Kriptoskiltis

Ar fokusininkas naudojasi matematika, kai iš tuščios skrybėlės ištraukia triušį, arba triušį skrybėlėje pradangina? Nežinau. Nuostabu, kaip lengva tokius fokusus atlikti kompiuteriu. Štai klasikinio anglų kalba parašyto teksto fragmentas * . Surenku kelias komandas ir ...

CJAIO QCE FOUAPPAPU HS UOH NOBW HABOL SR EAHHAPU FW XOB EAEHOB SP HXO FCPG, CPL SR XCNAPU PSHXAPU HS LS: SPIO SB HQAIO EXO XCL VOOVOL APHS HXO FSSG XOB EAEHOB QCE BOCLAPU, FKH AH XCL PS VAIHKBOE SB ISPNOBECHASPE AP AH, – CPL QXCH AE HXO KEO SR C FSSG, – HXSKUXH CJAIO – QAHXSKH VAIHKBOE SB ISPNOBECHASP?

ES EXO QCE ISPEALOBAPU AP XOB SQP MAPL (CE QOJJ CE EXO ISKJL, RSB HXO XSH LCW MCLO XOB ROOJ NOBW EJOOVW CPL EHKVAL), QXOHXOB HXO VJOCEKBO SR MCGAPU C LCAEW-IXCAP QSKJL FO QSBHX HXO HBSKFJO SR UOHHAPU KV CPL VAIGAPU HXO LCAEAOE, QXOP EKLLOPJW C QXAHO BCFFAH QAHX VAPG OWOE BCP IJSEO FW XOB.

HXOBO QCE PSHXAPU ES NOBW BOMCBGCFJO AP HXCH; PSB LAL CJAIO HXAPG AH ES NOBW MKIX SKH SR HXO QCW HS XOCB HXO BCFFAH ECW HS AHEOJR, – SX LOCB! SX LOCB! A EXCJJ FO JCHO! – (QXOP EXO HXSKUXH AH SNOB CRHOBQCBLE, AH SIIKB-BOL HS XOB HXCH EXO SKUXH HS XCNO QSPLOBOL CH HXAE, FKH CH HXO HAMO AH CJJ EOOMOL YKAHO PCHKBCJ); FKH QXOP HXO BCFFAH CIHKCJJW HSSG C QCHIX SKH SR AHE QCAEHIS-CHVSIGOH, CPL JSSGOL CH AH, CPL HXOP XKBBAOL SP, CJAIO EHCBHOL HS XOB ROOH, RSB AH RJCEXOL CIBSEE XOB MAPL HXCH EXO XCL PONOB FORSBO EOO C BCFFAH QAHX OAHXOB C QCAEHISCH-VSIGOH, SB C QCHIX HS HCGO SKH SR AH, CPL FKB-PAPU QAHX IKBASEAHW, EXO BCP CIBSEE HXO RAOJL CRHOB AH, CPL RSBHKPCHOJW QCE DKEH AP HAMO HS EOO AH VSV LSQP C JCBUO BCFFAH–XSJO KPLOB HXO XOLUO.

Prasmė pasislėpė.

Cezario šifrai

Cezario šifrų reikšmė kriptologijoje maždaug tokia pati kaip monetos (arba kauliuko) metymo tikimybių teorijoje. Praktinės reikšmės jie beveik neturi, tačiau puikiai tinka kriptologijos sąvokoms ir principams paaiškinti ir iliustruoti. Kaip rašoma šaltiniuose, Julius Cezaris naudojo šį šifrą rimtai. Mintis labai paprasta. Įsivaizduokime, kad lotyniškos abėcėlės raidės išdėstytos apskritimu, tarkime, laikrodžio rodyklės judėjimo kryptimi taip, kad pirmoji raidė stovi

* Suprantama, kad galėtume naudoti ir lietuviškus tekstus. Tačiau mano pagalbininkės – programos nežino, kaip elgtis su lietuviškomis raidėmis.

šalia paskutinės. Tada šifruojant, kiekviena raidė keičiama trečiąją jos kaimyne skaičiuojant pagal laikrodžio rodyklę. Taigi keitimo taisyklė yra tokia:

$$\begin{array}{cccccccccccc} A & B & C & D & E & F & G & H & I & J & K & L & M \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ D & E & F & G & H & I & J & K & L & M & N & O & P \end{array}$$

$$\begin{array}{cccccccccccc} N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ Q & R & S & T & U & V & W & X & Y & Z & A & B & C \end{array}$$

Šią taisyklę bus lengva užrašyti, jei raides keisime skaičiais, t. y. $A \to 0, \ldots, Z \to 25$. Tada skaičius m keičiamas skaičiumi c , kuris lygus skaičiaus $m+3$ dalybos iš 26 (abėcėlės raidžių skaičius!) liekanai, taigi šifravimo taisyklė tokia:

$$c \equiv m + 3 \pmod{26}.$$

Taip užrašytą šifravimo taisyklę nesunku apibendrinti. Tegu a, b yra skaičiai tarp 1 ir 26, be to, a ir 26 bendrasis didžiausias daliklis lygus vienetui ($(a, 26) = 1$). Tada raidę m (t. y. tą raidę atitinkantį skaičių) keisime (šifruosime) raide c randama iš lygybės

$$c \equiv am + b \pmod{26}.$$

Jeigu nepaisytume reikalavimo $(a, 26) = 1$, tai šifruodami ne tik paslėptume prasmę, bet gali būti, kad sudarkytume neatkuriamai, nes tada kelios skirtingos raidės būtų šifruojamos viena ir ta pačia. Taigi šio šifro paslaptį (raktą) sudaro du skaičiai a, b. Norėdami pagal šifro raidę c atkurti pradinę raidę m, turime iš pradžių surasti skaičių a^*, tenkinantį sąlygą $aa^* \equiv 1 \pmod{26}$, ir dešifruoti pagal taisyklę

$$m \equiv a^*(c + 26 - b) \pmod{26}.$$

Naudojant šį apibendrintą Cezario šifrą ir buvo sudarytas straipsnelio pradžioje pateiktas šifras (skyrybos ženklai ir tarpai tarp žodžių buvo nešifruoti). Ar galima jį iššifruoti nežinant rakto? Paprasčiausia idėja yra perrinkti visus raktų variantus. Tačiau jų yra ne tiek jau mažai – $12 \cdot 26 = 312$!

Triušis iš skrybėlės

Tačiau yra kitas kur kas paprastesnis būdas atkurti paslėptą prasmę.

Kiekvienam lošimo kauliukui egzistuoja jo savybes apibūdinantys skaičiai $0 \le p_1, p_2, \ldots, p_6 \le 1$, $p_1 + p_2 + \ldots + p_6 = 1$, kad, metus tą kauliuką pakankamai didelį skaičių N kartų, akučių $1, 2, \ldots, 6$ pasitaikymo skaičiai $N_1, N_2, \ldots, N_6$ tenkins tokias apytiksles lygybes

$$\frac{N_1}{N} \approx p_1, \quad \frac{N_2}{N} \approx p_2, \ldots, \frac{N_6}{N} \approx p_6.$$

Ilgokai pažaidus su kauliuku, galima bent jau apytiksliai nustatyti šiuos skaičius.

• • • $\alpha + \omega$ • • •

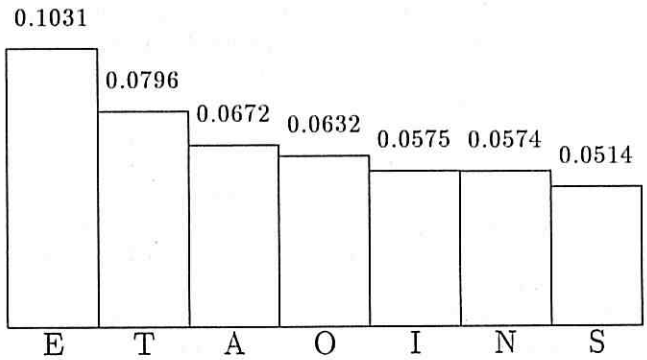
Panašiai yra ir su raidėmis. Anglų kalbos abėcėlės raidės $A, B, \ldots, Z$ (taip pat ir lietuvių) turi jai būdingą skaičių (dažnį):

$$0 \leq p_A, p_B, \ldots, p_Z \leq 1, \quad p_A + p_B + \ldots + p_Z = 1,$$

kad pakankamai ilgame natūralaus šaltinio pateiktame tekste (tarkime, sudarytame iš N raidžių), raidžių $A, B, \ldots, Z$ pasitaikymo skaičiai tenkina apytiksles lygybes

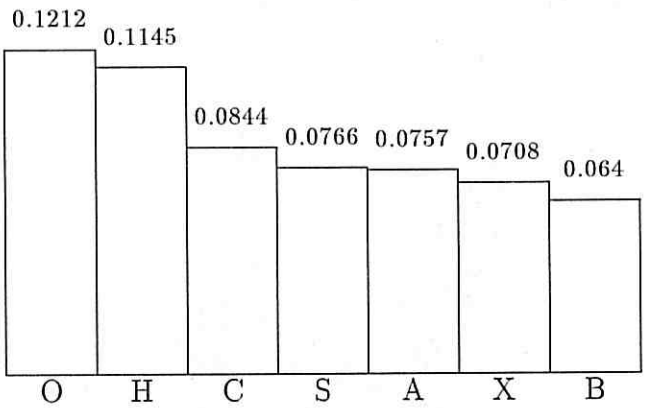
$$\frac{N_A}{N} \approx p_A, \ \frac{N_B}{N} \approx p_B, \ldots, \frac{N_Z}{N} \approx p_Z.$$

Štai šitaip atrodo anglų kalbos raidžių dažnių schema:



Tarkime, raidė E nešifruotame tekste pasitaiko n kartų ir šifruojant Cezario šifru yra keičiama raide R. Tada šifruotame tekste raidė R pasikartoja lygiai tiek kartų, kiek nešifruotame raidė E. Taigi šifruotame tekste raidės R dažnis lygus n/N, tačiau, jeigu tekstas pakankamai ilgas, turi galioti $n/N \approx p_E$. Žinodami p_E ir palyginę su kitų raidžių pasitaikymo šifruotame tekste dažniais galėsime nustatyti, kad šifruojant E buvo keista į R.

Dabar panagrinėkime mūsų šifro raidžių dažnius. Tekste yra 1031 raidė, daugiausiai kartų pasitaiko raidės O (125 kartų), H (118), C (87), S (79), A (78), X (73), B (66). Taigi dažnių diagrama yra tokia:



Natūralu padaryti prielaidą, kad šifruojant raidė E (skaičius 4) buvo keičiama raide O (skaičiumi 14), o raidė T (skaičius 19) – raide H (skaičiumi 7). Jeigu taip, tai rakto komponentės turi tenkinti lygybes

$$4a + b \equiv 14 \pmod{26}, \quad 19a + b \equiv 7 \pmod{26}.$$

• • • $\alpha + \omega$ • • •

Nesunkiai nustatysime, kad šias lygybes tenkina reikšmės $a = 3, b = 2$. Kadangi $3 \cdot 9 \equiv 1 (\mathrm{mod}\ 26)$, tai dešifravimo taisyklė tokia:

$$m \equiv 9(c + 24) \equiv 9c + 8 (\mathrm{mod}\ 26).$$

Patikrinkime savo prielaidą. Dešifravę jau pirmuosius kelis simbolius: ALICE, matome, kad pasisekė. Ištraukėme triušį beveik tiesiogine žodžio prasme, nes apie jį rašoma L. Kerolio knygos „Alisa stebuklų šalyje“ pirmajame skyriuje:

> ALICE WAS BEGINNING TO GET VERY TIRED OF SITTING BY HER SISTER ON THE BANK, AND OF HAVING NOTHING TO DO: ONCE OR TWICE SHE HAD PEEPED INTO THE BOOK HER SISTER WAS READING, BUT IT HAD NO PICTURES OR CONVERSATIONS IN IT, – AND WHAT IS THE USE OF A BOOK, – THOUGHT ALICE – WITHOUT PICTURES OR CONVERSATION?
>
> SO SHE WAS CONSIDERING IN HER OWN MIND (AS WELL AS SHE COULD, FOR THE HOT DAY MADE HER FEEL VERY SLEEPY AND STUPID), WHETHER THE PLEASURE OF MAKING A DAISY-CHAIN WOULD BE WORTH THE TROUBLE OF GETTING UP AND PICKING THE DAISIES, WHEN SUDDENLY A WHITE RABBIT WITH PINK EYES RAN CLOSE BY HER.
>
> THERE WAS NOTHING SO VERY REMARKABLE IN THAT; NOR DID ALICE THINK IT SO VERY MUCH OUT OF THE WAY TO HEAR THE RABBIT SAY TO ITSELF, – OH DEAR! OH DEAR! I SHALL BE LATE! – (WHEN SHE THOUGHT IT OVER AFTERWARDS, IT OCCURRED TO HER THAT SHE OUGHT TO HAVE WONDERED AT THIS, BUT AT THE TIME IT ALL SEEMED QUITE NATURAL); BUT WHEN THE RABBIT ACTUALLY TOOK A WATCH OUT OF ITS WAISTCOAT-POCKET, AND LOOKED AT IT, AND THEN HURRIED ON, ALICE STARTED TO HER FEET, FOR IT FLASHED ACROSS HER MIND THAT SHE HAD NEVER BEFORE SEE A RABBIT WITH EITHER A WAISTCOAT–POCKET, OR A WATCH TO TAKE OUT OF IT, AND BURNING WITH CURIOSITY, SHE RAN ACROSS THE FIELD AFTER IT, AND FORTUNATELY WAS JUST IN TIME TO SEE IT POP DOWN A LARGE RABBIT–HOLE UNDER THE HEDGE.

Vilius Stakėnas

• • • $\alpha + \omega$ • • •