Kriptografiniai protokolai: įrodymas su nuliniu išskelbimu ir konfidencialūs skaičiavimai

Viktor Novičenko

No Trolls Allowed 2014

Dvi istorijos:

Profesorius pateikia užduotį, o studentas išsprendžia tą užduotį, bet nenori rodyti užduoties sprendinio.

Du milijardieriai nori palyginti kas turi daugiau turto, bet nenori skelbti vienas kitam kiek jie to turto turi.

Kas išspręs pateiktą užduotį, gaus 10 be egzamino.

Jau išsprendžiau.

Parodyk sprendimą.

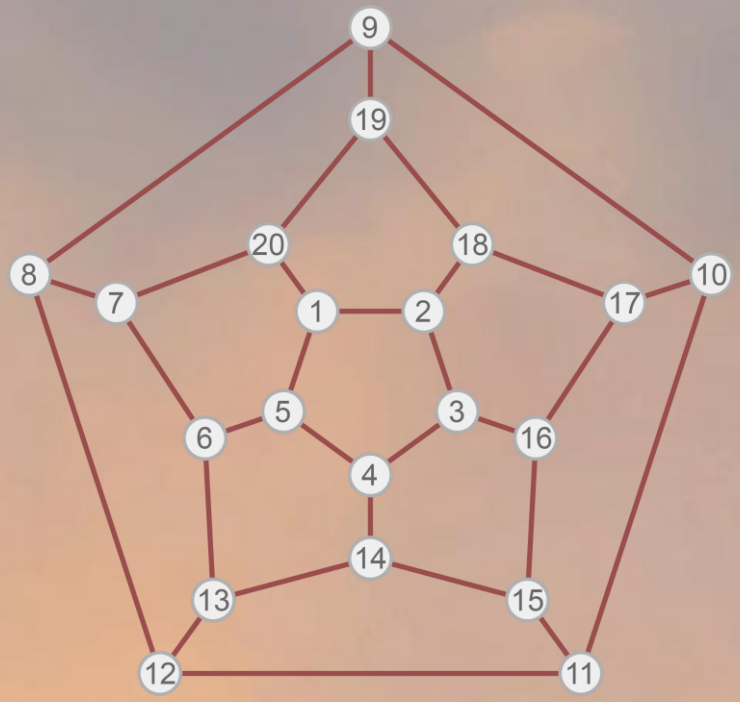
Ne, nerodysiu. Nes tada ir Jūs mokėsite ją spręsti.

Iš kur man tada žinoti, kad tu tikrai ją išsprendei?

Aš galiu įrodyti, kad turiu užduoties sprendimą, nerodydamas jo.

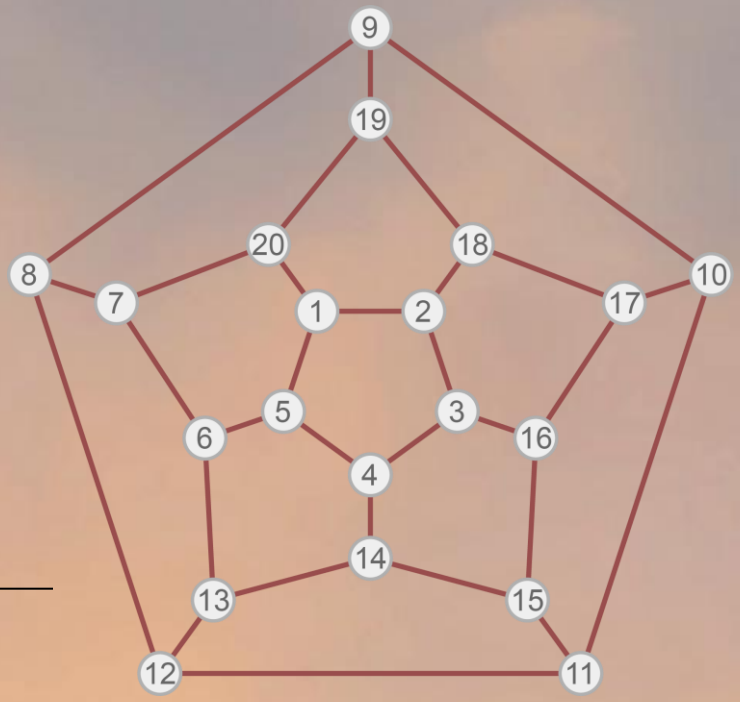
Zero-knowledge proof

Užduotis: duotas didelis grafas, reikia rasti jo Hamiltono ciklą.



Zero-knowledge proof

Užduotis: duotas didelis grafas, reikia rasti jo Hamiltono ciklą.

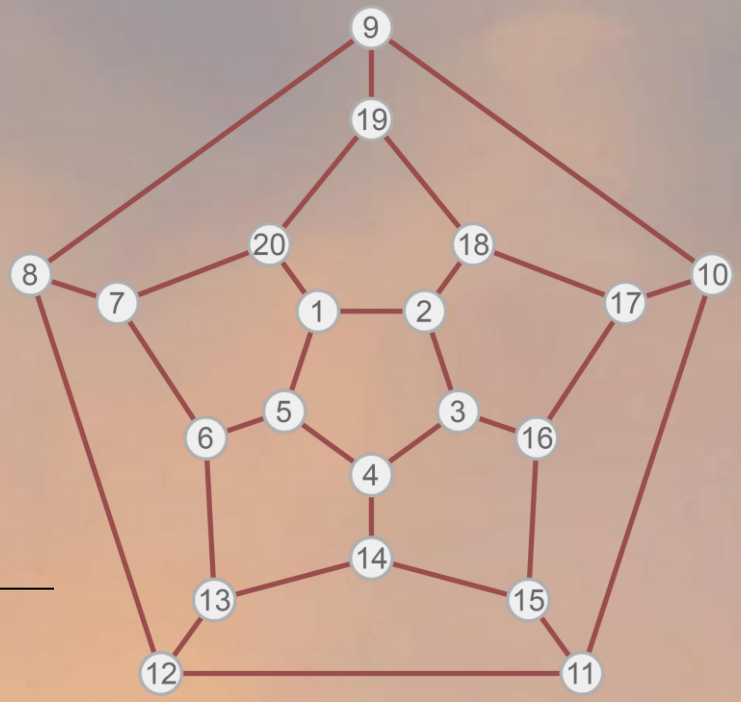


Matematiškai grafą galima užrašyti matricos pavidalu:

	1	2	3	4	5	.....	18	19	20
1									
2									
3									
4									
5									
..									
18									
19									
20									

Zero-knowledge proof

Užduotis: duotas didelis grafas, reikia rasti jo Hamiltono ciklą.



Matematiškai grafą galima užrašyti matricos pavidalu:

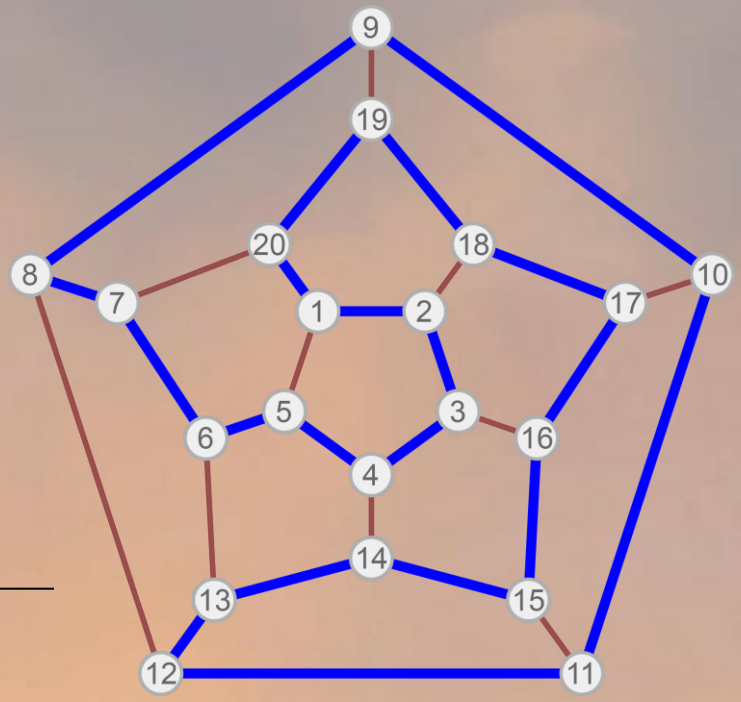
	1	2	3	4	5	.....	18	19	20
1	x	1	0	0	1	.....	0	0	1
2	1	x	1	0	0	.....	1	0	0
3	0	1	x	1	0	.....	0	0	0
4	0	0	1	x	1	.....	0	0	0
5	1	0	0	0	x	.....	0	0	0
..									
18	0	1	0	0	0	.....	x	1	0
19	0	0	0	0	0	.....	1	x	1
20	1	0	0	0	0	.....	0	1	x

Zero-knowledge proof

Užduotis: duotas didelis grafas, reikia rasti jo Hamiltono ciklą.

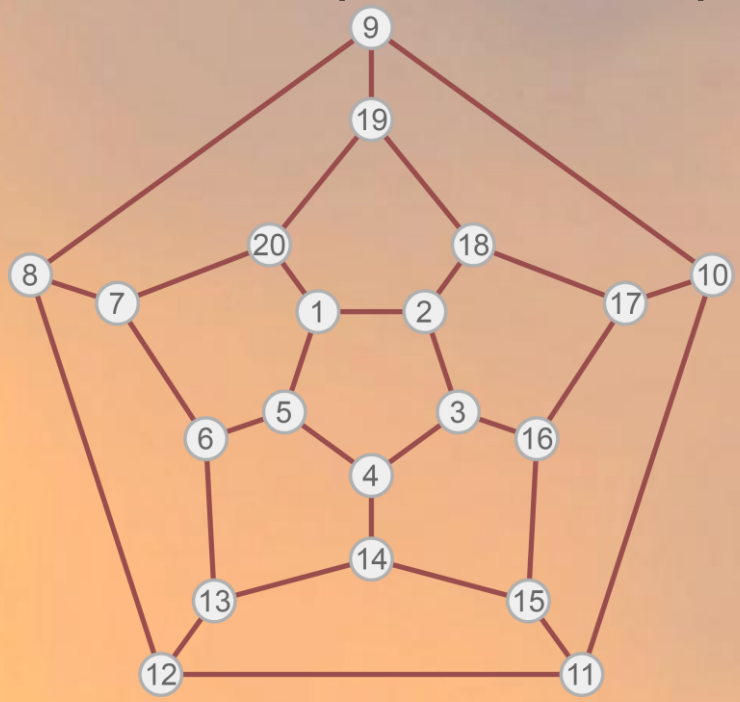
Matematiškai grafą galima užrašyti matricos pavidalu:

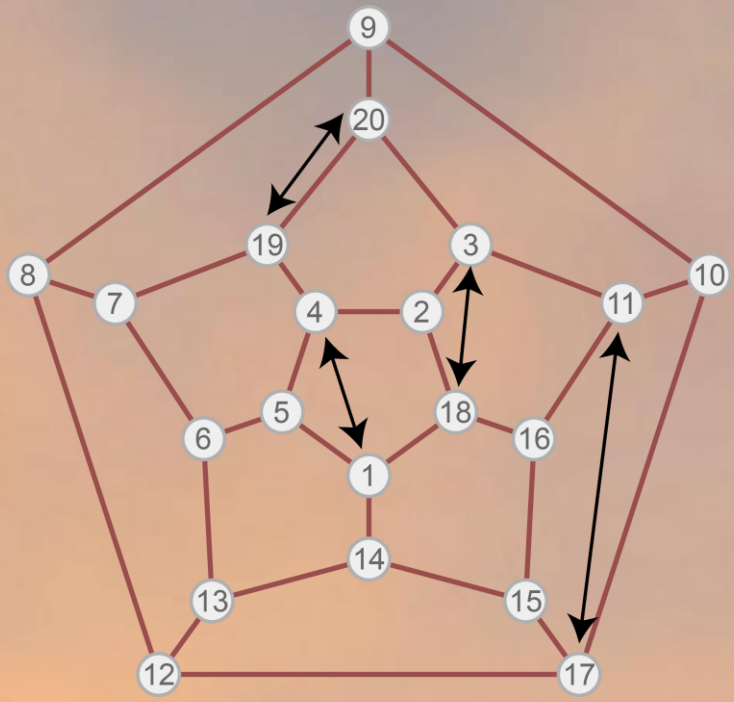
	1	2	3	4	5	.....	18	19	20
1	x	1	0	0	1	.....	0	0	1
2	1	x	1	0	0	.....	1	0	0
3	0	1	x	1	0	.....	0	0	0
4	0	0	1	x	1	.....	0	0	0
5	1	0	0	0	x	.....	0	0	0
..									
18	0	1	0	0	0	.....	x	1	0
19	0	0	0	0	0	.....	1	x	1
20	1	0	0	0	0	.....	0	1	x



Grafo Hamiltono ciklas:
1, 2, 3, 4, 5, ... 19, 20.

Izomorfinis (ekvivalentus) grafas:





Izomorfizmo (ekvivalentumo) lentelė:

1	2	3	4	5	.....	18	19	20
4	2	18	1	5	.....	3	20	19

Jei aš žinau originalaus grafo Hamiltono ciklą ir žinau izomorfizmo lentelę, galiu lengvai rasti Hamiltono ciklą izomorfiniam grafui.

Protokolas:

1) Studentas sugeneruoja izomorfinį grafą ir jį nusiunčia profesoriui;

2) Profesorius paprašo studento įrodyti vieną iš dviejų dalykų:

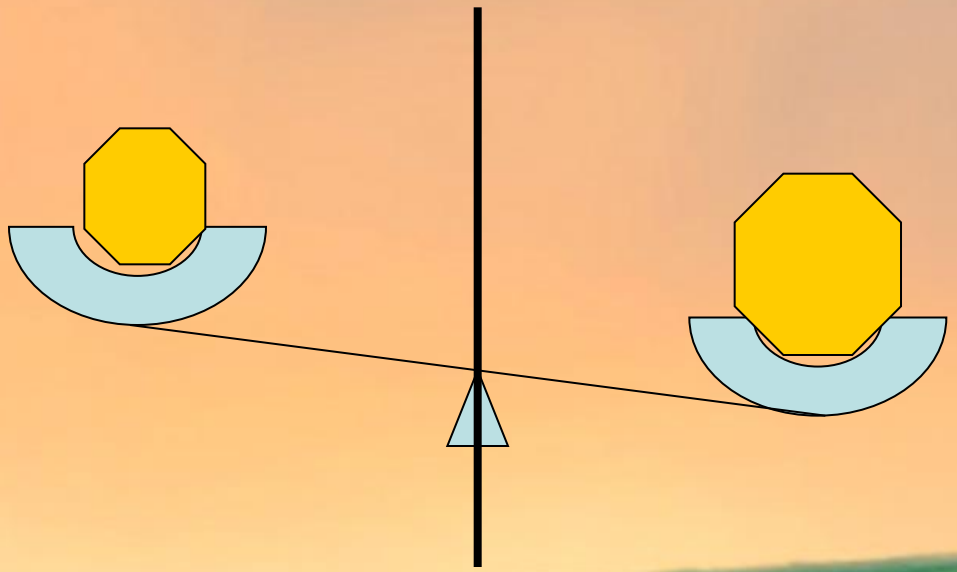
- arba reikia įrodyti, kad grafas yra tikrai izomorfinis originaliam;
- arba parodyti Hamiltono ciklą atsiustame izomorfiniame grafe.

Jei profesorius žino Hamiltono ciklą izomorfiniame grafe, bet nežino izomorfizmo lentelės, tai jam neduoda jokių žinių apie originalaus grafo Hamiltono ciklą.

Jei studentas apgavikas (neturi užduoties sprendimo), jis (jei žinotų profesoriaus užgaidą) galėtų praeiti patikrinimą.

Tikimybė, kad studentas-apgavikas N kartų praeis testą yra: $\frac{1}{2^N}$

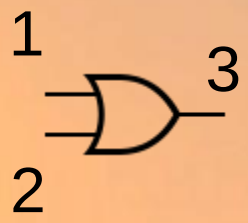
Konfidencialūs skaičiavimai:



$f(a,b)$

Funkcija, kurią galima pavaizduoti loginiu kontūru, susidedančių iš AND, NOT OR, XOR, ... loginių elementų.

Kiekvienas laidas ir kiekvienas bitas užkoduojamas dideliu skaičiumi: $k_{\text{laidas}}^{\text{bitas}}$



INPUT		OUTPUT
		OR
0	0	0
0	1	1
1	0	1
1	1	1

Įėjimo laidas 1	Įėjimo laidas 2	Išėjimo laidas 3	Užkoduota skaičiavimų lentelė
k_1^0	k_2^0	k_3^0	$c_1 = E(k_1^0, E(k_2^0, k_3^0))$
k_1^0	k_2^1	k_3^1	$c_2 = E(k_1^0, E(k_2^1, k_3^1))$
k_1^1	k_2^0	k_3^1	$c_3 = E(k_1^1, E(k_2^0, k_3^1))$
k_1^1	k_2^1	k_3^1	$c_4 = E(k_1^1, E(k_2^1, k_3^1))$

$E(k,m)$ - užkoduoja pranešimą “m” naudojant raktą “k”.

$D(k,m)$ - dekoduoja pranešimą “m” naudojant raktą “k”.


PABAIGA