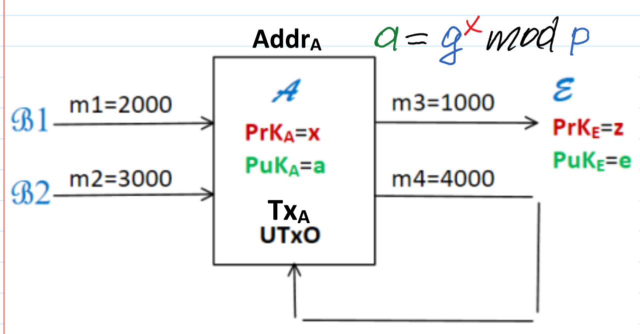
Exam problems.

https://docs.google.com/spreadsheets/d/1FN8fTPlnq2ZW6da5uFyy-z0yUe8036Fa/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

https://docs.google.com/spreadsheets/d/1PgtCjTYpUzpwn-MmOmHTkhXXXOxfV4im/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

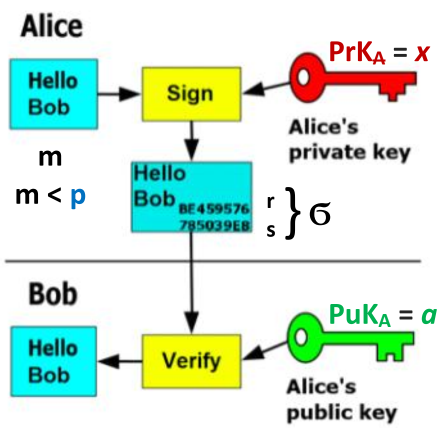
Transaction (Tx) information in simplified form consist of the following information:
1. The address of Tx creator.
2. The sums of Incomes and addresses of senders.
3. The sums of Expenses and addresses of receivers.



certificate for a is $Cert_a$

Schnorr Signature

In the case of Schnorr cryptosystem our simulation is performed with Public Parameters:
PP = (p, g); **p=268435019; g=2**; p=int64(268435019)
By having **PP** private key **PrK** and public key **PuK** are generated:
PrK = x <-- randi(p-1)
PuK = $a = g^x \bmod p$.



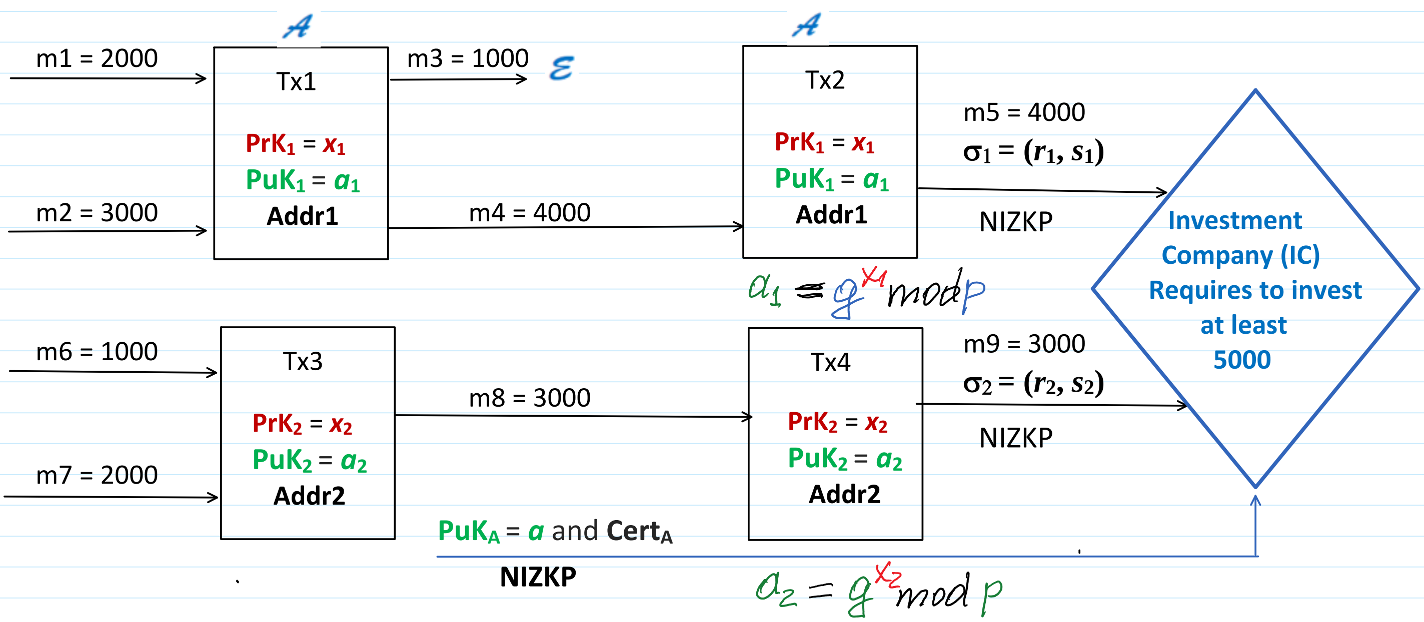
u <-- randi(p-1).
$r = g^u \bmod p$.
$h = H(M||r)$. >> con=concat(M,r)
>> h=hd28(con)
$s = u+xh \bmod (p-1)$. (*) >> s=mod(u+x*h,p-1)
Alice's signature on h is $\sigma = (r, s)$.

Notice that it is infeasible to find x from (*), when s and h are given, since there is 1 equation (*) and 2 unknowns u and x.

Signature is valid if: $\underbrace{g^s \bmod p}_{V1} = \underbrace{ra^h \bmod p}_{V2}$. (Eq.1)

But **Alice** do not want that all her incomes belonging to her Address were known and therefore and she prefers to be anonymous to the **Net**.
Then she creates a set of Addresses by generating a set of private keys {$PrK_i = x_i$} and a set of public keys {$PuK_i = a_i$}, where i=1, 2, ..., N.

But! There are the situations when **Alice** must prove some subjects that she possesses some amount of money distributed among a lot of her accounts and transactions with different addresses.
For example, she could pretend to tax concessions - mokesčiu lengvatos (according to the law) and she must prove to certain Investment Company that she possesses sufficient amount of money.
In this case she must prove that she controls some accounts with this sufficient amount of money for investment.
In this case **Alice** can prove that her transactions are authentic (i.e. are created by her) by proving that **PuK**=a belongs to her, e.g. using Certificate issued by Certificate Authority for **PuK**=a, but at the same time she remains **anonymous** for other part of the **Net**.



$\mathcal{A}$: must prove that she knows x_1 and x_2 by signing on x_1 and x_2

1) computes key $x_{12} = x_1 + x_2 \bmod (p-1)$

2) signs on $a_1 \cdot a_2 = a_{12} \bmod p$ with her $PrK = x$: $Sign(x, h_{12}(a_{12})) =$
$= \sigma_{12}(r_{12}, s_{12})$.

3) IC verifies $Ver(a, \sigma_{12}, h_{12}) \in \{T, F\}$

Realization.

$\mathcal{A}$:

$i_{12} \leftarrow randi\,(p-1)$

$r_{12} = g^{i_{12}} \bmod p$

$h_{12} = H(a_{12} \| r)$

$s_{12} = i_{12} + x_{12} \cdot h_{12} \bmod (p-1)$

$\sigma_{12} = (r_{12}, s_{12})$

$$\xrightarrow[a,\ Cert_a]{\sigma_{12} = (r_{12},\, s_{12})}$$

IC: 1) computes

$a_1 \cdot a_2 = a_{12} \bmod p$

$h_{12} = H(a_{12} \| r)$

2) Verifies σ_{12} on h_{12} with a_{12}

$a_{12} = g^{x_{12}} \bmod p$

If yes

$\sigma_{12} = (r_{12}, s_{12})$ if Yes

$$g^{x_{12}} \bmod p = g^{x_1 + x_2 \bmod (p-1)} \bmod p = g^{x_1} \cdot g^{x_2} \bmod p = a_1 \cdot a_2 = a_{12} \bmod p$$

Verification function: $\underbrace{g^{s_{12}}}_{V_1} = \underbrace{r_{12} \cdot (a_{12})^{h_{12}}}_{V_2} \bmod p$

A proved that she knows the sum x_{12} of private keys x_1, x_2 not disclosing x_{12} and using public key $a_{12} = g^{x_{12}} \bmod p$.
It is named as Non-Interactive Zero Knowledge Proof – NIZKP.

Deanonymization of A by A by signing on signature $\sigma_{12} = (r_{12}, s_{12})$ against TC.

$i \leftarrow \text{randi}(p-1)$

$r = g^{i} \bmod p$

$h = H(r_{12} \| s_{12} \| r)$

$s = i + x \cdot h \bmod (p-1)$

$\sigma = (r, s)$

$\xrightarrow[a,\ Cert_a]{\sigma = (r, s)}$

TC: 3) Verifies $Cert_a \to$ Yes

4) Verifies σ on h

$\underbrace{g^{s}}_{V_1} = \underbrace{r \cdot a^{h}}_{V_2} \bmod p$

$V_1 = V_2$

$\xleftarrow{\text{Equities}}$