8. PAVYZDYS IŠ KRIPTOGRAFIJOS

Kriptografija yra kriptologijos dalis, nagrinėjanti informacijos šifravimo bei dešifravimo būdus. Jų yra daug. Mes panagrinėsime vieną iš jų.

1. Kiekvienam tekste T naudojamam simboliui (simbolių grupei) vienareikšmiškai priskirkime vieną iš $\mathbb{Z}_n$ elementų.

2. Skaičius n turėtų tenkinti šias sąlygas:

a) $n = p \cdot q$ – dviejų didelių pirminių skaičių sandauga;

b) p ir q turėtų būti tokie dideli pirminiai skaičiai, kad net pasitelkus kompiuterius, reiktų labai daug laiko skaičiui n suskaidyti dauginamaisiais. Pavyzdžiui, šie skaičiai p ir q galėtų turėti po 100 dešimtainių skaitmenų.

3. Kadangi $\varphi(n) = \varphi(p \cdot q) = (p-1)(q-1)$, todėl parinkime tokį skaičių E taip, kad

$$\mathrm{DBD}\left(E, \varphi(n)\right) = 1,$$

t.y.

$$\mathrm{DBD}\,(E, p-1) = \mathrm{DBD}\,(E, q-1) = 1.$$

4. Iš skaičiaus E apibrėžimo matome, kad $E \in U_{\varphi(n)}$, todėl galime rasti $D = E^{-1} \pmod{\varphi(n)} : DE \equiv 1 \left(\mathrm{mod}\ (p-1)(q-1)\right)$.

Parametrai n, p, q, E, D apibrėžia mūsų teksto T įslaptinimo-išslaptinimo kriptosistemą. Skaičiai p, q ir D turėtų būti įslaptinti, o skaičių n ir E būtina neslėpti.

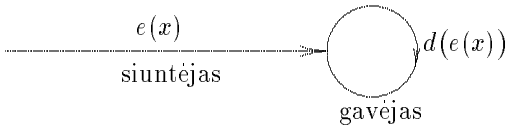
Kaip minėjome, tekstą (arba jo dalį), kurį įslaptinę norime perduoti, reikšime žiedo $\mathbb{Z}_n$ elementu $x \in \mathbb{Z}_n$. Šį elementą x įslaptinsime naudodamiesi bijektyvia funkcija $e : \mathbb{Z}_n \to \mathbb{Z}_n$:

$$e(x) = x^E \pmod{n}.$$

Teksto gavėjas, žinodamas skaičių D ir norėdamas išslaptinti $e(x) \in \mathbb{Z}_n$, turėtų pasinaudoti bijektyvia funkcija $d : \mathbb{Z}_n \to \mathbb{Z}_n$:

$$d(y) = y^D \pmod{n}.$$

$$d\big(e(x)\big) = \big(x^E\big)^D \pmod n \equiv x^{ED} \pmod n = x^{1+\varphi(n)\cdot k} =$$
$$= \big(x^{\varphi(n)}\big)^k x \equiv x \pmod n.$$



Išnagrinėkime konkretesnį pavyzdį. Kiekviename lietuvių kalba parašytame tekste naudojamam simboliui vienareikšmiškai priskirkime žiedo $\mathbb{Z}_{33}$ elementą

a	00	ą	01	b	02	c	03	č	04
d	05	e	06	ę	07	ė	08	f	09
g	10	h	11	i	12	į	13	y	14
j	15	k	16	l	17	m	18	n	19
o	20	p	21	r	22	s	23	š	24
t	25	u	26	ų	27	ū	28	v	29
z	30	ž	31.						

Taigi $n = 33 = 3 \cdot 11$, $\varphi(33) = 20$. Parinkime $E = 7$, DBD $(7, 20) = 1$. Tada $D \equiv E^{-1} \pmod{20} = 3$.

Tekstas, kurį norime perduoti, yra žodis $M =$„matematika“. Kiekvienai raidei vienareikšmiškai priskyrę kūno $\mathbb{Z}_{33}$ elementą, gausime tekstą $M =$„18002506180025121500“.

Pastebėsime, kad prieš įslaptinant labai ilgą tekstą, galima jį suskaidyti į blokus $M = M_1 M_2 \dots M_k$ taip, kad kiekviena iš šių blokų M_i, $1 \leqslant i \leqslant k$, skaitinių reikšmių neviršytų n: $0 \leqslant M_i \leqslant n-1$. Pavyzdžiui, jeigu n yra 100 skaitmenų dešimtainis skaičius, tai bloko M_i ilgis galėtų būti net 10^{100}.

Mūsų atveju $M_1 = 18$, $M_2 = 00$, $M_3 = 25$, $M_4 = 06$, $M_5 = 18$, $M_6 = 00$, $M_7 = 25$, $M_8 = 12$, $M_9 = 15$, $M_{10} = 00$.

Įslaptinę kiekvieną M_i, $1 \leqslant i \leqslant 10$, $e(M_i) = M^E = C_i$, gausime

tekstas	m	a	t	e	m	a	t	i	k	a
i	1	2	3	4	5	6	7	8	9	10
M_i	18	00	25	06	18	00	25	12	15	00
$C_i = M_i^7 \pmod{33}$	06	00	31	30	06	00	31	12	27	00

Siuntėjas, norėdamas išslaptinti gautą tekstą $C = C_1C_2 \ldots C_{10}$, turėtų pasinaudoti funkcija $d : \mathbb{Z}_{33} \to \mathbb{Z}_{33} : d(C_i) = C_i^3 \equiv M_i \pmod{33}$.

Įvertinkime sunkumus, kuriuos tektų įveikti nežinant įslaptintų parametrų p, q ir D, bet norint išslaptinti tekstą C.

Galimi du būdai. *Pirmasis* – bandymas surasti skaičių $D \equiv E^{-1} \pmod{\big((p-1)(q-1)\big)}$. Tam reiktų žinoti skaičius p ir q. Bet jeigu šie skaičiai labai dideli, tai skaičiaus $n = p \cdot q$ skaidymas dauginamaisiais užims labai daug laiko.

Antrasis – pabandyti rasti $\varphi(n)$ reikšmę, o tada ir išspręsti lyginį $D \cdot E \equiv 1 \pmod{\varphi(n)}$. Tiesa, ir šis būdas ne ką lengvesnis negu skaičiaus n skaidymas dauginamaisiais.

Žinodami $\varphi(n)$ reikšmę, skaičius p ir q galime rasti ir taip:

$$\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1.$$
$$(p-q)^2 = (p+q)^2 - 4pq = (p+q)^2 - 4n.$$

Taigi žinodami $\varphi(n)$ ir n, galėtume rasti $p+q$ ir $p-q$, taip pat ir skaičius p ir q (spręsdami paprasčiausią lygčių sistemą).

Pateiksime dar vieną kinų teoremos taikymo pavyzdį.

Tegu $f_1(x), f_2(x), \ldots, f_n(x)$ yra polinomai su sveikaisiais koeficientais ir mes norime atlikti aritmetinius veiksmus su jais kokioje nors šių polinomų aritmetinėje išraiškoje $I = I\big[f_1(x), f_2(x), \ldots, f_n(x)\big]$. Šių veiksmų rezultatą išraiškoje $I\big[f_1(x), f_2(x), \ldots, f_n(x)\big]$ pažymėkime $\operatorname{res}(x)$.

Sakykime, $\operatorname{res}(x) \in Z[x]$ ir galime įvertinti polinomo $\operatorname{res}(x) = a_t x^t + a_{t-1}x^{t-1} + \ldots + a_0$ koeficientus: $0 \leqslant |a_i| \leqslant m = m_1 m_2 \ldots m_l$, $0 \leqslant i \leqslant t$, $\operatorname{DBD}(m_\alpha, m_\beta) = 1$, $\alpha \neq \beta$.

Apibrėžkime polinomo $f(x) = b_r x^r + b_{r-1}x^{r-1} + \ldots + b_0 \in Z[x]$ redukavimo veiksmą moduliu m kaip funkciją $r_m : Z[x] \to Z_m[x]$, $r_m\big(f(x)\big) = r_m\big(b_r x^r + b_{r-1}x^{r-1} + \ldots b_0\big) = K_{b_r}x^r + K_{b_{r-1}}x^{r-1} + \ldots + K_{b_0} = \bar{b}_r x^r + \bar{b}_{r-1}x^{r-1} + \ldots + \bar{b}_0$.

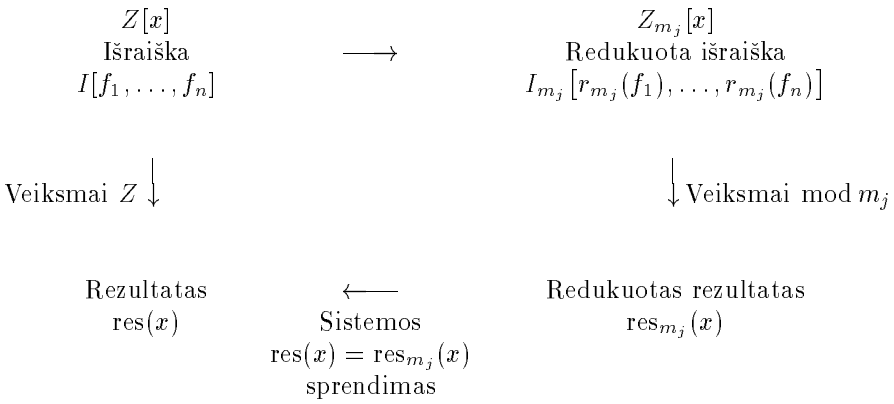
Aritmetinius veiksmus išraiškoje I pakeiskime aritmetiniais veiksmais paprastesnėse išraiškose

$$I_{m_j}\big[r_{m_j}\big(f_1(x)\big), r_{m_j}\big(f_2(x)\big), \ldots, r_{m_j}\big(f_n(x)\big)\big],$$

o šių veiksmų rezultatą pažymėkime $\operatorname{res}_{m_j}(x)$, $1 \leqslant j \leqslant l$. Polinomą $\operatorname{res}(x)$ galėsime rasti, išsprendę sistemą

$$\operatorname{res}(x) \equiv \operatorname{res}_{m_j}(x) \pmod{m_j}, \quad j = 1, 2, \ldots, l.$$

Visą šią procedūrą galima pavaizduoti diagrama:



6.37 pavyzdys. Sakykime, norime sudauginti du polinomus $f_1(x) = 7x + 3$ ir $f_2(x) = 2x^2 + 4$: $f(x) = f_1(x) \cdot f_2(x)$. Aišku, kad polinomo $f(x)$ koeficientai neviršys polinomų $f_1(x)$ ir $f_2(x)$ maksimalių koeficientų sandaugos. O ji yra $4 \cdot 7 = 28$. Tegu $m = 7 \cdot 5 > 28$.

Kai $m_1 = 5$, tai

$$\mathrm{res}_5(x) = r_5(7x+3) \cdot r_5(2x^2+4) = (2x+3)(2x^2+4) = 4x^3 + x^2 + 3x + 2.$$

Kai $m_2 = 7$, tai

$$\mathrm{res}_7(x) = r_7(7x+3) \cdot r_7(2x^2+4) = 3 \cdot (2x^2+4) = 6x^2 + 5.$$

Dabar turėtume spręsti šią lyginių sistemą:

$$\begin{aligned} \mathrm{res}(x) &\equiv 4x^3 + x^2 + 3x + 2 \pmod 5, \\ \mathrm{res}(x) &\equiv 6x^2 + 5 \pmod 7. \end{aligned}$$

Aišku, kad $\mathrm{res}(x) = ax^3 + bx^2 + cx + d$. Šio polinomo koeficientus rasime išsprendę lyginių sistemas:

$$\begin{aligned} &a \equiv 4 \pmod 5, \quad b \equiv 1 \pmod 5, \quad c \equiv 3 \pmod 5, \quad d \equiv 2 \pmod 5, \\ &a \equiv 0 \pmod 7, \quad b \equiv 6 \pmod 7, \quad c \equiv 0 \pmod 7, \quad d \equiv 5 \pmod 7. \end{aligned}$$

Pritaikę 4 kartus 6.29 algoritmą, gausime

$$a = 14, \quad b = 6, \quad c = 28, \quad d = 12, \quad \text{t.y. } f(x) = 14x^3 + 6x^2 + 28x + 12.$$

Pastebėsime, kad sprendžiant lyginių sistemą

$$\mathrm{res}(x) \equiv \mathrm{res}_{m_j}(x) \pmod{m_j}, \quad 1 \leqslant j \leqslant l,$$

buvo pasinaudota teiginiu: jeigu $u(x) = a_n x^n + \ldots + a_0$ ir $v(x) = b_n x^n + \ldots + b_0$ polinomai iš $Z[x]$, o $m \in N$, tai

$$u(x) \equiv v(x) \pmod m \iff u(x) - v(x) \text{ dalijasi iš } m \iff$$

$$(a_i - b_i) \text{ dalijasi iš } m,\ 1 \leqslant i \leqslant n \iff a_i \equiv b_i \pmod m, 1 \leqslant i \leqslant n.$$