



## Šifravimas

Ignas ir Simonas kartu susidomėjo klasikine kriptografija ir nusprendė šifruoti vienas kitam žinučių tekstus. Jų sutartas šifravimo procesas toks:

- Žinutėse naudoti **tik šiuos** simbolius ir juos sunumeruoti nuo 1 iki 29:
  - naudoti didžiąsias lotyniškas raides: 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, sunumeruoti nuo 1 iki 26 abėcėlės tvarka;
  - naudoti pabraukimo ženklą „\_“ vietoje tarpo – numeris 27;
  - naudoti kablelį „ , “ ir tašką „ . “ – numeriai 28 ir 29, atitinkamai.
- Žinutę šifruojame po simbolių:
  - Simbolio numeris keliamas kubu, tada paimama liekana dalinant iš 29 ir prie gautos liekanos pridedamas 1.
  - Randame naują simbolį, kuris atitinka pirmame punkte gautą skaičių. Tai bus mūsų užšifruotas simbolis.

Taip tęsiame su visais žinutės simboliais.

Paprastumo dėlei pateiksime atitinkamą lentelę su simbolių numeriais.

Simbolis	Numeris	Simbolis	Numeris	Simbolis	Numeris
A	1	K	11	U	21
B	2	L	12	V	22
C	3	M	13	W	23
D	4	N	14	X	24
E	5	O	15	Y	25
F	6	P	16	Z	26
G	7	Q	17	_	27
H	8	R	18	,	28
I	9	S	19	.	29
J	10	T	20		



## Lietuvos mokinių informatikos olimpiada

Miesto (rajono) etapas • 2021 m. gruodžio 14 d. • VIII–IX kl. sifravimas-jau

Pavyzdžiui, tekstas „GERI\_ORAI.“ pagal Igno ir Simono algoritmą bus užšifruotas kaip „YJDEVLDBEA“. Tai lengva patikrinti. Imkime pirmąją raidę G:

- raidės G numeris yra 7,
- kurio kubas yra  $7^3 = 343$ ,
- kurio dalybos iš 29 liekana yra 24,
- prie kurio pridėjus 1 gausime 25,
- o numerį 25 turi raidė Y.

Taigi, šifruodami G gauname Y. Analogiškai galime patikrinti ir kitų simbolių šifravimą.

Taškas „.“, kurio numeris yra 29, užšifruojamas raide A.  $29^3$  dalijasi iš 29 ir todėl liekana bus 0, o pridėjus 1, turėsime 1, t.y. raidę A.

Vyresnis Igno brolis pastebėjo, kad toks šifravimo algoritmas, deja, labai lengvai „sulaužomas“, nes pagal šifruotą tekstą galima greitai atstatyti pradinį, t.y. jį dešifruoti.

**Užduotis.** Parašykite programą, kuri dešifruoja teksto eilutę, užšifruotą pagal Igno ir Simono algoritmą.

**Pradiniai duomenys.** Pirmoje duomenų eilutėje pateikta šifruoto teksto eilutė.

**Rezultatai.** Pateikite dešifruoto teksto eilutę.

**Pavyzdžiai.**

Pradiniai duomenys	Rezultatai	Paaiškinimas
YJDEVLDBEA	GERI_ORAI.	Pavyzdys aptartas sąlygoje.

**Ribojimai.** Šifruoto teksto eilutės ilgis neviršys 80 simbolių.