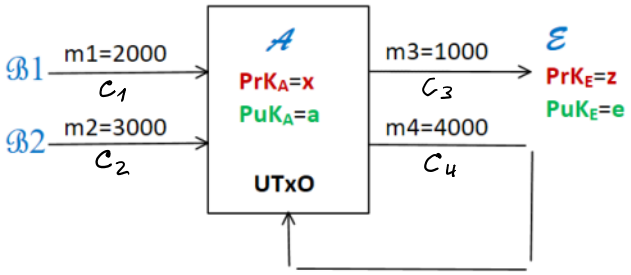
Zero Knowledge Proof (ZKP) of equivalence of 2 ciphertexts *c*3, *c*3*e* corresponding to the same plaintext *m* obtained by encryption with different Puks



How to provide anonymity of transaction amounts and to verify the **balance**: **m1+m2 = m3+m4** ?

n1= g^{m1} mod **p** **n3**= g^{m3} mod **p**

n2= g^{m2} mod **p** **n4**= g^{m4} mod **p**

If **(m1+m2) mod (p -1) = (m3+m4) mod (p-1)**,
Then **(n1*n2) mod p = (n3*n4) mod p**.

```
n1=mod_exp(g,m1,p)
n2=mod_exp(g,m2,p)
```

$n_1 \cdot n_2 \bmod p = g^{m_1+m_2} \bmod p$ $\quad n_3 \cdot n_4 = g^{m_3+m_4} \bmod p$

If $n_1 \cdot n_2 \bmod p = n_3 \cdot n_4 \bmod p$

$c_1 \cdot c_2 = c_3 \cdot c_4$

$c_1 = Enc(a, i_1, n_1) = (E_1, D_1)$ $\quad c_3 = Enc(a, i_3, n_3) = (E_3, D_3)$

$c_2 = Enc(a, i_2, n_2) = (E_2, D_2)$ $\quad c_4 = Enc(a, i_4, n_4) = (E_4, D_4)$

$in_1 = int64(randi(p-1))$

$in_2 = int64(randi(p-1))$

$E_1 = n_1 \cdot a^{in_1} \bmod p;$ ⟶ $a\_in_1 = mod\_exp(a, in_1, p)$

$D_1 = g^{in_1} \bmod p;$ $\quad E1 = mod(n1 * a\_in1, p)$

$D_1 = mod\_exp(g, in1, p)$

Su.Name	m1	m2	n1	n2	in1	in2	Enc(a,n1)	Enc(a,n2)	in1, cn1	inn2, cn2
							cn1	cn2	To: list.number	To: list.number
Be.Antanas										
Bu.Laurynas										
Bu.Karolis										
Če.Martynas										
Kv.Justas										
Kv.Tomas										
Ma.Povilas										
St.Tautvydas										
Tr.Kristupas										
p	26843 5019									

g	2									
PrK=x	88637397									
PuK=a	71787401									

$Enn1 * Enn2 \bmod p$

$Dec(x, cnn1) = Enn1 * (Dnn1)^{-x} \bmod p = nn1;$

$D^{-x} = (D^{-1})^{x} \bmod p$

```
>> Dnn1_m1 = mulinv(Dnn1, p)
>> mod(Dnn1_m1 * Dnn1, p) = 1
>> Dnn1_mx = mod_exp(Dnn1_m1, x, p)
>>  nn1 = mod(Enn1 * Dnn1_mx, p)
```

		inn1, cn1	inn2, n	From. actual	From. actual	From. actual	From. actual	Enn1*Enn2	Dec(x,cnn1)	Dec(x,cnn2)	nn1*nn2
		From: list. number	From: list. number	inn1	inn1	cnn1	cnn2				
6	Be.Antanas										
7	Bu.Laurynas										
8	Bu.Karolis										
9	Če.Martynas										
10	Kv.Justas										
11	Kv.Tomas										
12	Ma.Povilas										
13	St.Tautvydas										
14	Tr.Kristupas										

```
>> in3 = int64(randi(p-1))
>> in4 = (inn1+inn2-in3) mod (p-1)
```

$\Rightarrow (inn1 + inn2) \bmod (p-1) = (in3 + in4) \bmod (p-1).$

$Enc(a, in_3, n_3) = (E_3, D_3)$

$E_3 = n_3 * a^{in3} \bmod p$ $\quad E_4 = n_4 * a^{in4} \bmod p$

$D_3 = g^{in_3} \bmod p$ $\quad D_3 = g^{in4} \bmod p$

		m3	m4	n3	n4	in3	in4	Enc(a,n3)	Enc(a,n4)	cn3	cn4	cn3*cn4
								cn3	cn4	To-From-list.	To-From-list.	

										number	number	
6	Be.Antanas											
7	Bu.Laurynas											
8	Bu.Karolis											
9	Če.Martynas											
10	Kv.Justas											
11	Kv.Tomas											
12	Ma.Povilas											
13	St.Tautvydas											
14	Tr.Kristupas											