Declare **Public Parameters** to the network **PP** = (**p**, **g**); **p= 268435019**; **g=2;**

PrK = x <-- randi(Z_{p-1}) ==> PuK = a = g^x mod p

m = 111222. Then ***m*** **mod** ***p*** = ***m***.

```
>> p=genstrongprime(28)
p = 187725299
>>
>>  p= 268435019
p = 2.6844e+08
>>  p= int64(268435019)
p = 268435019
>> g=2
g = 2
```

```
>> x=int64(p)
x = 268435019
>> x=int64(randi(p))
x = 214253594
>> a=mod_exp(g,x,p)
a = 117821725
>>
>> m=111222
m = 111222
```

c = Enc(PuK_A, m) = (E, D)

i <-- randi(Z_{p-1})

E = m*a^i mod p; D = g^i mod p.

```
>> i=int64(randi(p))
i = 73575762
>> a_i=mod_exp(a,i,p)
a_i = 67787255
>> E=mod(m*a_i,p)
E = 168131976
>> D=mod_exp(g,i,p)
D = 198802768
```

D^{-x} mod p

$E*D^{-x}$ mod p = m.

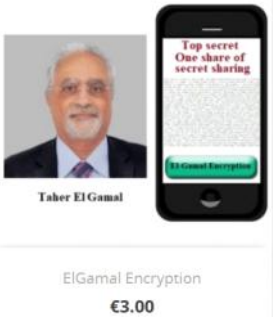
```
>> mx=mod(-x,p-1)
mx = 54181424
>> mod(x+mx,p-1)
ans = 0
>> D_mx=mod_exp(D,mx,p)
D_mx = 137399215
>> mm=mod(E*D_mx,p)
mm = 111222
```

During the exam you must solve the following 4 problems.



El Gamal E-Signature

€3.00



ElGamal Encryption

€3.00



Schnorr E-Signature

€3.00



Schnorr Identification

€3.00



MINI-HTTPS

€5.00