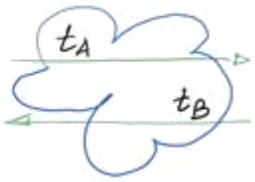
111_006 KAP MiMA
111_007 PKCS Scnorr-Id-Sig_AKAP
111_008 Blind_e-Sign e-Money

KAP MiMA

p = 268435019
g=2;

$u \leftarrow rand(Z_p^*)$
$g^u \bmod p = t_A$



$v \leftarrow rand(Z_p^*)$
$t_B = g^v \bmod p$

$k_{AB} = (t_B)^u \bmod p =$
$= (g^v)^u \bmod p = g^{vu} \bmod p$

$k_{BA} = (t_A)^v \bmod p =$
$= (g^u)^v \bmod = g^{uv} \bmod p$

$k_{AB} = k = k_{BA}$

```
>> u=int64(randi(p-1))
u = 26490635
>> tA=mod_exp(g,u,p)
tA = 188341502
>>
>> v=int64(randi(p-1))
v = 39531862
>> tB=mod_exp(g,v,p)
tB = 84587072
>> kAB=mod_exp(tB,u,p)
kAB = 62170746
>> kBA=mod_exp(tA,v,p)
kBA = 62170746
```

Scnorr-Sig

A:

```
>> x=int64(randi(p-1))
x = 126471976
>> a=mod_exp(g,x,p)
a = 98940112

>> mA=tA
mA = 188341502
>> i=int64(randi(p-1))
i = 222883282
>> r=mod_exp(g,i,p)
rA = 237483091
>> cc=concat(mA,rA)
cc = 188341502237483091
>> hA=hd28(cc)
```

B:

```
>> y=int64(randi(p-1))
y = 132995347
>> b=mod_exp(g,y,p)
b = 34480132

>> mB=tB
mB = 84587072
>> j=int64(randi(p-1))
j = 146464308
```

>> cc=concat(mA,rA)
cc = 188341502237483091
>> hA=hd28(cc)
hA = 73419365
>> s=mod(i+x*hA,p-1)
sA = 43671724

$$g^s \bmod p = ra^{h'} \bmod p.$$

>> cc1=concat(mA,rA)
cc1 = 188341502237483091
>> hA1=hd28(cc1)
hA1 = 73419365

>> g_sA=mod_exp(g,sA,p)
g_sA = 65647891
>> a_hA1=mod_exp(a,hA1,p)
a_hA1 = 126177872
>> rAa_hA1=mod(rA*a_hA1,p)
rAa_hA1 = 65647891

RSA masking $m = 12000$

>> p=int64(genprime(14))
p = 15329
>> q=int64(genprime(14))
q = 12379
>> n=p*q
n = 189757691
>> e=2^16+1
e = 65537
>> fy=(p-1)*(q-1)
fy = 189729984
>> d=mulinv(e,fy)
d = 175333121

$r \leftarrow randi(n-1)$

$m * r^e \bmod n$

>> r=int64(randi(n-1))
r = 29343062
>> r_e=mod_exp(r,e,n)
r_e = 105219877
>> m=12000
m = 12000
>> mr_e=mod(m*r_e,n)
mr_e = 180605777

$sign_{RSA}(d, m * r^e) = \sigma$

$\sigma = (m * r^e)^d \bmod n$

>> Sigma=mod_exp(mr_e,d,n)
Sigma = 117664816

r_m1 = mulinv(r,n) // $r^{-1} \bmod n$ computation

$\sigma \cdot r^{-1} \bmod n = mm = 12000$