

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

>>  $p = 11$

>>  $z = 37$

>>  $r = \text{mod}(z, p)$

PP = (p, g):  $g^x \text{ mod } p = a$

$2^5 \text{ mod } 11 = 10$

>>  $e = \text{mod\_exp}(2, 5, 11)$

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

>>  $p = \text{genstrongprime}(28)$

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

>> p=11

p = 11

>> z=37

z = 37

>> r=mod(z,p)

r = 4

>> e=mod\_exp(2,5,11)

e = 10

>> e=mod\_exp(4,8,11)

e = 9

>> e=mod\_exp(z,8,11)

e = 9

>> p=genstrongprime(28)

p = 135477227

>> isprime(p)

ans = 1

>> q=(p-1)/2

q = 67738613

>> isprime(q)

ans = 1

>> 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 = 11111111111111111111111111111111

ans = 11111111111111111111111111111111

>> p = 264043379

p = 264043379

>> dec2bin(p)

ans = 1111101111001111101101110011

ans = 1111101111001111101101110011

>> pmax28=268435019

pmax28 = 268435019

>> dec2bin(pmax28)

ans = 1111111111111111111111001001011

ans = 1111111111111111111111001001011

>> p=pmax28

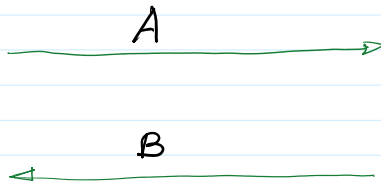
p = 268435019

>> g=2

g = 2

A:  $\ll u = \text{randi}(n, 1)$

A: >> u=randi(p-1)  
 u = 117781042  
 >> A=mod\_exp(g,u,p)  
 A = 12150717



B: >> v=randi(p-1)  
 v = 58037557  
 >> B=mod\_exp(g,v,p)  
 B = 117838929

>> kAB=mod\_exp(B,u,p)  
 kAB = 115454732

>> kBA=mod\_exp(A,v,p)  
 kBA = 115454732

$k$   
 ↓  
 https://

Let B is a Bank

M of money transfer to B<sub>2</sub>

$E(k, M) = C$        $C$  →       $D(k, C) = M$

B transfers money from A account to B<sub>2</sub>.

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

- [Euronews 17-03-2015 15-38 CET\\_150316\\_HTSU\\_121B0-172837\\_E.mp4](#)