Apsilankę svetainėje
[KriptoGama (ktu.lt)]
Peržiūrėkite populiarią paskaitą apie proveržio technologijas

B111 Kriptologija 1

- 111_001 Introd-Skills-of-Mass-Disruption.pdf
- 111_001_2023_09_06_13_34_55_547.mp4

Homomorphic CryptoSystems: Computation with encrypted data in Data Center.

Declare **Public Parameters** to the network **PP** = (p, g); p= **268435019**; g=**2**;
In real cryptosystem is chosen having 2048 bits and is of order $p=2^{2048} \sim 10^{700}$, i.e. $|p|$=2048 bits.
In our simulation we use $|p|$=2048 bits, i.e. $p < 2^{28} =$ 268 435 456.

$PrK_A = x$; $PuK_A = a$: $a = g^x \bmod p$.

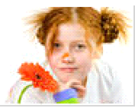
Received encrypted incomes $I1$, I_2 from $B1$, $B2$

B_1 : $I1 = 2000 \rightarrow n_1 = g^{I1} \bmod p \rightarrow Enc(a, i_1, n_1) = c_{1a} = (E_{1a}, D_{1a})$

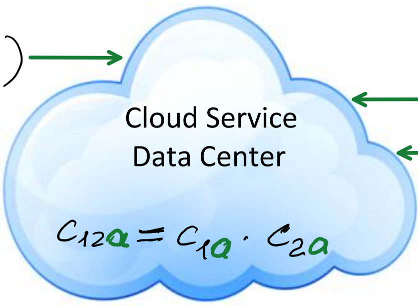
B_2 : $I2 = 3000 \rightarrow n_2 = g^{I2} \bmod p \rightarrow Enc(a, i_2, n_2) = c_{2a} = (E_{2a}, D_{2a})$

Total income of Alice is: $I_{12} = I_1 + I_2 \bmod (p-1)$

Since $I_1 + I_2 < p-1$, then $I_1 + I_2 \bmod (p-1) = I_1 + I_2$



Query (Total Incomes) →



← c_{1a}

← c_{2a}

$C_{12a} = (E_{12a}, D_{12a})$ ←

$Dec(x, C_{12a}) = n_{12}$

$n_{12} = n_1 \cdot n_2 \bmod p = g^{I1} g^{I2} \bmod p = g^{I1+I2} \bmod p = g^{I12} \bmod p$

Having n_{12} Alice finds I_{12} by the search procedure from the equation: $n_{12} = g^{I12} \bmod p$: $I_{12} = 100, 200, 300, \ldots, 5000$.

$$\left.\begin{aligned} E_{1a} &= n_1 \cdot a^{i_1} \bmod p \\ E_{2a} &= n_2 \cdot a^{i_2} \bmod p \end{aligned}\right\}$$

$i_{12} = (i_1 + i_2) \bmod (p-1)$.

$$\begin{aligned} E_{1a} \cdot E_{2a} &= n_1 \cdot n_2 \cdot a^{i_1} a^{i_2} \bmod p = \\ &= n_{12} \cdot a^{i_1 + i_2} \bmod p = \\ &= g^{I12} \cdot a^{i_{12}} \bmod p = E_{12a} \end{aligned}$$

$$\left.\begin{aligned} D_{1a} &= g^{i_1} \bmod p \\ D_2 &= g^{i_2} \bmod p \end{aligned}\right\}$$

$$\begin{aligned} D_{1a} \cdot D_{2a} &= g^{i_1} \cdot g^{i_2} \bmod p = \\ &= g^{i_1 + i_2} \bmod p = \end{aligned}$$

$$D_{2}=g^{i_2}\bmod p \quad D_{1a}\cdot D_{2a}=g^{i_1}\cdot g^{i_2}\bmod p=$$

$$=g^{i_1+i_2}\bmod p=$$

$$=g^{i_{12}}\bmod p=D_{12a}$$

$$C_{12a}=(E_{1a}\cdot E_{2a},\ D_{1a}\cdot D_{2a})=(E_{12a},D_{12a})$$

Realization:

For ElGamal Encryption, ElGamal Signature, Schnorr Identification, Schnorr Signature and Schnorr Homomorphic Multisignatures the same Public Parameters (**PP**) are used.
PP = (***p***, ***g***), where ***p*** - is a strong prime number defining set $\mathbf{Z}_p^* = \{1, 2, 3, \ldots, p\text{-}1\}$,
and ***g*** - is a generator in $\mathbf{Z}_p^*$, i.e. $g\in\Gamma$ where Γ is a set of generators.
If ***p*** is a strong prime then $p = 2*q + 1$, when ***q*** - is also prime.
Then for all $g\in\Gamma$ the following conditions hold:

$$g^q \neq 1 \ \mathbf{mod}\ p; \text{ and } g^2 \neq 1 \ \mathbf{mod}\ p. \qquad (*)$$

For example. Let ***p***=11 and is <u>prime</u>, then since ***p***=2*5+1 and ***q***=5 - is also <u>prime</u>, then ***p*** is a **strong prime**.
In this case Γ={2, 6, 7, 8}.

```
>> p=int64(genstrongprime(28))
>> p=int64(268435019)
p = 268435019
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 134217509
>> isprime(q)
ans = 1
```

Finding a generator in $\mathbf{Z}_p^* = \{1, 2, 3, \ldots, p\text{-}1\}$:

```
>> g=2;
>> mod_exp(g,q,p)
ans = 268435018
>> mod_exp(g,2,p)
ans = 4
```

Encryption-decryption formulas

B1: $m_1=2000$

$$n_1=g^{m_1}\bmod p$$

$$i_1\leftarrow randi(\mathcal{Z}_p^*)$$

$$\left.\begin{array}{l}E_{1a}=n_1\cdot a^{i_1}\bmod p\\ D_{1a}=g^{i_1}\bmod p\end{array}\right\}\ c=(E_{1a},D_{1a})$$

B2: $m_2=3000$

$$n_2=g^{m_2}\bmod p$$

$$i_2\leftarrow randi(\mathcal{Z}_p^*)$$

$$\left.\begin{array}{l}E_{2a}=n_2\cdot a^{i_2}\bmod p\\ D_{2a}=g^{i_2}\bmod p\end{array}\right\}\ c=(E_{2a},D_{2a})$$

$$C_{12a}=C_{1a}\cdot C_{2a}=(E_{1a}\cdot E_{2a}\bmod p,\ D_{1a}\cdot D_{2a}\bmod p)=(E_{12a},D_{12a})$$

A

```
>> x=int64(randi(p-1))
x = 132355164
>> a=mod_exp(g,x,p)
a = 133074594
```

B1 encryption

```
>> m1=2000
m1 = 2000
>> n1=mod_exp(g,m1,p)
n1 = 28125784
>> i1=int64(randi(p-1))
```

B2 encryption

```
>> m2=3000
m2 = 3000
>> n2=mod_exp(g,m2,p)
n2 = 222979214
>> i2=int64(randi(p-1))
```

```
>> a=mod_exp(g,x,p)
a = 133074594
```

```
>> n1=mod_exp(g,m1,p)
n1 = 28125784
 >> i1=int64(randi(p-1))
i1 = 206540100
>> a_i1=mod_exp(a,i1,p)
a_i1 = 167272090
>> E1a=mod(n1*a_i1,p)
E1a = 226124867
>> D1a=mod_exp(g,i1,p)
D1a = 204839485
```

```
>> n2=mod_exp(g,m2,p)
n2 = 222979214
>> i2=int64(randi(p-1))
i2 = 217548496
>> a_i2=mod_exp(a,i2,p)
a_i2 = 143126196
>> E2a=mod(n2*a_i2,p)
E2a = 23870093
>> D2a=mod_exp(g,i2,p)
D2a = 127689043
```

```
> E12a=mod(E1a*E2a,p)
E12a = 35955571
>> D12a=mod(D1a*D2a,p)
D12a = 117126824
```

A : is able to decrypt

$C=(E_{12a}, D_{12a})$ using her $PrK_A = x$.

1. $D_{12a}^{-x \bmod (p-1)} \bmod p$
2. $E \cdot D^{-x} \bmod p = n_{12}$

```
>> mx=mod(-x,p-1)
mx = 136079854
>> D12a_mx=mod_exp(D12a,mx,p)
D12a_mx = 23180506
>>
>> nn12=mod(E12a*D12a_mx,p)
nn12 = 143845522
>>
>> n12=mod(n1*n2,p)
n12 = 143845522
```

$Ax = b \rightarrow$ rasti x.