Algebros pratybos
Rimantas Grigutis

4 pratybos. 16 bitų RSA kriptosistema

Apibrėžkime 16 bitų RSA kriptosistemą tokia schema:

$$\boxed{\text{Tekstas } \mathbf{T}\text{: } A,B,C,D,\mathbf{...}}$$

$$\overset{\text{kodavimas ASCII kodu}}{\longrightarrow} \boxed{A,B,C,D,\mathbf{...}\rightarrow 65,66,67,68,...}$$

$$\overset{\text{ASCII simbolio 8 bitų dvejetainio kodo radimas}}{\longrightarrow} \boxed{A\rightarrow 01000001, B\rightarrow 01000010,...}$$

$$\overset{\text{16 bitų dvejetainio kodo sudarymas}}{\longrightarrow} \boxed{AB\rightarrow 01000001\ 01000010,...}$$

$$\overset{\text{10-io skaičiaus radimas}}{\longrightarrow} \boxed{01000001\ 01000010 \rightarrow \mathbf{x}=16706,... \in \mathbf{Z}_n,}$$

$$\overset{\text{kiekvieno 10-io skaičiaus šifravimas}}{\longrightarrow} \boxed{\mathbf{y}=e(\mathbf{x})=\mathbf{x}^{\mathbf{E}}\pmod n,...}$$

$$\overset{y,\text{... siuntimas}}{\rightsquigarrow} \boxed{\mathbf{y}\in\mathbf{Z}_n}$$

$$\overset{\text{dešifravimas}}{\longrightarrow} \boxed{d(\mathbf{y})=\mathbf{y}^{\mathbf{D}}=\mathbf{x}^{\mathbf{ED}(\bmod \varphi(n))}\equiv \mathbf{x}\pmod n,...} \rightarrow \boxed{\mathbf{x}=16706,...}$$

$$\overset{\text{dekodavimas}}{\longrightarrow} \boxed{\mathbf{T}: A,B,...}.$$

RSA kriptosistema - tai penketas$\{n,p,q,\mathbf{E},\mathbf{D}\}$ gaunamas šiomis sąlygomis:

1. Generuojami du (dideli) pirminiai skaičiai p ir q ir randama $n=p\cdot q$.

2. Skaičiuojama $\varphi(n)=(p-1)(q-1)$ ir parenkamas tarpusavyje pirminis su $\varphi(n)$ skaičius $\mathbf{E}$.

3. Sprendžiant lyginį $\mathbf{ED}\equiv 1\pmod{\varphi(n)}$ gaunamas $\mathbf{D}=\mathbf{E}^{-1}\pmod{\varphi(n)}$.

Skaičiai $(n,\mathbf{E})$ vadinami kriptosistemos *atviru raktu(public key)* ir talpinami į atvirą katalogą; skaičiai $(p,q,\mathbf{D})$ vadinami *slaptu raktu(private key)* ir reikalauja apsaugos.

Abonentas A norėdamas siųsti tekstą T abonentui B, renkasi pastarojo atvirame kataloge skaičių porą $(n,\mathbf{E})$, koduoja jį, šifruoja gautą kodą ir siunčia užšifruotą tekstą kartu su skaičių pora $(n,\mathbf{E})$ abonentui B, kuris, žinodamas slaptąjį raktą $(p,q,\mathbf{D})$, dešifruoja, o poto dekoduoja bei skaito gautą pranešimą.

Pavyzdys.
Duota: *n=49401, E=5*, siunčiamas pranešimas $\mathrm{x}_1\_\ \mathrm{x}_2$: 3070_40390.
Sprendimas.
1. Skaičiaus n faktorizacija $\mathrm{F}_{\mathrm{Ferma}}\mathrm{F}_{\mathrm{Faktorizacijos}}\mathrm{P}_{\mathrm{Pr\,ocesu}}$:

$$49601 = 193 \times 257.$$

2. Oilerio funkcijos reikšmės skaičiavimas($\varphi(n) = (p-1)(q-1)$):

$$\varphi(49601) = (193-1)(257-1) = 49\,152.$$

3. D radimas. lyginio $\mathbf{ED} \equiv 1 \pmod{\varphi(n)}$:

$$5 \cdot \mathbf{D} = 1 \pmod{49152}$$
$$\mathbf{D} = 19661.$$

4. Pranešimo dešifravimas. $\mathrm{x}_1^D \pmod n$ ir $\mathrm{x}_2^D \pmod n$ skaičiavimas rašant D dvejetainį kodą:

$$x_1^D \pmod n = 3070^{19661} \bmod 49601 = 21\,591 = \alpha$$
$$x_2^D \pmod n = 40390^{19661} \bmod 49601 = 18\,766 = \beta$$

5. α ir β dvejetainiai ir dešimtainiai kodai:

$$\alpha = 01010100\ 01010111 = 84\ 87$$
$$\beta = 01001001\ 01001110 = 73\ 78.$$

6. Dekodavimas ASCII simboliais ir pranešimo skaitymas:

$$84\ 87\ 73\ 78 = T\ W\ I\ N.$$

RSA kriptosistemos parametrų slaptumo minimumas:
1. Kiekvienas vartotojas turi nepriklausomai ir slaptai generuoti skaičius p ir q. Tas pats skaičius $n = p \cdot q$ negali būti bendras dviems vartotojams.
2. Skaičiai p ir q negali būti žinomuose pirminių skaičių sąrašuose. Jokių išorinių dėsningumų!
3. Skaičiai p ir q negali būti artimi pirminiai skaičiai tam, kad $\mathrm{F}_{Ferma}\mathrm{F}_{Faktorizacijos}\mathrm{P}_{\mathrm{Pr\,}ocesas}$ būtų neveiksmingas.
4. Skaičiai $p, p-1.p+1, \frac{p-1}{2}, \frac{p+1}{2}; q, q-1, q+1, \frac{q-1}{2}, \frac{q+1}{2}$ neturi turėti mažų pirminių daliklių, bei turėti bent vieną didelį pirminį daliklį.
5. Grupėje U_n neturi būti daug mažos eilės elementų.