Let us fix p, then any integer $z = t \cdot p + r$; Let $p = 11$

```
>> p = 11
>> z = 37
>> r = mod(z, p)
```

```
>> p=11
p =  11
>> z=37
z =  37
>> r=mod(z,p)
r =  4
```

$PP = (p, g)$: $g^x \bmod p = a$

$2^5 \bmod 11 = 10$

```
>> e = mod_exp(2,5,11)
```

```
>> e=mod_exp(2,5,11)
e = 10
>> e=mod_exp(4,8,11)
e = 9
>> e=mod_exp(z,8,11)
e = 9
```

strong prime p generation when $|p| = 28$ bits.

```
>> p = genstrongprime(28)
```

```
>> p=genstrongprime(28)
p = 135477227
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 67738613
>> isprime(q)
ans = 1
```

$PP = (p = 135477227, g = 2)$

```
>> g=2
g =  2
>> mod_exp(g,q,p)
ans = 135477226
>> mod_exp(g,2,p)
ans = 4
```

```
>> 2^28-1
ans =  268435455
```

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

```
>> max28=2^28-1
max28 =  268435455
>> dec2bin(max28)
ans = 1111111111111111111111111111
>> p = 264043379
p =  264043379
>> dec2bin(p)
ans = 1111101111001111101101110011
>> pmax28=268435019
pmax28 =  268435019
>> dec2bin(pmax28)
ans = 1111111111111111111001001011
```

```
ans = 1111111111111111111111111111
ans = 1111101111001111101101110011
ans = 1111111111111111111001001011
```

```
>> p=pmax28
p =  268435019
>> g=2
g =  2
```

At: >> u=randi(p-1)

A:

```
>> u=randi(p-1)
u =  117781042
>> A=mod_exp(g,u,p)
A = 12150717
```

A →

B:

```
>> v=randi(p-1)
v =  58037557
>> B=mod_exp(g,v,p)
B = 117838929
```

← B

```
>> kAB=mod_exp(B,u,p)
kAB = 115454732
```

k

```
>> kBA=mod_exp(A,v,p)
kBA = 115454732
```

https://

Let B is a Bank

M of money transfer to B_2

$E(k, M) = C$ → C → $D(k, C) = M$

B transfers money from A account to B_2.

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

- Euronews 17-03-2015 15-38 CET_150316_HTSU_121B0-172837_E.mp4