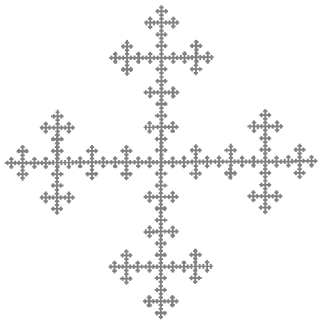
MĀJAS DARBA ATRISINĀJUMI

1. uzdevums.
Nofotografējiet kādu no dabas fraktāļiem un atsūtiet vai atnesiet fotogrāfiju (norādīt, ar kādu fotokameru (mobilo telefonu) iegūts attēls, kad un kurā vietā).

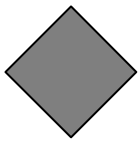
Atrisinājums.
Tiek vērtēta pašu uzņemtas fotogrāfijas atbilstība uzdevuma nosacījumiem. Internetā vai citur iegūtas fotogrāfijas netiek vērtētas.

2. uzdevums.
1. zīm. dots kaut kāda fraktāļa pirmfraktālis. Kāda ir sākotnējā kopa (0. iterācija)? Kāda ir 1. iterācija?

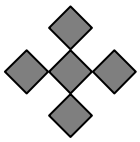


1. zīm.

Atrisinājums.

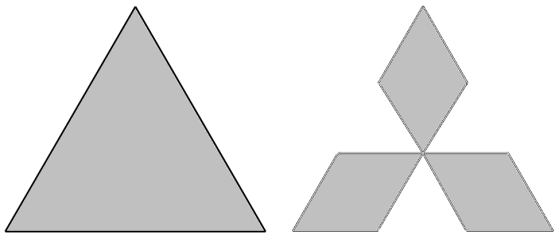


0. iterācija



1. iterācija

3. uzdevums.
2. zīm. dots trīsstūris (0. iterācija) un pirmā iterācija. Uzkonstruēt 2. iterāciju!



2. zīm.

Atrisinājums.

2. iterācija

4. uzdevums.
Izmantojot RSA algoritmu, kur atslēgas ģenerēšanai tiek izmantoti pirmskaitļi $p = 43$, $q = 53$, kā arī skaitlis $e = 5$, aizšifrēt tekstu „NĒ”.

Atrisinājums.
Atslēgas ģenerēšana:

a) Pirmskaitļi $p = 43$ un $q = 53$ ir doti, aprēķinām $n = 43 \cdot 53 = 2279$.
b) Aprēķinām $\varphi(n) = (43 - 1)(53 - 1) = 42 \cdot 52 = 2184$.
c) Ir jau dots, ka $e = 5$.
d) Aprēķinām $d = e^{-1} \bmod 2184 = 437$.
e) Tātad publiskā atslēga ir $(2279, 5)$, bet slepenā – 437.

Aizšifrēšana:

a) Izteiksim „NĒ” kā skaitli: $21 \cdot 34^0 + 8 \cdot 34^1 = 21 + 272 = 293$,
b) Aprēķinām kriptotekstu $c = 293^5 \bmod 2279 = 1374$, kas arī ir atbilde.
c) Vēl var pārbaudīt, ka $1374^{437} \bmod 2279 = 293$, t.i., ka aizšifrēts ir pareizi.

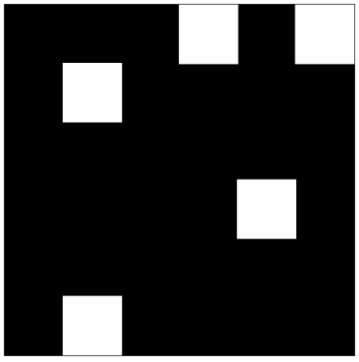
5. uzdevums.
Atminēt ziņojumu un uzzīmēt attiecīgo „Kardano sietu”, ja dots:

a) 4×4 kvadrāts ar kriptotekstu;

Ī	G	T	M
U	A	N	I
Ē	S	R	R
Ķ	T	I	S

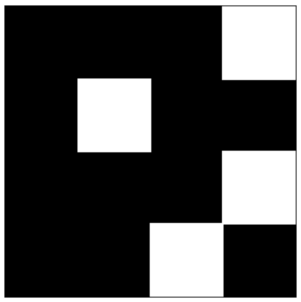
b) 6×6 kvadrāts ar kriptotekstu un „siets”, kurā izgriezti jau 5 lodziņi.

.	E	O	S	S	M
T	U	B	A	S	L
I	G	A	A	F	D
B	D	I	I	Z	Ā
E	S	K	A	O	.
S	M	.	A	.	J



Atrisinājums.
Pamatteksts (ieliekot atstarpes) un attiecīgais „Kardano siets” ir:

a) „MARINĒTS GURĶĪTIS”



b) „ESMU FIZMATS LABĀKAJOS GADOS ... BAIDIES.”