```
>> p =   268 435 019;
 >> p=int64(268435019)
p = 268435019
>> g = 2
g = 2
```

```
>> x=int64(randi(p-1))
x = 129138532
>> a=mod_exp(g,x,p)
a = 17509257
```

```
>> y=int64(randi(p-1))
y = 170809567
>> b=mod_exp(g,y,p)
b = 10745328
```

```
>> m1=1;
>> m2=2;
>> i1=int64(randi(p-1))
i1 = 75904059
>> i2=int64(randi(p-1))
i2 = 189040215
>> a_i1=mod_exp(a,i1,p)
a_i1 = 54795516
>> E1A=mod(m1*a_i1,p)
E1A = 54795516
>> D1A=mod_exp(g,i1,p)
D1A = 65025036
```

```
>> a_i2=mod_exp(a,i2,p)
a_i2 = 132463546
>> E2A=mod(m2*a_i2,p)
E2A = 264927092
>> D2A=mod_exp(g,i2,p)
D2A = 141521659
```

$C_{1A} = (E_{1A}, D_{1A})$

$C_{2A} = (E_{2A}, D_{2A})$

```
>> b_i3=mod_exp(b,i3,p)
b_i3 = 134842101
>> E2AB=mod(E2A*b_i3,p)
E2AB = 79455767
>> D2AB=mod_exp(g,i3,p)
D2AB = 55442606
```

E_{2AB}

```
>> D2A_m1=mulinv(D2A,p)
D2A_m1 = 246968779
>> mod(D2A*D2A_m1,p)
ans = 1
>> D2A_mx=mod_exp(D2A_m1,x,p)
D2A_mx = 163872965
>> D2A_x=mod_exp(D2A,x,p)
D2A_x = 132463546
>> mod(D2A_x*D2A_mx,p)
ans = 1
```

```
>> E2ABA=mod(E2AB*D2A_mx,p)
E2ABA = 1249183
```

```
>> D2AB_my=mod_exp(D2AB_m1,y,p)
D2AB_my = 229393008
>> D2AB_y=mod_exp(D2AB,y,p)
D2AB_y = 134842101
>> mod(D2AB_y*D2AB_my,p)
ans = 1
```

mm2, i3

```
>> mm2=mod(E2ABA*D2AB_my,p)
mm2 = 2
```

```
>> b_mi3=mod_exp(b_m1,i3,p)
b_mi3 = 229393008
>> mmm3=mod(E2ABA*b_mi3,p)
mmm3 = 2
```