAPTIEJI RAŠTAI. Uždėkime trafaretą ant pradinio kvadrato ir įrašykime pirmas keturias teksto raides (žr. 5 pav.). Po to pasukime trafaretą 90° kampu pagal laikrodžio rodyklę ir įrašykime dar keturias raides.



5 pav.

Tokiu būdu gausime šifrą TŠSITI LRAAEPAJI.

Ar yra daug tokių trafaretų? Pakankamai. Kvadratui 4×4 jų yra 256, o 6×6 – daugiau nei 100 tūkstančių.

Tačiau čia aprašyti šifrai yra įdomūs tik kaip istoriniai pavyzdžiai. Na, apsisaugoti nuo smalsios Jaunesniosios Sesutės gal ir tiktų.

Vilius Stakėnas

Skaičiai ir skaitmenys

Pasikartojimų magija: 77

$$77\cdot(10+0\cdot 13)=0770 \qquad 77\cdot(10+5\cdot 13)=5775$$
$$77\cdot(10+1\cdot 13)=1771 \qquad 77\cdot(10+6\cdot 13)=6776$$
$$77\cdot(10+2\cdot 13)=2772 \qquad 77\cdot(10+7\cdot 13)=7777$$
$$77\cdot(10+3\cdot 13)=3773 \qquad 77\cdot(10+8\cdot 13)=8778$$
$$77\cdot(10+4\cdot 13)=4774 \qquad 77\cdot(10+9\cdot 13)=9779$$

Genius Strazdas

Etiudas apie skaičiaus 99...9 laipsnius

Suskaičiuokime:

$$\begin{aligned} 9^2&=81, & 9^4&=6561,\\ 9^3&=729, & 9^5&=59049. \end{aligned} \tag{1}$$

Įdomu, kad kiekviena iš šių lygybių nustato ir skaičiaus $\underbrace{99\ldots9}_{n}$ laipsnių dešimtainių skaitmenų sekos tvarką. O ta tvarka tokia

$$\begin{aligned} \underbrace{99\ldots9}_{n}{}^2 &= \underbrace{99\ldots9}_{n-1}8\underbrace{00\ldots0}_{n-1}1,\\ \underbrace{99\ldots9}_{n}{}^3 &= \underbrace{99\ldots9}_{n-1}7\underbrace{00\ldots0}_{n-1}2\underbrace{99\ldots9}_{n-1}9,\\ \underbrace{99\ldots9}_{n}{}^4 &= \underbrace{99\ldots9}_{n-1}6\underbrace{00\ldots0}_{n-1}5\underbrace{99\ldots9}_{n-1}6\underbrace{00\ldots0}_{n-1}1,\\ \underbrace{99\ldots9}_{n}{}^5 &= \underbrace{99\ldots9}_{n-1}5\underbrace{00\ldots0}_{n-1}9\underbrace{99\ldots9}_{n-1}0\underbrace{00\ldots0}_{n-1}4\underbrace{99\ldots9}_{n-1}9. \end{aligned} \tag{2}$$

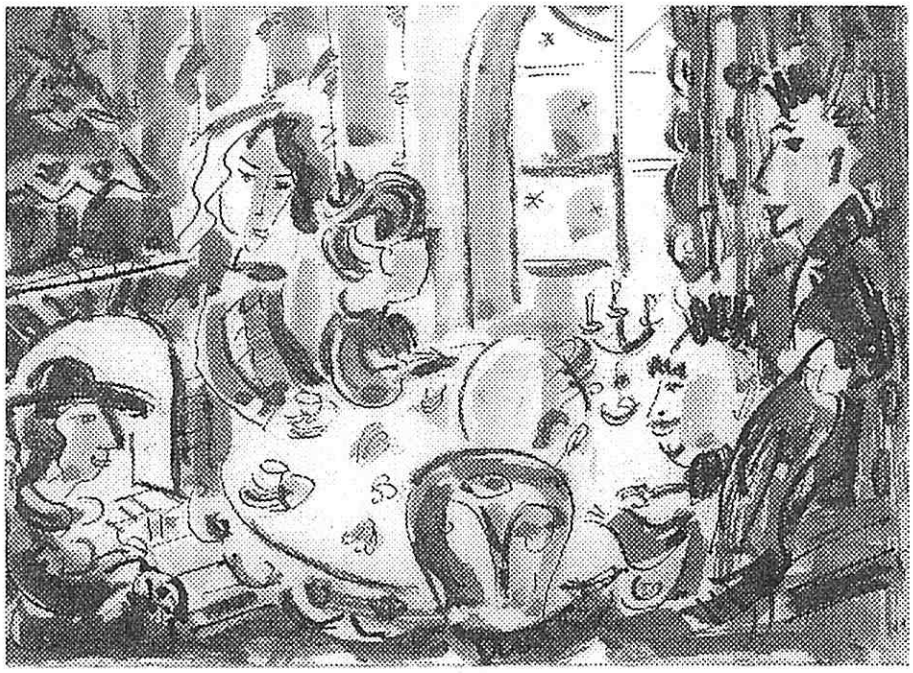
Nesunku pastebėti, koks (1) ir (2) lygybių ryšys. Pavyzdžiui, $\underbrace{99\ldots9}_{n}{}^5$ skaitmenys gaunami įrašant pakaitomis skaitmenų $\underbrace{99\ldots9}_{n-1}, \underbrace{00\ldots0}_{n-1}$ grupes tarp skaičiaus $9^5 = 59049$ skaitmenų. Ta pati taisyklė tinka ir kitiems laipsniams. Štai matematinis pirmosios (2) lygybės įrodymas:

$$\underbrace{99\ldots9}_{n}{}^2 = (10^n-1)^2 = 10^{2n}-2\cdot 10^n+1 =$$

$$(10^{n-1}-1)\cdot 10^{n+1}+8\cdot 10^n+1 = \underbrace{99\ldots9}_{n-1}\cdot 10^{n+1}+8\cdot 10^n+1 = \underbrace{99\ldots9}_{n-1}8\underbrace{00\ldots0}_{n-1}1.$$

Igoris Belovas

Po Alfa + omega skliautais



Kavinėje sklandė Melancholija. Ji tvyrojo virš Fraktalinės Eglutės, lyg dulsva beaistrė šviesa kybojo virš negausių svečių staliukų, tarsi migla skverbėsi į jų mintis.

– Jeigu žurnalui pritrūks autorių ir skaitytojų, – mąstė žvelgdamas į apytuštę salę daktaras Matas, – ir kavinę reikės uždaryti. Būtų gaila...

Lauke snigo. Didelės ir tyros snaigės, kokios būna tik prieš Kalėdas, tykiai sklandė palei langų stiklus.

– Sninga... – pusbalsiu tarė docentė Odeta. – Atrodo, kad tų snaigių yra be galo daug.

– Kaip uodų vasarą, – ironiškai tarstelėjo profesorius Antanas.

– Jų ir yra be galo daug, – pabudo iš susimąstymo daktaras Matas.

– Nesąmonė! – kažkodėl užsiplieskė doktorantas Darius. – Uodų skaičius Žemėje yra baigtinis. Galima nurodyti šio skaičiaus viršutinį rėžį. Štai įrodymas: tegu M – Žemės, o m – vieno uodo masė. Tada uodų skaičius Žemėje neviršija dydžio M/m.

– Jūsų įrodymas remiasi prielaida, mielasis kolega, – vis dar kovodamas su melancholija pastebėjo daktaras Matas. – Jūsų prielaida – uodo masė negali būti mažesnė už tam tikrą teigiamą dydį.

– Tai suprantama, juk uodas negali sverti mažiau už elektroną!

– O, fizika! – vėl atsiduso daktaras Matas. – Kas gi galų gale ką taiko: fizikai matematiką, ar matematikai fiziką?

– Daktaras Matas teisus! – nelauktai įsiterpė profesorius Antanas. – Uodų vasarą iš tikrųjų be galo daug. Tik pagalvokime, ką reiškia teiginys, kad tam

tikra aibė yra begalinė. Tai reiškia, kad jeigu jau parinkote n jos elementų, tai būtinai atsiras ir $n+1$. Argi vasarą, kai jūs sutraiškote n-ąjį jūsų kraujo ištroškusį uodą, neatskrenda $(n+1)$-asis?

– Ar jūsų samprotavimas taip pat tinka skruzdėlėms, erkėms ir vapsvoms? – kiek kandokai pasidomėjo mokytoja Liucija.

Ir kavinėje vėl įsigalėjo Melancholija.

– Tos būtinos ir pakankamos sprendinio egzistavimo sąlygos, – mąstė docentė Odeta. – Visus metus jas vaikausi. Ne kartą atrodė, jau sugavau. Ir vėl žiūrėk – rankose pakankamos sąlygos, o būtinosios vėl išslydo. Tarsi nesugaunamoji Mėlynoji Paukštė...

Paskutinį sakinį ji nejučiomis ištarė balsiai.

– Ar bandėte pritaikyti matematinės liūtų gaudymo teorijos metodus? – pasiteiravo daktaras Matas.

– ... ?

– Tai didelė teorija! Visos matematikos sritys yra joje pritaikytos. Štai pavyzdžiui, Bolcano–Vejerštraso metodas. Dykumą, kurioje yra liūtas, dalijate į dvi dalis: šiaurinę ir pietinę. Tada liūtas patenka į vieną iš jų. Jeigu jis šiaurinėje – pertverkime ją ir atskirkime rytinę dalį nuo vakarinės. Tą dalį, kurioje yra liūtas, vėl dalykime į šiaurinę ir pietinę. Kadangi tos dykumos dalies, kurioje yra liūtas, skersmuo artėja prie nulio, liūtą galima aptverti kiek norima mažo ilgio tvora.

– Aš abejoju, – tarė studentas Giedrius, – ar Bolcano–Vejerštraso metodas tinka paukščiams gaudyti. Jie juk skrajoja trimatėje erdvėje. Geriausia pasiremti inversijos savybėmis. Pagaminkite sferos formos narvą ir įsitaisykite jo viduje (tik jokiu būdu ne sferos centre!). Po to pritaikykite inversiją, kurios centras sutampa su sferos centru, o spindulys lygus sferos spinduliui. Kadangi sferos išorė atvaizduojama į vidų ir atvirkščiai, paukštis atsidurs narve, o jūs – išorėje.

– Gal būt kur nors vandenyne, jei gerai neapskaičiuosite pradinės savo padėties, – pastebėjo doktorantas Darius.

– Prisiminiau vieną istoriją, – kažką braižydamas pirštu ant stalo paviršiaus vėl prašneko profesorius Antanas. – Tai istorija su moralu. O buvo taip. Trys valstybės sumanė pasidalyti pasaulį įtakos sferomis. Ne visiems tai, žinoma, patiko. Tačiau prieš supervalstybių užmačias ne ką padarysi. Tada vienas europietis pareiškė, kad jeigu jau mažesniųjų nuomonės nepaisoma, tai bent jau nė viena iš trijų didžiųjų valstybių po pasidalijimo neturėtų įgyti pranašumo. Nė vienai iš trijų įtakos zonų neturėtų priklausyti du skersmeniškai priešingi Žemės paviršiaus taškai. Juk iš karinių bazių, įrengtų tokiose vietose, būtų galima kontroliuoti visą pasaulį. Trys supervalstybės sutiko, kad tai teisinga ir pradėjo braižyti padalijimo planus. Braižė, braižė, skaičiavo, skaičiavo, tačiau taip ir nepasidalijo pasaulio...

Kurį laiką visi tylėjo.

– Bet kur gi šios istorijos moralas? – pagaliau paklausė mokytoja Liucija.

– Jis visai paprastas. Jeigu kas rengiasi pasidalyti pasaulį, tegu pirma

išstudijuoja Liusterniko–Šnirelmano teoremą.

– O ką teigia ta teorema? – išdrįso paklausti studentas Giedrius ir nuraudo susilaukęs kelių dėkingų žvilgsnių.

– Ji tvirtina: *jeigu n-matę sferą dengia n uždarų aibių, tai bent vienai iš jų priklauso du skersmeniškai priešingi sferos taškai.*

– Aš irgi manau, kad be matematikos neverta net žingsnio žengti, – tarė daktaras Matas. – Mūsų kavinės virtuvėje ant sienos kabo toks užrašas:

> *Jeigu n uždarų ir rišlių aibių dengia n-matės aprėžtos aibės B sieną, tai tos aibės dengia ir visą aibę B.*

– Na ir kaip gi jūs taikote šią teoremą? – pasiteiravo mokytoja Liucija.

– Tai veikiau įspėjimas, panašiai kaip „atsargiai, elektros srovė!“ arba „nežaisk su ugnimi!“ Iš šios teoremos išplaukia, kad jeigu bandysi nuskusti bulvę trimis pjūviais, tai visa bulvė pavirs lupenomis.

Visi vėl nutilo ir paskendo savo mintyse. Gyvenimas toks sudėtingas. Reikia žinoti tiek daug teoremų, kad galėtum jame orientuotis. O už lango su kalėdiniais pirkiniais pro šalį skubėjo žmonės. Kaip jie sugeba gyventi? Ar studijuoja matematiką ir įrodinėja teoremas? Ar jie egzistuoja? Kokiose erdvėse ir kokia prasme?

Pokalbį užrašė Vytautas Gylys
Kavinės lankytojus nupiešė Jaroslavas Rakickis

SL 334. 1998 01 09. 13,5 leidyb. apsk. l. Tiražas 500 egz. Užsakymas 18.

Išleido Lietuvos matematikų draugija, Naugarduko 24, 2006 Vilnius.

Spausdino AB "Informacinio verslo paslaugų įmonė"
Gedimino pr. 31, 2746 Vilnius