Paskaita 9

-1-

Public-Key encryption

Viešojo rakto kriptografija

Dauguma simetrinių kriptografinių algoritmų naudoja raktą, kuris ir yra šių sistemų saugumo pagrindas.

Tada labai svarbus uždavinys – paskirstyti raktus (e-prekyvimų, pervedimo, bankinės operacijos, internetinės paslaugos – raktais keičiasi nepažįstami dalyviai ir jų atsiradimas nėra iš anksto prognozuojamas). Enigma – istorinis pvz., kai raktų paskirstymas tapo labai aktualus.

Jeigu tinkle yra n - dalyvių ir juos reikia komunikuoti tarpusavyje, tai turime $\frac{n(n-1)}{2}$ porų. Jei $n = 10^4$, tai $\frac{n(n-1)}{2} = \frac{1}{2} 10^8$ - raktų.

Viešo rakto sistema: pranešimas koduojamas viešu raktu (visi jį žino), kiekvienas vartotojas (public key) savo raktą gali publikuoti viešai.

Private key – jį žino tik siuntimas

(tai secret key): ~~ki~~

Svarbu, kad žinodamas public key pašalinis negalėtų sužinoti private key

Aišku, reikia garantuoti, kad viešojo rakto negalėtų pakeisti pašalinis.

a) pašto siunta su 2 spynom

b) ~~da~~ mūsų naudojimas pasikeisti raktais (priminti).

RSA - kriptografinė sistema

(iki šiol tai populiariausias rakto pasikeitimo algoritmas)

1. Pasirenkame ~~du~~ atsitiktinai du pirminius skaičius p ir q

$$n = pq$$

2. Pasirenkame $e \in \mathbb{N}$

$$1 < e < \varphi(n) = (p-1)(q-1)$$

tokį, kad $\gcd(e, (p-1)(q-1)) = 1$

(tarpusavyje pirminiai)

3. Apskaičiuojame d:

$$1 < d < (p-1)(q-1) \quad \text{ir}$$

$$de \equiv 1 \bmod (p-1)(q-1).$$

(toks $d = e^{-1}$ egzistuoja, nes $\gcd(e, (p-1)(q-1)) = 1$, jį skaičiuojame Euklido algoritmu)

Viešasis raktas: (n, e)

Privatusis raktas: d.

Saugumas: grindžiamas faktu, kad žinant n, labai sudėtingas uždavinys rasti p ir q.

Šifravimo žingsnis

Pranešimas: $0 \le m < n$

m – plain text

Užšifruotas pranešimas (ciphertext)

$$\boxed{C = m^e \bmod n}$$

Dešifravimo žingsnis

T. Tegul (n, e) yra RSA viešasis raktas, o d – privatusis raktas. Tada

$$(m^e)^d \bmod n = m \quad (C^d \bmod n = m)$$

Žinodami d galime greitai dešifruoti pranešimą

Pavyzdys.

$p = 3, \quad q = 7 \Rightarrow n = 21.$

$\varphi(21) = 2 \cdot 6 = 12 = 4 \cdot 3$

$e = 5 \quad (\gcd(5, 12) = 1)$

$d = 5 \quad (ed = 25 \equiv 1 \bmod 12).$

Pasirenkame pranešimą $m = 14$.

Apskaičiuojame $C = 14^5$. (~~ka~~ mod 21

$14^2 = 196 \equiv 7 \bmod 21$

$14^4 \equiv 49 \equiv 7 \bmod 21.$

$\boxed{C = 98 \equiv 14 \bmod 21.}$

Tai nesunku buvo ir prognozuoti

$m = C^5 \equiv 14 \bmod 21.$

Kadangi $ed \equiv 1 \mod (p-1)(q-1)$

tai $\exists\, l \in \mathbb{Z}$ ~~toks~~, kad

$$ed = 1 + l(p-1)(q-1)$$

(Priminti svarbiausius faktus
Euklido algoritmas:

$$ex + (p-1)(q-1)y = 1.$$

$\cancel{x>0}$ $d = x$, $l = -y$.)

$$(m^e)^d = m^{ed} = m\left(m^{(p-1)(q-1)}\right)^l$$

Tada galime įrodyti, kad p ir q atžvilgiu ~~turime teiginius~~

T1 $\boxed{(m^e)^d \equiv m\left(m^{(p-1)(q-1)}\right)^l \equiv m \mod p}$

Bet m mes dar neradome
įrodėme tik ekvivalentumą

a) jeigu p yra m daliklis
tai $0 \equiv 0 \mod p$.

p - pirminis sk.

b) jeigu p nėra m daliklis, tai
teiginys seka iš mažosios Ferma
teoremos.

Analogiškai įrodome, kad

$$(m^e)^d \equiv m \mod q.$$

Priminsime, kad p ir q yra skirtingi pirminiai skaičiai.

Pasinaudosime tokiu rezultatu:

$$\begin{matrix} a \equiv m \mod p \\ a \equiv m \mod q \end{matrix} \Rightarrow a \equiv m \mod pq$$

$a - m = p \cdot l$, $a - m = q k$

Kadangi $a-m$ dalijasi iš q, ir q yra pirminis skaičius, tai q yra arba p, arba l daliklis. Bet p irgi pirminis, todėl $l = q \cdot s \Rightarrow a - m = p \cdot q \cdot s$

$$\Rightarrow \boxed{a \equiv m \mod pq.}$$

Gavome, kad

$$(m^e)^d \equiv m \mod n.$$

Bet $0 \le m < n \Rightarrow$

$$\boxed{(m^e)^d = m \mod n.}$$

$$\boxed{c^d = m \mod n}$$

Tegul $a \in \mathbb{Z}$, $e \geq 1$.

$$e=\sum_{i=0}^{k} e_i 2^i = e_0 1 + e_1 2 + \dots + e_k 2^k$$

(skaičius e – užrašytas dvejetainėje sistemoje)

$$a^e = a^{\sum_{i=0}^{k} e_i 2^i} = \prod_{i=0}^{k} \left(g^{2^i}\right)^{e_i}$$

$$= \prod_{\substack{0 \le i \le k \\ e_i = 1}} g^{2^i}$$

$$\boxed{g^{2^{i+1}} = \left(g^{2^i}\right)^2 = g^{2^i} \cdot g^{2^i}}$$

Greitoji daugyba

Pav. $6^{73} \bmod 100$

$73 = 1 + 2^3 + 2^6$ $\quad \boxed{e_0 = e_3 = e_6 = 1.}$

$\boxed{6}$, $6^2 = 36$, $6^4 = 36 \cdot 36 \equiv -4 \bmod 100$

$\boxed{6^8 \equiv 16 \bmod 100}$, $6^{16} \equiv 16^2 \equiv 56 \bmod 100$

$\cancel{\tau \cdot \tau^2 = \tau^3}$

$\cancel{2 \cdot \frac{\tau}{2} \left(\frac{\tau}{2}\right)^2 = \frac{\tau^3}{4}}$

$6^{32} \equiv 56^2 \, \cancel{\text{mod}} \equiv 36 \mod 100$

$\boxed{6^{64} \equiv 36^2 \equiv -4 \mod 100}$

$-4 \mod 100$

$6^{73} = 6^1 \cdot 6^8 \cdot 6^{64} = 6 \cdot 16 \cdot (-4) \equiv 16 \mod 100$

$\boxed{6 \cdot 16 = 96 \equiv -4 \mod 100}$

Algoritmas

```
pow( ~~base~~ base, e )
result = 1;  ~~base = a~~ ;
while ( e > 0 ) {
    if ( e % 2 == 1 )
        result = result · base (mod n)
    base = base · base mod n;
    e = e / 2;
}
return (result);
```