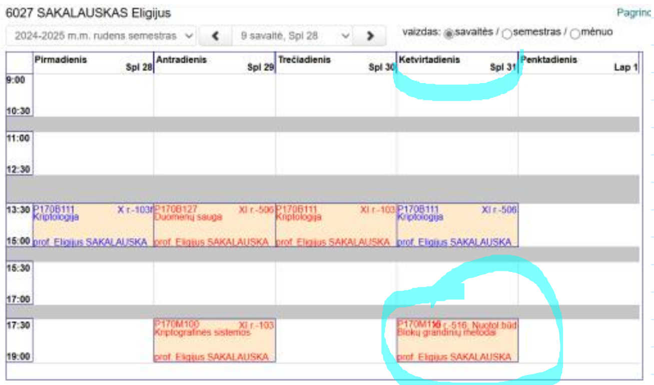
Koliokviumas: Ciphertexts equivqlency proof.
IV-nis, Spalio 31 d., 17:30, gyvai, 516a.



Confidential Verifiable Transactions - 5 **PP** = (*p*, *g*).

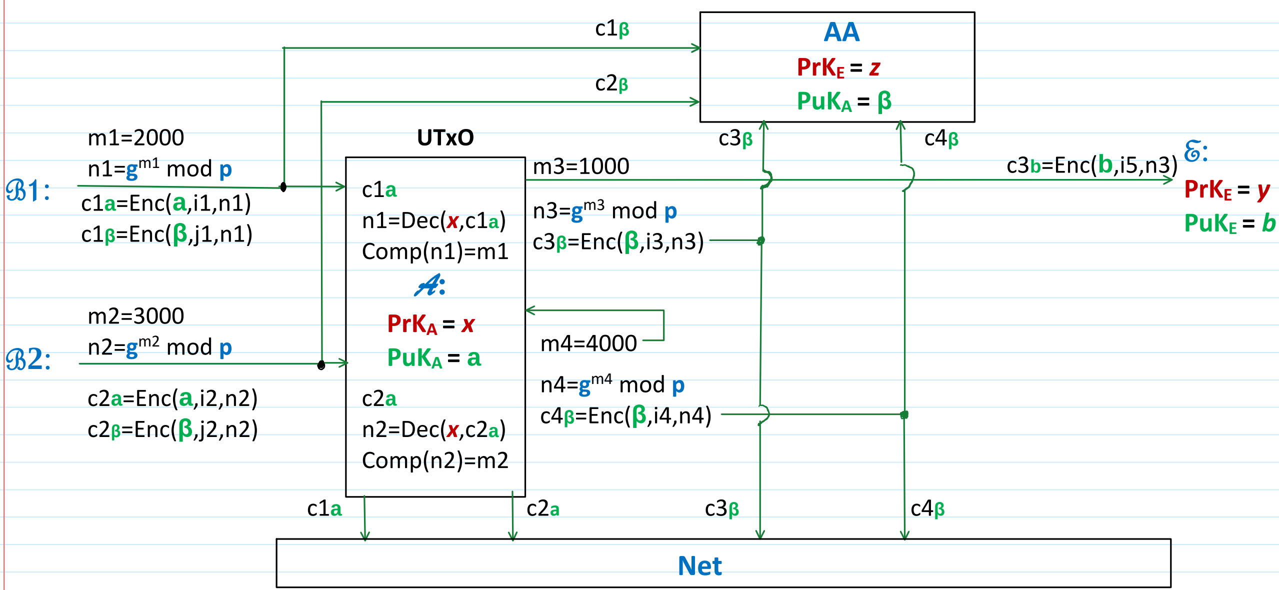
```
>> p=int64(268435019)
p = 268435019
>> g=2;
```

Declare **Public Parameters** to the network **PP** = (**p**, **g**); **p= 268435019**; **g=2;**

𝒜: PrKA = *x* <-- randi ==> PuKA = *a* = g^x mod p; AA: PrK_{AA} = *z* <-- randi ==> PuK_{AA} = *beta* = g^z mod p

```
>> x=int64(randi(p-1))
x = int64(220099152)
>> a=mod_exp(g,x,p)
a = 174059961
```

```
>> z=int64(randi(p-1))
z = int64(49750938)
>> beta=mod_exp(g,z,p)
beta = int64(213338364)
```



$$Enc(a, i_1, n_1) = c_{1a} = (E_{1a}, D_{1a}) = (n_1 \cdot a^{i_1}, g^{i_1}) \bmod p$$

$$Enc(a, i_2, n_2) = c_{2a} = (E_{2a}, D_{2a}) = (n_2 \cdot a^{i_2}, g^{i_2}) \bmod p$$

$$c_{1a} \cdot c_{2a} = c_{12a} = Enc(a, i_{12}, n_{12}) = (E_{12a}, D_{12a}) = (n_{12} \cdot a^{i_{12}}, g^{i_{12}}) = c_{12a}$$

$$i_{12} = (i_1 + i_2) \bmod (p-1)$$

$$n_{12} = n_1 \cdot n_2 \bmod p$$

C12a = (E12*a* mod *p* , D12*a* mod *p*)

C12a = (E1*a**E2*a* mod *p*, D1*a** D2*a* mod *p*)

$$Enc(\beta, i_3, n_3) = c_{3\beta} = (E_{3\beta}, D_{3\beta}) = (n_3 \cdot \beta^{i_3}, g^{i_3}) \bmod p$$
$$Enc(\beta, i_4, n_4) = c_{4\beta} = (E_{4\beta}, D_{4\beta}) = (n_4 \cdot \beta^{i_4}, g^{i_4}) \bmod p$$
$$c_{3\beta} \cdot c_{4\beta} = c_{34\beta} = Enc(\beta, i_{34}, n_{34}) = (E_{34\beta}, D_{34\beta}) = (n_{34} \cdot \beta^{i_{34}}, g^{i_{34}}) = C_{34\beta}$$
$$i_{34} = (i_3 + i_4) \bmod (p-1)$$
$$n_{34} = n_3 \cdot n_4 \bmod p$$

C34beta = (E34**beta** mod ***p*** , D34**beta** mod ***p***)

C34beta = (E3**beta***E3**beta** mod ***p***, D3**beta***D4**beta** mod ***p***)

If transaction balance is valid: $m_1 + m_2 = 2000 + 3000 = 1000 + 4000 = m_3 + m_4$

Then since: $n_{12} = n_1 \cdot n_2 = g^{m_1} \cdot g^{m_2} \bmod p = g^{m_1+m_2} \bmod p$

$n_{34} = n_3 \cdot n_4 = g^{m_3} \cdot g^{m_4} \bmod p = g^{m_3+m_4} \bmod p.$

$\Big\}\ n_{12} = n_{34} = n$

Incomes

```
>> m1=2000;
>> n1=mod_exp(g,m1,p)
n1 = 28125784
>> i1=int64(randi(p-1))
i1 = int64(207414820)
>> a_i1=mod_exp(a,i1,p)
a_i1 = 192148999
>> E1a=mod(n1*a_i1,p)
E1a = 207347548
>> D1a=mod_exp(g,i1,p)
D1a = 202537833
```

c1***a*** = (E1***a***, D1***a***)

Verification: Dec(***x***, c1***a***) = nn1

```
>> mx=mod(-x,p-1)
mx = 48335866
>> D1a_mx=mod_exp(D1a,mx,p)
D1a_mx = 75547583
>> nn1=mod(E1a*D1a_mx,p)
nn1 = 28125784
```

```
>> m2=3000;
>> n2=mod_exp(g,m2,p)
n2 = 222979214
>> i2=int64(randi(p-1))
i2 = int64(67446699)
>> a_i2=mod_exp(a,i2,p)
a_i2 = 211790072
>> E2a=mod(n2*a_i2,p)
E2a = 77938423
>> D2a=mod_exp(g,i2,p)
D2a = 82080815
```

c2***a*** = (E2***a***, D2***a***)

Verification: Dec(***x***, c2***a***) = nn2

```
>> mx=mod(-x,p-1)
mx = 48335866
>> D2a_mx=mod_exp(D2a,mx,p)
D2a_mx = 57701660
>> nn2=mod(E2a*D2a_mx,p)
nn2 = 222979214
```

```
>> E12a=mod(E1a*E2a,p)
E12a = 52532683
>> D12a=mod(D1a*D2a,p)
D12a = 32918394
```

C12a = (E12a, D12a)

C12a = (E1a*E2a, D1a* D2a)

Verification: Dec(***x***, c12***a***) = nn12

```
>> mx=mod(-x,p-1)
mx = 48335866
>> D12a_mx=mod_exp(D12a,mx,p)
D12a_mx = 253324389
>> nn12=mod(E12a*D12a_mx,p)
nn12 = 143845522
```

```
>> n12=mod(n1*n2,p)
n12 = 143845522
```

Expenses

```
>> m3=1000;
>> n3=mod_exp(g,m3,p)
n3 = 260099963
>> i3=int64(randi(p-1))
i3 = int64(137379932)
>> beta_i3=mod_exp(beta,i3,p)
beta_i3 = 14259017
>>  E3beta=mod(n3*beta_i3,p)
E3beta = 167897317
>> D3beta=mod_exp(g,i3,p)
```

```
>> m4=4000;
>> n4=mod_exp(g,m4,p)
n4 = 246637967
>> i4 = int64(randi(p-1))
i4 = int64(225960178)
>> beta_i4=mod_exp(beta,i4,p)
beta_i4 = 159771180
>> E4beta=mod(n4*beta_i4,p)
E4beta = 195130083
>>  D4beta=mod_exp(g,i4,p)
```

```
>> E34beta=mod(E3beta*E4beta,p)
E34beta = 57420210
>> D34beta=mod(D3beta*D4beta,p)
D34beta = 107062668
```

C34beta= (E34beta, D34beta)

C34beta=(E3beta*E3beta, D3beta, D4beta)

beta_i3 = 14259017
>> E3beta=mod(n3*beta_i3,p)
E3beta = 167897317
>> D3beta=mod_exp(g,i3,p)
D3beta = 65145889

Verification: Dec(*z*, c3**beta**) = nn3
>> mz=mod(-z,p-1)
mz = 218684080
>> D3beta_mz=mod_exp(D3beta,mz,p)
D3beta_mz = 258869169
>> nn3=mod(E3beta*D3beta_mz,p)
nn3 = 260099963

beta_i4 = 159771180
>> E4beta=mod(n4*beta_i4,p)
E4beta = 195130083
>> D4beta=mod_exp(g,i4,p)
D4beta = 229603826

Verification: Dec(*z*, c3**beta**) = nn3
>> mz=mod(-z,p-1)
mz = 218684080
>> D4beta_mz=mod_exp(D4beta,mz,p)
D4beta_mz = 218460911
>> nn4=mod(E4beta*D4beta_mz,p)
nn4 = 246637967

C34beta=(E3beta*E3beta, D3beta, D4beta)

Verification: Dec(*z*, c34***beta***) = nn34

>> mz=mod(-z,p-1)

>> D34beta_mz=mod_exp(D34beta,mz,p)
D34beta_mz = 169945498
>> nn34=mod(E34beta*D34beta_mz,p)
nn34 = 143845522

>> n34=mod(n3*n4,p)
n34 = 143845522

>> nn12=mod(nn1*nn2,p)
nn12 = **143845522**

n12 = **n** = n34 = **143845522**

>> nn34=mod(nn3*nn4,p)
nn34 = **143845522**

$\mathcal{A}$: must prove to the net, that $c_{12\alpha}$ and $c_{34\beta}$ encrypted the same value $n_{12} = n_{34} = n$; ⟶ Ciphertexts Equivalency Proof.

The statement St for this proof is the following:

$$St = \{c_{12\alpha}, c_{34\beta}, \alpha, \beta\};$$ For example: $\alpha = g^x \bmod p$

$PuK = \alpha$ is a statement for x.

For proof $\mathcal{A}$ randomly generates integers u, v and $(-v) \bmod (p-1)$

$u \leftarrow randi(\mathcal{I}_{p-1})$; $\mathcal{I}_{p-1} = \{0, 1, 2, ..., p-2\}$

$v \leftarrow randi(\mathcal{I}_{p-1})$

$-v \bmod (p-1)$ ⟶ >> mv = mod(-v, p-1)

>> u = int64(randi(p-1))
u = 234711265
>> v=int64(randi(p-1))
v = 223454508
>> mv=mod(-v,p-1)
mv = 44980510

1. The following commitments $\{t_1, t_2, t_3\}$ are computed:

$t_1 = g^u \bmod p$

$t_2 = g^v \bmod p$

$t_3 = (D_{12\alpha})^u \cdot \beta^{-v} \bmod p$

>> t1=mod_exp(g,u,p)
t1 = 160710747
>> t2=mod_exp(g,v,p)
t2 = 131605032

>> D12a_u=mod_exp(D12a,u,p)
D12a_u = 46284380
>> beta_mv=mod_exp(beta,mv,p)
beta_mv = 81562027
>> t3=mod(D12a_u*beta_mv,p)
t3 = **8217992**

2. The following h-value is computed using secure h-function H:

$$h = H(\alpha \| \beta \| t_1 \| t_2 \| t_3)$$

α β t_1 t_2 t_3 t3 = **8217992**

>> hsymb='174059961||213338364||160710747||131605032||202608126' % t3 in hsymb is incorrect
hsymb = 174059961||213338364||160710747||131605032||202608126
>> h=hd28(hsymb)
h = 264802094

% leave this h=264802094
% for further computations

3. A having her PrK = x and $i_{34} = (i_3 + i_4) \bmod (p-1)$ computes r and s

$$r = (x \cdot h + u) \bmod (p-1)$$

$$s = (i_{34} \cdot h + v) \bmod (p-1)$$

```
>> xh=mod(x*h,p-1)
xh = 2537232
>> r=mod(xh+u,p-1)
r = 237248497

>> i3
i3 = 137379932
>> i4
i4 = 225960178
>> i34=mod(i3+i4,p-1)
i34 = 94905092

>> i34h=mod(i34*h,p-1)
i34h = 50935534
>> s=mod(i34h+v,p-1)
s = 5955024
```

A: declares the following set of data to the Net

$$\{c_{1a}, c_{2a}, c_{3\beta}, c_{4\beta}\} \cup \{a, \beta, t_1, t_2, t_3, r, s\} \longrightarrow \text{Net}$$

Net computes

$$c_{12a} = c_{1a} * c_{2a} \qquad c_{34\beta} = c_{3\beta} * c_{4\beta}$$

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

$$(E_{12a} = n_{12} \cdot a^{i_{12}}, D_{12} = g^{i_{12}})$$

$$c_{34\beta} = (E_{3\beta} \cdot E_{4\beta}, D_{3\beta} \cdot D_{4\beta})$$

$$(E_{34\beta} = n_{34} \cdot \beta^{i_{34}}, D_{34\beta} = g^{i_{34}})$$

Net verifies transaction correctness by verifying the following identities

$g^r = a^h \cdot t_1 \bmod p$ // A proves that she knows her PrK = x

$g^s = (D_{34\beta})^h \cdot t_2 \bmod p$ // A proves that she knows her random parameter i_{34} used for encryption

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

$$g^s = g^{i34*h+v} = g^{i34*h} \cdot g^v = (g^{i34})^h \cdot g^v = (D_{34\beta})^h \cdot t_2 \bmod p;$$

$$(E_{34\beta})^h \cdot (E_{12a})^{-h} \cdot (D_{12a})^r \cdot \beta^{-s} = t_3 \bmod p$$

A proves that based on her knowledge of x and i_{34} the ciphertexts c_{12a} and $c_{34\beta}$ are equivalent.

$(E_{34\beta})^h = (n34 \cdot \beta^{i34})^h = (n34)^h \cdot \beta^{i34*h}.$

$(E_{12a})^{-h} = (n12 \cdot a^{i12})^{-h} = (n12)^{-h} \cdot a^{-(i12*h)} \bmod p;$

$(D_{12a})^r = (g^{i12})^r = (g^{i12*x*h+i12*u}) = (g^x)^{i12*h} \cdot (g^{i12})^u = a^{h*i12} \cdot (g^{i12})^u = a^{i12*h} \cdot (D_{12a})^u \bmod p;$

$\beta^{-s} = \beta^{-i34*h-v} = \beta^{-i34*h} \cdot \beta^{-v} = \beta^{-i34*h} \cdot \beta^{-v} \bmod p;$

$$(E_{34\beta})^h \quad \cdot \quad (E_{12a})^{-h} \quad \cdot \quad (D_{12a})^r \quad \cdot \quad \beta^{-s} \quad \text{mod } p ===$$

$$=== (n34)^h \cdot \beta^{i34*h} \quad \cdot \quad (n12)^{-h} \cdot a^{-(i12*h)} \quad \cdot \quad a^{i12*h} \cdot (D_{12a})^u \quad \cdot \quad \beta^{-i34*h} \cdot \beta^{-v} \quad \text{mod } p ===$$

If balance equation is valid, then $n34 = n12 = n$ mod p then $(n34)^h \cdot (n12)^{-h} = n^h \cdot n^{-h} = 1$ mod p.

$$=== (n34)^h \cdot (n12)^{-h} \cdot (D_{12a})^u \cdot \beta^{-v} \text{ mod } p \;===$$

$$=== \quad 1 \quad \cdot (D_{12a})^u \cdot \beta^{-v} \;===\; (D_{12a})^u \cdot \beta^{-v} = t_3.$$

Net

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

$$\{C_{1a}, C_{2a}, C_{3\beta}, C_{4\beta}\} \cup \{a, \beta, t_1, t_2, t_3, r, s\}$$

$$g^r = g^{xh+u} = g^{xh} \cdot g^u = (g^x)^h \cdot g^u = a^h \cdot t_1 \text{ mod } p;$$

$$g^s = g^{i34*h+v} = g^{i34*h} \cdot g^v = (g^{i34})^h \cdot g^v = (D_{34\beta})^h \cdot t_2 \text{ mod } p;$$

$$(E_{34\beta})^h \cdot (E_{12a})^{-h} \cdot (D_{12a})^r \cdot \beta^{-s} = t_3 \text{ mod } p$$

```
>> h = int64(264802094)
h = 264802094
>> mh=mod(-h,p-1)
mh = 3632924
>> beta = int64(213338364)
beta = 213338364
>> r = int64(237248497)
r = 237248497
>> s = int64(5955024)
s = 5955024
>> ms=mod(-s,p-1)
ms = 262479994
```

```
>> E34beta = int64(57420210)
E34beta = 57420210

>> E12a = int64(52532683)
E12a = 52532683
>> D12a = int64(32918394)
D12a = 32918394
```

```
> t1 = int64(160710747)
t1 = 160710747
>> t2 = int64(131605032)
t2 = 131605032
>> t3=mod(D12a_u*beta_mv,p)
t3 = 8217992
```

```
>> E34beta_h=mod_exp(E34beta,h,p)
E34beta_h = 187587888
>> E12a_mh=mod_exp(E12a,mh,p)
E12a_mh = 166027856
Ver1=mod(E34beta_h*E12a_mh,p)
Ver1 = 137483493
```

```
>> D12a_r=mod_exp(D12a,r,p)
D12a_r = 81546199
>> beta_ms=mod_exp(beta,ms,p)
beta_ms = 104897990
>> Ver2=mod(D12a_r*beta_ms,p)
Ver2 = 179105215
```

```
>> Ver=mod(Ver1*Ver2,p)
Ver = 8217992
```

Bobs actions

B1			B2
		C_{1a}	
$m_1 = \ldots$	$n_1 = \ldots$	E_{1a} D_{1a}	

Alice actions

$Dec(x, C_1a)$ $Dec(x, C_2a)$ $m_3 = \ldots$ $n_3 = \ldots$ $Enc(\beta, n_1)$ $Enc(\beta, n_2)$

$C_3\beta$ $C_4\beta$

$E_3\beta$ $D_3\beta$ $E_4\beta$ $D_4\beta$

The correctness of (30), (31) is proved by the following identities:

$$g^r = g^{xh+u} = g^{xh} \cdot g^u = (g^x)^h \cdot g^u = a^h \cdot t_1; \quad (33)$$

$$g^s = g^{lh+v} = g^{lh} \cdot g^v = (g^l)^h \cdot g^v = (\delta_{\beta,E})^h \cdot t_2. \quad (34)$$

The correctness of (32) is proved by considering every multiplier separately:

$$(\varepsilon_{\beta,E})^h = (E \cdot \beta^l)^h = E^h \cdot \beta^{lh}; \quad (35)$$

$$(\varepsilon_{a,I})^{-h} = (I \cdot a^k)^{-h} = I^{-h} \cdot a^{-kh}; \quad (36)$$

$$(\delta_{a,I})^r = (g^k)^r = (g^{kxh+ku}) = (g^x)^{hk} \cdot (g^k)^u = a^{hk} \cdot (g^k)^u = a^{hk} \cdot (\delta_{a,I})^u; \quad (37)$$

$$\beta^{-s} = \beta^{-lh-v} = \beta^{-lh} \cdot \beta^{-v}. \quad (38)$$

Notice that k is not known to Alice and is included in $(\delta_{a,I})$. If the transaction is honest, then the transaction balance (1) is satisfied and $I=E$ since. Then $E^h \cdot I^{-h} = 1 \bmod p$, and putting it all together, we obtain:

$$E^h \cdot \beta^{lh} \cdot I^{-h} \cdot a^{-kh} \cdot a^{hk} \cdot (\delta_{a,I})^u \cdot \beta^{-lh} \cdot \beta^{-v} = (\delta_{a,I})^u \cdot \beta^{-v} = t_3. \quad (39)$$

This is the proof to the Net that the balance equation (1) is valid.