Midterm exam on the 14-th of April. Registration:
Firstname in the students list
Medina
P

Sign and Encrypt or Encrypt and Sign ??
To ensure message confidentiality, authenticity and integrity.
ElGamal Encryption and Schnorr Signature.

$B: (PrK_B, PuK_B)$
(PuK_A)

$Lo: (PrK_{Lo}, PuK_{Lo})$
(PuK_A, PuK_B)
$Enc(PuK_A, m_z) = c_z \longrightarrow$

$A: (PrK_A, PuK_A)$
(PuK_B)
$Dec(PrK_A, c_z) = m_z$

m – message to be sent
$Enc(PuK_A, m) = c = (E, D)$
m and c are short messages used in asymmetric cryptosystem (cs).
$|m| \approx |c| \approx 2048$ bit length $\Rightarrow$
$\Rightarrow$ no H-function can be applied and signature can be placed directly on the m, since $m < p$ and $c < p$.

$Sig(PrK_B, c) = S$ $\xrightarrow{c, S}$
If $h = H(c)$
$Sig(PrK_B, h) = S_h$ $\xrightarrow{c, S_h}$

$A: PuK_B = b$
1. $Ver(PuK_B, S, c) = True$
2. $Dec(PrK_A, c) = m$

1. $h = H(c)$
2. $Ver(PuK_B, S_h, c) = True$
3. $Dec(PrK_A, c) = m.$

p = 264043379, g = 2

```
>> y=randi(p-1)
y =  127785403
>> b=mod_exp(g,y,p)
b = 261066476
```

```
>> x=randi(p-1)
x =  30634143
>> a=mod_exp(g,x,p)
a = 193219330
```

ElGamal Encryption

$t \leftarrow randi(p-1)$
$E = m \cdot a^t \bmod p$
$D = a^t \bmod p$

```
>> m=777888
m =  777888
>> t=randi(p-1)
t =  43164139
```

$E = m \cdot a^t \bmod p$

$D = g^t \bmod p$

$c = (E, D)$

```
>> t=randi(p-1)
t =  43164139
>> a_t=mod_exp(a,t,p)
a_t = 99889152
>> E=mod(m*a_t,p)
E = 151142235
>> D=mod_exp(g,t,p)
D = 199602063
```

Schnorr signature

$c \longrightarrow$ 'E, D'

$u \leftarrow randi(p-1)$

$r = g^u \bmod p$

$h = H('E, D, r')$

$s = (u + y \cdot h) \bmod (p-1)$

$S_h = (r, s)$

```
>> u=randi(p-1)
u =  146721989
>> r=mod_exp(g,u,p)
r = 156600857
>> h=hd28('E=151142235,D=199602063,r=156600
857')
h =  18127646
>> yh=mod(y*h,p-1)
yh =  219051386
>> s=mod(u+yh,p-1)
s =  101729997
```

$c = (E, D), S_h = (r, s)$ → A: $PrK_A = x$; $PuK_B = b$

A: verification

$g^s = r \cdot b^h \bmod p$

```
>> h=hd28('E=151142235,D=199602063,r=156600857')
h =  18127646

>> g_s=mod_exp(g,s,p)
g_s = 126520362

>> b_h=mod_exp(b,h,p)
b_h = 243911860
>> rb_h=mod(r*b_h,p)
rb_h = 126520362
```

A: decryption

To find $D^{-x} \bmod p = D^{p-1-x} \bmod p$

$m = E \cdot D^{-x} \bmod p$

```
>> b_h=mod_exp(b,h,p)
b_h = 243911860
>> rb_h=mod(r*b_h,p)
rb_h = 126520362
>>
>> pm1mx=p-1-x
pm1mx =  233409235
>> D_pm1mx=mod_exp(D,pm1mx,p)
D_pm1mx = 56127130
>>
>> mm=mod(E*D_pm1mx,p)
mm = 777888
```