Algebraic structures: groups ***G***, semigroups ***S***, fields ***F***, F_p, Z_p, rings ***R***, Z_{p-1}.

$<G, *>$	$<S, *>$	$<F, \bullet, +>$	$<F, \bullet, +>$
$<Z_p^*, \bullet>$	$<Z_{p-1}, \bullet>$	$<Z_p, \bullet, +>$	$<Z_{p-1}, \bullet, +>$
	$<Z_{p-1}, +>$		

$Z_p^* = \{1, 2, 3, \dots, p-1\}$ $Z_{p-1} = \{0, 1, 2, 3, \dots, p-2\}$ $\bullet \bmod p-1$; $+ \bmod (p-1)$

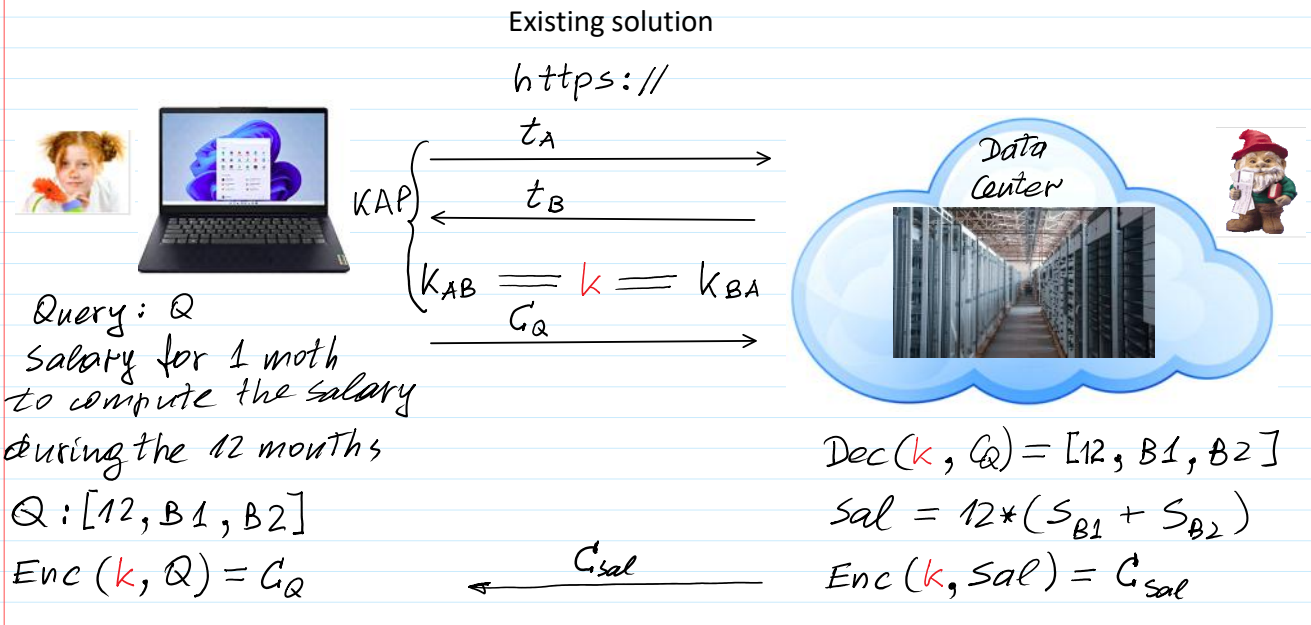
Commutative algebraic structures

Algebraic strukture	Number of binary operations	Multiplicative operation •	Inverse operation /	Additive operation +	Inverse operation -	Distributivity property a· (b+c) = a· b+a· c	Examples
Multiplicative **Semigroup**	1	Yes	No	No	No	No	$<Z_n, \bullet>$ • mod n
Additve **Semigroup**	1	No	No	Yes	No	No	**Set of reals N**
Multiplicative **Group**	1	Yes	Yes	No	No	No	$<Z_p^*, \bullet>$ • mod p
Additve **Group**	1	No	No	Yes	Yes	No	$<Z_n, +>$ + mod n
Ring	2	Yes	No	Yes	Yes	Yes	$<Z_n, \bullet, +>$
Field	2	Yes	Yes	Yes	Yes	Yes	$<Z_p, \bullet, +>$

DEF : $Z_{p-1} \to Z_p^*$, where p - is prime.

DEF : is defined by public parameter $PP = (p, g)$

Homomorphic CryptoSystems: Computation with encrypted data in Data Center.



$Dec(k, C_{sal}) = sal$

Cloud services

$Enc(k, B1) = C_{B1}$

$Enc(k, B2) = C_{B2}$

$Enc(k, 12) = C_{12}$

C_{B1}, C_{B2}, C_{12} →

← C_S

$C_S = C_{12} * (C_{B1} + C_{B2})$

$Dec(k, C_S) = sal$

Homomorphic encryption

$sal = 12 * (B1 + B2)$

$F : S_1 \to S_2$; $F \in \{surjective, injective, \overset{1-to-1}{bijective}\}$

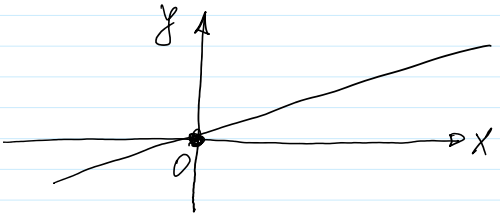
$< S_1, * >$, $< S_2, \bullet >$

$\forall x, y \in S_1 : F(x * y) = F(x) \bullet F(y)$ where $F(x) = a$, $F(y) = b$, $a, b \in S_2$.

If mapping F is bijective (1-to-1) then homomorphism F is isomorphism

Let R be a field of reals: $< R, \cdot, + >$

$f : R \to R$; $f(x) = kx$



1. check: $f(x_1 + x_2) = k(x_1 + x_2) = kx_1 + kx_2 = f(x_1) + f(x_2)$

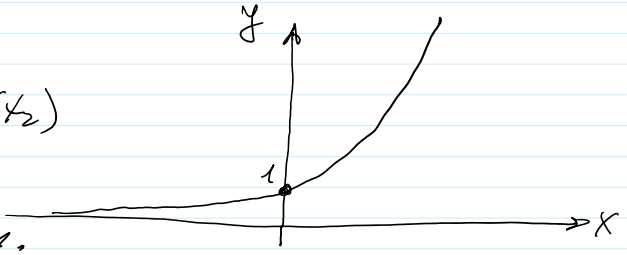
2. check: $f(x_1 \cdot x_2) = k \cdot x_1 \cdot x_2 \neq kx_1 \cdot kx_2 = k^2 \cdot x_1 \cdot x_2$

3. check: $f(x) = e^x$; $f : R \to R^+$

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

$< R, + > \to < R^+, \cdot >$

Additively – multiplicative isomorphism.



3) check. $f(x) = g^x \bmod p$; $PP = (p, g)$

Ferma theorem: If $x \neq 0$, then for $\forall x \in \mathbb{Z}_{p-1}$

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

$f : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ and is 1-to-1 (bijective) mapping.

$x^{\cdot} = 1 \mod p$

$f: \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ and is 1-to-1 (bijective) mapping.

$f(x_1 + x_2) = g^{x_1+x_2} \mod p = g^{x_1} \cdot g^{x_2} \mod p = f(x_1) \cdot f(x_2) = a \cdot b \mod p.$

Additively - multiplicative homomorphism.

4 check. $f_i(m) = m g^i \mod p$

$f_i(m_1 + m_2) = (m_1 + m_2) g^i \mod p = m_1 g^i \mod p + m_2 g^i \mod p = f_i(m_1) + f_i(m_2)$

$f_i : \mathbb{Z}_p^* \to \mathbb{Z}_p^*.$

5. check. $f_{i,g}(m) = g^m \cdot g^i \mod p$

$f_{i,g}(m_1 + m_2) = g^{m_1+m_2} \cdot g^i \mod p = g^{m_1} \cdot g^{m_2} \cdot g^i \mod p \neq f_{i,g}(m_1) \cdot f_{i,g}(m_2)$

6. check. $f_{i_1,g}(m_1) = g^{m_1} \cdot g^{i_1} \mod p$; $f_{i_2,g}(m_2) = g^{m_2} \cdot g^{i_1} \mod p$

$f_{i,g}(m_1 + m_2) = g^{m_1+m_2} \cdot g^i \mod p = g^{m_1} \cdot g^{m_2} \cdot g^i \mod p =$

$i = (i_1 + i_2) \mod (p-1)$

$= g^{m_1} \cdot g^{m_2} \cdot g^{i_1+i_2} \mod p = g^{m_1} \cdot g^{i_1} \cdot g^{m_2} \cdot g^{i_2} \mod p$

$= f_{i_1,g}(m_1) \cdot f_{i_2,g}(m_2).$

Additively - multiplicative isomorphism if $i = (i_1 + i_2) \mod (p-1)$.

If p - is strong prime, then $p = 2q + 1$, where q - is prime as well.

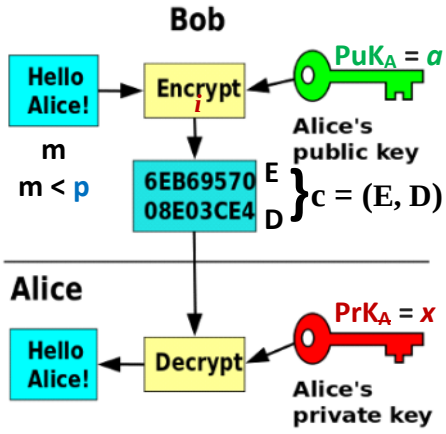
An element $g \in \mathbb{Z}_p^*$ is a generator in $\mathbb{Z}_p^*$

```
>> p=genstrongprime(28)
p = 232702259
>> pb=dec2bin(p)
pb = 1101 1101 1110 1100 0001 0011 0011
```

if and only if: 1) $g^q \neq 1 \mod p$

2) $g^2 \neq 1 \mod p$

El-Gamal Encryption-Decryption



Confidentiality

B: $i \leftarrow randi(p-1)$

$E = m \cdot a^i \bmod p$

$D = g^i \bmod p$

$c = (E, D) \longrightarrow A$

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

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

Additively-multiplicative homomorphic El-Gamal encryption

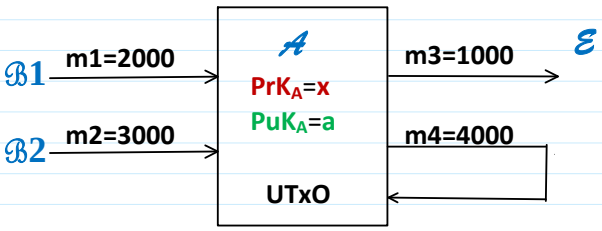
Public parameters: PP = (p, g); p=268435019; g=2;

```
>> p=genstrongprime(28)
p = 228247259

>> p=int64(268435019)
p = 268435019
>> q=(p-1)/2
q = 134217509
>> g=2
g = 2
>> mod_exp(g,q,p)     % Since g^q mod p ≠ 1 and
ans = 232702258
>> mod_exp(g,2,p)     % since g^2 mod p ≠ 1 then
ans = 4        % g = 2 is a generator in Zp* = {1, 2, 3, ..., p-1}
```

```
>> x=int64(randi(2^28-1))
x = 18245447   % Private Key - PrK = x generation
>> a=mod_exp(g,x,p)
a = 53702048   % Public key - PuK = a generation
```

Transaction - **Tx** in blockchain



Balance: $m_1 + m_2 = m_3 + m_4$

How to verify balance when inputs and expenses are encrypted?

```
>> m1=2000
m1 = 2000
>> m2=3000
m2 = 3000
>> n1=mod_exp(g,m1,p)   % n1=g^m1 mod p
n1 = 228510651
>> n2=mod_exp(g,m2,p)   % n2=g^m2 mod p
n2 = 220266692
```

Additively-homomorphic relation:

$n1 = g^{m1} \bmod p$

$n2 = g^{m2} \bmod p$

$g^{m1+m2 \bmod (p-1)} \bmod p = n1 * n2 \bmod p = n12 \bmod p$

$g^{m1+m2 \bmod (p-1)} \bmod p = g^{m1} * g^{m2} \bmod p = n1 * n2 \bmod p =$
$= n12 \bmod p.$

>> n12=mod(n1*n2,p)
n12 = 181510254

Enc(**a**, i1, n1) = (E1, D1) = (n1*$\mathbf{a}^{i1}$ mod p, $\mathbf{g}^{i1}$ mod p).
Enc(**a**, i2, n2) = (E2, D2) = (n2*$\mathbf{a}^{i2}$ mod p, $\mathbf{g}^{i2}$ mod p).
Enc(**a**, i12, n1*n2 mod p) = (E12, D12) = c12, when i12 = i1 + i2 mod (p-1).
E12 = n1*n2*$\mathbf{a}^{i1+i2}$ mod p = n12*$\mathbf{a}^{i12}$ mod p = $g^{m1+m2 \bmod (p-1)}$ mod p.
D12 = $\mathbf{g}^{i1+i2}$ mod p = $\mathbf{g}^{i12}$ mod p.