Koliokviumas: Lapkričio 5 d., 17:30. Kontaktiniu būdu.

Vieta, laikas

	Data		Laikas	Auditorija	Adresas
☐	2024.11.05	An	17:30-18:00	X r.- 103ab (24), Kompiuterių klasė X r.- 103f (17), Kompiuterių klasė X r.- 105 (25), Kompiuterių klasė	Studentų g. 48a, Kaunas

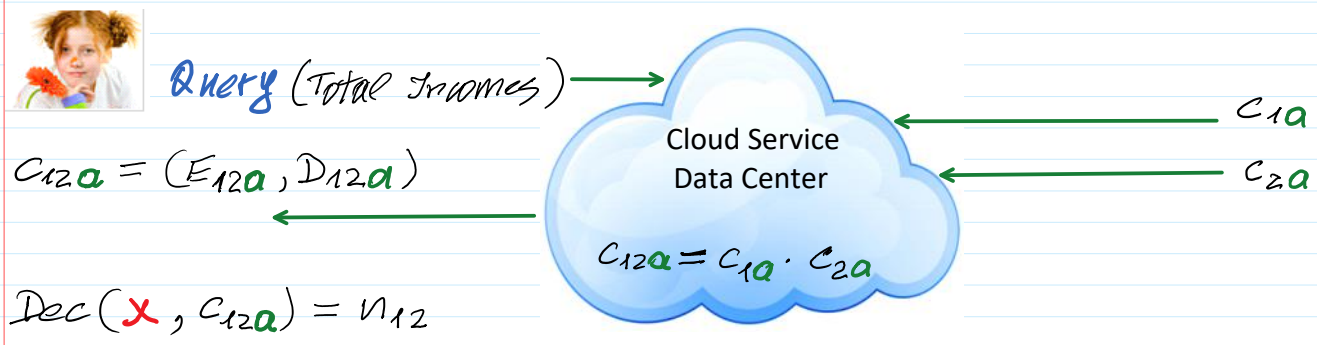
Tema: **Computation with encrypted data.**
Reikia turėti savo kompiuterius su Octave ir instaliuotais .m failais.
Skaičiavimo rezultatus reikės užpildyti Google drive lentelėje, kurios nuorodą pateiksiu.

Homomorphic CryptoSystems: Computation with encrypted data in Data Center.

Declare **Public Parameters** to the network **PP** = (***p***, ***g***); ***p***= **268435019**; ***g***=**2**;
In real cryptosystem is chosen having 2048 bits and is of order ***p***=2^{2048} ~ 10^{700},
i.e. |***p***|=2048 bits.
In our simulation we use |***p***|=28 bits, i.e. ***p*** < 2^{28} = 268 435 456.
>> dec2bin(p)
ans = 1111 1111 1111 1111 1110 0100 1011

>> p=int64(268435019)
p=268435019
>> g=2;

You must realize computations presented in my Google drive:
https://docs.google.com/spreadsheets/d/1ZVSZMGheC2RCZIpJr8XltwvmKe1I6Zwh/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true



		Alice		Bob1					Bob2				
							c1a					c2a	
Pa.Vardas	Num.	x	a	m1	n1	i1	E1a	D1a	m2	n2	i2	E2a	D2a
Kuprusevičius Rokas	1												
Nescerenko Artūras	2												
Aliuškevičius Matas	3												
Anikanovas Martynas	4												
Bačkieriūtė Monika	5												
Binkauskas Tautvydas	6												
Blauzdys Edgaras	7												
Brūzga Lukas	8												
Daranda Kasparas	9												
Dombrovskis Paulius	10												
Dronovas Povilas	11												
Druceika Augustas	12												
Gataveckas Nojus	13												
Gedmantas Gytis	14												
Grigėnas Karolis	15												
Jankūnas Vilius	16												
Kazlauskas Tomas	17												

Full table is in Google drive

Klimakaitė Paulina	18												
Kliokys Aurimas	19												
Kuzmenko Artas	20												
Lisajus Justas	21												
Liutkus Evaldas	22												
Martinaitis Aurimas	23												
Naprys Ugnius	24												
Ordinaitė Rūta	25												
Paliukas Vytas	26												
Ropė Vytenis	27												
Ruslys Justinas	28												
Samuolis Mantas	29												
Šaltanė Toma	30												
Tambakevičius Edvardas	31												
Tarutis Karolis	32												
Trumpauskas Robertas	33												
Verenius Simonas	34												
Žilius Karolis	35												
Ambrakaitytė Rugilė	36												
Burmonaitė Austėja	37												
Jakubauskas Domas	38												
Orinaitė Ugnė	39												
Sargautis Tomas	40												
Stankevičius Gintaras	41												
	42												
	43												
	44												
	45												

PrK = *x* <-- randi ==> PuK = *a* = g^x mod p

$$c_{12a} = c_{1a} \cdot c_{2a} = (E_{1a} \cdot E_{2a} \bmod p,\ D_{1a} \cdot D_{2a} \bmod p) = (E_{12a}, D_{12a})$$

Dec(*x*,c12*a*) = n12 = $g^{i1+i2 \bmod(p-1)} \bmod p$.
How to find *i*1+*i*2 when n12, *g* and *p* are given?

```
% Finds discrete logarithm value corresponding to exponent value i
% by total scan of i from start by step until fin
% p - is a strong prime (Public Parameter)
% g - is a generator (Public Parameter)
% def - is a discrete exponent function value computed by mod_exp(g,i,p)
%       where dl=i is a searchable value of exponent
%
function dl = dlog(p, g, def, start, step, fin)
 dl=0;
 i=start;
 while i<fin
    ee=mod_exp(g,i,p);
    if ee==def
      dl=i;
      return;
    endif
    i+=step;
 endwhile
 disp('Exponent is not found!');
end
```

```
>> i1pi2=5000;
>> def=mod_exp(g,i1pi2,p);
def = 143845522
>> n12=def;
start = 0;
>> step=100
step = 100
>> fin=9900
fin = 9900

>> def=mod_exp(g,5000,p)
def = 143845522
>> dl = dlog(p, g, def, start, step, fin)
dl = 5000
```