Koliokviumas vyks kontaktiniu būdu per paskaitą, Balandžio 17 d., 17:30, 140 a.
Atsineškite savo asmeninius kompiuterius.
Kolioviumo tvarka pateikta Moodle.

We considered a set of integers defined as $\mathbf{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$.
This set is a commutative multiplicative algebraic group with binary multiplication operation $*$**mod** p defined in $\mathbf{Z}_p^*$.
Binary operation means that it is defined between two elements-operands of the set.

Let we have any set G (do not confuse with generator G in Elliptic Curve Group) with some arbitrary binary operation $\odot$ defined in it.
The set with defined any binary operation $\odot$ is an algebraic group if it satisfies 3 main axioms and 1 additional axiom for commutative groups:

Axiom 1. The set G is closed under the operation $\odot$
Axiom 2. For all a in G there exists a neutral element **1** such that $1 \odot a = a \odot 1 = a$.
Axiom 3. For all a in G there exists unique inverse element a^{-1} such that $a \odot a^{-1} = a^{-1} \odot a = 1$.

The group is commutative if the following conditions holds:
Axiom 4. For all a, b in G the following commutative condition holds $a \odot b = b \odot a$.
We were dealing with the commutative groups exclusively.

Any kind of operation can be defined in G but we mainly were dealing with the following operations:
$*$ for multiplication;
+ for addition;
$\boxplus$ for addition of Elliptic Curve(**EC**) points in Elliptic Curve Group (**ECG**).

Remark. If operation $\odot$ in G is an addition operation **+** then usually in
Axiom 2 the neutral element is denoted by **0**; then for all a in G the following condition holds $0+a = a+0 = a$.
Axiom 3 the inverse element a^{-1} is replaced by $-a$: $a + (-a) = 0$.

Symbolically the group G with defined operation is denoted by $<G, \odot>$.

Examples.
1. The infinite multiplicative group of real numbers: $<\mathbf{R}, *>$.
2. The infinite additive group of real numbers: $<\mathbf{R}, +>$.
3. The infinite additive group of integers $\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$: $<\mathbf{Z}, +>$.

4. The finite multiplicative group of integers $\mathbf{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$: $<\mathbf{Z}_p^*, *\mathbf{mod}\ p>$.
   It is a set of values a of Discrete Exponent Function - **DEF**: $a = g^x \bmod p$.
5. The finite additive group of integers $\mathbf{Z}_{p-1} = \{0, 1, 2, 3, \ldots, p-2\}$: $<\mathbf{Z}_p, +\mathbf{mod}\ p-1>$.
   It is a set of exponents x of Discrete Exponent Function - **DEF**.
6. The finite additive group of points of Elliptic Curve Group (**ECG**): $<\mathbf{ECG}, \boxplus>$.

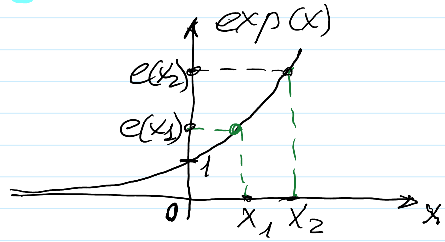
$\exp(x) = e^x$; $\exp: R \to R^+$; $e = 2{,}71\ldots$

$$x \in R \to e^x \in R^*_+$$

$$\exp(x_1 + x_2) = e^{(x_1+x_2)} = e^{x_1} * e^{x_2} = \exp(x_1) \cdot \exp(x_2) = e_1 * e_2$$

Additively – multiplicative homomorphism.

Since it is 1-to-1, then it is isomorphism.




```
g = 2
>> x1=3
x1 = 3
>> x2=4
x2 = 4
```

```
>> ee12=2^(x1+x2)
e12 = 128

>> e1=g^x1
e1 = 8
>> e2=g^x2
e2 = 16
>> ee12=e1*e2
ee12 = 128
```

Let $\langle G, + \rangle$ and $\langle H, * \rangle$ be a groups.

Let φ be mapping $\varphi : G \to H$.

Mapping φ is called a homomorphism if for all elemets $x_1, x_2 \in G$ there exist the elements $e_1, e_2 \in H$ such that

$$\varphi(x_1 + x_2) = \varphi(x_1) * \varphi(x_2) = e_1 * e_2. \qquad (1)$$

If φ is 1-to-1 mapping: for any $x_1 \in G$ there exists unique value $\varphi(x_1) \in H$, then mapping φ, satisfying (1) is an isomorphism.

DEF homomorphism-isomorphism

$DEF(x) = g^x \bmod p$; p – strong prime

g – generator in $\mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$

$x \in \mathbb{Z}_{p-1} = \{0, 1, 2, 3, ..., p-2\}$; $+ \bmod (p-1)$, $* \bmod (p-1)$, $- \bmod (p-1)$

$|\mathbb{Z}_{p-1}| = p-1$ $\qquad$ $/ \bmod (p-1)$.

$DEF(x) = a \in \mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$; $* \bmod p$, $/ \bmod p$.

$|\mathbb{Z}_p^*| = p-1 = |\mathbb{Z}_{p-1}|$

DEF is 1-to-1 mapping: one value of x is mapped to unique value $a = g^x \bmod p$.

Proof is based on

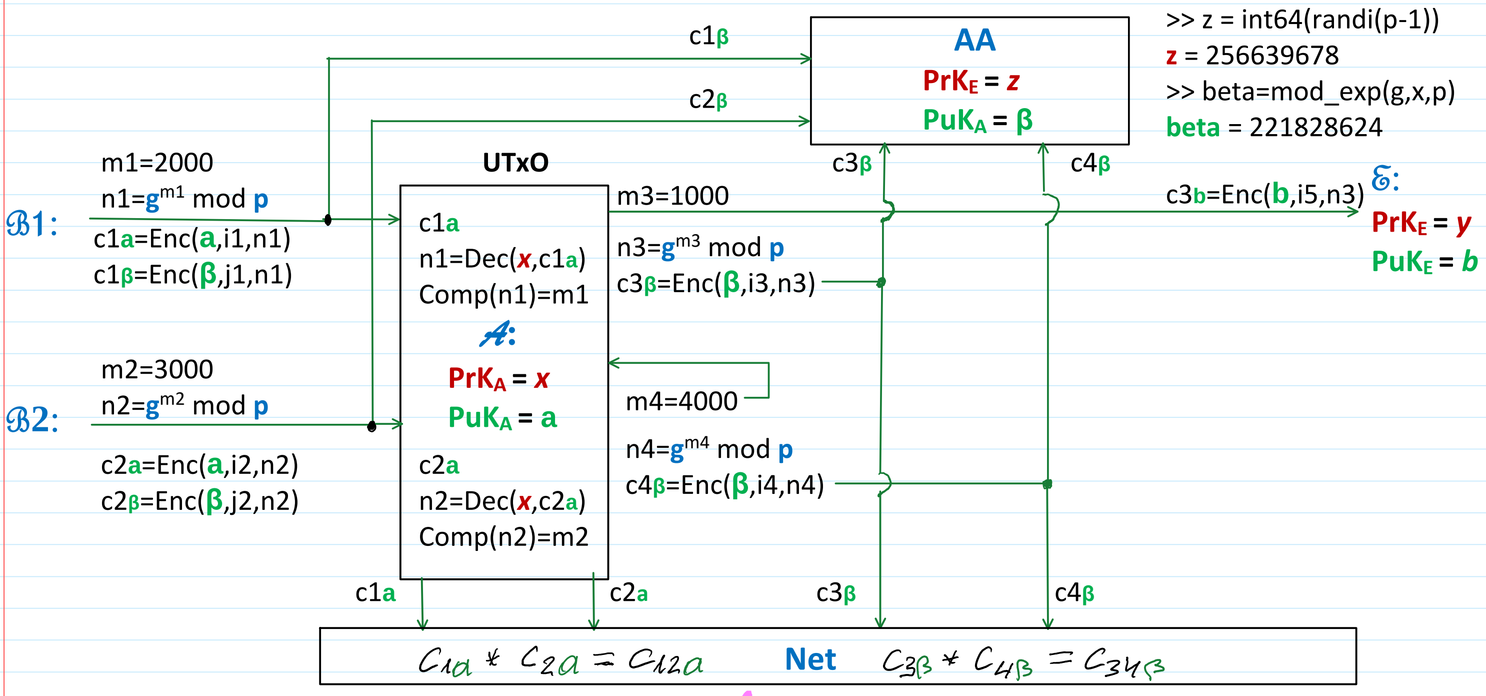
Referencing to Fermat little theorem the expressions in exponents are computed mod $(p-1)$.

$$DEF(x_1+x_2) = g^{(x_1+x_2) \bmod (p-1)} \bmod p = g^{x_1} * g^{x_2} \bmod p =$$
$$= ((g^{x_1} \bmod p) * (g^{x_2} \bmod p)) \bmod p = DEF(x_1) * DEF(x_2) = a_1 * a_2.$$

Additively – multiplicative homomorphism.

Since it is 1–to–1, then it is isomorphism.

Confidential - Verifiable Transactions **PP** = (p, g).



$C_{12a} \neq C_{34\beta}$

A: must prove to the Net that C_{12a} and $C_{34\beta}$ encrypts the same value, not revealing this value (e.g. 5000).

Till this place

Net: Computes $C12a = C1a * C2a = (E1a, D1a) * (E2a, D2a) =$
$= (E1a * E2a \bmod p,\ D1a * D2a \bmod p) = (E12a, D12a)$

$$C34\beta = C3\beta * C4\beta = (E3\beta, D3\beta) * (E4\beta, D4\beta) =$$
$$= (E3\beta * E4\beta \bmod p,\ D3\beta * D4\beta \bmod p) = (E34\beta, D34\beta)$$

$$E3\beta = n_3 \cdot \beta^{i_3} \bmod p;\ D3\beta = g^{i_3} \bmod p;\quad E34\beta = n_3 \cdot n_4 \cdot \beta^{(i_3+i_4) \bmod (p-1)} \bmod p$$
$$E4\beta = n_4 \cdot \beta^{i_4} \bmod p;\ D4\beta = g^{i_4} \bmod p;\quad D34\beta = g^{(i_3+i_4) \bmod (p-1)} \bmod p$$

$$C_{34\beta} = (E34\beta = n_{34} \circ \beta^{i} \bmod p,\ D34\beta = g^{i} \bmod p)$$

Taking in mind that:

1) If $m_{12} = m_1 + m_2 \bmod (p-1) = m_{34} = m_3 + m_4 \bmod (p-1)$

$n_{12} = n_1 \cdot n_2 \bmod p \quad = \quad n_{34} = n_3 \cdot n_4 \bmod p$

2) Then $Dec(PrK = x, c12a) = n_{12} = g^{(m_1+m_2) \bmod (p-1)} \bmod p$

$Dec(PrK = z, c34\beta) = n_{34} = g^{(m_3+m_4) \bmod (p-1)} \bmod p$

Then $c12a$ and $c34\beta$ encrypts the same number $n_{12} = n_{34} = n$.

But since $a \neq \beta$ ⟶ $c12a \neq c34\beta$ in any way!

A: Must prove that ciphertexts $c12a$ and $c34\beta$ encrypted the same number $n = n_{12} = n_{34}$ ⟷

⟷ balance $= (m_1 + m_2) \bmod (p-1) = (m_3 + m_4) \bmod (p-1) = 5000$.

This is named as ciphertexts equivalency probeem.

Proof. $i = i_{34} = (i_3 + i_4) \bmod (p-1)$

```
>> i34=mod(i3+i4,p-1)
i34 = 115795473
```

1) A proves to the Net that she knows her $PrK_A = x$ by declaring her $PuK_A = a$ using NIZKP.

2) A proves to the Net that she knows her random parameter $i = i_{34}\ (i_3 + i_4) \bmod (p-1)$ for $n_{34} = n_3 * n_4 \bmod p$ encryption.

Random parameters i_3 and i_4 must be secret otherwice encrypted values n_3 and n_4 can be decrypted without a

Random parameters i_3 and i_4 must be secret otherwise encrypted values n_3 and n_4 can be decrypted without a knowledge of her $PrK = x$.

3) $\mathcal{A}$ referencing to these proofs provides a ciphertexts equivalency proof.

Non-Interactive Zero Knowledge Proof - NIZKP **PP** = (p, g).

$\mathcal{A}$: **NIZKP of knowledge x:**

$PrK_A = x =$ **randi(p-1)**

$PuK_A = a = g^x \bmod p$

1. Computes r for random number u:

$u = \text{randi}(p-1)$

$r = g^u \bmod p$

2. Generates h:

$h = \text{randi}(p-1)$

3. Computes:

$s = u + xh \bmod (p-1)$

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

$\mathcal{B}$: $PuK_A = a$

Verifies:

$g^s = r a^h \bmod p$

$PrK_A = x$ is called witness
for a statement $PuK_A = a$.

Let $\mathcal{A}$ wants to prove the knowledge of x and $i = i_{34}$.

Then the statement $st = \{a = g^x \bmod p\ ,\ D_{34\beta} = g^i \bmod p\}$

$u \leftarrow \text{randi}(\mathbb{Z}_p^*)$

$v \leftarrow \text{randi}(\mathbb{Z}_p^*)$

Commitments t_1 and t_2 are generated:

$$\left.\begin{aligned} t_1 &= g^u \bmod p \\ t_2 &= g^v \bmod p \end{aligned}\right\} h = H(a \| D_{34\beta} \| t_1 \| t_2) \xrightarrow{\text{Net}} \begin{aligned} &\{a, D_{34\beta}, t_1, t_2\} \\ &h = H(a \| D_{34\beta} \| t_1 \| t_2) \end{aligned}$$

$$\begin{aligned} r &= x \cdot h + u \bmod (p-1) \\ s &= i \cdot h + v \bmod (p-1) \end{aligned} \xrightarrow{\text{Net verifies}} \begin{aligned} g^r &= t_1 \cdot a^h \bmod p \\ g^s &= t_2 \cdot (D_{34\beta})^h \bmod p \end{aligned}$$

Correctnes:

$$g^r = g^{(x \cdot h + u) \bmod (p-1)} \bmod p = g^{xh} \cdot g^u = (g^x)^h \cdot g^u = a^h \cdot t_1$$

$$g^s = g^{(i \cdot h + v) \bmod (p-1)} \bmod p = g^{ih} \cdot g^v = (g^i)^h \cdot g^v = (D_{34\beta})^h \cdot t_2$$