

p = 264043379 Check that p is strong prime;	p = 268435019
g = 2	g = 2

$P = 268435019$; P - is strong prime; $P = 2Q + 1$,
 where Q - is prime;
 g - is a generator iff: 1) $g^Q \pmod P \neq 1$
 2) $g^2 \pmod P \neq 1$

PP = (p = 268435019, g = 2)

p = 268435019, g = 2

```
>> p = 268435019
p = 268435019
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 134217509
>> isprime(q)
ans = 1
>> g = 2
g = 2
>> mod_exp(g,q,p)
ans = 268435018
>> mod_exp(g,2,p)
ans = 4
```

A:

```
>> u=randi(p-1)
u = 196333506
>> A=mod_exp(g,u,p)
A = 111926898
```

A
Loe:

```
>> z=randi(p-1)
z = 244646552
>> A1=mod_exp(g,z,p)
A1 = 207016610
```

A1
B:

```
>> w=randi(p-1)
w = 257956572
>> B1=mod_exp(g,w,p)
B1 = 99413947
```

```
>> v=randi(p-1)
v = 93013145
>> B=mod_exp(g,v,p)
B = 52377747
```

B1

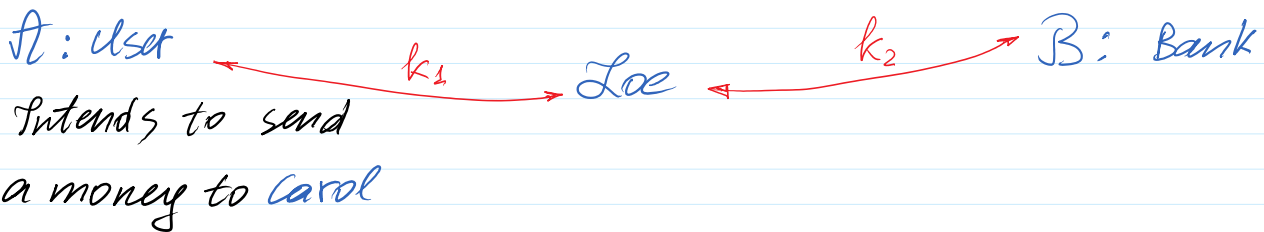
B

```
>> k1=mod_exp(B1,u,p)
k1 = 238551491
```

```
>> k11=mod_exp(A,w,p)
k11 = 238551491
```

```
>> k22=mod_exp(B,z,p)
k22 = 166390100
```

```
>> k2=mod_exp(A1,v,p)
k2 = 166390100
```



M; money transfer doc.
 from *A* account to *C* account

from A account to C account
with the sum m .

AccA

AccC

$M = 'AccA, AccC, m'$

$c = AES(k_1, M)$

C Joe

$D(k_1, c) = M$

$M' = 'AccA, AccI, m'$

$m' > m$

$c' = AES(k_2, M')$

B

$D(k_2, c') = M'$

Transfers money m'
to AccI

<http://crypto.fmf.ktu.lt/xdownload/>

- [Euronews 17-03-2015 15-38 CET_150316 HTSU_121B0-172837_E.mp4](#)

Telegram, Whatup