Compatibility relations of modular arithmetic:
(a + b)mod p = (a mod p + b mod p) mod p.
(a * b) mod p =((a mod p) * (b mod p)) mod p.
a^p mod p = (a mod p)^p mod p.

Fermat little theorem: If p is prime, then for any integer a holds **$a^p = a \bmod p$**.

1. We may assume that a is in the range $0 \le a \le p - 1$.
This is a simple consequence of the laws of modular arithmetic; we are simply saying that we may first reduce a modulo p since
a^p mod p = ((a)mod p)^p mod p.
1. It suffices to prove that for a in the range $1 \le a \le p - 1$.

$a^p = a \bmod p$ $\quad / \; a^{-1} \bmod p$

$$a^p \cdot a^{-1} = a \cdot a^{-1} \bmod p$$

$$\boxed{a^{p-1} = 1 \bmod p} \qquad 0 < a < p.$$

Indeed, if the previous assertion holds for such a, multiplying both sides by a yields the original form of the theorem.

Computation of exponents mod (p-1):

$$s = xh + r \longrightarrow g^{s \bmod (p-1)} \bmod p$$

$$g^{p-1} = 1 \;\&\; g^0 = 1 \Longrightarrow 0 \equiv p-1$$

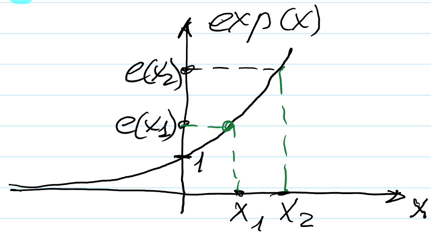
$$s = (xh + r) \bmod (p-1) \longrightarrow g^s \bmod p.$$

DEF homomorphism

$$exp(x) = e^x; \quad exp: R \to R; \quad e = 2{,}71\ldots$$
$$x \in R \to e^x \in R.$$

$$exp(x_1 + x_2) = e^{(x_1+x_2)} = e^{x_1} \cdot e^{x_2} = exp(x_1) \cdot exp(x_2)$$

Additively – multiplicative homomorphism.
Since it is 1–to–1, then it is isomorphism.



$$DEF(x) = g^x \bmod p; \quad p\text{ – strong prime}$$
$$g\text{ – generator in } Z_p^* = \{1, 2, 3, \ldots, p-1\}$$

$$x \in Z_{p-1} = \{0, 1, 2, 3, \ldots, p-2\}; \; + \bmod (p-1), \; * \bmod (p-1), \; - \bmod (p-1)$$
$$|Z_{p-1}| = p \ldots \qquad / \bmod (p-1).$$

$x \in \mathbb{Z}_{p-1} = \{0, 1, 2, 3, ..., p-2\}$; $+\bmod(p-1)$, $*\bmod(p-1)$, $-\bmod(p-1)$, $/\bmod(p-1)$.

$|\mathbb{Z}_{p-1}| = p-1$

$DEF(x) = a \in \mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$; $*\bmod p$, $/\bmod p$.

$|\mathbb{Z}_p^*| = p-1 = |\mathbb{Z}_{p-1}|$

$$DEF(x_1+x_2) = g^{(x_1+x_2) \bmod (p-1)} \bmod p = g^{x_1} \cdot g^{x_2} \bmod p =$$
$$= ((g^{x_1} \bmod p) \cdot (g^{x_2} \bmod p)) \bmod p = DEF(x_1) \cdot DEF(x_2)$$

Additively - multiplicative homomorphism.

Since it is 1-to-1, then it is isomorphism.

ElGamal Encryption-Decryption

Public Parameters generation $PP = (p, g)$.

Asymmetric Signing - Verification

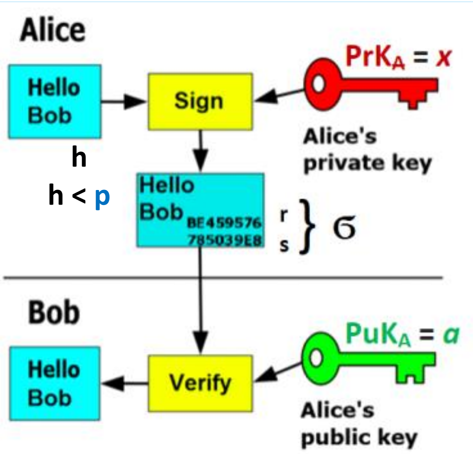
Sign(PrK_A, h) = σ = (r, s)

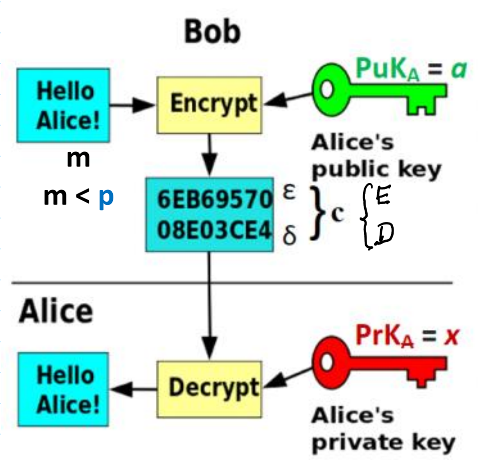
V=Ver(PuK_A, h, σ), V $\in \{\text{True, False}\} \equiv \{1, 0\}$

Asymmetric Encryption - Decryption

c=Enc(PuK_A, m)

m=Dec(PrK_A, c)





ElGamal Cryptosystem

1.Public Parameters generation $PP = (p, g)$.

Generate strong prime number **p**: >> p=genstrongprime(28) % strong prime of 28 bit length

Find a generator **g** in $Z_p^* = \{1, 2, 3, ..., p-1\}$ using condition.

Strong prime $p=2q+1$, where q is prime, then g is a generator of Z_P^* iff $g^q \neq 1 \bmod p$ and $g^2 \neq 1 \bmod p$.

Declare **Public Parameters** to the network $PP = (p, g)$;

p= 268435019; g=2;

2^28-1= 268,435,455

>> 2^28-1
ans = 2.6844e+08
>> int64(2^28-1)
ans = 268435455

PrK = x <-- randi(Z_p^*) ==> PuK = a = g^x mod p

Asymmetric Encryption-Decryption: El-Gamal Encryption-Decryption

p=268435019; g=2;

Let message ***m~*** needs to be encrypted, then it must be encoded in decimal number ***m***: 1< ***m*** < ***p***.
E.g. ***m*** = 111222. Then ***m* mod *p* = *m***.

$\mathcal{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$; $*\ \mathrm{mod}\ p$

A: $\xrightarrow{PuK_A = a}$ B: is able to encrypt m to A: $m < p$

B: $i \leftarrow \mathrm{randi}(\mathcal{Z}_p^*)$

$$\left.\begin{array}{l} E = m \cdot a^i \bmod p \\ D = g^i \bmod p \end{array}\right\} c = (E, D) \longrightarrow$$

A: is able to decrypt $c = (E, D)$ using her $PrK_A = x$.

1. $D^{-x \bmod (p-1)} \bmod p$
2. $E \cdot D^{-x} \bmod p = m$

```
> x=123
x = 123
>> pp=127
pp = 127
>> isprime(pp)
ans = 1
>> mx=mod(-x,pp-1)
mx = 3
>> mod(x+mx,pp-1)
ans = 0
```

$(-x) \bmod (p-1) = (0 - x) \bmod (p-1) =$
$= (p - 1 - x) \bmod (p-1)$

$(p-1) \bmod (p-1) = 0$ since

$$\begin{array}{r|l} p-1 & p-1 \\ \hline -\,p-1 & 1 \\ \hline 0 & \end{array}$$

$(-x) \bmod (p-1) = (p-1-x)$

$D^{-x} \bmod (p-1) = D^{p-1-x} \bmod (p-1)$

$>> D\_mx = \mathrm{mod\_exp}(D, p-1-x, p)$

D^{-x} mod ***p*** computation using Fermat theorem:
If ***p*** is prime, then for any integer ***a*** in Z_p* holds **a^{p-1} = 1 mod *p***.

$D^{p-1} = 1 \bmod p \qquad / \cdot D^{-x \bmod (p-1)} \bmod p$

$\underbrace{D^{p-1} \cdot D^{-x}} = 1 \cdot D^{-x} \bmod p \Rightarrow \underbrace{D^{p-1-x}} = D^{-x} \bmod p$

$$\boxed{D^{-x} \bmod p = D^{p-1-x} \bmod p}$$

Correctness

$Enc(PuK_A = a, i, m) = c = (E, D) = (E = m \cdot a^i \bmod p;\ D = g^i \bmod p)$

$Dec(PrK_A = x, c) = E \cdot D^{-x} \bmod p = m \cdot a^i \cdot (g^i)^{-x} \bmod p =$

$= m \cdot (\underbrace{g^x}_{a})^i \cdot g^{-ix} = m \cdot g^{xi} \cdot g^{-ix} = m \cdot g^{xi-ix} \bmod p = m \cdot g^0 \bmod p =$

$= m \cdot 1 \bmod p = m \bmod p = m = 111222$

since $m < p$

$$\begin{array}{r|l} 27 & 5 \\ \hline 25 & 5 \\ \hline 2 & \end{array}$$

since $m < p$

$$27 \mid 5 \quad 25 \quad 5 \quad 2$$

If $m > p \rightarrow m \bmod p \neq m$; $27 \bmod 5 = 2 \neq 27$.

If $m < p \rightarrow m \bmod p = m$; $19 \bmod 31 = 19$.

Decryption is correct if $m < p$.

ASCII: 8 bits per char.

$$\frac{2048}{8} = 256 \text{ char.}$$

Homomorphic Encryption

Let m_1 and m_2 have to be encrypted.

$$Enc(PuK_A = a, i_1, m_1) = c_1 = (E_1, D_1) = (E_1 = m_1 a^{i_1} \bmod p, D_1 = g^{i_1} \bmod p)$$

$$Enc(PuK_A = a, i_2, m_2) = c_2 = (E_2, D_2) = (E_2 = m_2 a^{i_2} \bmod p, D_2 = g^{i_2} \bmod p)$$

$$c_{12} = c_1 \cdot c_2 = (E_1, D_1) \cdot (E_2, D_2) = (E_1 \cdot E_2, D_1 \cdot D_2) = (E_{12}, D_{12})$$

$$E_{12} = m_1 \cdot m_2 \cdot a^{i_1} a^{i_2} \bmod p = m_1 \cdot m_2\, a^{(i_1+i_2) \bmod (p-1)} \bmod p =$$

$$= m_1 \cdot m_2\, a^{i_{12}} \bmod p = m_{12}\, a^{i_{12}} \bmod p$$

$$D_{12} = D_1 \cdot D_2 = g^{i_1} \cdot g^{i_2} \bmod p = g^{i_1+i_2} \bmod p = g^{i_{12}} \bmod p$$

$$\begin{cases} m_{12} = m_1 \cdot m_2 \bmod p \\ i_{12} = (i_1 + i_2) \bmod (p-1) \end{cases}$$

$$Enc(PuK_A = a, i_{12}, m_1 \cdot m_2) = c_{12} = c_1 \cdot c_2 = (E_1 \cdot E_2, D_1 \cdot D_2) = (E_{12}, D_{12})$$

Multiplicatively homomorphic encryption.

We need an additively-multiplicative encryption.

$$n_1 = g^{m_1} \bmod p \Rightarrow Enc(PuK_A = a, i_1, n_1) = (E_1, D_1) =$$

$$= (E_1 = n_1 \cdot a^{i_1} \bmod p, D_1 = g^{i_1} \bmod p).$$

$$n_2 = g^{m_2} \bmod p \Rightarrow Enc(PuK_A = a, i_2, n_2) = (E_2, D_2) =$$

$$= (E_2 = n_2 \cdot a^{i_2} \bmod p, D_2 = g^{i_2} \bmod p.$$

Till this place