Exam:

1.To solve remaining problems in imimsociety.net
(DH, MiMAttack, ElGamal-Enc, Schnorr-Id, Schnorr-Sig)

2.To mine a block: to create a transaction, to sign a transaction, compose a block, to mine a block.

```
>> p = 264043379
p =  264043379
>> eA=genprime(28)
eA = 141897127
>> dA=mulinv(eA,p-1)
dA = 9616167
>> mod(eA*dA,p-1)
ans = 1
```

```
>> M1=19000
M1 =  19000
>> C1=mod_exp(M1,eA,p)
C1 = 38104487
```

C999C2C3