```
>> p=268435019;
>> g=2;
>> x=int64(randi(p))
x = 234688513
>> a=mod_exp(g,x,p)
a = 77653678
>> t=int64(randi(p))
t = 13333507
>> b=mod_exp(g,t,p)
b = 240517601
>> tb=mod(t*b,p-1)
tb = 153859073
>> y=mod(x+tb,p-1)
y = 120112568
```

```
>> g_y=mod_exp(g,y,p)
g_y = 40914369
>> b_b=mod_exp(b,b,p)
b_b = 322491
>> ab_b=mod(a*b_b,p)
ab_b = 40914369
```

```
>> Soft='Python 3.7'
Soft = Python 3.7
>> h=hd28(Soft)
h = 157508636
>> ksy=int64(randi(p))
ksy = 108371952
>> r=mod_exp(g,ksy,p)
r = 173850748
>> s=mod(ksy+y*h,p-1)
s = 172249966
```

```
>> g_s=mod_exp(g,s,p)
g_s = 191736342
>> b_b=mod_exp(b,b,p)
b_b = 322491
>> ab_b=mod(a*b_b,p)
ab_b = 40914369
>> ab_b_h=mod_exp(ab_b,h,p)
ab_b_h = 95351894
>> rab_b_h=mod(r*ab_b_h,p)
rab_b_h = 191736342
```

Bit Commitment using RSA modification

```
>> p=int64(268435019)
p = 268435019
```

A

```
>> eA=int64(randi(p))
eA = 124258335
>> gcd(eA,p-1)
ans = 1
>> dA=mulinv(eA,p-1)
dA = 186613915
>> mod(eA*dA,p-1)
ans = 1
```

```
>> M=100000
M = 100000
>> c1=mod_exp(M,eA,p)
c1 = 227304331
>> c2=mod_exp(c1,eB,p)
c2 = 27347937
>> c3=mod_exp(c2,dA,p)
c3 = 240597342
>> c4=mod_exp(c3,dB,p)
c4 = 100000
```

B

```
>> eB=int64(randi(p))
eB = 143240865
>> gcd(eB,p-1)
ans = 1
>> dB=mulinv(eB,p-1)
dB = 206897595
>> mod(eB*dB,p-1)
ans = 1
```

Subliminal Channel - Steganography
Using Schnorr Signature

Corrected version

M - masking message to be sign.

h = k - secret message to be sent.

$r = g^k \bmod p$

$h = H(M \| r)$

$s = k + x \cdot h \bmod (p-1)$

$M, \sigma = (r, s) \rightarrow$ B: $h = H(M \| r)$

$V1 = g^s \bmod p$

$V2 = g^{k+xh} = g^k \cdot (g^x)^h = r \cdot a^h \bmod p$

$V1 \stackrel{?}{=} V2$

```
>> p
p = 268435019
>> g
g = 2
>> x
x = 164448909
>> a=mod_exp(g,x,p)
a = 219396659
```

```
>> k
k = 77000
>> r
r = 136365479
>> M='My sorrow and tears, Bob'
M = My sorrow and tears, Bob
>> cc=concat(M,r)
cc = My sorrow and tears, Bob136365479
>> h=hd28(cc)
h = 24944974
>> xh=mod(x*h,p-1)
xh = 11605732
>> s=mod(k+xh,p-1)
s = 11682732
```

```
>> v1=mod_exp(g,s,p)
v1 = 181549966
>> a_h=mod_exp(a,h,p)
a_h = 146278252
>> v2=mod(r*a_h,p)
v2 = 181549966
```

Value k=n recovery:

k = s - **x***h mod (**p**-1)

```
>> k=mod(s-xh,p-1)
k = 77000
```