Public Parameters - **PP** generation : $PP = (p, g)$

p - strong prime $\Rightarrow$ $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$; $*$ mod p
g - generator in $\mathbb{Z}_p^*$

Discrete Exponent Function (3/14)

Let Γ be the set of generators in $\boldsymbol{Z_p}^*$. How to find a generator in $\boldsymbol{Z_p}^*$?

In general, it is a hard problem, but using strong prime $\boldsymbol{p}$ and *Lagrange theorem in group theory* the generator in $\boldsymbol{Z_p}^*$ can be found by random search satisfying two following conditions.

Let $\boldsymbol{p}$ is strong prime $\boldsymbol{p} = 2*\boldsymbol{q} + 1$, when $\boldsymbol{q}$ - is prime, then for all $\boldsymbol{g}\in\Gamma$

$$g^q \neq 1 \textbf{ mod } p\text{; and } g^2 \neq 1 \textbf{ mod } p.$$

Then $\boldsymbol{q} = (\boldsymbol{p}-1)/2$

```
>> g=2
g = 2
>> mod_exp(g,q,p)
ans = 230988322
```

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

```
>> p=genstrongprime(28)
p = 230988323
>> isprime(p)
ans = 1
>> dec2bin(p)
ans =
1101110001001001101000100011
>>
>> q=(p-1)/2
q = 115494161
>> isprime(q)
ans = 1
```

p = int64(230988323)
g = 2

p = int64(268435019)
g = 2

Discrete Exponent Function (4/14)

$$\boldsymbol{a = g^x \textbf{ mod } p}$$

Private and public keys generation: **PrK** = $\boldsymbol{x}$ and **PuK** = $\boldsymbol{a}$.

```
>> s=int64(2^28-1)
s = 268435455
>> x=int64(randi(2^28-1))
x = 225687078
>> a=mod_exp(g,x,p)
a = 35030005
```

Fermat little theorem: If $\boldsymbol{p}$ is prime then for all integers $\boldsymbol{i}$:

$$i^{p-1} = 1 \textbf{ mod } p.$$

Corollaries:

1. The exponent $\boldsymbol{p}$-1 is equivalent to the exponent 0, since $\boldsymbol{i}^0 = \boldsymbol{i}^{p-1} = 1 \text{ mod } \boldsymbol{p}$.
$\boldsymbol{i^e} \textbf{ mod } \boldsymbol{p} = \boldsymbol{i}^{e \textbf{ mod } (p-1)} \textbf{ mod } \boldsymbol{p}$.

```
>> i=int64(123456789123)
i = 123456789123
>> i_pm1=mod_exp(i,p-1,p)
```

2. Any exponent e can be reduced **mod** (p-1), i.e.

3. All non-equivalent exponents x are in the set $Z_{p-1} = \{0, 1, 2, \ldots, p-2\}$.
4. Sets Z_{p-1} and Z_p^* have the same number of elements.

```
i_pm1 = 1
>> i_0=mod_exp(i,0,p)
i_0 = 1
>> g
g = 2
>> g_e=mod_exp(g,e,p)
g_e = 18879246
>> g_ep=mod_exp(g,ep,p)
g_ep = 191242163
```

```
>> p
p = 268435019
>> e=int64(987654321987)
e = 987654321987
>> g
g = 2
>> g_e=mod_exp(g,e,p)
g_e = 18879246
>> g_ep=mod_exp(g,ep,p)
g_ep = 191242163
```

result is incorrect since e is not reduced mod (p-1)

$Z_{p-1} = \{0, 1, 2, \ldots, p-2\}$ $p-1 \equiv 0 \mod (p-1)$

In Z_{p-1} addition +, subtraction - operations and multiplication $*$ are realized **mod** (p-1).
/ is realized **mod** (p-1) with exception.

Subtraction operation (h-d) **mod** (p-1) is replaced by the following addition operation (h + (-d)) **mod** (p-1)).

Therefore, it is needed to find -d **mod** (p-1) such that d + (-d) = 0 **mod** (p-1), then assume that

$$-d \bmod (p-1) = (p-1-d).$$

Indeed, according to the distributivity property of modular operation

$$(d + (-d)) \bmod (p-1) = (d + (p-1-d) \bmod (p-1) = (p-1) \bmod (p-1) = 0.$$

Then

$$(h-d) \bmod (p-1) = (h + (p-1-d)) \bmod (p-1)$$

```
>> d=123456
d = 123456
>> md=int64(p-1-d)
md = 268311562
>> dpmd=mod(d+md,p-1)
dpmd = 0
>> mdd=mod(-d,p-1)
mdd = 268311562
>> h=1234
h = 1234
>> hmd=mod(h-d,p-1)
hmd = 268312796
>> hmdd=mod(h+md,p-1)
hmdd = 268312796
```

Till this place

Discrete Exponent Function (5/14)

Statement: If greatest common divider between p-1 and i is equal to 1, i.e., gcd(p-1, i) = 1, then there exists unique inverse element i^{-1} **mod** (p-1) such that $i * i^{-1}$ **mod** (p-1) = 1. This element can be found by *Extended Euclide algorithm* or using *Fermat little theorem*. We do not fall into details how to find

i^{-1} **mod** (p-1) since we will use the ready-made computer code instead in our modeling.

Division operation / **mod** (p-1) of any element in Z_{p-1} by some element i is replaced by multiplication $*$ operation with i^{-1} **mod** (p-1) if gcd(i, p-1) = 1 according to the *Statement* above.

To compute u/i **mod** (p-1) it is replaced by the following relation $u * i^{-1}$ **mod** (p - 1) since

$$u / i \bmod (p-1) = u * i^{-1} \bmod (p-1).$$

Discrete Exponent Function (6/14)

<u>*Example 1*</u>: Let for given integers u, x and h in Z_{p-1} we compute exponent s of generator g by the expression

$$s = u + xh.$$

Then

$$g^s \bmod p = g^{s \bmod (p-1)} \bmod p.$$

Therefore, s can be computed **mod** (p-1) in advance, to save a multiplication operations, i.e.

$$s = u + xh \bmod (p-1).$$

<u>*Example 2*</u>: Exponent s computation including subtraction by xr **mod** (p-1) and division by i in Z_{p-1} when gcd(i, p-1) = 1.

$$s = (h - xr)i^{-1} \bmod (p-1).$$

Firstly $d = xr$ **mod** (p-1) is computed:
Secondly $-d = -xr$ **mod** (p-1) = (p-1-d) is found.

Thirdly i^{-1} **mod** (p-1) is found.
And finally exponent $s = (h + (p-1-d))i^{-1}$ **mod** (p-1) is computed.