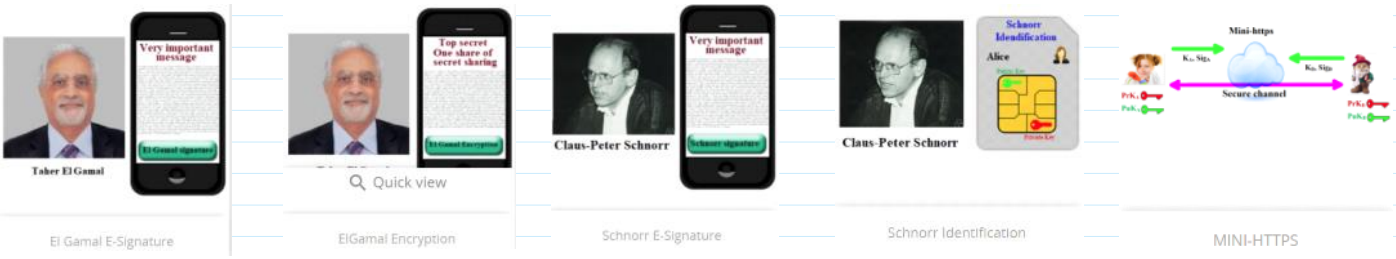
Egzaminas Pram. Pr. 20-327: Birželio 17 d. 10:50
https://imimsociety.net/en/14-cryptography
https://imimschool.net/index.php?id_category=14&controller=category&id_lang=1



UTxO blockchain to provide confidentiality and verifiability of transferred money amounts.

Public Parameters PP = (p, g); p=268435019; g=2;

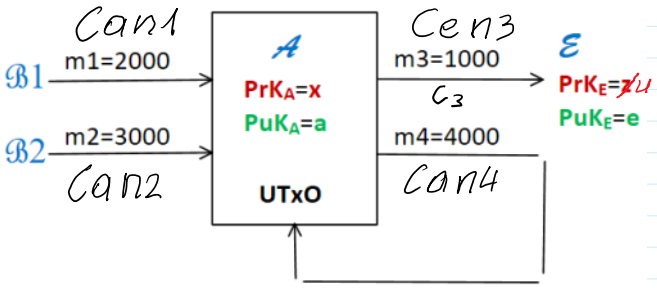
$\mathcal{A}$ - Alice: PrK_A=x, PuK_A=a.

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

$\mathcal{AA}$ - Audit Authority: PrK_{AA}=z, PuK_{AA}=A.

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

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** 1-to-1 function

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**.

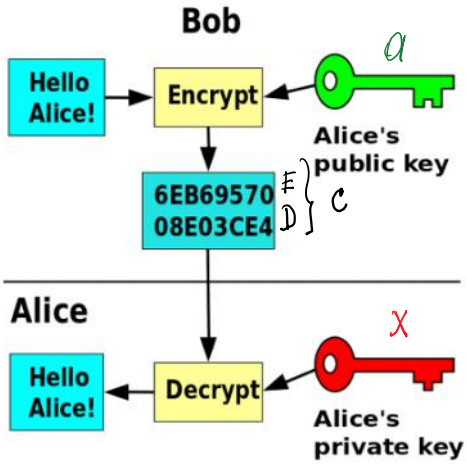
$n_1 \cdot n_2 \bmod p = g^{m_1+m_2 \bmod (p-1)} \bmod p$ $\quad n_3 \cdot n_4 = g^{m_3+m_4 \bmod (p-1)} \bmod p$

If $m_1+m_2 \bmod (p-1) = m_3+m_4 \bmod (p-1)$

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

ElPublic and Private keys generation
PrK_A = ***x*** = randi(***p***-1).
PuK_A = ***a*** = g^x mod ***p***.

ElGamal Encryption - Decryption
c=Enc(PuK_A, m)=(E,D)
m=Dec(PrK_A, c)



$\mathcal{B}$: intends to encrypt message M to $\mathcal{A}$.

$F_{encod}(M) = m$

$m \in Z_p^* = \{1, 2, 3, \dots, p-1\}$; $i \xleftarrow{rand} Z_{p-1}$

$Enc(a, i, m) = Cam = (Eam, Dam)$

$Eam = m \cdot a^i \bmod p$; $Dam = g^i \bmod p$.

$\mathcal{B}$: $Cam = (Eam, Dam)$ → $\mathcal{A}$: $PrK_A = (x)$ Decrypts Cam with x.

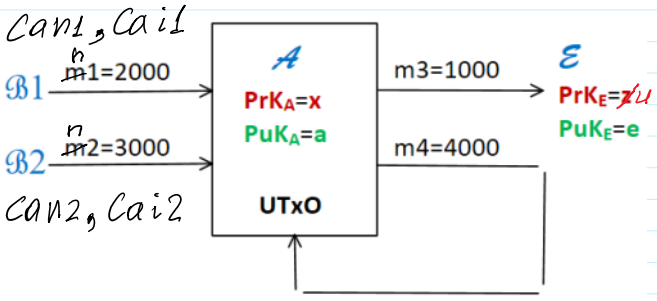
1. $(Dam)^{-x \bmod (p-1)} \bmod p$

2. $m = Eam * (Dam)^{-x} \bmod p = m * a^r * g^{-rx} =$

$= m * (g^x)^r * g^{-rx} \bmod p =$

$= m * g^{xr} * g^{-xr} \bmod p = m.$

```
>> mx=mod(-x,p-1)
mx = 98109258
>> mod(x+mx,p-1)
ans = 0
```



$\mathcal{B}1$: i1 = randi(**p**-1)
Enc(**a**, i1, **n1**) = Can1
Ean1= n1*$\mathbf{a}^{i1}$ mod **p**
Dan1= $\mathbf{g}^{i1}$ mod **p**
Can1=(Ean1,Dan1)

j1 = randi(**p**-1)
Enc(**a**, j1, **i1**) = Cai1
j1 = randi(**p**-1)
Eai1= i1*$\mathbf{a}^{j1}$ mod **p**
Dai1= $\mathbf{g}^{j1}$ mod **p**
Cai1=(Eai1,Dai1)

$\mathcal{B}2$: i2 = randi(**p**-1)
Enc(**a**, i2, **n2**) = Can2
E2= n2*$\mathbf{a}^{i2}$ mod **p**
D2= $\mathbf{g}^{i2}$ mod **p**
Can2=(Ean2,Dan2)

j2 = randi(**p**-1)
Enc(**a**, j2, **i2**) = ci2
Ei2= i2*$\mathbf{a}^{j2}$ mod **p**
Di2= $\mathbf{g}^{j2}$ mod **p**
Cai2=(Eai2,Dai1)

Ex. $27 \bmod 54 = 27$

$= m * g^0 \bmod p = m \bmod p = m$

Ex. $27 \bmod 54 = 27$

$27 \bmod 23 = 4 \neq 27$

$= m * g^0 \bmod p = m \bmod p = m$

since $1 < m < p$

```
>> m1=2000;
>> m2=3000;
>> m12=m1+m2
m12 = 5000

>> nn12=mod_exp(g,m12,p)
nn12 = 143845522
```

```
>> n1=mod_exp(g,m1,p)
n1 = 28125784
>> n2=mod_exp(g,m2,p)
n2 = 222979214

>> n12=mod(n1*n2,p)
n12 = 143845522
>> nn12=mod_exp(g,m1+m2,p)
nn12 = 143845522
```

```
>> i1=int64(148308050)
i1 = 148308050
>> a_i1=mod_exp(a,i1,p)
a_i1 = 124551071
>> Ean1=mod(n1*a_i1,p)
Ean1 = 194643296
>> Dan1=mod_exp(g,i1,p)
Dan1 = 52535541
```

```
>> i2=int64(72210493)
i2 = 72210493
>> a_i2=mod_exp(a,i2,p)
a_i2 = 235524548
>> Ean2=mod(n2*a_i2,p)
Ean2 = 234318333
>> Dan2=mod_exp(g,i2,p)
Dan2 = 201744006
```

$(Dan1)^x \cdot (Dan1)^{-x} \bmod p = 1$

$\frac{(Dan1)^x}{(Dan1)^x} \bmod p = 1$

Decryption of Can1=(Ean1,Dan1):

```
>> Dan1_mx=mod_exp(Dan1,mx,p)
Dan1_mx = 110813605
>> Dan1_x=mod_exp(Dan1,x,p)
Dan1_x = 124551071
>> Dan1_xDan1_mx=mod(Dan1_x*Dan1_mx,p)
Dan1_xDan1_mx = 1

>> nn1=mod(Ean1*Dan1_mx,p)
nn1 = 28125784
```

			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	194643296	52535541	234318333	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

```
>> mx=mod(-x,p-1)
mx = 98109258
>> mod(x+mx,p-1)
ans = 0
```

```
>> Dan1_mx=mod_exp(Dan1,mx,p)
Dan1_mx = 110813605
>> Dan1_x=mod_exp(Dan1,x,p)
Dan1_x = 124551071
>> Dan1_xDan1_mx=mod(Dan1_x*Dan1_mx,p)
Dan1_xDan1_mx = 1

>> nn1=mod(Ean1*Dan1_mx,p)
```

```
>> Dan2_mx=mod_exp(Dan2,mx,p)
Dan2_mx = 148593508

>> nn2=mod(Ean2*Dan2_mx,p)
nn2 = 222979214
```

>> nn1=mod(Ean1*Dan1_mx,p)
nn1 = 28125784

>> nn2=mod(Ean2*Dan2_mx,p)
nn2 = 222979214

			1234567890	1234567890	1234567890	1234567890			
	Can1*Can2=Can12			Enc(a,j1,i1)=(Eai1,Dai1)=Cai1			Enc(a,j2,i2)=(Eai2,Dai2)=Cai2		
Nr.	Ean1*Ean2=Ean12	Dan1*Dan2=Dan12	j1	Eai1	Dai1	j2	Eai2	Dai2	
1	211462699	48312418	97428832	165277205	214402638	7862004	209474480	139926535	1
2	206344988	205788087		44105851	17906247		100216034	62108827	2
3	181434247	214130430		31316867	127216070		15627351	139685459	3
4	180502841	190596808		24097221	26548892		86784264	229018399	3
5	3565480	8804970		132436059	234550569		187795354	228907772	5
6	254633531	141999977		91638180	2330131		116823325	174872029	6
7	96445960	245489855		32671915	137646849		154195718	106589198	7

>> j1=int64(randi(p-1))
j1 = 97428832
>> a_j1=mod_exp(a,j1,p)
a_j1 = 29948619
>> Eai1=mod(i1*a_j1,p)
Eai1 = 165277205

>> Dai1=mod_exp(g,j1,p)
Dai1 = 214402638

>> j2=int64(randi(p-1))
j2 = 7862004
>> a_j2=mod_exp(a,j2,p)
a_j2 = 118699749
>> Eai2=mod(i2*a_j2,p)
Eai2 = 209474480

>> Dai2=mod_exp(g,j2,p)
Dai2 = 139926535

>> mx
mx = 98109258

>> Dai1_mx=mod_exp(Dai1,mx,p)
Dai1_mx = 237356214
>> ii1=mod(Eai1*Dai1_mx,p)
ii1 = 148308050

>> Dai2_mx=mod_exp(Dai2,mx,p)
Dai2_mx = 247946579
>> ii2=mod(Eai2*Dai2_mx,p)
ii2 = 72210493

>> i1pi2=mod(i1+i2,p-1)
i1pi2 = 220518543

	1234567890	1234567890			1234567890	1234567890	1234567890	1234567890	1234567890	
	Dec(x,Can1)	Dec(x,Can2)	m1	m2	Dec(x,Cai1)	Dec(x,Cai2)	i1	i2	i1+i2 mod(p-1)	Nr.
1	28125784	222979214	2000	3000	148308050	72210493	148308050	72210493	220518543	1
2	236183964	222979214								2
3	222979214	143845522								3
3	143845522	28125784								4
5	246637967	28125784								5
6	222979214	246637967								6
7	260099963	246637967								7

>> m3=1000;
>> m4=4000;

>> n3=mod_exp(g,m3,p)
n3 = 260099963
>> n4=mod_exp(g,m4,p)
n4 = 246637967

>> i3=int64(randi(p-1))
i3 = 28525739
>> i4=mod(i1+i2-i3,p)
i4 = 191992804

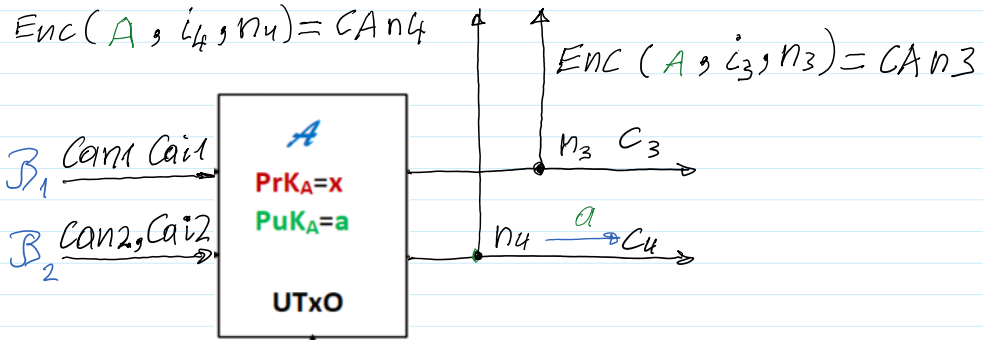
>> mod(i1+i2,p-1)
ans = 220518543
>> mod(i3+i4,p-1)
ans = 22051854
>> i=ans

i = 220518543

A: 1) after decryption Cai1, Cai2 finds i_1, i_2
2) finds $i_1 + i_2 \mod (p-1)$
3) generates at random $i_3 \leftarrow randi$
4) computes $i_4 = i_1 + i_2 - i_3 \mod (p-1)$
5) assigns $i = i_1 + i_2 \mod (p-1) = i_3 + i_4 \mod (p-1)$
6) computes EAn3 with random int. i_3
7) computes DAn3 with random int. i_4

AA - Audit Authority: $PrK_{AA}=z$, $PuK_{AA}=A$.

>> z=int64(randi(p-1))
z = 168034742
>> A=mod_exp(g,z,p)
A = 258784798



>> z
z = 90521943

>> A
A = 268254303

>> mz=mod(-z,p-1)
mz = 177913075

>> A_i3=mod_exp(A,i3,p)
A_i3 = 210678746
>> EAn3=mod(n3*A_i3,p)
EAn3 = 70392372
>> DAn3=mod_exp(g,i3,p)
DAn3 = 266313679

>> Dan3_mz=mod_exp(DAn3,mz,p)
Dan3_mz = 211572765
>> nn3=mod(EAn3*Dan3_mz,p)
nn3 = 260099963

>> A_i4=mod_exp(A,i4,p)
A_i4 = 235111288
>> EAn4=mod(n4*A_i4,p)
EAn4 = 242658874
>> DAn4=mod_exp(g,i4,p)
DAn4 = 64259930

>> Dan4_mz=mod_exp(DAn4,mz,p)
Dan4_mz = 41441944
>> nn4=mod(EAn4*Dan4_mz,p)
nn4 = 246637967

			1234567890	1234567890	1234567890	1234567890	1234567890	1234567890				
									Enc(A,i3,n3)=(EAn3,DAn3)=CAn3		Enc(A,i4,n4)=(EAn4,DAn4)=CAn4	
Nr.	m3	m4	n3	n4	i3	i4	i3+i4 mod(p-1)	i	EAn3	DAn3	EAn4	DAn4
1	1000	4000	260099963	246637967	28525739	191992804	220518543	220518543	70392372	266313679	242658874	64259930
2												
3												
4												
5												
6												
7												

>> i
i = 220518543

i = 220518543

$$\left(\frac{a}{A}\right)^i \bmod p = \left(a * A^{-1}\right)^i \bmod p \quad \text{Net:} \quad \frac{EA\,n12}{EA\,n34} \bmod p = EAn12 * (EAn34)^{-1} \bmod p.$$

$$\left.\begin{aligned} Ean1 &= n_1 * a^{i1} \bmod p \\ Ean2 &= n_2 * a^{i2} \bmod p \end{aligned}\right\} \quad \begin{aligned} Ean12 &= n_1 * a^{i1} * n_2 a^{i2} \bmod p = \\ &= n_1 * n_2 * a^{i1} * a^{i2} \bmod p = \\ &= n_{12} * a^{i1+i2 \bmod (p-1)} \bmod p = \\ &= n_{12} * a^i \bmod p. \end{aligned}$$

$$\left.\begin{aligned} EA\,n3 &= n_3 * A^{i3} \bmod p \\ EA\,n4 &= n_4 * A^{i4} \bmod p \end{aligned}\right\} \quad \begin{aligned} EA\,n34 &= n_3 * A^{i3} * n_4 * A^{i4} \bmod p = \dots \\ \dots &= n_{34} * A^i \bmod p \end{aligned}$$

$$\frac{Ean12}{EA\,n34} \bmod p = \frac{n_{12} * a^i}{n_{34} * A^i} \bmod p = \frac{a^i}{A^i} \bmod p = \left(\frac{a}{A}\right)^i \bmod p$$

```
>> Ean12
Ean12 = 211462699
>> Dan12
Dan12 = 48312418
```

```
>> EAn34=mod(EAn3*EAn4,p)
EAn34 = 110631558
>> DAn34=mod(DAn3*DAn4,p)
DAn34 = 48312418
```

```
>> m1=mod(-1,p-1)
m1 = 268435017
>> m1p1=mod(m1+1,p-1)
m1p1 = 0
```

```
>> A_m1=mod_exp(A,m1,p)
A_m1 = 64233026
>> aA_m1=mod(a*A_m1,p)
aA_m1 = 190973001
>> aA_m1_i=mod_exp(aA_m1,i,p)
aA_m1_i = 58108479
```

```
>> EAn34_m1=mod_exp(EAn34,m1,p)
EAn34_m1 = 53781976
>> Ean12EAn34_m1=mod(Ean12*EAn34_m1,p)
Ean12EAn34_m1 = 58108479
```

			1234567890	1234567890
	CAn3*CAn4=CAn34			
Nr.	EAn3*EAn4=EAn34	DAn3*DAn4=DAn34	(a/A)^i	(Ean12/EAn34)
1	110631558	48312418	58108479	58108479
2				
3				
4				
5				
6				
7				