https://docs.google.com/spreadsheets/d/15AqiZvP9TEg8qaJ9OocOTS9aqyOkg3G4/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

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

>> x=int64(170325760)
x = 170325760
>> a=mod_exp(g,x,p)
a = 8239057

>> z=int64(90521943)
z = 90521943
>> A=mod_exp(g,z,p)
A = 268254303

Op. simboliniame pavidale: pakartoti.

			123456789	123456789	123456789	123456789				
							Enc(a,i1,n1)=(Ean1,Dan1)=Can1		Enc(a,i2,n2)=(Ean2,Dan2)=Can2	
Nr.	m1	m2	n1	n2	i1	i2	Ean1	Dan1	Ean2	Dan2
1	2000	3000	28125784	222979214	148308050	72210493	200625217	52535541	124804048	201744006
2	6000	3000	236183964	222979214	109472856	97125717	143868972	193531382	175024019	232629344
3	3000	5000	222979214	143845522	177544488	52810116	249983456	120274163	116189367	188122293
4	5000	2000	143845522	28125784	92888439	147727088	254438923	129363870	126782285	62615199
5	4000	2000	246637967	28125784	223263092	66296785	160789822	16321949	70874947	253676820
6	3000	4000	222979214	246637967	135084189	69568274	7752656	258664479	29438928	38252554
7	1000	4000	260099963	246637967	237364983	2230566	58748673	261811191	30578219	87872122
8	2000	5000	28125784	143845522	142568382	255161473	180231637	130726569	29985812	75958809
9	2000	4000	28125784	246637967	255089090	255790067	14042424	129417439	41028941	259091349

			123456789	123456789				123456789	123456789		
	Can1*Can2=Can12		Enc(a,j1,i1)=(Eai1,Dai1)=Cai1								
Nr.	Ean1*Ean2=Ean12	Dan1*Dan2=Dan12	Eai1	Dai1	Eai2	Dai2		Dec(x,Can1)	Dec(x,Can2)	m1	m2
1	175453592	48312418	251905498	40270879	38288929	44403423	1	28125784	222979214		
2	206344988	205788087	44105851	17906247	100216034	62108827	2	236183964	222979214		
3	181434247	214130430	31316867	127216070	15627351	139685459	3	222979214	143845522		
4	180502841	190596808	24097221	26548892	86784264	229018399	4	143845522	28125784		
5	3565480	8804970	132436059	234550569	187795354	228907772	5	246637967	28125784		
6	254633531	141999977	91638180	2330131	116823325	174872029	6	222979214	246637967		
7	96445960	245489855	32671915	137646849	154195718	106589198	7	260099963	246637967		
8	214972985	79496377	138188980	249012243	84959486	252856422	8	28125784	143845522		
9	214858037	151754215	201928165	215589863	185079007	23230511	9	28125784	246637967		

B1 : $m_1 = 2000 \rightarrow n_1 = g^{m_1} \bmod p$

$i_1 \leftarrow randi \rightarrow Enc(a, i_1, n_1) = Can1 = (Ean1, Dan1)$

$j_1 \leftarrow randi \rightarrow Enc(a, j_1, i_1) = Cai1 = (Eai1, Dai2)$

$i_1 \leftarrow randi \rightarrow Enc(a, i_1, n_1) = can_1 = (Ean_1, Dan_1)$

$j_1 \leftarrow randi \rightarrow Enc(a, j_1, i_1) = cai_1 = (Eai_1, Dai_2)$

B2: $m_2 = 3000 \rightarrow n_2 = g^{m_2} \bmod p$

$i_2 \leftarrow randi \rightarrow Enc(a, i_2, n_2) = can_2 = (Ean_2, Dan_2)$

$j_2 \leftarrow randi \rightarrow Enc(a, j_2, i_2) = cai_2 = (Eai_2, Dai_2)$

A: $Dec(X, can_1) = Ean_1 * (Dan_1)^{-X} = nn1 == n1$

Verifies if $n_1 = g^{m_1} \bmod p$ by scaning over possible values of m_1

$Dec(X, cai_1) = Eai_1 * (Dai_1)^{-X} = ii_1 == i_1$

$Dec(X, can_2) = Ean_2 * (Dan_2)^{-X} = nn_2 == n_2$

Verifies if $n_2 = g^{m_2} \bmod p$ by scaning over possible values of m_2.

$Dec(X, cai_2) = Eai_2 * (Dai_2)^{-X} = ii_2 == i_2$

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**.

A: makes her expenses $m_3 = 1000$ and $m_4 = 4000$ and declares m_3, m_4 to Audit Authority (AA) by encrypting n_3, n_4 with AA public key $PuK_{AA} = A$: **A** = 268254303

A: by having i_1, i_2 computes $(i_1 + i_2) \bmod (p-1) = i$

$i_3 \leftarrow randi \rightarrow i_4 = (i - i_3) \bmod (p-1)$.

$(i_1 + i_2) \bmod (p-1) = (i_3 + i_4) \bmod (p-1) = i$

A: $Enc(A, i_3, n_3) = CAn_3 = (EAn3, DAn3)$

$Enc(A, i_4, n_4) = CAn_4 = (EAn4, DAn4)$

Net: data $PuK_A = a$ & $PuK_{AA} = A$.

B1 → A B2 → A A → AA A → AA

$can_1 = (Ean_1, Dan_1)$; $can_2 = (Ean_2, Dan_2)$ $CAn_3 = (EAn_3, DAn_3)$; $CAn_4 = (EAn_4, DAn_4)$

$can_1 * can_2 = (Ean_1 * Ean_2, Dan_1 * Dan_2)$ $(CAn_3 * CAn_4) =$

$can_1 * can_2 = (Ean_1 * Ean_2 ,\ Dan_1 * Dan_2)$ $(CAn_3 * CAn_4) =$

$can_{12} = (Ean_{12} ,\ Dan_{12}) = (EAn_3 * EAn_4 ,\ DAn_3 * DAn_4)$

$(EAn_{34} ,\ DAn_{34})$

$Ean_{12} = Ean_1 * Ean_2 =$

$= n_1 * a^{i_1} * n_2 a^{i_2} \bmod p =$

$= n_1 * n_2 \, a^{i_1} a^{i_2} \bmod p =$

$= n_{12} \, a^{i_1 + i_2 \bmod (p-1)} \bmod p =$

$= n_{12} \, a^{i} \bmod p$

$EAn_{34} = EAn_3 * EAn_4 =$

$= n_3 * A^{i_3} * n_4 * A^{i_4} \bmod p =$

$= n_3 * n_4 * A^{i_3} A^{i_4} \bmod p =$

$= n_{34} * A^{i_3 + i_4 \bmod (p-1)} \bmod p =$

$= n_{34} * A^{i} \bmod p$

$r \leftarrow randi(\mathcal{I}_p^*)$; $\mathcal{I}_p^* = \{1, 2, 3, \ldots, p-1\}$; $* \bmod p$; $/ \bmod p$

$u = g^r \bmod p$; $v = \left(\frac{a}{e}\right)^r \bmod p$.

$h = H(u \| v)$

$w = (i_3 \cdot h + r) \bmod (p-1)$ $\xrightarrow[a, e]{u, v, w}$ Net : $h = H(u \| v)$

Ver1 : $g^w = (D_3)^h \cdot u \bmod p =$

Ver2 : $\left(\frac{a}{e}\right)^w = \left(\frac{E_3}{E_{3e}}\right)^h \cdot v \bmod p =$

Correctness:

Ver1 : $g^w = g^{(i_3 \cdot h + r) \bmod (p-1)} \bmod p = (g^{i_3})^h \cdot g^r \bmod p = (D_3)^h \cdot u \bmod p.$

Ver2 : $\left(\frac{a}{e}\right)^w \bmod p = \left(\frac{a}{e}\right)^{(i_3 \cdot h + r) \bmod (p-1)} \bmod (p-1) =$

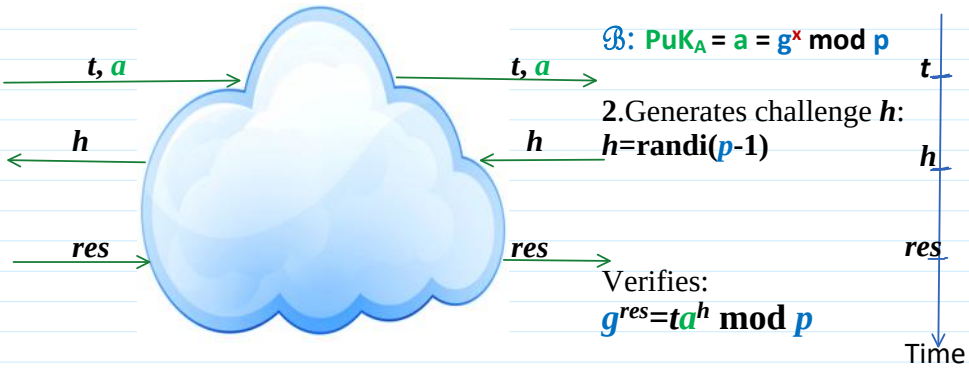
$= \left(\frac{a}{e}\right)^{i_3 \cdot h} \cdot \left(\frac{a}{e}\right)^r \bmod p = \left(\frac{a^{i_3}}{e^{i_3}}\right)^h \cdot v \bmod p =$

$= \left(\frac{n_3 a^{i_3}}{n_3 e^{i_3}}\right)^h \cdot v \bmod p = \left(\frac{E_3}{E_{3e}}\right)^h \cdot v \bmod p.$

Schnorr Identification: Zero Knowledge Proof - ZKP

Schnorr Id scenario: **Alice** wants to prove **Bank** that she knows her Private Key - $PrK_A = x$ which corresponds to her Public Key - $PuK_A = a = g^x \bmod p$ not revealing $PrK_A = x$.

𝒜: ZKP of knowledge x:
$PrK_A = x =$ **randi(p-1)**
$PuK_A = a = g^x \bmod p$
1.Computes commitment ***t*** for ***i***:
i=randi(p-1)
$t=g^i \bmod p$
3.Computes response ***res***:
$res=i+xh \bmod (p-1)$



Correctness:
$g^{res} \bmod p = g^{i+xh} \bmod p = g^i g^{xh} \bmod p = t(g^x)^h \bmod p = ta^h \bmod p$.

𝒜: ⟶ ***Net***