Results of Midterm Exam:
https://docs.google.com/spreadsheets/d/1me-P-rJ00RbNwoy_iCsvRVevmk2WuIGn/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

>> p = 268435019; % 2^28 --> >> int64(2^28-1) % ans = **268 435 455**
>> g=2; % testing g=2, g=3, ...

Homomorphic property of ElGamal encryption

Let we have 2 messages m_1, m_2 to be encrypted

$t_1 \leftarrow randi(\mathbb{Z}_p^*)$

$Enc_a(t_1, m_1) = (E_1, D_1) = c_1$

$E_1 = m_1 \cdot a^{t_1} \bmod p$

$D_1 = g^{t_2} \bmod p$

$t_2 \leftarrow randi(\mathbb{Z}_p^*)$

$Enc_a(t_2, m_2) = (E_2, D_2) = c_2$

$E_2 = m_2 \cdot a^{t_2} \bmod p$

$D_2 = g^{t_2} \bmod p$

Multiplicative homomorphic encryption:

$$Enc_a(t_1 + t_2, m_1 \cdot m_2) = Enc_a(t_1, m_1) \cdot Enc_a(t_2, m_2)$$

$$\boxed{c_{12} = c_1 \cdot c_2}$$

$$(E_{12}, D_{12}) = (E_1, D_1) \cdot (E_2 \cdot D_2)$$

$E_{12} = m_{12} \cdot a^{t_1 + t_2}$; $D_{12} = g^{t_1 + t_2}$

$$(E_1 \cdot E_2, D_1 \cdot D_2)$$

$$(m_1 \cdot m_2 \cdot a^{t_1 + t_2} \bmod p, g^{t_1 + t_2} \bmod p) = (m_1 a^{t_1} \bmod p, g^{t_1} \bmod p) \cdot (m_2 a^{t_2} \bmod p, g^{t_2} \bmod p)$$

```
>> p=268435019;
>> g=2;
>> x=int64(randi(p-1))
x = 96997711
>> a=mod_exp(g,x,p)
```

m_1 Enc.

```
>> t1=int64(randi(p-1))
t1 = 186399292
>> a_t1=mod_exp(a,t1,p)
a_t1 = 8797082
>> E1=mod(m1*a_t1,p)
```

m_2 Enc.

```
>> t2=int64(randi(p-1))
t2 = 15179782
>> a_t2=mod_exp(a,t2,p)
a_t2 = 17517376
>> E2=mod(m2*a_t2,p)
```

```
>> x=int64(randi(p-1))
x = 96997711
>> a=mod_exp(g,x,p)
a = 238604564
>> m1=111;
>> m2=222;
```

```
>> a_t1=mod_exp(a,t1,p)
a_t1 = 8797082
>> E1=mod(m1*a_t1,p)
E1 = 171171045
>> D1=mod_exp(g,t1,p)
D1 = 227685358
```

```
>> a_t2=mod_exp(a,t2,p)
a_t2 = 17517376
>> E2=mod(m2*a_t2,p)
E2 = 130767206
>> D2=mod_exp(g,t2,p)
D2 = 137330014
```

```
>> m12=m1*m2
m12 = 24642
>> t12=mod(t1+t2,p-1)
t12 = 201579074
>> a_t12=mod_exp(a,t12,p)
a_t12 = 227999426
>> E12=mod(m12*a_t12,p)
E12 = 16907822
>> D12=mod_exp(g,t12,p)
D12 = 29978883
```

```
>> a_t12=mod_exp(a,t12,p)
a_t12 = 227999426
>> E12=mod(m12*a_t12,p)
E12 = 16907822
>> D12=mod_exp(g,t12,p)
D12 = 29978883
>>
>> E1E2=mod(E1*E2,p)
E1E2 = 16907822
>> D1D2=mod(D1*D2,p)
D1D2 = 29978883
```

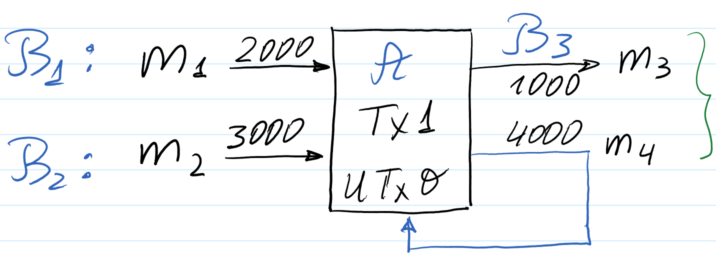
Additively multiplicative encryption:

Let n_1, n_2 are messages to be encrypted

$$\left.\begin{array}{l} Enc_a(r_1, n_1) = c_1 \\ Enc_a(r_2, n_2) = c_2 \end{array}\right\} \quad c_1 \cdot c_2 = c_{12}^{\oplus} \equiv Enc_a(r_1 + r_2, m_1 + m_2)$$

$$\left.\begin{array}{l} n_1 = g^{m_1} \bmod p \\ n_2 = g^{m_2} \bmod p \end{array}\right\} \Rightarrow n_1 \cdot n_2 = g^{m_1} \cdot g^{m_2} = g^{m_1 + m_2} \bmod p$$

1. App.: for confid & verifiable transactions



$$m_1 + m_2 = m_3 + m_4 = 5000$$

$$Enc(m_1 + m_2) = c_{12} = c_{34} = Enc(m_3 + m_4)$$

$$c_1 \cdot c_2 = c_3 \cdot c_4$$ Net verification

ElGamal - Enc : $PP = (p, g)$ A: $PrK = x$; $PuK = a = g^x \bmod p$

ElGamal-Enc : $PP=(p,g)$ A: $PrK=x$; $PuK=a=g^x \bmod p$

B_1: $n_1=g^{m_1} \bmod p \longrightarrow Enc_a(t_1,n_1)=c_1=(E_1,D_1)=(n_1a^{t_1} \bmod p,$

B_2: $n_2=g^{m_2} \bmod p \longrightarrow Enc_a(t_2,n_2)=c_2=(E_2,D_2)=(n_2a^{t_2} \bmod p,$

Net: $c_1\cdot c_2=c_{12}=(E_{12},D_{12})=(E_1\cdot E_2, D_1\cdot D_2)$

$$E_{12}=E_1\cdot E_2=n_1a^{t_1}\cdot n_2a^{t_2} \bmod p = n_1\cdot n_2\cdot a^{t_1+t_2} \bmod p =$$
$$= g^{m_1}\cdot g^{m_2} a^{r_1+r_2} \bmod p = g^{m_1+m_2}\cdot a^{r_1+r_2} \bmod p$$
$$C_{12}=g^{m_1+m_2}\cdot a^{t_1+t_2} \bmod p$$

```
>> m1=2000;
>> m2=3000;
>> m3=1000;
>> m4=4000;
>> n1=mod_exp(g,m1,p)
n1 = 28125784
>> n2=mod_exp(g,m2,p)
n2 = 222979214
>> n3=mod_exp(g,m3,p)
n3 = 260099963
>> n4=mod_exp(g,m4,p)
n4 = 246637967
```

```
>> EE1=mod(n1*a_t1,p)
EE1 = 218099418
>> EE2=mod(n2*a_t2,p)
EE2 = 153907571
>>
>> EE3=mod(n3*a_t1,p)
EE3 = 196508353
>> EE4=mod(n4*a_t2,p)
EE4 = 184150428
```

Compute DD1, ---, DD4

```
>> n12=mod(n1*n2,p)
n12 = 143845522
>> n34=mod(n3*n4,p)
n34 = 143845522
>> a_t12
a_t12 = 227999426
```

$Enc(n_{12},t_{12})=(EE_{12},D_{12})=cc_{12}$; $Enc(n_{34},t_{12})=(EE_{34},D_{34})=cc_{34}$

```
>> EE12=mod(n12*a_t12,p)
EE12 = 209506
>> EE34=mod(n34*a_t12,p)
EE34 = 209506
```

```
>> mod(EE1*EE2,p)
ans = 209506
>> mod(EE3*EE4,p)
ans = 209506
```

Network checked that $n_1\cdot n_2=n_3\cdot n_4$
$$\Downarrow$$
$$m_1+m_2=m_3+m_4$$

$\rightarrow$ Since $n=g^n \bmod p$ is 1-to-1 mapping

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

A: decrypts n_1 & n_2 where $n_1 = g^{m_1} \bmod p$ & $n_2 = g^{m_2} \bmod p$

A: knows in advance the sums m_1 & m_2 she must receive from B_1 & B_2 $\longrightarrow$ after decryption of n_1 & n_2 she simply verifies if $n_1 = g^{m_1} \bmod p$ & $n_2 = g^{m_2} \bmod p$.

Drawback: Let $p = 11 \rightarrow p-1 = 10 \rightarrow m_1 + m_2$ are computed mod $(p-1)$ since $m_1 + m_2$ are in the exponents.

Then if $m_1 = 2$; $m_2 = 3 \rightarrow (m_1 + m_2) \bmod 10 = 5 \bmod 10 = 5$.

but if $m_3 = 7$; $m_4 = 8 \rightarrow (m_3 + m_4) \bmod 10 = 15 \bmod 10 = 5$.

Balance mod$(p-1)$ is hold while the B due to A earned $7 - 1 = 6$ BTC

and A due to herself got $8 - 4 = 4$ BTC.

The network must introduce range proof for transactions: all $\sum_i m_i < (p-1)/2$.