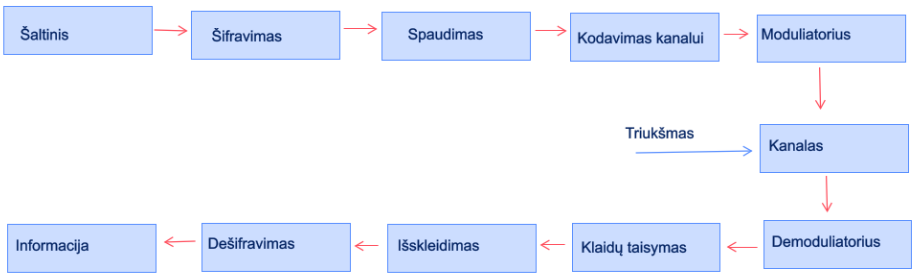
Informacijos kodavimo algoritmai

VILIUS STAKĖNAS
VU 2023

Informacijos perdavimo schema



Koduodami siekiame:

- taupumo;
- patikimumo;
- apsaugos.

Informacijos teorijos pagrindai

Abėcėlės ir žodžiai

Ženklų, kuriais užrašome žinias, aibę vadinsime abėcėle. Abėcėlė – baigtinė simbolių aibė

$$\mathcal{A} = \{a_1, a_2, \ldots, a_r\}, \quad |\mathcal{A}| = r.$$

Iš abėcėlės simbolių galime sudaryti žodžius:

$$\mathrm{a} = a_{i_1} a_{i_2} \cdots a_{i_n}, \quad a_{i_j} \in \mathcal{A}.$$

n-ilgio žodžių, sudarytų iš abėcėlės $\mathcal{A}$ simbolių aibę žymėsime $\mathcal{A}^n$; $|\mathcal{A}^n| = r^n$. Visų žodžių aibę žymėsime $\mathcal{A}^*$; ši aibė yra begalinė:

$$\mathcal{A}^* = \mathcal{A}^1 \cup \mathcal{A}^2 \cup \cdots$$

Kodai

Apibrėžimas. Tegu $\mathcal{A}, \mathcal{B}$ yra dvi abėcėlės. Kodu vadinsime atvaizdį

$$c^* : \mathcal{A}^* \to \mathcal{B}^*.$$

Kad duomenys koduojant nebūtų pakeičiami be galimybės juos visada atkurti, atvaizdis turi būti injektyvus: a_1, a_2 yra du skirtingi aibės $\mathcal{A}^*$ žodžiai, tai $c^*(a_1), c^*(a_2)$ irgi skirtingi.

Priešdėliai ir priesagos

Apibrėžimas. Baigtinę abėcėlės $\mathcal{A}$ simbolių seką $x_1 \dots x_m$ vadinsime m ilgio žodžiu.
Jei x yra žodis, tai $|x|$ žymėsime jo ilgį.
Jei x, y yra du tos pačios abėcėlės žodžiai, tai xy žymėsime sudurtinį žodį, kuris gaunamas tiesiog sujungiant x ir y. Žodį x vadinsime šio sudurtinio žodžio priešdėliu, o y – priesaga.

Kodavimo taisyklė

Apibrėžimas. Tegu $\mathcal{A}$ ir $\mathcal{B}$ yra dvi baigtinės abėcėlės, o $c : \mathcal{A} \to \mathcal{B}^*$ injektyvus atvaizdis. Kodavimo taisyklę $c^* : \mathcal{A}^* \to \mathcal{B}^*$,

$$c^*(x_1 x_2 \cdots x_n) = c(x_1)c(x_2)\cdots c(x_n), \quad x_i \in \mathcal{A},$$

vadinsime atvaizdžio c tęsiniu. Abėcėlės $\mathcal{B}$ žodį $c^*(x_1 x_2 \cdots x_n)$ vadinsime žodžio $x_1 x_2 \cdots x_n$ kodu.

Svarbiausias šios konstrukcijos elementas yra atvaizdis $c : \mathcal{A} \to \mathcal{B}^*$, tai dažnai būtent jį ir vadinsime kodu.

Kodas – žodžių seka

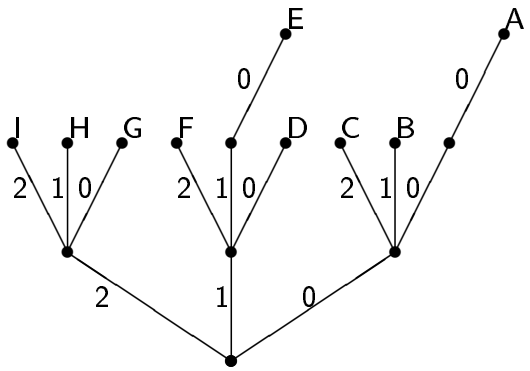
Tegu $\mathcal{A} = \{a_1, a_2, \ldots, a_r\}$.
Tada kodą $c : \mathcal{A} \to \mathcal{B}^*$ galime apibrėžti tiesiog surašydami žodžius $c(a_i)$ į eilę (sudarydami gretinį):

$$\langle \mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_r \rangle, \quad \mathrm{c}_i = c(a_i).$$

Dažnai kodu vadinsime tiesiog atitinkamos abėcėlės žodžių gretinį, arba tiesiog žodžių poaibį

$$\mathrm{C} = \{\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_r\} \subset \mathcal{B}^*.$$

Kodai ir medžiai



Kodo $c : \mathcal{A} \to \mathcal{B}^*$ medis, $\mathcal{A} = \{A, B, C, D, E, F, G, H, I\}$, $\mathcal{B} = \{0, 1, 2\}$.

Polibijaus ugnies kodas

α	11	ι	24	ρ	42
β	12	κ	25	σ	43
γ	13	λ	31	τ	44
δ	14	μ	32	υ	45
ϵ	15	ν	33	ϕ	51
ζ	21	ξ	34	χ	52
η	22	o	35	ψ	53
θ	23	π	41	ω	54

Morzės kodas

a	·—	*j*	· — ——	*s*	· · ·
b	— · ··	*k*	— · —	*t*	—
c	— · —·	*l*	· — ··	*u*	· · —
d	— · ·	*m*	——	*v*	· · ·—
e	·	*n*	—·	*w*	· — —
f	· · —·	*o*	— — —	*x*	— · ·—
g	— — ·	*p*	· — —·	*y*	— · ——
h	· · ··	*q*	— — ·—	*z*	— — ··
i	··	*r*	· — ·		

Baudot kodas

Raidė	Kodas	Simbolis	Raidė	Kodas	Simbolis
A	10000	1	*Q*	10111	/
B	00110	8	*R*	00111	–
C	10110	9	*S*	00101	*Tarpas*
D	11110	0	*T*	10101	∅
E	01000	2	*U*	10100	4
F	01110	∅	*V*	11101	′
G	01010	7	*W*	01101	?
H	11010	+	*X*	01001	,
I	01100	∅	*Y*	00100	3
J	10010	6	*Z*	11001	:
K	10011	(	*RP*	00001	*RP*
L	11011	=	*SP*	11000	*SP*
M	01011	)	*IV*	11000	*IV*
N	01111	∅	*EP*	10001	*EP*
O	11100	5	*ER*	00011	*ER*
P	11111	%	∅	00000	∅

Dekoduojami kodai

Apibrėžimas. Kodą $c : \mathcal{A} \to \mathcal{B}^*$ vadinsime dekoduojamu, jeigu jo tęsinys $c^* : \mathcal{A}^* \to \mathcal{B}^*$ yra injektyvus atvaizdis.

Tai reiškia, kad gavėjas niekada negaus simbolių eilutės, kurią būtų galima suvokti nevienareikšmiškai.
Dekoduojamo kodo sąvoką apibrėžkime neminėdami šaltinio abėcėlės $\mathcal{A}$.
Apibrėžimas. Kodą $C = \{c_1, c_2, \ldots, c_r\} \subset \mathcal{B}^*$ vadinsime dekoduojamu, jeigu lygybė

$$x_1 x_2 \ldots x_k = y_1 y_2 \ldots y_l, \quad x_i, y_j \in C,$$

galima tada ir tik tada, kai $k = l$ ir $x_i = y_i,\ i = 1, 2, \ldots, k$.

Momentiniai kodai

Apibrėžimas. Kodą $c : \mathcal{A} \to \mathcal{B}^*$ vadinsime momentiniu kodu, jeigu nei vienas žodis $c(a),\ a \in \mathcal{A}$, nėra jokio kito žodžio $c(a'),\ a' \in \mathcal{A}, a \neq a'$, priešdėlis.

Jeigu kuris nors žodis būtų ilgesnio žodžio priešdėliu, tai gavę jį perduodamų simbolių sraute, dar turėtume palaukti ir įsitikinti, kad jis nėra tik ilgesniojo žodžio pradžia.

Pavyzdžiai

Kiek ir kokio ilgio žodžių gali turėti kodas, kad jis būtų dekoduojamas?

Pavyzdys. Tegu kodo abėcėlė dvejetainė: $\mathcal{B} = \{0, 1\}$. Ar galime iš šios abėcėlės žodžių sudaryti momentinį kodą, kad jų ilgiai būtų $2; 2; 2; 3; 3$? Galime:

$$c_1 = 00, \quad c_2 = 01, \quad c_3 = 10, \quad c_4 = 111, \quad c_5 = 110.$$

Pavyzdys. Ar galima iš dvejetainės abėcėlės žodžių sudaryti momentinį kodą, kad žodžių ilgiai būtų $2; 2; 2; 2; 3$?

$$c_1 = 00, \quad c_2 = 01, \quad c_3 = 10, \quad c_4 = 11, \quad c_5 = ?$$

Momentinio kodo nesudarysime.

Krafto-Makmillano nelygybė

Teorema. Tegu $\mathcal{B}$ yra abėcėlė, $b = |\mathcal{B}|$, o $s_1, s_2, \ldots, s_n$ yra natūralieji skaičiai, tenkinantys nelygybę:

$$\sum_{i=1}^{n} b^{-s_i} \leqslant 1.$$

Tada egzistuoja momentinis kodas $C = \{c_1, c_2, \ldots, c_n\}$, kad $|c_i| = s_i, \ i = 1, 2, \ldots, n$.

Bet kokio dekoduojamo kodo žodžiai tenkina šią nelygybę.

Informacijos šaltiniai

Apibrėžimas. Informacijos šaltiniu vadinsime atsitiktinių dydžių, įgyjančių reikšmes iš tos pačios abėcėlės $\mathcal{A}$, seką

$$\mathcal{U} = \langle U_1, U_2, \ldots \rangle.$$

Jeigu apsiribosime tik šaltinio perduotu n ilgio simbolių srautu, tai sakysime, kad nagrinėjame dalinį šaltinį

$$\mathcal{U}_n = \langle U_1, U_2, \ldots, U_n \rangle.$$

Šaltinį $\mathcal{U}_1$ galime tiesiog sutapatinti su atsitiktiniu dydžiu U_1. Pažymėkime simbolių perdavimo tikimybes:

$$p_i = P(U_1 = a_i), \quad i = 1, 2, \ldots, r.$$

Vidutinis kodo žodžių ilgis

Nagrinėsime vieno simbolio dekoduojamus kodus $c : \mathcal{A} \to \mathcal{B}^*$.
Apibrėžimas. Vidutiniu momentinio kodo $c : \mathcal{A} \to \mathcal{B}^*$ žodžių ilgiu vadinsime skaičių

$$\lambda(c) = \sum_{i=1}^{r} |c(a_i)| \cdot p_i.$$

Momentinį kodą $\hat{c} : \mathcal{A} \to \mathcal{B}^*$ vadinsime optimaliu šaltinio $\mathcal{U}_1$ kodu, jeigu

$$\lambda(\hat{c}) = \min_c \lambda(c),$$

čia minimumas imamas pagal visus momentinius kodus $c : \mathcal{A} \to \mathcal{B}^*$.

Shannono kodai

Sudarant kodą, geriausiai tinkantį šaltiniui, reikia siekti, kad rečiau pasitaikantys simboliai būtų koduojami ilgesniais, o dažniau – trumpesniais žodžiais.
Tarkime, šaltinio tikimybės išrikiuotos mažėjimo tvarka:

$$p_1 \geqslant p_2 \geqslant \ldots \geqslant p_r.$$

Parinkime natūraliuosius skaičius $1 \leqslant s_1 \leqslant s_2 \leqslant \ldots \leqslant s_r$, kad jie tenkintų nelygybes

$$b^{-s_i} \leqslant p_i < b^{-s_i+1}, \quad i = 1, 2, \ldots, r.$$

Kadangi

$$\sum_{i=1}^{r} b^{-s_i} \leqslant \sum_{i=1}^{r} p_i = 1,$$

tai galima sudaryti momentinį kodą $\hat{c} : \mathcal{A} \to \mathcal{B}^*$, kad $|\hat{c}(a_i)| = s_i$.
Tokie kodai vadinami Shannono kodais.

Shannono kodai

Tegu $b > 1$ yra natūralusis skaičius (abėcėlės simbolių skaičius).
Kiekvieną intervalo $(0; 1)$ skaičių α galime užrašyti b-aine trupmena:

$$\alpha = \frac{d_1}{b} + \frac{d_2}{b^2} + \frac{d_3}{b^3} + \ldots, \quad d_i \in \{0, 1, \ldots, b-1\}.$$

Tegu p_i yra šaltinio simbolių tikimybės, o s_i – Shannono kodo žodžių ilgiai:

$$p_1 \geqslant p_2 \geqslant \ldots \geqslant p_n,$$
$$b^{-s_i} \leqslant p_i < b^{-s_i+1}, \quad i = 1, 2, \ldots, r.$$

Sudarykime tikimybių sumas:

$$F_1 = 0,\ F_2 = p_1,\ F_3 = p_1 + p_2,\ \ldots,\ F_r = p_1 + p_2 + \ldots + p_{r-1}.$$

Shannono kodą $\hat{c} : \mathcal{A} \to \mathcal{B}^*, \mathcal{A} = \{a_1, \ldots, a_r\},\ \mathcal{B} = \{1, 2, \ldots, b\}$ apibrėžkime:

$\hat{c}(a_i) =$ žodis iš pirmųjų s_i F_i b-ainės trupmenos skaitmenų.

Pavyzdys

Tikimybės $p_1 = p_2 = 0,3$; $p_3 = 0,2$; $p_4 = p_5 = 0,1$ ir $b = 2,3$. Shannono kodų žodžių ilgiai bus tokie:

	s_1	s_2	s_3	s_4	s_5
$b = 2$	2	2	3	4	4
$b = 3$	2	2	2	3	3

Taigi dvejetainės abėcėlės atveju pakaks trijų skleidinio skaitmenų, o trejetainės – dviejų.

	F_0	F_1	F_2	F_3	F_4
$b = 10$	0	$0,3$	$0,6$	$0,8$	$0,9$
$b = 2$	$0,00\ldots$	$0,01\ldots$	$0,100\ldots$	$0,1100\ldots$	$0,1110\ldots$
$b = 3$	$0,00\ldots$	$0,02\ldots\ldots$	$0,12\ldots$	$0,210\ldots$	$0,220\ldots$

Huffmano kodai

Tegu $\mathcal{A} = \{a_1, a_2, \ldots, a_r\}$ yra šaltinio abėcėlė, $p(a_i)$, $i = 1, 2, \ldots, r$, – abėcėlės simbolių perdavimo tikimybės,

$$P(\mathcal{A}) = \langle p(a_1), p(a_2), \ldots, p(a_r)\rangle.$$

Pasirinkime abėcėlę $\mathcal{B}$ kodo žodžiams sudaryti. Mūsų tikslas – išsiaiškinti, kaip, turint porą $\langle \mathcal{A}, P(\mathcal{A})\rangle$, galima sudaryti optimalų kodą

$$c : \mathcal{A} \to \mathcal{B}^*.$$

Optimalaus kodo sudarymo algoritmą 1952 m. paskelbė D. A. Huffmanas, tad algoritmas ir vadinamas jo vardu. Juo naudojantis sudarytus kodus vadinsime **Huffmano kodais** (r-nariais Huffmano kodais).

Huffmano kodai

Tegu $\mathcal{B} = \{0, 1\}$. Huffmano algoritmą galima suskaidyti į dvi procedūras. Pirmoji – abėcėlių redukcija:

$$\langle \mathcal{A}_1, P(\mathcal{A}_1)\rangle \to \langle \mathcal{A}_2, P(\mathcal{A}_2)\rangle \to \ldots \to \langle \mathcal{A}_{r-1}, P(\mathcal{A}_{r-1})\rangle;$$

čia $\mathcal{A}_k$ yra abėcėlės, $\mathcal{A}_1 = \mathcal{A}, |\mathcal{A}_k| = r - k + 1$, o $P(\mathcal{A}_k)$ – šias abėcėles atitinkantys simbolių tikimybių rinkiniai.
Antroji procedūra – Huffmano kodų sudarymas:

$$c_{r-1} \to c_{r-2} \to \ldots \to c_1;$$

čia c_k – porą $\langle \mathcal{A}_k, P(\mathcal{A}_k)\rangle$ atitinkantis Huffmano kodas.

Huffmano kodai

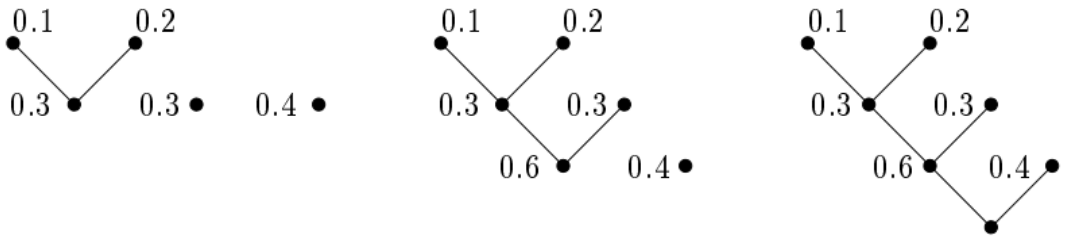
Abėcėlių redukcijos procese žingsniai atliekami pagal tokią taisyklę: *jei* $\mathcal{A}_k = \{a_1, \ldots, a_{r-k+1}\}, P(\mathcal{A}_k) = \langle p(a_1), \ldots, p(a_{r-k+1})\rangle$ *ir tikimybės* $p(a_i), p(a_j)$ *yra mažiausios, tai*

$$\begin{aligned} \mathcal{A}_{k+1} &= \big(\mathcal{A}_k \setminus \{a_i, a_j\}\big) \cup \{\langle a_i, a_j\rangle\}, \\ P(\mathcal{A}_{k+1}) &= \big(P(\mathcal{A}_k) \setminus \{p(a_i), p(a_j)\}\big) \cup \{p(\langle a_i, a_j\rangle)\}, \\ p(\langle a_i, a_j\rangle) &= p(a_i) + p(a_j). \end{aligned}$$

Pereinant prie naujos abėcėlės, du mažiausias tikimybes turintys simboliai keičiami nauju (mūsų schemoje šis naujas simbolis vaizduojamas tiesiog simbolių pora), o jam priskiriama tikimybė lygi mažiausiųjų tikimybių sumai.

Huffmano kodai

Abėcėlių redukcijos procesą atitinka kodo medžio braižymas „nuo viršaus“.



Huffmano kodo sudarymas tikimybių skirstiniui $P(\mathcal{A}) = \langle 0,1; 0,2; 0,3; 0,4\rangle$. *Vienas iš kodų, sudarytas pagal kodo medį, toks:* $\mathsf{C} = \{111, 110, 10, 0\}$. *Jo vidutinis ilgis lygus* $1,9$.

Huffmano kodai

Patogu vaizduoti abėcėlių redukciją ir lentele. 1 lentelė sudaryta tam pačiam skirstiniui kaip ir diagramoje pavaizduotas medis. Stulpelyje $\mathcal{A}_k$ surašytos abėcėlės $\mathcal{A}_k$ simbolius atitinkančios tikimybės. Tušti stulpeliai skirti kodams, kuriuos gausime atlikę perėjimus, užrašyti.

$\mathcal{A}_1$	c_1	$\mathcal{A}_2$	c_2	$\mathcal{A}_3$	c_3
0.4		0.4		<u>0.6</u>	
0.3		0.3*		0.4	
0.2*		<u>0.3*</u>			
0.1*					

Huffmano kodo sudarymas

Huffmano kodai

1. *Abėcėlės $\mathcal{A}_{r-1}$ simbolius koduojame 0 ir 1.*
2. *Jei abėcėlei $\mathcal{A}_k$, $k \geqslant r-1$, kodas c_k sudarytas ir simbolis $a \in \mathcal{A}_{k-1} \cap \mathcal{A}_k$, tai $c_{k-1}(a) = c_k(a)$. Jei $\langle a, a' \rangle \in \mathcal{A}_k$, tai $c_{k-1}(a) = c_k(\langle a, a' \rangle)0$, $c_{k-1}(a') = c_k(\langle a, a' \rangle)1$.*

$\mathcal{A}_1$	c_1	$\mathcal{A}_2$	c_2	$\mathcal{A}_3$	c_3
0.4	0	0.4	0	$\underline{0.6}$	1
0.3	10	0.3^*	10	0.4	0
0.2^*	110	$\underline{0.3^*}$	11		
0.1^*	111				

Huffmano kodo sudarymas

Huffmano kodai

Jei $|\mathcal{A}| = r, |\mathcal{B}| = s$ ir abėcėlių redukcijos procese atlikome t žingsnių, pirmajame sujungdami $u \leqslant r$ simbolių, o visuose kituose po s, tai $r = (u-1) + (t-1)(s-1) + s$, arba

$$u \equiv r \pmod{(s-1)}, \quad 2 \leqslant u \leqslant s.$$

Ši sąlyga vienareikšmiškai apibrėžia pirmuoju žingsniu sujungiamų simbolių skaičių.

Huffmano kodo sudarymas

Kadangi koduojamų simbolių skaičius $r = 6,\ s = 3$, tai pirmuoju žingsniu reikia sujungti 2 simbolius.

$\mathcal{A}_1$	c_1	$\mathcal{A}_2$	c_2	$\mathcal{A}_3$	c_3
0.4	1	0.4	1	$\underline{0.4}$	0
0.2	2	0.2	2	0.4	1
0.2	00	0.2^*	00	0.2	2
0.1	01	0.1^*	01		
0.05^*	020	$\underline{0.1^*}$	02		
0.05^*	021				

Huffmano kodai

Teorema. Huffmano kodai yra optimalūs.

Informacijos kiekio matas

1. Įvykio A „nuostabos matas“ turi būti tolydi įvykio tikimybės $p = P(A)$ funkcija $f(p)$, įgyjanti neneigiamas reikšmes.
2. Kadangi mažiau tikėtini įvykiai stebina labiau, tai funkcija $f(p)$ turi būti nedidėjanti intervale $(0; 1]$.
3. Jeigu tuo pačiu metu įvyksta du nepriklausomi įvykiai, tai jų sukelta nuostaba turi būti lygi abiejų įvykių skyrium sukeltų nuostabų sumai, t. y. turi būti

$$f(p \cdot q) = f(p) + f(q), \quad p, q \in (0, 1].$$

4. Įvykiai, kurie visada įvyksta, mūsų nestebina, taigi $f(1) = 0$.

Informacijos kiekio matas

Teorema. Jeigu funkcija $f(p)$, apibrėžta intervale $(0; 1]$, tenkina 1)-4) sąlygas, tai egzistuoja toks $b > 1$, kad

$$f(p) = \log_b \frac{1}{p}.$$

Kita vertus, kiekvienam $b > 1$ funkcija $f(p)$ tenkina 1)-4) sąlygas.

Pasirinksime $b = 2$.

Informacijos kiekio matas

Informacijos šaltinis atsitiktinių dydžių seka $\mathcal{U} = \langle U_1, U_2, \ldots \rangle$. Dalinis šaltinis – atsitiktinis dydis U_1. Jo reikšmės $U_1 = u$ suteikiamos informacijos kiekis yra $\log_2(1/P(X = u))$.

Apibrėžimas. Diskrečiojo atsitiktinio dydžio X, įgyjančio reikšmes iš baigtinės abėcėlės, entropija vadinsime skaičių

$$H(X) = \sum_{x, P(X=x)>0} \log_2 \frac{1}{P(X = x)} \cdot P(X = x).$$

Dalinio šaltinio $\mathcal{U}_n = \langle U_1, U_2, \ldots, U_n \rangle$ entropija (suteikiamos informacijos kiekiu) laikysime $H(U_1, U_2, \ldots, U_n)$.

Apibrėžimas. Jeigu informacijos šaltiniui $\mathcal{U} = \langle U_1, U_2, \ldots \rangle$ egzistuoja riba

$$H = \lim_{n\to\infty} \frac{H(U_1, U_2, \ldots, U_n)}{n},$$

tai H vadinsime šaltinio entropija.

Bernulio šaltinis

Monetos mėtymas: $U_i = 0$, jei i-ajame metime moneta atvirto herbu į viršų ir $U_i = 1$, jei skaičiumi,
$P(U_i = 0) = p, P(U_i = 1) = q, p + q = 1.$

$$H(U_i) = p \log_2 \frac{1}{p} + q \log_2 \frac{1}{q}.$$

Dydžiai U_i nepriklausomi, galima įrodyti, kad

$$H(\mathcal{U}_n) = nH(U_1).$$

$$H = \lim_{n\to\infty} \frac{H(U_1, U_2, \ldots, U_n)}{n} = p \log_2 \frac{1}{p} + q \log_2 \frac{1}{q}.$$

Šis šaltinis vadinamas Bernulio šaltiniu.

Du šaltiniai

Tarkime yra du informacijos šaltiniai, abėcėlės yra vienodo dydžio, o simbolių tikimybės $p_1, p_2, ..., p_n$ ir $q_1, q_2, ..., q_n$. Pirmojo šaltinio simbolių suteikiami informacijos kiekiai yra $\log_2 \frac{1}{p_i}$, antrojo – $\log_2 \frac{1}{q_i}$,

$$H = \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i}.$$

Teorema. Teisinga nelygybė

$$\sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i} \leqslant \sum_{i=1}^{n} p_i \log_2 \frac{1}{q_i}.$$

Teorema. Jeigu atsitiktinis dydis X įgyja n reikšmių, tai

$$H(X) \leqslant \log_2 n.$$

Lygybė $H(X) = \log_2 n$ teisinga tada ir tik tada, kai visos reikšmės įgyjamos su vienodomis tikimybėmis.

Du šaltiniai

Du informacijos šaltiniai – atsitiktiniais dydžiais X, Y. X įgyja reikšmes $x_1, x_2, \ldots, x_n$, o Y – $y_1, y_2, \ldots, y_m$. Tada

$$H(X, Y) = \sum_{i,j} P(X = x_i, Y = y_j) \log \frac{1}{P(X = x_i, Y = y_j)}.$$

Pritaikę nelygybę su $P(X = x_i, Y = y_j)$ vietoje p_i ir $P(X = x_i)P(Y = y_j)$ bei sutvarkę reiškinius, gautume

$$H(X, Y) \leqslant H(X) + H(Y).$$

Du stebimi informacijos šaltiniai negali suteikti daugiau informacijos kiekio, nei šaltinių atskirai suteikiamų informacijos kiekių suma. Skirtumą

$$H(X, Y) - H(X)$$

galime suvokti, kaip papildomą informacijos kiekį, kurį suteikia šaltinis Y, jeigu jau sužinojome informaciją iš X.

Sąlyginė entropija

Apibrėžimas. Tegu X, Y yra atsitiktiniai dydžiai, įgyjantys reikšmes iš baigtinių aibių. Sąlygine Y entropija su sąlyga X vadinsime dydį

$$H(Y|X) = H(X,Y) - H(X).$$

Sąlyginė entropija

$$\begin{aligned} H(Y|X) &= H(X,Y) - H(X), \\ H(X,Y) &= H(X) + H(Y|X) = H(Y) + H(X|Y), \\ I(X,Y) &= H(X) - H(X|Y) = H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(X,Y). \end{aligned}$$

Dydį $I(X,Y)$ galime suvokti, kaip tos pačios informacijos, kurią suteikia ir X, ir Y kiekį.

Pavyzdys

Atsitiktinai parenkama eilutės

$$aABBccABbbbbCCCAaBBb$$

raidė. Dydžio X reikšmė – parinktoji raidė, dydis $Y = 0$, jei raidė didžioji, $Y = 0$, jei mažoji. Dydžių poros $\langle X, Y \rangle$ reikšmių tikimybių lentelė:

	0	1
A	$\frac{3}{20}$	$\frac{2}{20}$
B	$\frac{5}{20}$	$\frac{5}{20}$
C	$\frac{5}{20}$	0

Pavyzdys

	0	1
A	$\frac{3}{20}$	$\frac{2}{20}$
B	$\frac{5}{20}$	$\frac{5}{20}$
C	$\frac{5}{20}$	0

$$\begin{aligned} H(X,Y) &= 3 \cdot \frac{5}{20} \cdot \log_2 \frac{20}{5} + \frac{3}{20} \cdot \log_2 \frac{20}{3} + \frac{2}{20} \cdot \log_2 \frac{20}{2} \\ &= \frac{3}{2} + \frac{3}{20} \log_2 \frac{20}{3} + \frac{1}{10} \log_2 10 \approx 2.243, \\ H(X) &= 2 \cdot \frac{5}{20} \cdot \log_2 \frac{20}{5} + \frac{10}{20} \cdot \log_2 \frac{20}{10} = \frac{3}{2}, \\ H(Y) &= \frac{13}{20} \cdot \log_2 \frac{20}{13} + \frac{7}{20} \cdot \log_2 \frac{20}{7} \approx 0.771. \end{aligned}$$

Pavyzdys

$$
\begin{aligned}
H(X,Y) &\approx 2.243 \\
H(X) &= 1.5 \\
H(Y) &\approx 0.771 \\
H(Y|X) &= H(X,Y) - H(X) \approx 0,743, \\
H(X|Y) &= H(X,Y) - H(Y) \approx 1,472, \\
I(X,Y) &= H(X) - H(X|Y) \approx 0,029.
\end{aligned}
$$

Šaltinio entropija ir kodo žodžių ilgis

$U_i i = 1, 2, \ldots$ yra atsitiktiniai dydžiai, įgyjantys reikšmes iš aibės $\mathcal{A} = \{a_1, a_2, \ldots, a_r\}$,

$$\mathcal{U} = \langle U_1, U_2, \ldots \rangle$$

Teorema. Optimalus šaltinio $\mathcal{U}_1$ kodas tenkina nelygybę

$$\frac{H(U_1)}{\log_2 b} \leqslant \lambda(\hat{c}) < \frac{H(U_1)}{\log_2 b} + 1.$$

Šaltinio entropija ir kodo žodžių ilgis

$$p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r.$$

Parinkime skaičius $1 \leqslant s_1 \leqslant s_2 \leqslant \ldots \leqslant s_r$, kad jie tenkintų nelygybes

$$b^{-s_i} \leqslant p_i < b^{-s_i+1}, \quad i = 1, 2, \ldots, r; \quad \sum_{i=1}^{r} b^{-s_i} \leqslant \sum_{i=1}^{r} p_i = 1.$$

Galima sudaryti momentinį kodą $\hat{c} : \mathcal{A} \to \mathcal{B}^*$, kad $|\hat{c}(a_i)| = s_i$. Iš nelygybės $p_i < b^{-s_i+1}$ gauname

$$s_i - 1 < \log_b \frac{1}{p_i}, \quad s_i < \frac{1}{\log_2 b} \cdot \log_2 \frac{1}{p_i} + 1.$$

$$\lambda(\hat{c}) = \sum_{i=1}^{r} p_i s_i < \frac{1}{\log_2 b} \sum_{i=1}^{r} p_i \log_2 \frac{1}{p_i} + \sum_{i=1}^{r} p_i = \frac{H(U_1)}{\log_2 b} + 1.$$

Kodo vienetinės sąnaudos koeficientas

Apibrėžimas. Tegu $c_n : \mathcal{A}^n \to \mathcal{B}^*$ yra šaltinio $\mathcal{U}_n = \langle U_1, U_2, \ldots, U_n \rangle$ kodas. Kodo vienetinės sąnaudos koeficientu vadinsime skaičių

$$\bar{\lambda}(c_n) = \frac{\lambda(c_n)}{n}.$$

Teorema. Jeigu $\mathcal{U} = \langle U_1, U_2, \ldots \rangle$ yra Bernulio šaltinis, tai kiekvienam n egzistuoja dalinio šaltinio $\mathcal{U}_n = \langle U_1, U_2, \ldots, U_n \rangle$ kodas $c_n : \mathcal{A}^n \to \mathcal{B}^*$, tenkinantis sąlygą

$$\frac{H(\mathcal{U})}{\log_2 b} \leqslant \bar{\lambda}(c_n) < \frac{H(\mathcal{U})}{\log_2 b} + \frac{1}{n},$$

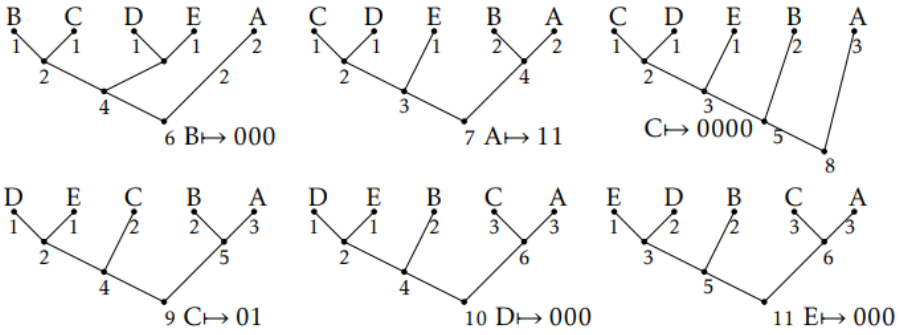
čia $H(\mathcal{U}) = H(U_1)$ yra šaltinio entropija.

Kintamų kodų metodas

Susitarimas dėl Huffmano kodų sudarymo:

- abėcėlės simbolius visada išdėstysime dažnių didėjimo tvarka iš kairės į dešinę;
- konstruojant kodo medį, jungiant mažiausius dažnius turinčių viršūnių porą, visada bus jungiami patys „kairiausieji“ elementai; sujungus viršūnių porą, gautoji viršūnė bus vaizduojama vienu lygiu žemiau už žemesniojo lygio viršūnę.
- į kairę vedančioms briaunoms visada priskirsime 0, į dešinę – 1.

Kintamų kodų metodas



Brėžinyje parodyta, kaip keitėsi kodo medis, koduojant žodį ABACCDE. Pirmajai raidei koduoti buvo panaudotas medis, atitinkantis vienodus abėcėlės simbolių pasirodymo dažnius.

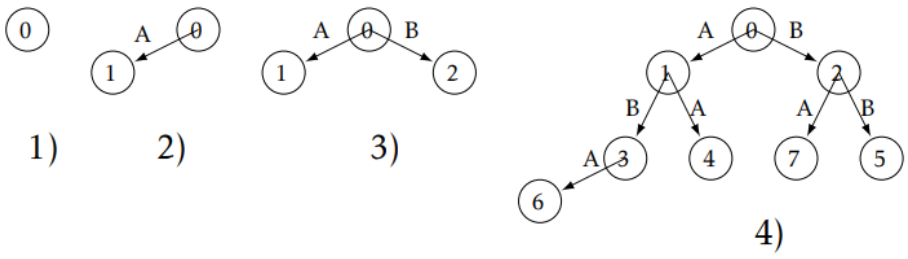
A	B	A	C	C	D	E
00	000	11	0000	01	000	000

Žodžio ABACCDE kodavimas naudojant kintamų Huffmano kodų metodą

LZ77

$m = 8, n = 4$	Kodas
VASA RIS VASARA PAVASARIS	0;0;V;
V ASAR IS VASARA PAVASARIS	0;0;A;
VA SARI S VASARA PAVASARIS	0;0;S;
VAS ARIS VASARA PAVASARIS	2;1;R;
VASAR IS V ASARA PAVASARIS	0;0;I;
VASARI S VA SARA PAVASARIS	4;1; :
VASARIS VASA RA PAVASARIS	8;4;R;
VASAR IS VASAR A PA VASARIS	2;1; ;
VASARIS VASARA PAVA SARIS	0;0;P;
VASARIS VASARA P AVAS ARIS	3;1;V;
VASARIS VA SARA PAV ASAR IS	2;1;S;
VASARIS VASA RA PAVAS ARIS	2;1;R;
VASARIS VASARA PAVASAR IS	0;0;I;
VASARIS VASARA PAVASARI S	4;1;

LZ78



1) 2) 3) 4)

Kodavimo žingsnis	Kodo papildymas	Žodyno papildymas
1	0; *A*	*A*
2	0; *B*	*B*
3	1; *B*	*AB*
4	1; *A*	*AA*
5	2; *B*	*BB*
6	3; *A*	*ABA*
7	2; *A*	*BA*
8	6; *B*	*ABAB*

Kodavimo LZ78 eiga

Aritmetinio kodavimo idėja

Bernulio šaltinis, abėcėlė $\mathcal{A} = \{a_1, a_2, \ldots, a_r\}$ simbolių pasirodymo dažniai $p_1, p_2, \ldots, p_r$.
Koduojami n ilgio žodžiai, žodžių aibė yra $\mathcal{A}^n$.
Kiekvienam šios aibės žodžiui $\mathrm{x} = a_{i_1} a_{i_2} \ldots a_{i_n}$ intervale $I = [0; 1]$ tam tikru būdu priskirkime jo „teritoriją“ – intervalą $I(\mathrm{x}) = I(i_1, i_2, \ldots, i_n)$.
Pasirūpinę, kad skirtingiems žodžiams x, y jų intervalai $I(\mathrm{x}), I(\mathrm{y})$ nesikirstų, žodžio x kodu galėtume laikyti bet kurį skaičių $\rho \in I(\mathrm{x})$.

Aritmetinis kodavimas

Žodį $\mathrm{x} = a_{i_1} a_{i_2} \ldots a_{i_n}$ atitiks intervalas $I(\mathrm{x})$

$$I(i_1) \supset I(i_1, i_2) \supset \ldots \supset I(i_1, i_2, \ldots, i_{n-1}) \supset I(i_1, i_2, \ldots, i_{n-1}, i_n) = I(\mathrm{x}).$$

Pirmiausia paskirsime intervalus pavienėms raidėms:

$$\begin{aligned} I(1) &= [0; p_1), \; I(2) = [p_1; p_1 + p_2), \\ I(3) &= [p_1 + p_2; p_1 + p_2 + p_3), \; \ldots, I(r) = [p_1 + \ldots + p_{r-1}; 1). \end{aligned}$$

Jeigu

$$I(i_1, i_2, \ldots, i_{m-1}) = [\alpha; \alpha + \beta),$$

tai

$$\begin{aligned} I(i_1, i_2, \ldots, i_{m-1}, 1) &= [\alpha; \alpha + p_1\beta), \\ I(i_1, i_2, \ldots, i_{m-1}, 2) &= [\alpha + p_1\beta; \alpha + (p_1 + p_2)\beta), \\ &\ldots\ldots\ldots \\ I(i_1, i_2, \ldots, i_{m-1}, r) &= [\alpha + (p_1 + \ldots + p_{r-1})\beta; \alpha + \beta). \end{aligned}$$

Pavyzdys

Tegu abėcėlės $\mathcal{A} = \{1, 2, 3, 4, 5\}$ simbolių tikimybės yra

$$p_1 = 0,2;\ \ p_2 = 0,25;\ \ p_3 = 0,15;\ \ p_4 = 0,1;\ \ p_5 = 0,3.$$

Reikia koduoti žodį x = 213552. Konstruojame intervalus:

$$\begin{aligned} I(2) &= [p_1; p_1 + p_2] = [0,2; 0,45) \\ I(21) &= [0,2; 0,25) \\ I(213) &= [0,2225; 0,23) \\ I(2135) &= [0,222775; 0,23) \\ I(21355) &= [0,229325; 0,23) \\ I(213552) &= [0,22946; 0,22962875) \end{aligned}$$

Taigi kaip žodžio x = 213552 kodą galėtume siųsti, pavyzdžiui, dešimtainę trupmeną $\rho = 0,2295$.

Aritmetinis kodavimas dvejetainiais žodžiais

Tarkime, intervalas, kuriame norime parinkti skaičių – žodžio kodą yra $I(\mathrm{x}) = [a; a + \delta)$. Surasime skaičius c ir n, kad būtų

$$\frac{(c-1)}{2^n} \leqslant a < \frac{c}{2^n} < a + \delta.$$

Tada žodžio x kodu galėsime imti skaičių $\frac{c}{2^n}$, kurį galėsime perduoti siųsdami skaičiaus c dvejetainės išraiškos n bitų, papildydami nuliais, jei reikia iš kairės.
Skaičius n – mažiausias nelygybės $\frac{1}{2^n} < \delta$ sprendinys.

$$n = \lceil \log_2(1/\delta) \rceil, \quad (c-1) \leqslant a2^n < c, \quad c = \lceil a2^n \rceil.$$

Klaidas taisantys kodai

Informacijos perdavimo kanalai

Kanalas: informacijos šaltinių – siuntėjo ir gavėjo – pora. Siuntėjo abėcėlę žymėsime $\mathcal{A}$, o atsitiktinius dydžius, kurių reikšmės – siuntėjo perduodami simboliai, $U_1, U_2, \ldots$
Gavėjo abėcėlę žymėsime $\mathcal{B}$, o atsitiktinius dydžius, kurių reikšmės – gavėjo gauti simboliai, $V_1, V_2, \ldots$
Gavėjo gaunami duomenys gali skirtis nuo siųstųjų. Sakome, kad perduota iškraipyta informacija, o visas aplinkybes, dėl kurių tai įvyko, vadinsime triukšmu.

Informacijos perdavimo kanalai

Simbolius kraipantys ar trinantys kanalai: jei siuntėjas pasiuntė n ilgio žodį, tai tokio pat ilgio žodį gaus ir gavėjas (ištrintus simbolius jis gali pakeisti, pavyzdžiui, klaustukais).
$\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$ yra siuntėjo, o $\mathcal{B} = \{b_1, b_2, \ldots, b_s\}$ – gavėjo abėcėlė.
Siuntėjo siunčiami žodžiai yra atsitiktinio vektoriaus $U^{(n)}$ reikšmės, o gavėjo gaunami žodžiai – atsitiktinio vektoriaus $V^{(n)}$ reikšmės.
Statistines kanalo triukšmo savybes nusako tikimybės

$$P(V^{(n)} = \mathrm{v} | U^{(n)} = \mathrm{u}), \quad \mathrm{u} \in \mathcal{A}^n, \ \mathrm{v} \in \mathcal{B}^n.$$

Kanalai be atminties

Apibrėžimas. Perdavimo kanalą vadinsime kanalu be atminties, jeigu visiems žodžiams $\mathrm{u} = u_1 u_2 \ldots u_n \in \mathcal{A}^n, \mathrm{v} = v_1 v_2 \ldots v_n \in \mathcal{B}^n$ teisinga lygybė

$$P(V^{(n)} = \mathrm{v} | U^{(n)} = \mathrm{u}) = p(v_1|u_1)p(v_2|u_2)\ldots p(v_n|u_n).$$

Kanalo tikimybių matrica

Kanalo tikimybių $p(b_j|a_i)$, $a_i \in \mathcal{A}$, $b_j \in \mathcal{B}$, matrica:

$$\mathrm{P} = \begin{pmatrix} p(b_1|a_1) & p(b_2|a_1) & \dots & p(b_s|a_1) \\ p(b_1|a_2) & p(b_2|a_2) & \dots & p(b_s|a_2) \\ \dots & \dots & \vdots & \dots \\ p(b_1|a_t) & p(b_2|a_t) & \dots & p(b_s|a_q) \end{pmatrix}.$$

Perdavimo kanalai

Apibrėžimas. Perdavimo kanalą su dvejetaine siuntėjo ir gavėjo abėcėle $\mathcal{A} = \mathcal{B} = \{0, 1\}$ vadinsime dvejetainiu simetriniu kanalu, jeigu perdavimo tikimybių matrica yra

$$\mathrm{P} = \begin{pmatrix} p(0|0) & p(1|0) \\ p(0|1) & p(1|1) \end{pmatrix} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix},$$

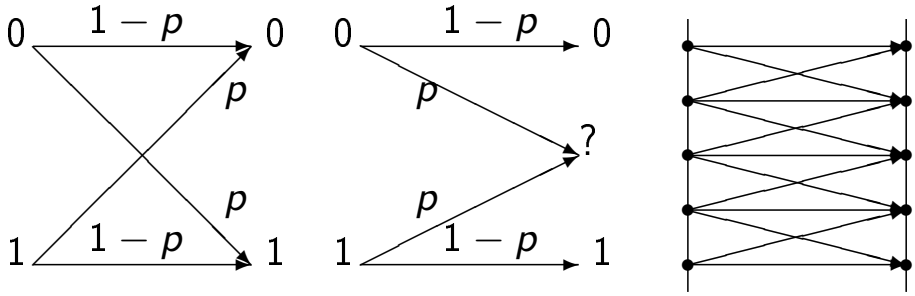
čia p, $0 \leqslant p \leqslant 1$, reiškia vieno simbolio iškraipymo tikimybę.

Apibrėžimas. Perdavimo kanalą su dvejetaine siuntėjo abėcėle $\mathcal{A}$ ir gavėjo abėcėle $\mathcal{B} = \mathcal{A} \cup \{?\}$ vadinsime trinančiu kanalu, jei simbolio perdavimo tikimybės tokios:

$$p(?|a) = p, \quad p(a|a) = 1 - p, \quad p(b|a) = 0, \quad a, b \in \mathcal{A}, a \neq b,$$

čia $0 \leq p \leq 1$ yra simbolio trynimo tikimybė.

Perdavimo kanalai



Trys perdavimo kanalų modeliai: simetrinis, trinantis, klaviatūros

Entropijos ir informacijos kiekiai

Jeigu X ir Y yra du diskretieji atsitiktiniai dydžiai, tai abipuse informacija pavadinome skaičių

$$I(X, Y) = H(X) - H(X|Y) = H(X) + H(Y) - H(X, Y).$$

Siuntėją sutapatinkime su atsitiktiniu dydžiu U, o gavėją – su V. Dydžio U reikšmės – siuntėjo abėcėlės simboliai, o V reikšmės – gavėjo gauti simboliai.
Tada gavėjo siunčiamos informacijos kiekis yra $H(U)$, $H(U|V)$ – kiekis, pradingęs kanale, o $I(U, V)$ – perduotas informacijos kiekis.

Kanalo talpa

Žymėkime $P_U = \langle p(a_1), p(a_2), \ldots, p(a_q)\rangle$ šaltinio tikimybių, t. y. tikimybių $p(a) = P(U = a)$, rinkinį.

Apibrėžimas. Kanalo talpa vadinsime skaičių

$$C = \max\{I(U, V) : P_U\}.$$

Teorema. Dvinario simetrinio kanalo talpa yra

$$C = 1 - p\log_2 p - (1 - p)\log_2(1 - p).$$

Simbolių kartojimo kodas

Galvojame: kaip patikimiau perduoti informaciją? Pirmoji mintis – kartokime perduodamus simbolius. Šitaip perduodamos informacijos kiekio nepadidinsime, tačiau galbūt saugiau „įpakuosime“.
Jeigu siunčiamą simbolį pakartosime tris kartus ir nurodysime, kad tris gautus simbolius reikia pakeisti tuo, kuris toje trijulėje pasitaiko dažniausiai, tai simbolio teisingo perdavimo tikimybę nuo $P_t = 1 - p$ padidinsime iki

$$P_t^* = (1 - p)^3 + 3p(1 - p)^2,$$

čia p žymi tikimybę, kad siunčiamas simbolis kanale bus iškreiptas.

Simbolių kartojimo kodas

$n=$	3	5	7	9
$p=0,1$	$0,0028$	$0,0856$	$0,002728$	$0,0009$
$p=0,2$	$0,104$	$0,05792$	$0,03334$	$0,01958$

Kai vieno simbolio iškraipymo tikimybė lygi $0,1$, o perduodant kiekvienas simbolis kartojamas devynis kartus, vis tiek maždaug vienas iš tūkstančio simbolių bus perduotas klaidingai. Jeigu teksto simbolis koduojamas aštuoniais bitais, tai klaidingai perskaitytas bus maždaug vienas simbolis iš 125.

Kodas

Pradinis šaltinio simbolių srautas bus skaidomas į m ilgio žodžius, o šie žodžiai koduojami (keičiami) tos pačios abėcėlės n ilgio žodžiais, parenkamais pagal tam tikrą taisyklę iš aibės $C = \{c_1, \ldots, c_N\}$.

Apibrėžimas. Abėcėlės $\mathcal{A}$ n ilgio skirtingų žodžių rinkinį, turintį N elementų, vadinsime (n,N) kodu.
Parametrą n vadinsime kodo ilgiu, N – kodo dydžiu.

Kodo koeficientas

Jeigu (n, N) kodo elementais koduojami m ilgio pradinio srauto žodžiai, tai perdavimo greičio sumažėjimą galime apibūdinti koeficientu

$$R = \frac{m}{n}.$$

Apibrėžimas. Tegu C yra (n, N) kodas, sudarytas iš q elementų turinčios abėcėlės žodžių. Dydį

$$R(\mathrm{C}) = \frac{\log_q N}{n}$$

vadinsime kodo C koeficientu.

Kad kodo žodžių užtektų, turi būti patenkinta nelygybė

$$q^m \leqslant N, \quad \text{arba} \quad m \leqslant \log_q N.$$

Pasirinkus didžiausią m

$$R = \frac{m}{n} = \frac{[\log_q N]}{n}.$$

Informacijos perdavimo tikimybės

Šaltinį galime tapatinti su atsitiktiniu vektoriumi, įgyjančiu reikšmes iš C, gavėją – su vektoriumi, įgyjančiu reikšmes iš D.

$$\begin{aligned}
p(\mathrm{c_i}) &= P(\text{bus siųstas žodis } \mathrm{c_i}),\ \mathrm{c_i} \in \mathrm{C};\\
p(\mathrm{d_j}) &= P(\text{bus gautas žodis } \mathrm{d_j}),\ \mathrm{d_j} \in \mathrm{D};\\
p(\mathrm{c_i}, \mathrm{d_j}) &= P(\text{bus siųstas žodis } \mathrm{c_i},\ \text{o gautas } \mathrm{d_j}),\ \mathrm{c_i} \in \mathrm{C},\ \mathrm{d_j} \in \mathrm{D};\\
p(\mathrm{d_j}|\mathrm{c_i}) &= P(\text{jei bus siųstas žodis } \mathrm{c_i}, \text{tai gautas } \mathrm{d_j}),\ \mathrm{c_i} \in \mathrm{C},\ \mathrm{d_j} \in \mathrm{D};\\
p(\mathrm{c_i}|\mathrm{d_j}) &= P(\text{jei gautas žodis } \mathrm{d_j}, \text{tai buvo siųstas } \mathrm{c_i}),\ \mathrm{c_i} \in \mathrm{C},\ \mathrm{d_j} \in \mathrm{D}.
\end{aligned}$$

Jei $\mathrm{c_i} = a_1 a_2 \ldots a_n$, $\mathrm{d_j} = b_1 b_2 \ldots b_n$; čia $a_u \in \mathcal{A}$, $b_v \in \mathcal{B}$, tai

$$p(\mathrm{d_j}|\mathrm{c_i}) = p(b_1|a_1)p(b_2|a_2) \cdot \ldots \cdot p(b_n|a_n).$$

Dekodavimo taisyklės

Apibrėžimas. Tegu **C** yra kodas, o **D** priimamų žodžių aibė. Dekodavimo taisykle vadinsime funkciją

$$f : \mathrm{D} \to \mathrm{C}.$$

$$P(\mathit{klaida}|\mathrm{c}) = \sum_{\mathrm{d}:\mathrm{d}\notin f^{-1}(\mathrm{c})} p(\mathrm{d}|\mathrm{c}).$$

$$P(\mathit{klaida}|\mathrm{d}) = \sum_{\mathrm{c}\neq f(\mathrm{d})} p(\mathrm{c}|\mathrm{d}) = 1 - p(f(\mathrm{d})|\mathrm{d}).$$

Vidutinė klaidos tikimybė:

$$p_{vid} = \sum_{\mathrm{c}} P(\mathit{klaida}|\mathrm{c})p(\mathrm{c}) = \sum_{\mathrm{d}} P(\mathit{klaida}|\mathrm{d})p(\mathrm{d}).$$

Didžiausio tikėtinumo dekodavimo taisyklė

Apibrėžimas. Tegu C yra kodas, o D – priimamų žodžių aibė. Dekodavimo taisyklę $f : \mathrm{D} \to \mathrm{C}$ vadinsime didžiausio tikėtinumo taisykle, jei kiekvienam $\mathrm{d} \in \mathrm{D}$ f tenkina sąlygą

$$p(\mathrm{d}|f(\mathrm{d})) = \max_{\mathrm{c}} p(\mathrm{d}|\mathrm{c}).$$

Didžiausio tikėtinumo taisyklei sudaryti pakanka žinoti tik kanalo tikimybes.

Minimalaus atstumo taisyklė

Apibrėžimas. Tegu $\mathrm{x} = x_1 \dots x_n$, $\mathrm{y} = y_1 \dots y_n$ yra du abėcėlės $\mathcal{A}$ žodžiai. Hammingo atstumu tarp jų vadinsime skaičių

$$h(\mathrm{x}, \mathrm{y}) = \sum_{\substack{i=1,\dots,n \\ x_i \neq y_i}} 1.$$

Hammingo atstumas tarp dviejų to paties ilgio žodžių lygus nesutampančių komponenčių skaičiui.

Apibrėžimas. Dekodavimo taisyklę $f : \mathrm{D} \to \mathrm{C}$ vadinsime minimalaus atstumo taisykle, jei kiekvienam **d**

$$h(f(\mathrm{d}), \mathrm{d}) = \min_{\mathrm{c}} h(\mathrm{c}, \mathrm{d}).$$

Shannono teorema

Teorema. Tegu dvinario simetrinio kanalo talpa lygi $\mathcal{C}$, o vieno simbolio iškraipymo tikimybė $p \neq 0,5$. Tada bet kokiam skaičiui R, $0 < R < \mathcal{C}$, egzistuoja kodų C_m ir juos atitinkančių dekodavimo taisyklių seka, kad

$$R(\mathrm{C}_m) \geqslant R, \quad p_{max}(\mathrm{C}_m) \to 0, \quad m \to \infty.$$

Kodui **C** apibrėžėme

$$p_{max}(\mathrm{C}) = \max_{\mathrm{c} \in \mathrm{C}} P(klaida|\mathrm{c}).$$

Išvada. *Tegu dvinario simetrinio kanalo talpa lygi $\mathcal{C}$, o vieno simbolio iškraipymo tikimybė $p \neq 0,5$. Tada egzistuoja kodų C_m bei juos atitinkančių dekodavimo taisyklių seka, kad*

$$R(\mathrm{C}_m) \to \mathcal{C}, \quad p_{max}(\mathrm{C}_m) \to 0, \quad m \to \infty.$$

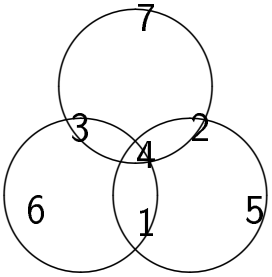
Atvirkštinė Shannono teorema

Teorema. Tegu diskretaus be atminties su dvinare šaltinio abėcėle kanalo talpa yra $\mathcal{C}$, o $\mathbf{C}$ – koks nors (n, N) kodas, kuriam turime sudarę dekodavimo taisyklę.
Kiekvienam $R > \mathcal{C}$ egzistuoja $\delta(R) > 0$, kad iš $R(\mathrm{C}) > R$ išplaukia

$$p^*_{vid}(\mathrm{C}) > \delta(R).$$

Hammingo kodas

Kanalu reikia perduoti keturis dvejetainius simbolius (bitus).



Žodis, sudarytas iš bitų $1-4$, *papildomas dar trimis taip, kad bitų, kurių numeriai užrašyti tame pačiame skritulyje, suma būtų lyginė.*
Hammingas pastebėjo, kad šį kodą galima šiek tiek pagerinti. Jeigu prie septynių kodo žodžių bitų pridėsime dar vieną – aštuntąjį taip, kad visų simbolių suma būtų lyginė, tai galėsime atpažinti, kada įvyko viena klaida, o kada – dvi.

Hammingo kodai

Tegu n yra natūralusis skaičius, $2^m \leqslant n < 2^{m+1}$. Sudarysime kodą iš žodžių

$$x_1 x_2 \dots x_n \in \{0,1\}^n.$$

Pavyzdys: $n = 10$. Kodo žodyje $x_1 x_2 \dots x_{10}$ simboliai $x_3, x_5, x_6, x_7, x_9, x_{10}$ bus informaciniai, o simboliai x_1, x_2, x_4, x_8 – kontroliniai, suskaičiuoti panaudojant informacinių simbolių reikšmes.

$$\begin{aligned}
3 &= 1\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2 + 0\cdot 2^3,\\
5 &= 1\cdot 2^0 + 0\cdot 2^1 + 1\cdot 2^2 + 0\cdot 2^3,\\
6 &= 0\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^2 + 0\cdot 2^3,\\
7 &= 1\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^2 + 0\cdot 2^3,\\
9 &= 1\cdot 2^0 + 0\cdot 2^1 + 0\cdot 2^2 + 1\cdot 2^3,\\
10 &= 0\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2 + 1\cdot 2^3.
\end{aligned}$$

Hammingo kodai

Sudarysime lentelę, eilutėse išrašydami koeficientų prie 2^i reikšmes skaičių $3, 5, 6, 7, 9, 10$ išraiškose:

	x_3	x_5	x_6	x_7	x_9	x_{10}
2^0	1	1	0	1	1	0
2^1	1	0	1	1	0	1
2^2	0	1	1	1	0	0
2^3	0	0	0	0	1	1

Pastebėkime, kad lentelėje nėra vienodų stulpelių.

$$\begin{aligned}
x_1 &= 1\cdot x_3 + 1\cdot x_5 + 0\cdot x_6 + 1\cdot x_7 + 1\cdot x_9 + 0\cdot x_{10},\\
x_2 &= 1\cdot x_3 + 0\cdot x_5 + 1\cdot x_6 + 1\cdot x_7 + 0\cdot x_9 + 1\cdot x_{10},\\
x_4 &= 0\cdot x_3 + 1\cdot x_5 + 1\cdot x_6 + 1\cdot x_7 + 0\cdot x_9 + 0\cdot x_{10},\\
x_8 &= 0\cdot x_3 + 0\cdot x_5 + 0\cdot x_6 + 0\cdot x_7 + 1\cdot x_9 + 1\cdot x_{10}.
\end{aligned}$$

$$011011 \mapsto **0*110*11 \mapsto 0000110011$$

Stačiakampiai kodai $S(m, n)$

$$x_1 x_2 \dots x_{nm} \to \begin{array}{cccc} x_1 & x_2 & \dots & x_n \\ x_{n+1} & x_{n+2} & \dots & x_{2n} \\ \dots & \dots & \dots & \dots \\ x_{m(n-1)+1} & x_{m(n-1)+2} & \dots & x_{mn} \end{array}$$

Papildykime lentelę pridėdami prie eilučių bitus $y_1, y_2, \dots, y_m$, o prie stulpelių – $z_1, z_2, \dots, z_n$. Jų reikšmės – atitinkamų eilučių (stulpelių) informacinių bitų sumos moduliu 2.

$$\begin{array}{cccccc} x_1 & x_2 & x_3 & x_4 & y_1 \\ x_5 & x_6 & x_7 & x_8 & y_2 \\ x_9 & x_{10} & x_{11} & x_{12} & y_3 \\ z_1 & z_2 & z_3 & z_4 \end{array}$$

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + y_1 &= 0, & x_1 + x_5 + x_9 + z_1 &= 0, \\ x_5 + x_6 + x_7 + x_8 + y_2 &= 0, & x_2 + x_6 + x_{10} + z_2 &= 0, \\ x_9 + x_{10} + x_{11} + x_{12} + y_3 &= 0, & x_3 + x_7 + x_{11} + z_3 &= 0, \\ & & x_4 + x_8 + x_{12} + z_4 &= 0. \end{aligned}$$

Trikampiai kodai $T(r)$

$T(4)$ kodo informaciniai bitai:

$$x_1 x_2 \dots x_{10} \to \begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & \\ x_8 & x_9 & & \\ x_{10} & & & \end{array}$$

$$\begin{array}{ccccc} x_1 & x_2 & x_3 & x_4 & y_1 \\ x_5 & x_6 & x_7 & y_2 & \\ x_8 & x_9 & y_3 & & \\ x_{10} & y_4 & & & \\ y_5 & & & & \end{array}$$

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + y_1 &= 0, \\ x_4 + x_5 + x_6 + x_7 + y_2 &= 0, \\ x_3 + x_7 + x_8 + x_9 + y_3 &= 0, \\ x_2 + x_6 + x_9 + x_{10} + y_4 &= 0, \\ x_1 + x_5 + x_8 + x_{10} + y_5 &= 0. \end{aligned}$$

Hammingo atstumas

$\mathcal{A}_q$ žymi abėcėlę, turinčią q simbolių, $|\mathcal{A}| = q$.

$$\mathcal{A}_q^n = \mathcal{A}_q \times \mathcal{A}_q \times \ldots \times \mathcal{A}_q.$$

Apibrėžimas. Tegu $\mathrm{x} = x_1 \ldots x_n$, $\mathrm{y} = y_1 \ldots y_n$ yra du aibės $\mathcal{A}_q^n$ žodžiai. Hammingo atstumu tarp $\mathbf{x}$, $\mathbf{y}$ vadinsime dydį

$$h(\mathrm{x}, \mathrm{y}) = \sum_{\substack{i=1,\ldots,n \\ x_i \neq y_i}} 1.$$

Teorema. Hamingo atstumas aibėje $\mathcal{A}_q^n$ turi šias savybes:

- $h(\mathrm{x}, \mathrm{x}) = 0, \quad \mathrm{x} \in \mathcal{A}_q^n$;
- $h(\mathrm{x}, \mathrm{y}) = h(\mathrm{y}, \mathrm{x}), \quad \mathrm{x}, \mathrm{y} \in \mathcal{A}_q^n$;
- $h(\mathrm{x}, \mathrm{y}) \leqslant h(\mathrm{x}, \mathrm{z}) + h(\mathrm{y}, \mathrm{z}), \quad \mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathcal{A}_q^n$.

Minimalaus atstumo taisyklė

Apibrėžimas. (n, N) kodu iš abėcėlės $\mathcal{A}_q$ žodžių vadinamas bet koks poaibis $\mathrm{C} \subset \mathcal{A}_q^n$, čia $|\mathrm{C}| = N$.

Apibrėžimas. Dekodavimo taisyklę $f : \mathcal{A}_q^n \to \mathrm{C}$ vadinsime minimalaus atstumo taisykle, jei su kiekvienu $\mathrm{d} \in \mathcal{A}_q^n$

$$h(\mathrm{d}, f(\mathrm{d})) = \min_{\mathrm{c} \in \mathrm{C}} h(\mathrm{d}, \mathrm{c}).$$

Minimalus kodo atstumas

Apibrėžimas. Kodo C minimaliu atstumu vadinsime dydį

$$d(\mathrm{C}) = \min_{\substack{\mathrm{c,d}\in\mathrm{C}\\ \mathrm{c}\neq\mathrm{d}}} h(\mathrm{d},\mathrm{c}).$$

Jei (n, N) kodo C minimalus atstumas yra d, tai kodą vadinsime (n, N, d) kodu.

Klaidas randantys kodai

Apibrėžimas. Kodą **C** vadinsime t klaidų randančiu kodu, jei, bet kuriame kodo žodyje įvykus m, $m \leqslant t$, iškraipymų, gautas rezultatas **d** jau nebėra kodo žodis, t. y. $\mathrm{d} \notin \mathrm{C}$.
t klaidų randantį kodą vadinsime tiksliai t klaidų randančiu kodu, jei jis nėra $t+1$ klaidų randantis kodas.

Teorema. (n, N, d) kodas **C** yra tiksliai t klaidų randantis kodas tada ir tik tada, kai $d = t + 1$.

Klaidas taisantys kodai

Apibrėžimas. Kodą $\mathbf{C}$ vadinsime t klaidų taisančiu kodu, jei, siunčiamame žodyje įvykus m, $m \leqslant t$, iškraipymų ir dekoduojant pagal minimalaus atstumo taisyklę, visada bus dekoduojama teisingai. Tokį kodą vadinsime tiksliai t klaidų taisančiu kodu, jeigu jis ne visada taiso $t+1$ klaidų.

Kiek klaidų taiso kodas C, lemia minimalus jo atstumas.

Teorema. Kodas C yra tiksliai t klaidų taisantis kodas tada ir tik tada, kai $d(\mathrm{C}) = 2t+1$ arba $d(\mathrm{C}) = 2t+2$.

Rutulio tūris

Apibrėžimas. Žodžių aibės $\mathcal{A}_q^n$ spindulio $r \geq 1$ rutuliu su centru $\mathrm{x} \in \mathcal{A}_q^n$ vadinsime aibę

$$B_q(\mathrm{x}, r) = \{\mathrm{y} \in \mathcal{A}_q^n : h(\mathrm{x}, \mathrm{y}) \leqslant r\}.$$

Šios aibės elementų skaičių vadinsime rutulio tūriu.

Teorema. Teisinga lygybė

$$|B_q(\mathrm{x}, r)| = \sum_{0 \leqslant k \leqslant r} C_n^k (q-1)^k.$$

Pakavimo ir dengimo spinduliai

Apibrėžimas. Tegu **C** yra koks nors (n, N) kodas. Didžiausią sveikąjį skaičių t, kuriam

$$B_q(c_1, t) \cap B_q(c_2, t) = \emptyset, \quad \text{jei} \quad c_1, c_2 \in C, \quad c_1 \neq c_2,$$

vadinsime kodo **C** pakavimo spinduliu. Jį žymėsime $r_p = r_p(C)$.

Rutuliai $B_q(c, t), c \in C, t \leqslant r_p(C)$, sudaro nesikertančių aibių šeimą; jei $t \geqslant r_p(C) + 1$, bent du rutuliai kertasi.

Apibrėžimas. Mažiausią sveikąjį skaičių s, tenkinantį sąlygą

$$\mathcal{A}_q^n \subset \bigcup_{c \in C} B_q(c, s),$$

vadinsime kodo dengimo spinduliu ir žymėsime $r_d = r_d(C)$.

Tobulieji kodai

Apibrėžimas. Kodą **C** vadinsime tobulu, jei

$$r_p(C) = r_d(C).$$

Teorema. (n, N, d) kodas **C** yra tobulas tada ir tik tada, kai $d = 2t + 1$ ir galioja lygybė

$$NV_q(n, t) = q^n.$$

Hammingo kodai yra tobuli.

Kodai su kontroliniu simboliu

Knygų žymėjimo sistema ISBN – tai kodas su abėcėle

$$\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\},$$

čia X žymi skaičių 10. Informacija apie knygą užrašoma devyniais šios abėcėlės simboliais, suskirstytais į tris grupes: pirmoji simbolių grupė žymi šalį, antroji – leidyklą, trečioji – knygą. Devynių simbolių žodis papildomas dešimtuoju – kontroliniu, kad galiotų lygybė

$$X \cdot x_1 + 9 \cdot x_2 + 8 \cdot x_3 + 7 \cdot x_4 + 6 \cdot x_5 + \ldots + 2 \cdot x_9 + 1 \cdot x_{10} \equiv 0 \pmod{11}.$$

Kodai su kontroliniu simboliu

ISBN kodas visada „pastebi“, jei įvyko viena klaida. Pavyzdžiui, jeigu nuskaitant žodį $x_1 x_2 \ldots x_9$ simbolis x_2 pasikeitė į x_2^*, tai tikrinant kontrolinę lygybę gausime

$$\begin{aligned} &X \cdot x_1 + 9 \cdot x_2^* + 8 \cdot x_3 + 7 \cdot x_4 + \ldots + 2 \cdot x_9 + 1 \cdot x_{10} = \\ &X \cdot x_1 + 9 \cdot x_2 + 8 \cdot x_3 + 7 \cdot x_4 + \ldots + 2 \cdot x_9 + 1 \cdot x_{10} + 9(x_2 - x_2^*) \\ &\equiv 0 + 9(x_2 - x_2^*) \pmod{11}. \end{aligned}$$

Kodai su kontroliniu simboliu

EAN (European Article Numeration) ženklinamos prekės žymimos abėcėlės

$$\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

trylikos skaitmenų kodu. Kontrolinė lygybė

$$1 \cdot x_1 + 3 \cdot x_2 + \ldots + 3 \cdot x_{12} + 1 \cdot x_{13} \equiv 0 \pmod{10}.$$

EAN kodas taip pat atpažįsta, jei vienas simbolis perduodamas neteisingai, o taip pat daug ir kitokios rūšies klaidų.

Kodai su kontroliniu simboliu

Olandų matematikas J. Verhoeff 1969 metais[1] paskelbė tyrimų apie dažniausiai įvykstančias klaidas, kai skaitmeninę informaciją perduoda žmonės.

Klaidos rūšis	Pavyzdys	Dažnumas
Pavienės klaidos	$a \mapsto b$	$60 - 95\%$
Gretimos perstatos	$ab \mapsto bb$	$10 - 20\%$
Dvynių klaidos	$aa \mapsto bb$	$0,5 - 1,5\%$
Trijų perstatos	$acb \mapsto bca$	$0,5 - 1,5\%$
Dvynių perstatos	$aca \mapsto bcb$	$< 1\%$
Tarimo klaidos	$50 \mapsto 15$	$0,5 - 1,5\%$
Pridėta ar praleista		$10 - 20\%$

[1] Verhoeff, Jacobus (1969) "Error Detecting Decimal Codes," Mathematical Center Tract 29, Amsterdam.

Kodai su kontroliniu simboliu

Banko kreditinėms kortelėms žymėti taip pat naudojamas kodas su kontroliniu simboliu. Penkiolikos skaitmenų žodis $d_1 d_2 \dots d_{15}$ papildomas šešioliktuoju skaitmeniu d_{16},

$$s(2\cdot d_1)+d_2+s(2\cdot d_3)+\cdots+d_{14}+s(2\cdot d_{15})+d_{16}\equiv 0 \pmod{10};$$

čia $s(n)$ reiškia skaičiaus išraiškos dešimtainių skaitmenų sumą, pavyzdžiui, $s(13)=4$.

Kodai su kontroliniu simboliu

IBM kodą su kontroliniu simboliu galima naudoti bet kokio ilgio žodžiui, sudarytam iš dešimtainių skaitmenų.
Kodui sudaryti naudojamas keitinys

$$\sigma=\begin{pmatrix}0&1&2&3&4&5&6&7&8&9\\0&2&4&6&8&1&3&5&7&9\end{pmatrix}$$

Tarkime, informacija užrašoma dešimtainiais skaitmenimis $d_1 d_2 \dots d_n$ ir n lyginis. Tada kontrolinis skaitmuo d_{n+1} pridedamas taip, kad būtų teisinga lygybė

$$d_1+\sigma(d_2)+d_3+\sigma(d_4)+\cdots+d_{n-1}+\sigma(d_n)+d_{n+1}\equiv 0 \pmod{10}.$$

Pavyzdžiui, jei $d_1 d_2 d_3 d_4 = 2314$, tai

$$d_1+\sigma(d_2)+d_3+\sigma(d_4)=2+6+1+8=17\equiv 7 \pmod{10}$$

ir kontrolinis simbolis yra $d_5=10-7=3$.
Jeigu n yra nelyginis, tai kontrolinis simbolis d_{n+1} yra skaitmuo, su kuriuo teisinga lygybė

$$\sigma(d_1)+d_2+\sigma(d_2)+d_3+\cdots+d_{n-1}+\sigma(d_n)+d_{n+1}\equiv 0 \pmod{10}.$$

Dalybos liekanų aibė

Jeigu du sveikieji skaičiai a ir b, dalijant juos iš n, duoda tą pačią liekaną, žymėsime

$$a \equiv b \pmod{n}.$$

Taip užrašytą sąryšį vadinsime lyginiu.

Teorema. Teisingi tokie teiginiai:

- jei $a \equiv b \pmod{n}$ ir $c \equiv d \pmod{n}$, tai $a + c \equiv b + d \pmod{n}$;
- jei $a \equiv b \pmod{n}$ ir c yra sveikasis skaičius, tai $ca \equiv cb \pmod{n}$;
- jeigu $ca \equiv cb \pmod{n}$ ir skaičiai c, n neturi bendrųjų daliklių, išskyrus vienetą, tai $a \equiv b \pmod{n}$.

Dalybos liekanų aibė

Pažymėkime visų galimų dalybos iš n liekanų aibę

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Šios aibės skaičių sumos ar sandaugos rezultatas, žinoma, nebūtinai priklauso $\mathbb{Z}_n$. Apibrėžkime naujus liekanų sudėties ir sandaugos veiksmus, kurių rezultatai visada priklauso $\mathbb{Z}_n$.

Apibrėžimas. Elementų $a, b \in \mathbb{Z}_n$ suma moduliu n $(n > 1)$ vadinsime natūrinio skaičiaus $a + b$ dalybos iš n liekaną, o sandauga – skaičiaus $a \cdot b$ dalybos iš n liekaną. Apibrėžtųjų veiksmų rezultatus žymėsime

$$a +_n b, \quad a \times_n b.$$

Dalybos liekanų žiedas

Teorema. Suma ir sandauga moduliu n turi šias savybes

- $(a +_n b) +_n c = a +_n (b +_n c)$;
- $a +_n b = b +_n a$;
- $a +_n 0 = a$;
- bet kokiam a lygtis $a +_n x = 0$ turi vienintelį sprendinį;
- $a \times_n b = b \times_n a$;
- $1 \times_n a = a$;
- $(a \times_n b) \times_n c = a \times_n (b \times_n c)$;
- $a \times_n (b +_n c) = a \times_n b +_n a \times_n c$.

Aibė, su kurios elementais apibrėžtos dvi operacijos (paprastai vadinamos sudėtimi ir daugyba), tenkinančios teoremoje išvardytas sąlygas, vadinama žiedu.

Dalybos liekanų žiedas

Teorema. Jeigu n yra pirminis skaičius, tai kiekvienam a, $a \neq 0$, lygtis

$$a \times_n x = 1$$

turi vienintelį sprendinį.

Taigi kai n yra pirminis, visi nenuliniai $\mathbb{Z}_n$ elementai turi atvirkštinius.

Baigtiniai kūnai

Norėdami pabrėžti, kad nagrinėjamas skaičius yra pirminis, žymėsime jį p.

Kūną $\mathbb{Z}_p$ žymėsime, kaip įprasta algebroje, $\mathbb{F}_p$. Vietoj ženklų $+_p, \times_p$ rašysime įprastinius sudėties ir sandaugos ženklus, žodžiu nurodydami, kokiu moduliu turi būti atliekami skaičiavimai.

Nenulinio elemento $\alpha \in \mathbb{F}_p$ atvirkštinį žymėsime α^{-1}.
Turime be galo daug kūnų, kuriuos galime naudoti kaip kodų abėcėles:

$$\mathbb{F}_2,\ \mathbb{F}_3,\ \mathbb{F}_5,\ \ldots$$

Veiksmai su žodžiais

Žodžiams sudaryti naudosime abėcėlę $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$, čia $p > 1$ yra pirminis skaičius, $V_n = \mathbb{F}_p^n$.
Apibrėžimas. Žodžių $\mathrm{x}, \mathrm{y} \in V_n, \mathrm{x} = x_1 x_2 \ldots x_n, \mathrm{y} = y_1 y_2 \ldots y_n$, suma vadinsime žodį $\mathrm{z} = z_1 z_2 \ldots z_n$, čia

$$z_1 = x_1 + y_1,\ z_2 = x_2 + y_2,\ \ldots, z_n = x_n + y_n.$$

Žodžių sudėties savybės – tokios pat kaip skaičių.
Teorema. Tegu $\mathrm{x}, \mathrm{y}, \mathrm{z}$ yra bet kokie aibės V_n elementai. Teisingi šie teiginiai:

- $(\mathrm{x} + \mathrm{y}) + \mathrm{z} = \mathrm{x} + (\mathrm{y} + \mathrm{z})$;
- $\mathrm{x} + \mathrm{y} = \mathrm{y} + \mathrm{x}$;
- egzistuoja $0 \in V_n$, kad $\mathrm{x} + 0 = \mathrm{x}$;
- egzistuoja $\bar{\mathrm{x}}$, kad $\mathrm{x} + \bar{\mathrm{x}} = 0$.

Veiksmai su žodžiais

Elementas $0 = 00\ldots0$ atlieka nulio vaidmenį; jį taip ir vadinsime – nuliniu žodžiu arba elementu. Žodį $\bar{x}$ vadinsime priešingu žodžiui x ir žymėsime $-x$.

Apibrėžimas. Elemento $\alpha \in \mathbb{F}_p$ ir žodžio $x = x_1x_2\ldots x_n \in \mathbb{F}_p^n$ sandauga vadinsime žodį $y = y_1y_2\ldots y_n$, kad

$$y_1 = \alpha x_1,\ y_2 = \alpha x_2,\ \ldots,\ y_n = \alpha x_n.$$

Veiksmai su žodžiais

Teorema. Su bet kokiais $\alpha, \beta \in \mathbb{F}_p$ ir $x, y \in \mathbb{F}_p$ teisingi teiginiai

- $\alpha(x + y) = \alpha x + \alpha y$;
- $(\alpha + \beta)x = \alpha x + \beta x$;
- $(\alpha\beta)x = \alpha(\beta x)$;
- $1x = x$.

Tiesinis apvalkas

Apibrėžimas. Elementų $x_1, x_2, \ldots, x_m \in \mathbb{F}_p$ tiesiniu apvalku vadinsime aibę

$$\mathcal{L}(x_1, x_2, \ldots, x_m) = \{\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m : \alpha_i \in \mathbb{F}_p\}.$$

Visa erdvė V_n yra žodžių

$$e_1 = 100\ldots00,\ e_2 = 010\ldots00,\ \ \ldots\ ,\ e_n = 000\ldots01$$

tiesinis apvalkas, t. y. $V_n = \mathcal{L}(e_1, e_2, \ldots, e_m)$.

Tiesinis poerdvis

Apibrėžimas. Tiesinės erdvės V_n poaibį L vadinsime tiesiniu poerdviu, jeigu

- bet kokiems $x, y \in L$ jų suma $x + y \in L$;
- bet kokiems $\alpha \in \mathbb{F}_p$, $x \in L$ sandauga $\alpha x \in L$.

Tiesiškai nepriklausomi žodžiai

Apibrėžimas. Sakysime, kad žodžiai $x_1, x_2, \ldots, x_m$ yra tiesiškai nepriklausomi, jeigu lygybė

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m = 0, \quad 0 = 00\ldots0,$$

teisinga tik tuomet, kai $\alpha_1 = \alpha_2 = \ldots = \alpha_m = 0$. Priešingu atveju sakysime, kad žodžiai yra tiesiškai priklausomi.

Jeigu žodžiai $x_1, x_2, \ldots, x_m$ yra tiesiškai priklausomi, tai galime sudaryti nulinę jų kombinaciją

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m = 0,$$

panaudoję ne vien tik nulinius koeficientus.

Tiesinio poerdvio bazė

Apibrėžimas. Tegu $L \subset \mathbb{F}_p^n$ yra tiesinis poerdvis. Tiesiškai nepriklausomų žodžių sistemą $x_1, x_2, \ldots, x_m$ vadinsime poerdvio baze, jei

$$L = \mathcal{L}(x_1, x_2, \ldots, x_m).$$

Teorema. Bet kuris poerdvis $L \subset \mathbb{F}_p^n$ turi bazę. Visos poerdvio bazės turi tą patį žodžių skaičių.

Teorema. Tiesinio poerdvio L bazės žodžių skaičių vadinsime jo dimensija ir žymėsime dim(L).

Dualūs poerdviai

Apibrėžimas. Tegu $x = x_1 x_2 \dots x_n$, $y = y_1 y_2 \dots y_n$ yra du erdvės V_n žodžiai. Jų vidine sandauga vadinsime $\mathbb{F}_p$ elementą, apibrėžiamą lygybe

$$x \cdot y = x_1 y_1 + \dots + x_n y_n.$$

Teorema. Tegu L yra tiesinis poerdvis. Žodžių aibė

$$L^{\perp} = \{y \in V_n : x \cdot y = 0 \text{ su visais } x \in L\}$$

taip pat yra tiesinis poerdvis. Poerdvių dimensijos susijusios lygybe

$$\dim(L) + \dim\left(L^{\perp}\right) = n.$$

Tiesinį poerdvį $L^{\perp}$ vadinsime dualiu poerdviui L. Beveik akivaizdu, kad

$$\left(L^{\perp}\right)^{\perp} = L.$$

Dualus poerdvis

Teorema. Tegu L yra tiesinis poerdvis, $\dim(L) = k$, o $h_1, \dots, h_{n-k}$ yra dualaus poerdvio $L^{\perp}$ bazė. Tada

$$L = \{x \in V_n : x \cdot h_1 = x \cdot h_2 = \dots = x \cdot h_{n-k} = 0\}.$$

Tiesinis kodas

Apibrėžimas. Tiesinį erdvės $\mathbb{F}_q^n$ žodžių poerdvį $\mathrm{L} \subset \mathbb{F}_q^n$ vadinsime tiesiniu kodu. Jeigu šio kodo dimensija yra k, o minimalus atstumas – d, sakysime, kad tai $[n, k, d]$ kodas.

Bet kokio kodo parametrus žymime (n, N, d), o $[n, k]$ ir $[n, k, d]$ – tik tiesinių kodų parametrus. Jei L yra abėcėlės $\mathbb{F}_q$ žodžių $[n, k, d]$ kodas, tai $|\mathrm{L}| = q^k$, o jo koeficientas

$$R(\mathrm{L}) = \frac{\log_q |\mathrm{L}|}{n} = \frac{k}{n}.$$

Kodavimas tiesiniais kodais

Apibrėžimas. Tegu $\mathrm{L} \subset \mathbb{F}_q^n$ yra tiesinis $[n, k]$ kodas. Kūno $\mathbb{F}_q$ elementų $k \times n$ matricą G vadinsime generuojančia kodo **L** matrica, jei n ilgio žodžiai, gauti surašant matricos G eilučių elementus, sudaro kodo **L** bazę.

Atvaizdis

$$\mathrm{x} \to \mathrm{x}G$$

apibrėžia abipusiškai vienareikšmę erdvės $\mathbb{F}_q^k$ ir kodo **L** žodžių atitiktį. Tad šį priskyrimą galime interpretuoti kaip šaltinio informacijos, pateikiamos erdvės $\mathbb{F}_q^k$ žodžiais, kodavimą kodo **L** žodžiais.

Pavyzdys

Kodavimui naudojamas dvinaris tiesinis $[4, 3]$ kodas su generuojančia matrica

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Šaltinis perdavė tokį iš nulių ir vienetų sudarytą informacijos srautą:

$$110\ 010\ 001\ 111\ 101\ 010\ldots$$

Tada kanalu siųsime tokią simbolių seką:

$$1011\ 0111\ 1010\ 0001\ 0110\ 0111\ldots$$

Elementarieji pertvarkiai

Apibrėžimas. Tegu G yra kūno $\mathbb{F}_q$ elementų $k \times n$ matavimų matrica. Elementariaisiais matricos G pertvarkiais vadinsime šiuos veiksmus:

- dviejų eilučių (arba stulpelių) keitimą vietomis;
- eilutės daugybą iš $f \in \mathbb{F}_q,\ f \neq 0$;
- eilutės keitimą jos bei kitos eilutės suma;
- stulpelio daugybą iš $f \in \mathbb{F}_q,\ f \neq 0$.

Jei matrica G yra tiesinio $[n, k]$ kodo **L** generuojanti matrica, o matrica G' gaunama iš G, atlikus elementariųjų pertvarkių seką, tai G' yra taip pat tam tikro tiesinio $[n, k]$ kodo L$'$ generuojanti matrica.

Teorema. Tegu G yra tiesinio kodo L generuojanti matrica, o G' yra matrica, gauta iš G, atlikus elementariųjų jos pertvarkių seką. Tada G' yra kodo, ekvivalentaus L, t.y., turinčio tuos pačius parametrus ir tas pačias klaidų taisymo galimybes, generuojanti matrica.

Standartinio pavidalo generuojanti matrica

Jei G yra $[n, k]$ kodo generuojanti matrica, tai atitinkamais elementariaisiais pertvarkiais iš jos galima gauti tokio pavidalo matricą:

$$G' = \begin{pmatrix} 1 & 0 & \dots & 0 & a_{1,1} & \dots & a_{1,n-k} \\ 0 & 1 & \dots & 0 & a_{2,1} & \dots & a_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & a_{k,1} & \dots & a_{k,n-k} \end{pmatrix} = (I_k, A); \qquad (1)$$

čia: I_k yra vienetinė $k \times k$ matrica, A – kūno $\mathbb{F}_q$ elementų $k \times (n-k)$ matrica. Susitarsime sakyti, jog matrica yra **standartinio pavidalo**.

Standartinio pavidalo generuojanti matrica

Teorema. Kiekvienas $[n, k]$ kodas yra ekvivalentus $[n, k]$ kodui, turinčiam standartinio pavidalo generuojančią matricą.

Bet kokį tiesinį kodą galime pakeisti jam ekvivalenčiu kodu, turinčiu standartinio pavidalo generuojančią matricą. Todėl pakanka nagrinėti tik tokius kodus. Kodavimas su matrica $G = (I_k, A)$:

$$\mathrm{x} \to \mathrm{xy}, \quad \mathrm{y} = \mathrm{x}A,$$

koduojami žodžiai tiesiog pailginami pridedant $n-k$ kontrolinių klaidoms taisyti skirtų simbolių.

Svoris ir minimalus kodo atstumas

Apibrėžimas. Žodžio $\mathrm{x} \in \mathbb{F}_q^n$, $\mathrm{x} = x_1 \dots x_n$, svoriu vadinsime skaičių

$$w(\mathrm{x}) = \sum_{x_i \neq 0} 1.$$

Žodžio svoris – tiesiog nenulinių jo komponenčių skaičius. Tik vienas žodis „nieko nesveria“, t. y. jo svoris lygus nuliui: $w(00\dots0) = 0$; kitų žodžių svoriai ne mažesni už 1.

Teorema. Tegu d yra tiesinio kodo $\mathbf{L}$ minimalus atstumas. Tada

$$d = \min\{w(\mathrm{x}) : \mathrm{x} \in \mathrm{L}, \mathrm{x} \neq 00\dots0\}.$$

Kontrolinė kodo matrica

Teorema. Tegu $G = (I_k, A)$ yra tiesinio $[n, k]$ kodo $\mathrm{L} \subset \mathbb{F}_p^n$ generuojanti matrica. Tada matrica

$$H = (-A^T, I_{n-k})$$

yra kontrolinė šio kodo matrica.

Norint įrodyti šį teiginį, reikia įsitikinti, kad teisinga lygybė

$$G \cdot H^T = (I_k, A) \cdot \begin{pmatrix} -A \\ I_{n-k} \end{pmatrix} = O_{k,n-k}.$$

Kontrolinė kodo matrica ir minimalus atstumas

Teorema. Tegu H yra tiesinio kodo $\mathbf{L}$ kontrolinė matrica. Jeigu egzistuoja d tiesiškai priklausomų H stulpelių, o bet kuri $d-1$ šios matricos stulpelių sistema yra tiesiškai nepriklausoma, tai minimalus kodo atstumas lygus d.

Trynimo klaidų taisymas

Kodavimui naudojamas $[n,k]$ tiesinis kodas $\mathrm{C} \subset \mathbb{F}_q^n$ su kontroline $(n-k)\times n$ matavimų matrica $H=(h_{ij})$. Jeigu $\mathrm{c}=c_1c_2\ldots c_n$ yra kodo žodis, tai $\mathrm{c}H^T=0$:

$$\begin{aligned} h_{11}c_1+h_{12}c_2+\ldots+h_{1n}c_n &= 0,\\ h_{21}c_1+h_{22}c_2+\ldots+h_{2n}c_n &= 0,\\ &\ldots\ldots\ldots\\ h_{n-k,1}c_1+h_{n-k,2}c_2+\ldots+h_{n-k,n}c_n &= 0. \end{aligned}$$

Tarkime, kad perdavimo kanalas simbolių neiškraipo, tačiau gali ištrinti. Tada vietoj žodžio $\mathrm{c}=c_1c_2c_3\ldots c_n$ gausime, pavyzdžiui, $\mathrm{d}=?c_2?\ldots c_n$. Perduotas simbolių reikšmes reikia įstatyti į sistemos lygybes, o ištrintų simbolių vietoje – nežinomuosius; pavyzdyje – $x_1, x_3, \ldots$

Standartinė kodo lentelė

Tegu $L \subset \mathbb{F}_q^n$ yra tiesinis $[n, k]$ kodas. Suskaidysime žodžių erdvę $\mathbb{F}_q^n$ sluoksniais

$$L_x = x + L = \{x + c : c \in L\}, \quad x \in \mathbb{F}_q^n.$$

$$\begin{pmatrix} a_0 & c_1 & c_2 & \dots & c_N \\ a_1 & a_1 + c_1 & a_1 + c_2 & \dots & a_1 + c_N \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_s & a_s + c_1 & a_s + c_2 & \dots & a_s + c_N \end{pmatrix}.$$

Kiekvienoje eilutėje surašyti atitinkamos klasės L_a elementai, o pirmasis iš jų turės mažiausią svorį. Matricą vadinsime **standartine** kodo **L lentele**, o žodžius a_i – atitinkamų klasių **lyderiais**.

Dekodavimas su lentele

Turint standartinę kodo lentelę, dekodavimo algoritmą galima aprašyti taip:

- randame, kurioje standartinės lentelės eilutėje yra gautasis žodis **x**;
- randame šios eilutės lyderį **a** ir dekoduojame **x** žodžiu $f(x) = x - a$.

Žodžio sindromas

Tegu H yra kontrolinė kodo **L** matrica. Jei **c** yra kodo **L** žodis, tai $cH^T = 0$. Jei $x = a_j + c$, tai $xH^T = a_jH^T$. Taigi sandaugos $xH^T, x \in \mathbb{F}_q^n$, reikšmė priklauso tik nuo to, kuriai aibės $\mathbb{F}_q^n/L$ klasei priklauso **x**.

Apibrėžimas. Tegu H yra $[n, k]$ kodo **L** kontrolinė matrica, $x \in \mathbb{F}_q^n$. Žodžio **x** sindromu vadinsime $\mathbb{F}_q^{n-k}$ elementą $s(x) = xH^T$.

Skirtingiems aibės $\mathbb{F}_q^n/L$ sluoksniams priklausančių žodžių sindromai yra skirtingi.

Dekodavimas su sindromais ir lyderiais

Sindromai	s_1	s_2	$\ldots$	s_m
Lyderiai	a_1	a_2	$\ldots$	a_m.

Dekodavimo algoritmas:

- *randame gautojo žodžio sindromą.*
- randame šios eilutės lyderį **a** ir dekoduojame **x** žodžiu $f(x) = x - a$.

Kriptografijos pagrindai

Duomenų apsaugos uždaviniai

Šiuolaikinę kriptografiją „pagimdė“ kompiuteriniai tinklai.
Duomenų apsaugos tikslai:

- duomenų slaptumas (konfidencialumas);
- duomenų vientisumas (integralumas);
- duomenų šaltinio autentiškumo užtikrinimas;
- vartotojo autorizavimas (naudojimosi sistemos ištekliais valdymas);
- užkarda „bandymams išsisukti“
- ... kiti specialūs uždaviniai

Kriptografijos įrankiai

- be raktų: maišos funkcijos, atsitiktinės bitų sekos, keitiniai;
- su simetriniais raktais: simetriniai šifravimo algoritmai, autentifikavimo kodai, pseudoatsitiktinių bitų srautai;
- su viešuoju raktu: viešo rakto šifravimo algoritmai, parašai...

Kriptosistema – įrankių sistema, naudojama duomenų apsaugai.

Kriptografija ir kriptoanalizė

Kriptografija kuria duomenų apsaugos įrankius.
Kriptoanalizė bando juos įveikti.
Kriptologija = kriptografija + kriptoanalizė

Kriptografiniai protokolai

Kriptografija kuria įrankius informacijos apsaugos uždaviniams spręsti.

Protokolas nurodo, kaip turi elgtis dalyviai, kad pasiektų norimą rezultatą.

Kriptografinis protokolas - protokolas, kuriame naudojami kriptografiniai įrankiai (algoritmai).

Kriptografinių protokolų ypatybė

Protokolų, kurie naudojami kompiuterių tinkluose ypatybė: subjekto, dalyvaujančio protokole tapatybės negalima nustatyti tiesiogiai, t.y. remiantis fizinėmis jo savybėmis.

Veikiantieji asmenys

Algis, Birutė, Justas, Zigmas, ...

Kriptografinės apsaugos atakos

Atakos gali būti nukreiptos

- į kriptografinius algoritmus
- į algoritmų naudojimo metodus
- į kriptografinius protokolus

Kriptografinių protokolų atakos

Pasyvios (kriptografinių protokolų vykdymo duomenų analizė)

Aktyvios (įsibrovimas į kanalą, duomenų keitimas, apsimetimas...)

Aktyvios kriptografinių protokolų atakos

- Žinomų raktų ataka
- Protokolo kartojimas
- Apsimetimo ataka
- Žodyno ataka
- Įsiterpimo ataka

Prielaidos apie Z

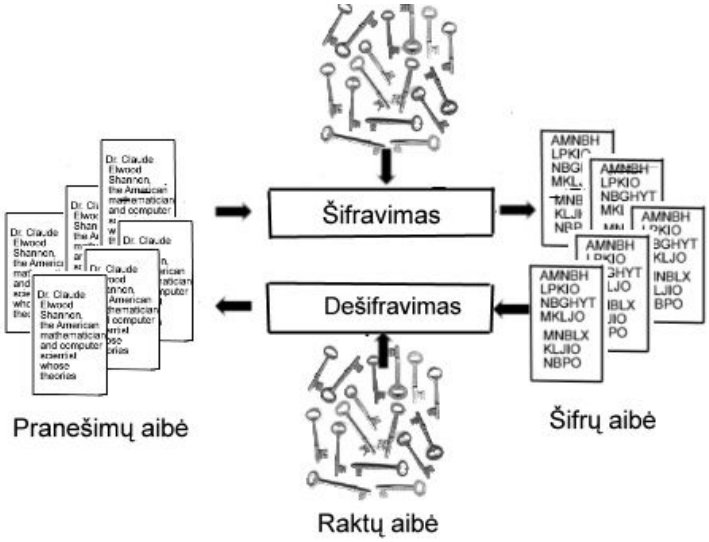
- gali nukopijuoti bet kokius seanso metu siunčiamus duomenis
- gali pakeisti bet kurį pranešimą
- gali pasiųsti seanso pranešimą kitu adresu
- Z gali būti pašalinis asmuo, o taip pat – teisėtas protokolo dalyvis
- gali gauti ankstesnių protokolų slaptus duomenis (raktus)

Kriptografinės duomenų apsaugos įrankiai

- simetrinės kriptosistemos
- viešojo rakto kriptosistemos
- skaitmeniniai parašai
- maišos funkcijos (h-funkcijos)
- ...

Kriptosistema

Duomenų slaptumą užtikrina šifravimas



Kriptosistema

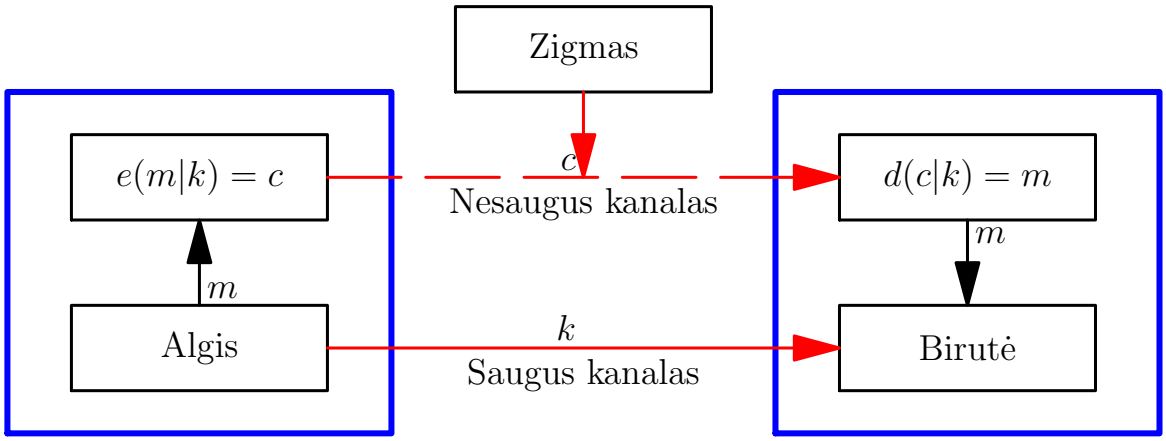
Apibrėžimas. Kriptografine sistema (kriptosistema) vadinsime aibių trejetą $\langle \mathcal{M}, \mathcal{K}, \mathcal{C} \rangle$ ir atvaizdžių porą

$$e(\cdot|K) : \mathcal{M} \to \mathcal{C}, \quad d(\cdot|K) : \mathcal{C} \to \mathcal{M}, \quad K \in \mathcal{K}.$$

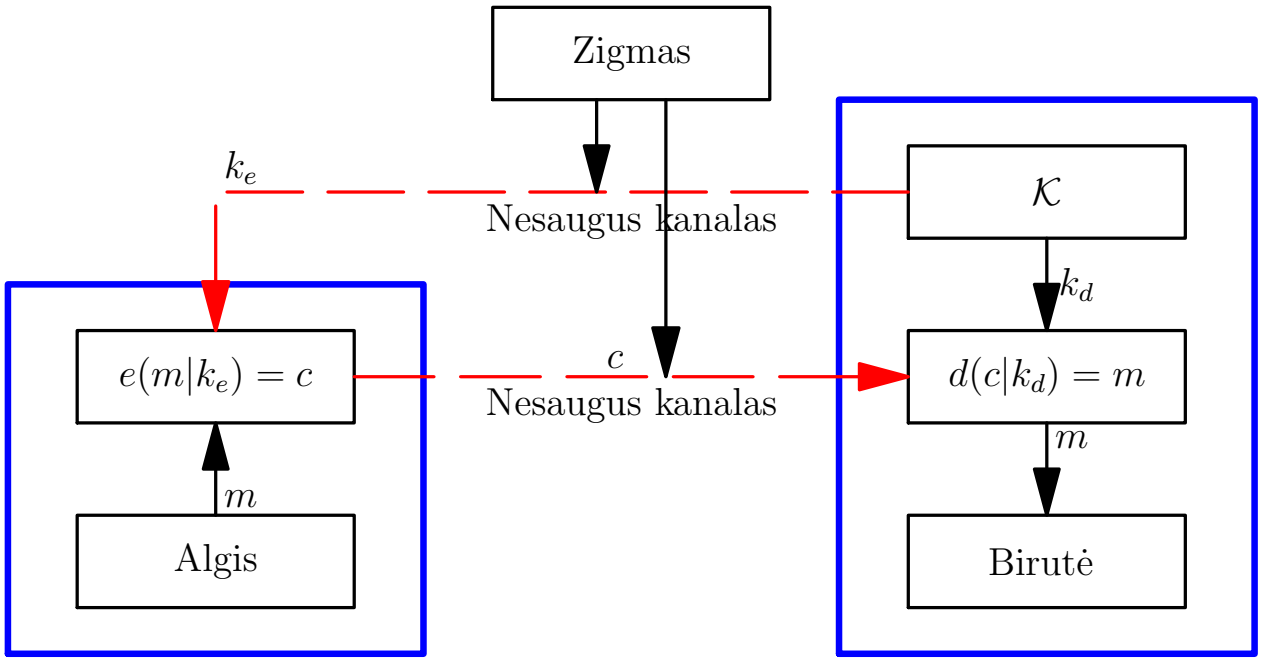
Apie kriptosistemos elementus galvojame taip:

- $\mathcal{M}$ – pranešimų, kuriuos galima šifruoti, aibė;
- $\mathcal{K}$ – raktų, kuriuos galima naudoti, aibė;
- $\mathcal{C}$ – šifrų aibė;
- $e(\cdot|K)$ – šifravimo algoritmas, kurį valdo raktas K;
- $d(\cdot|K)$ – dešifravimo algoritmas, kurį valdo raktas K,

Simetrinės kriptosistemos

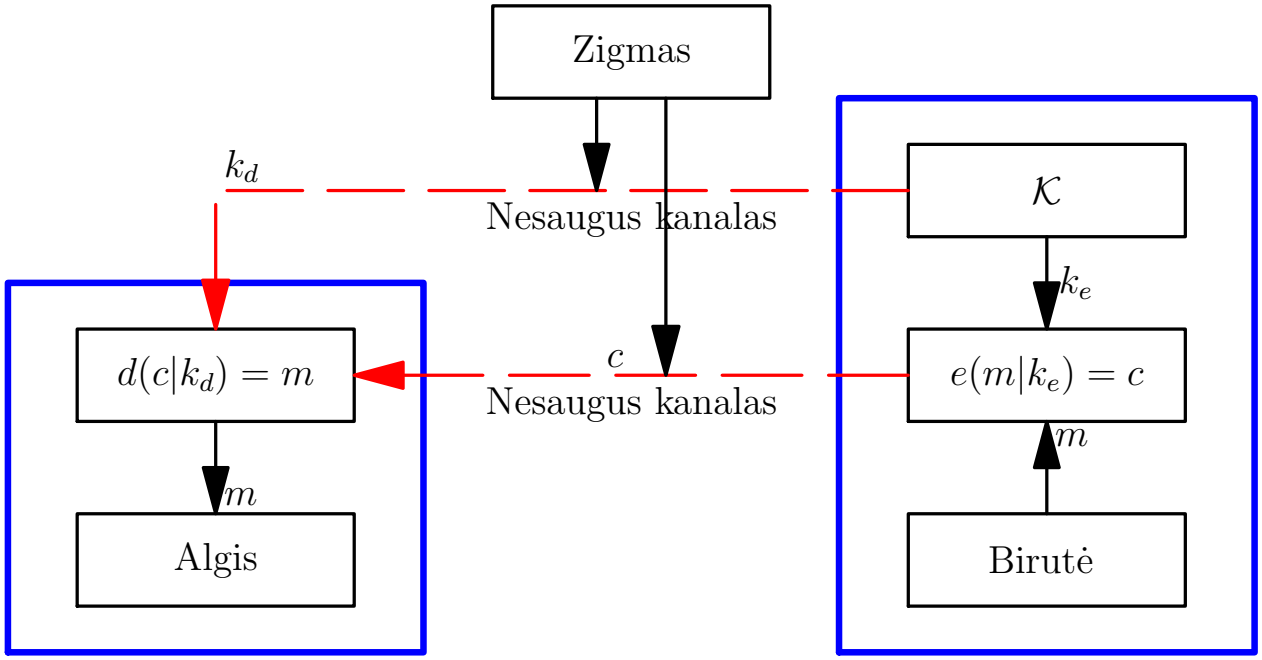


Nesimetrinės kriptosistemos

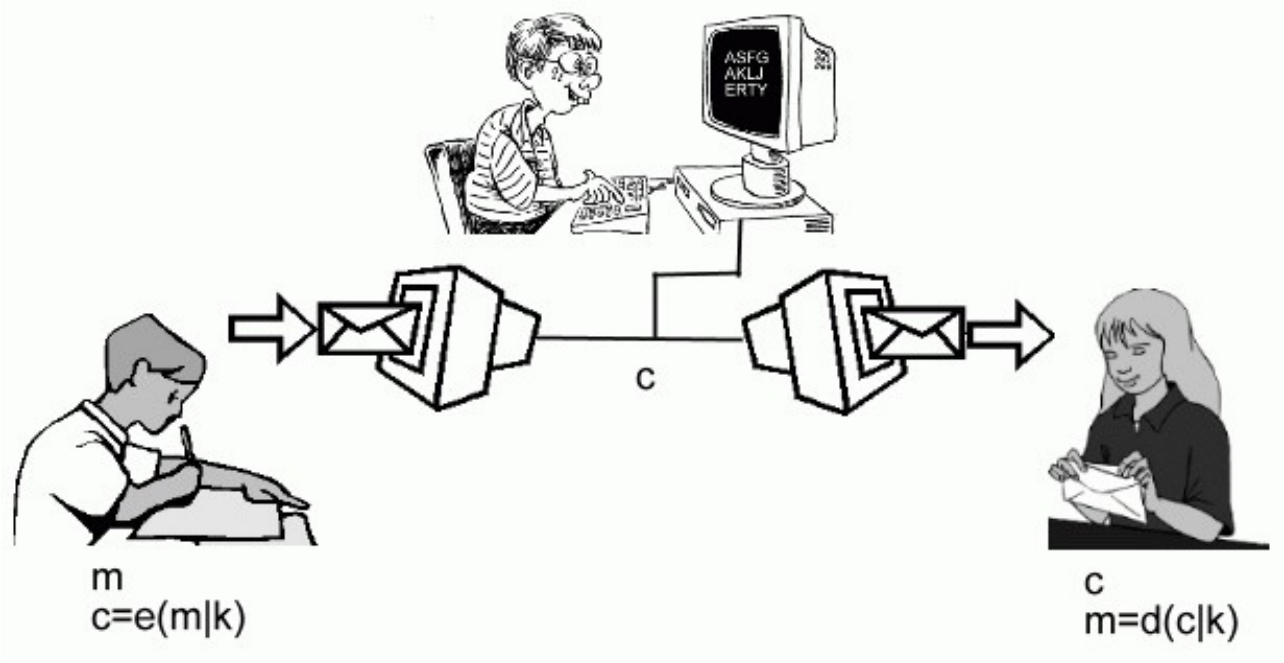


Skaitmeniniai parašai

Pranešimo autentiškumo užtikrinimo įrankis – skaitmeninis parašas



Atakos



Tikslas: naudojantis turima informacija apie kriptosistemą įgyti galimybę dešifruoti šifrus.

Kerckhoffo aksioma

Priešininkas žino apie kriptosistemą viską, išskyrus raktą.

Atakų rūšys:

- kriptosistemų struktūros atakos
- kriptosistemų realizacijos (kanalų) atakos
- protokolų atakos

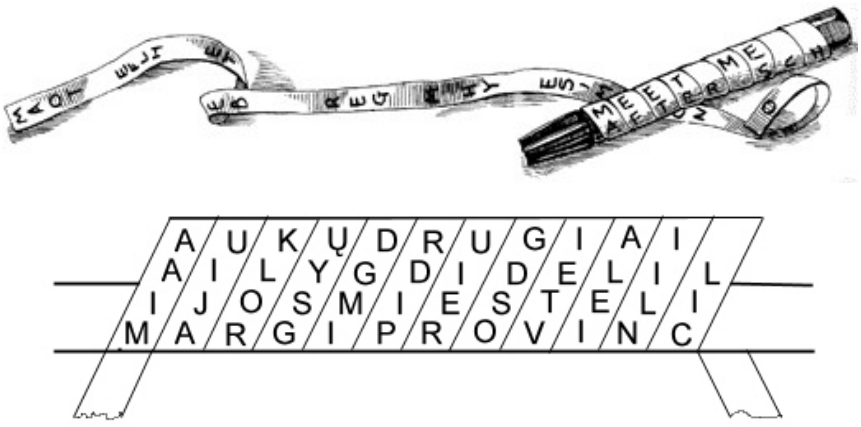
Kriptosistemų saugumo vertinimas

- besąlygiškas saugumas;
- saugumas sudėtingumo teorijos požiūriu;
- saugumas skaičiavimų išteklių požiūriu;
- įrodytas saugumas;
- ad hoc saugumas.

Klasikinė kriptografija

Perstatų šifrai

Informacijos struktūra paslepiama perstatant simbolius.
Kaip užrašyti perstatų šifro raktą?



Skytalė: šie tiek Sage kodo

```
abc=unicode('AaĄąBbC....RrSsŠšTtUuŲųŪūVvZzŽž','utf-8')
abcD=unicode('AĄBCČDEĘĖFGHIĮYJKLMNOPRSŠTUŲŪVZŽ','utf-8')

def pertv(text): # Pašalina ne abėcėlės ženklus
    textn=''
    for a in text:
        if a in abc:
            textn+=a
    return textn.upper()


tx=unicode('aa22čččč sssddūūū','utf-8')
print pertv(tx)

AAČČČČSSSDDŪŪŪ
```

Skytalė: šie tiek Sage kodo

```
def skytale(text,key):
    textn=pertv(text)
    c=''
    ilg=len(text)
    r=key-ilg%key
    if r<key:
        textn+=textn[0:r]
    ilg=len(textn)
    eil=ilg//key
    for i in range(0,eil):
        for j in range(0,key):
            c+=textn[i+j*eil]
    return c
tekstas=unicode('žvarbus vėjas pūtė visą dieną','utf-8')
print skytale(tekstas,4)

ŽVTIVĖĖEAJVNRAIĄBSSŽUPĄVSŪDA
```

Perstatų šifras

P	R	I	S	I	P	A	Ž	I	N
O	J	O	N	A	V	A	Š	I	L
U	T	E	I	L	A	B	A	I	K
A	U	N	U	Ž	I	N	O	K	I
T	N	O	R	I	S	B	Ū	T	I
T	U	R	I	U	G	A	M	Y	K
L	Ą	P	U	I	K	I	Ą	I	L
G	Ą	K	A	M	I	N	Ą	U	Ž
T	E	R	Š	T	T	I	K	R	A
I	P	A	J	Ė	G	Č	I	A	U
J	Ū	S	Ų	N	E	M	U	N	Ą

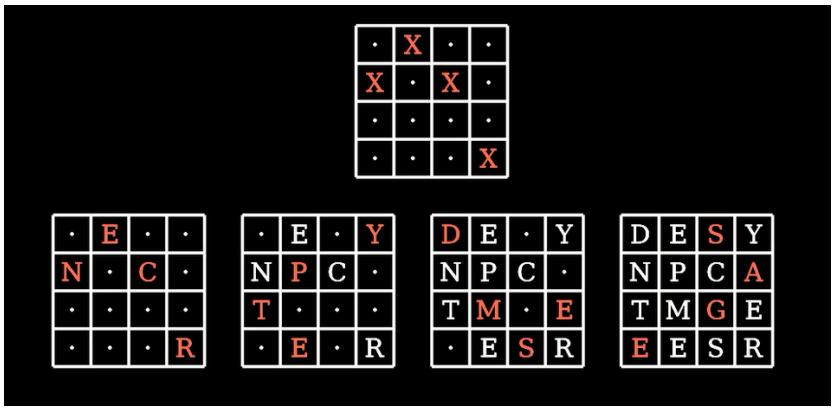
Raktas: SAULĖTEKIS $\rightarrow$ 7-1-10-6-3-9-2-5-4-8 Perstatų šifras

Geležinkelio tvorelės šifras

Ž T I N M S T
E E Ū R N I T E E Ū L N A
M I S A I R A Ž M N A I I
E L V S A K O O P I B R
J A I P A I

Fleissnerio šifras

Pranešimas=ENCRYPTEDMESSAGE



Šifras=DESYNPCATMGEEESR

Keitinių šifrai

$\mathcal{A}, \mathcal{B}$ – teksto ir šifro abėcėlės,

$$e(\cdot|K) : \mathcal{A} \to \mathcal{B}$$

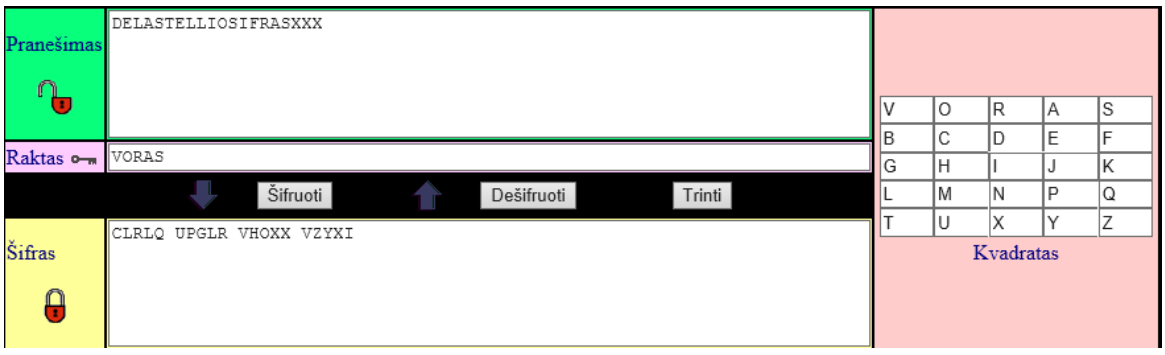
injektyvus atvaizdis,

$$e(m_1 m_2 \dots m_n|K) = e(m_1|K)e(m_2|K)\dots e(m_n|K)$$

Polibijaus kodas

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

Dellastelio šifras (1895)

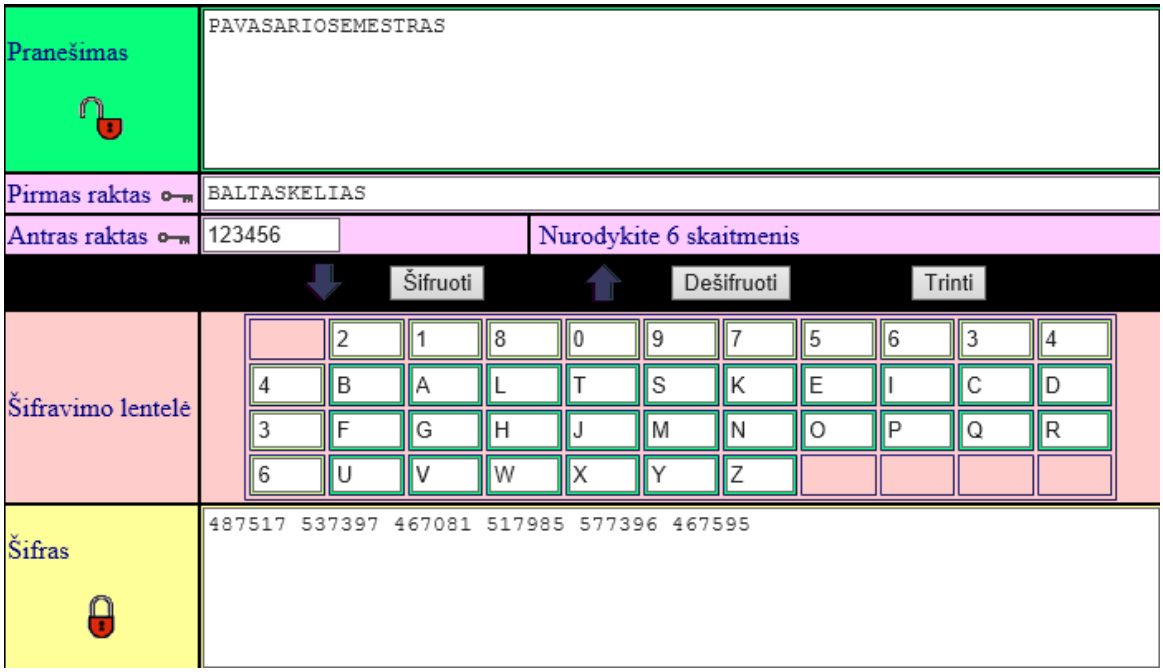


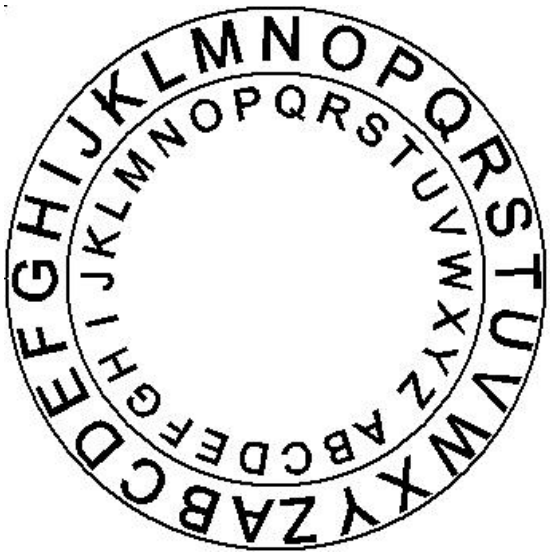
Dellastelio šifras

Pranešimas=KEEPSILENCE Raktas=RAKTAS

Šifras=AEKHNDPQLNE

Hayhaneno šifras (1953)





Cezario šifras

$$\mathcal{A} = \mathcal{B} = \mathcal{K} = \{0, 1, 2, \ldots, n-1\}$$

$$e(a|k) = a + k \pmod{n}$$

Afininiai Cezario šifrai:

$$\mathcal{A} = \mathcal{B} = \{0, 1, 2, \ldots, n-1\},$$
$$\mathcal{K} = \{\langle k_1, k_2\rangle : (k_1, n) = 1\}$$

$$e(a|k_1, k_2) = k_1 a + k_2 \pmod{n}$$

Playfairo (Wheatstono) šifras

P	L	A	Y	F	P	L	A	Y	F
I	R	E	X	M	I	R	E	X	M
B	C	D	G	H	B	C	D	G	H
K	N	O	Q	S	K	N	O	Q	S
T	U	V	W	Z	T	U	V	W	Z

Hilo šifras

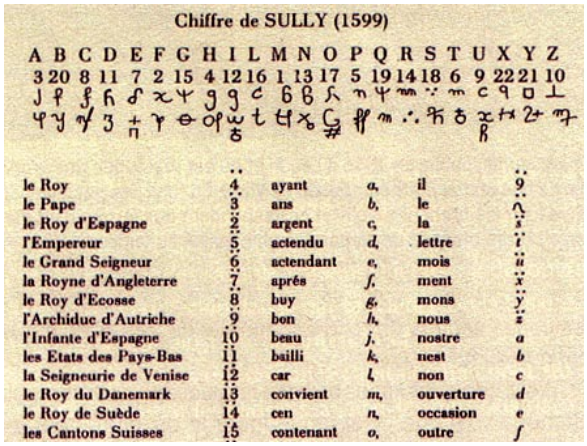
$\mathcal{A} = \mathcal{B} = \{\langle i, j\rangle : 0 \leqslant i, j < n\},$

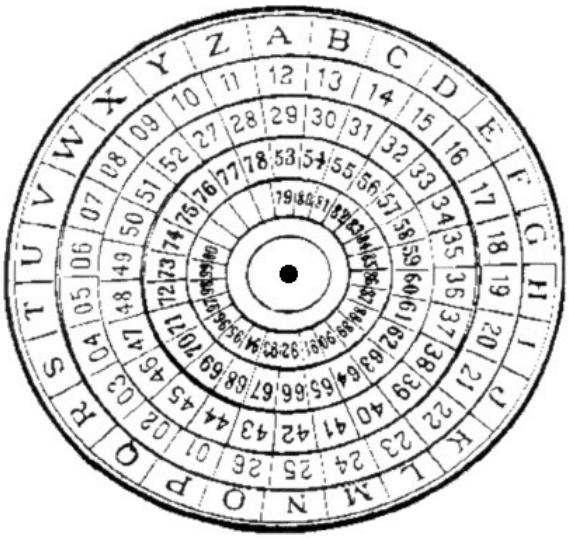
$$\mathcal{K} = \left\{ K : K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}, 0 \leqslant k_{ij} < n, (det(K), n) = 1 \right\}$$

$e(\langle m_1, m_2\rangle | K) = \langle m_1, m_2\rangle \cdot K \pmod{n}$

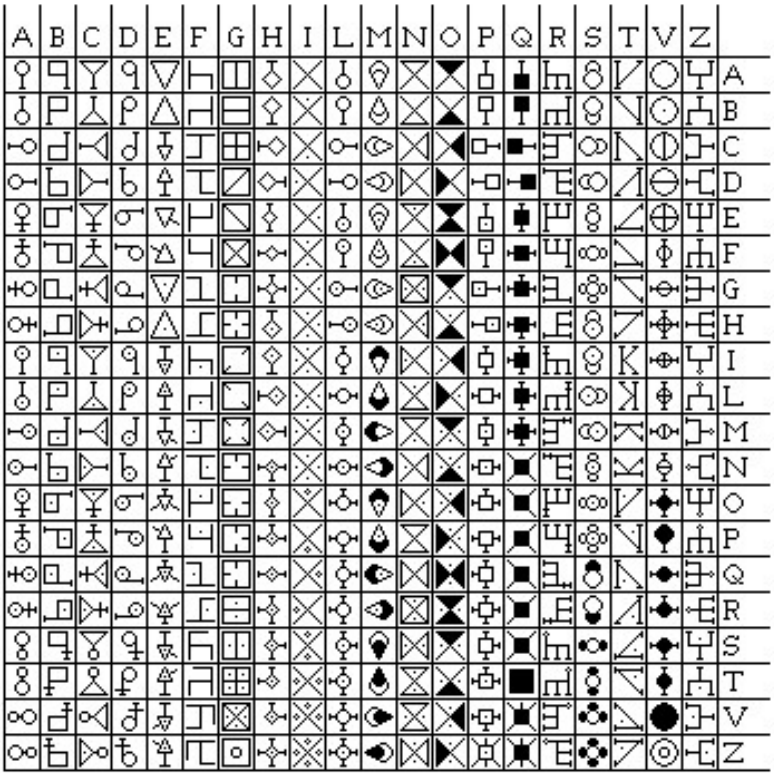
Galima šifruoti ne tik poras, bet ir ilgesnes sekas.

Homofonai

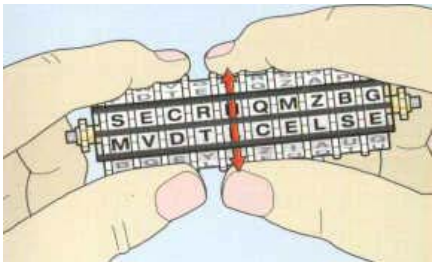




De la Porta homofonų šifras

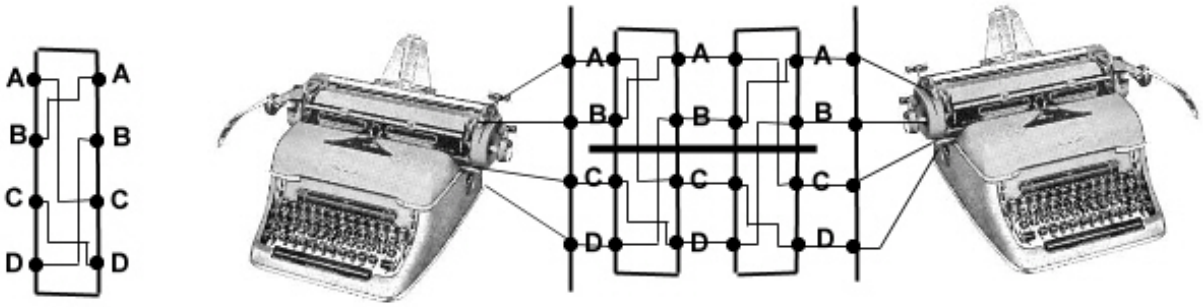


Mechaniniai šifravimo prietaisai



Thomo Jeffersono (1743-1826) ritiniai.
Išrasta pakartotinai keletą kartų (Etienne Bazeries (1891), Ducros (1900), Parker Hitt (1914)).
Amerikiečiai naudojo Pirmajame pasauliniame kare Word War I (įrenginys M-94).

Rotoriai. Enigma



$$\rho = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}, \quad \lambda_1 = \lambda_2 = \begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}$$

$$\begin{aligned} \textit{Tekstas} &= t_0 t_1 t_2 \ldots, \quad t_k, \quad k = m_1 + 4m_2 + \ldots \\ c_k &= \rho^{-m_2} \lambda_2 \rho^{m_2} \rho^{-m_1} \lambda_1 \rho^{m_1}(t_k), \\ t_k &= \rho^{-m_1} \lambda_1^{-1} \rho^{m_1} \rho^{-m_2} \lambda_2^{-1} \rho^{m_2}(c_k) \end{aligned}$$

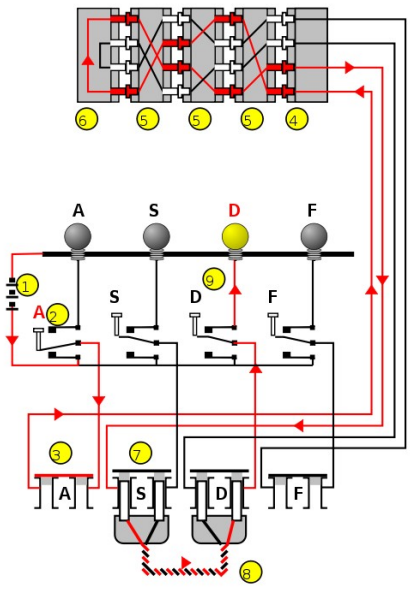
Enigma su dviem rotoriais. Matematinis apibrėžimas

$$
\begin{aligned}
\mathcal{A} &= \{0, 1, \ldots, n-1\}, \\
\rho &= \begin{pmatrix} 0 & 1 & \ldots & n-2 & n-1 \\ 1 & 2 & \ldots & n-1 & 0 \end{pmatrix} = [1, 2, 3, \ldots, n-1, 0], \\
\rho^m(a) &= a + m \pmod{n}
\end{aligned}
$$

Rotoriai pradinėje padėtyje nepasukti.

$$
\begin{aligned}
\textit{Tekstas} &= t_0\, t_1\, t_2 \ldots, \quad t_k, \\
\text{Šifras} &= c_0\, c_1\, c_2 \ldots, \quad c_k, \\
k &= m_1 + n \cdot m_2 + \ldots \\
c_k &= \rho^{-m_2} \lambda_2 \rho^{m_2} \rho^{-m_1} \lambda_1 \rho^{m_1}(t_k), \\
t_k &= \rho^{-m_1} \lambda_1^{-1} \rho^{m_1} \rho^{-m_2} \lambda_2^{-1} \rho^{m_2}(c_k)
\end{aligned}
$$

ENIGMA diagrama



Be rotorių dar buvo naudojami du keitiniai sujungimų ir atspindžio (plugboard and reflector).

Matematinis pilnos ENIGMA schemos aprašymas

$$
\begin{aligned}
\mathit{Tekstas} &= t_0\, t_1\, t_2 \ldots, \quad t_k, \\
k &= m_1 + m_2 \cdot n + m_3 \cdot n^2 + \ldots \\
\alpha(m, \lambda) &= \rho^{-m} \lambda \rho^m, \\
\alpha^{-1}(m, \lambda) &= \rho^m \lambda^{-1} \rho^{-m} \\
\sigma &= \sigma^{-1} \\
c_k &= \sigma^{-1}\alpha^{-1}(m_1, \lambda_1)\alpha^{-1}(m_2, \lambda_2)\alpha^{-1}(m_3, \lambda_3)\pi \leftarrow \\
&\quad \alpha(m_3, \lambda_3)\alpha(m_2, \lambda_2)\alpha(m_1, \lambda_1)\sigma(t_k) \\
t_k &= \sigma^{-1}\alpha^{-1}(m_1, \lambda_1)\alpha^{-1}(m_2, \lambda_2)\alpha^{-1}(m_3, \lambda_3)\pi \leftarrow \\
&\quad \alpha(m_3, \lambda_3)\alpha(m_2, \lambda_2)\alpha(m_1, \lambda_1)\sigma(c_k)
\end{aligned}
$$

Blokiniai šifrai

Šiuolaikiniai šifrai: dvejetainė abėcėlė

Šiuolaikiniai šifrai šifruoja dvejetainės abėcėlės $\mathcal{B} = \{0, 1\}$ žodžius. Kalbų abėcėlių raidės keičiamos dvejetainės abėcėlės žodžiais naudojantis Unicode koduote.
Dvejetainės abėcėlės žodžiai gali būti užrašomi dešimtainės ar šešioliktainės skaičiavimo sistemos skaitmenimis.

Šiuolaikiniai šifrai: dvejetainė abėcėlė

Base64 kodas paverčia bet kokią dvejetainę seką spausdinamų simbolių eilute.

Tekstas	Latin	abc
	decimal	97 98 99
	hexadecimal	61 62 63
	binary	1100001 1100010 1100011
	Base64	YWJj

Base64 kodas naudoja simbolius A — Z, a -– z, 0 -– ir + , /. Šiais simboliais keičiami 6 bitų ilgio dvejetainiai žodžiai.

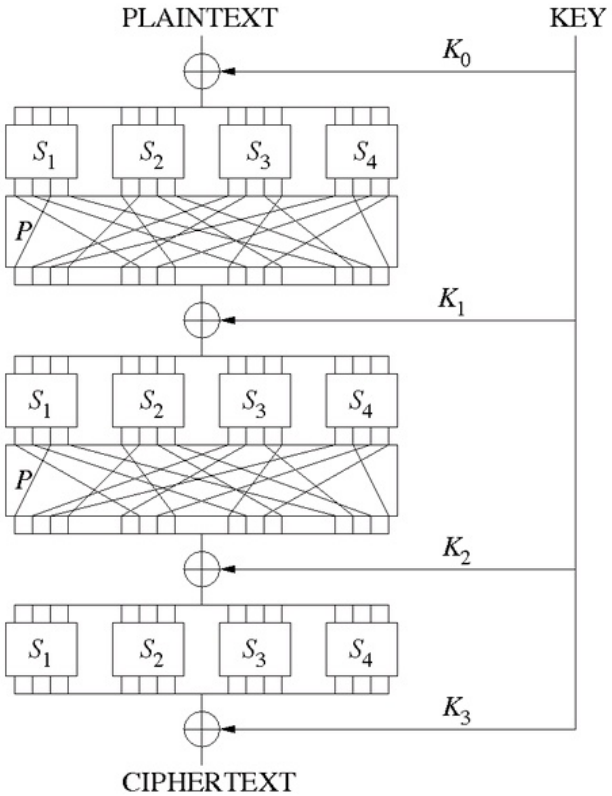
KPT – keitinių-perstatų tinklas (SPN – substitution-permutation network)

Šiuolaikinių blokinių šifrų struktūros schema.

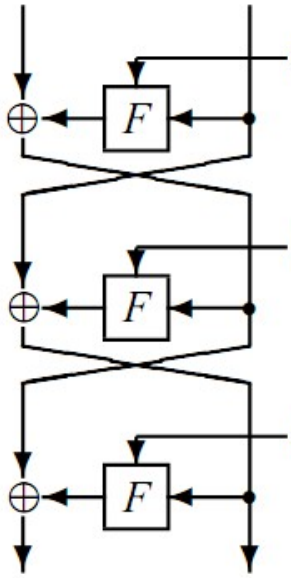
Difuzijos savybė: pakeitus vieną šifruojamo teksto bitą, tikimybė, kad j-asis šifro bitas pasikeis, apytiksliai lygi 1/2 (griūties kriterijus).

Sumaišymo (confusion) savybė: pakeitus vieną rakto bitą, teksto šifre pasikeičia maždaug pusė bitų.

KPT – keitinių-perstatų tinklas



Feistelio tinklas

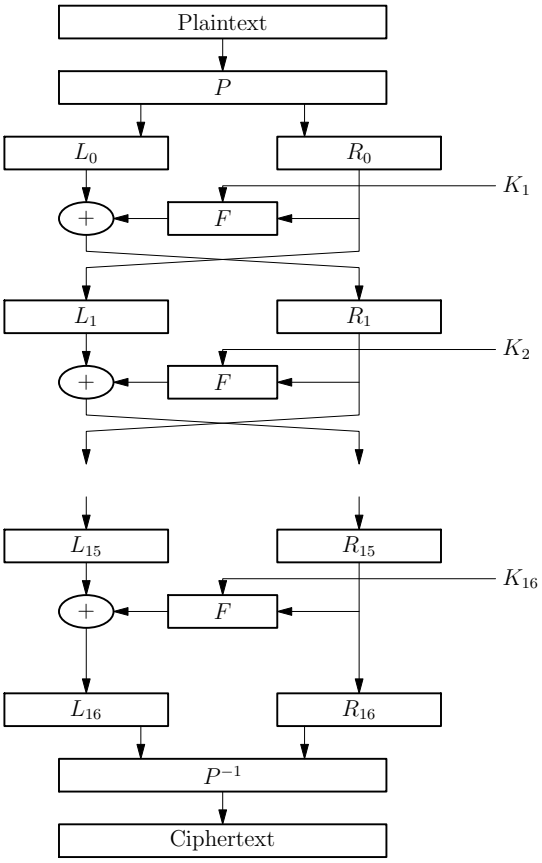


Šifravimo ir dešifravimo schemos vienodos:

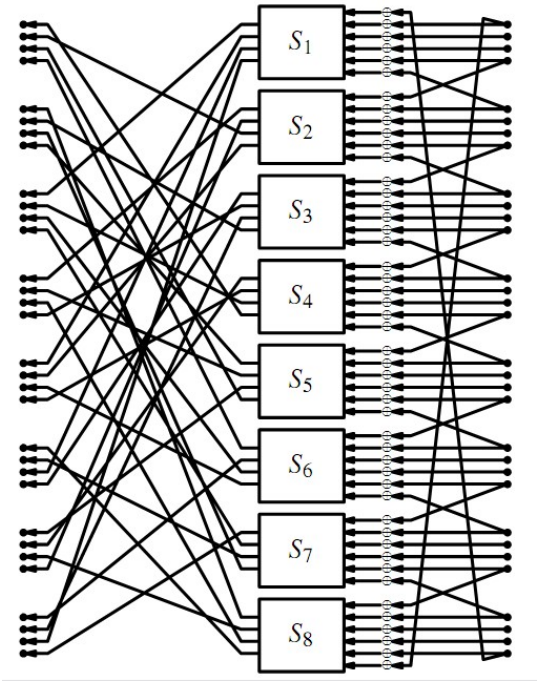
Raktas	Kairė	Dešinė		Raktas	Kairė	Dešinė
K_1	L_0	R_0		K_3	R_3	R_2
K_2	R_0	R_1		K_2	R_2	R_1
K_3	R_1	R_2		K_1	R_1	R_0
	R_2	R_3			R_0	L_0
$C =$	R_3	R_2		$M =$	L_0	R_0

$R_m = R_{m-2} \oplus F(K_m, R_{m-1}), R_{-1} = L_0$

DES



DES raundas



DES dėžės

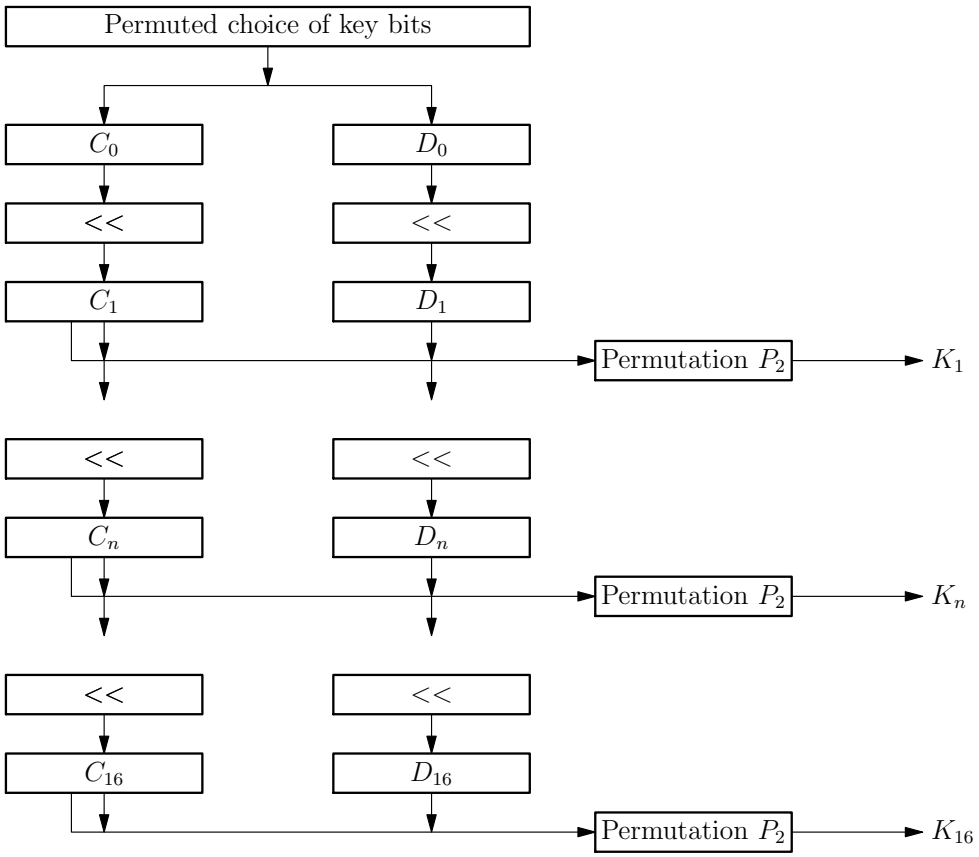
S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

DES raktų sudarymas



Keitiniai ir postūmiai raktų sudarymo schemoje

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Poslinkių ilgiai

1, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1.

Griūties efektas pakeitus teksto bitą

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbc	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33

Round		δ
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
14	c6a62c4e56b0bd75 4bc1a8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP^{-1}	da02ce3a89ecac3b 057cde97d7683f2a	32

Griūties efektas pakeitus rakto bitą

Round		δ
	02468aceeca86420 02468aceeca86420	0
1	3cf03c0fbad22845 3cf03c0f9ad628c5	3
2	bad2284599e9b723 9ad628c59939136b	11
3	99e9b7230bae3b9e 9939136b768067b7	25
4	0bae3b9e42415649 768067b75a8807c5	29
5	4241564918b3fa41 5a8807c5488dbe94	26
6	18b3fa419616fe23 488dbe94aba7fe53	26
7	9616fe2367117cf2 aba7fe53177d21e4	27
8	67117cf2c11bfc09 177d21e4548f1de4	32

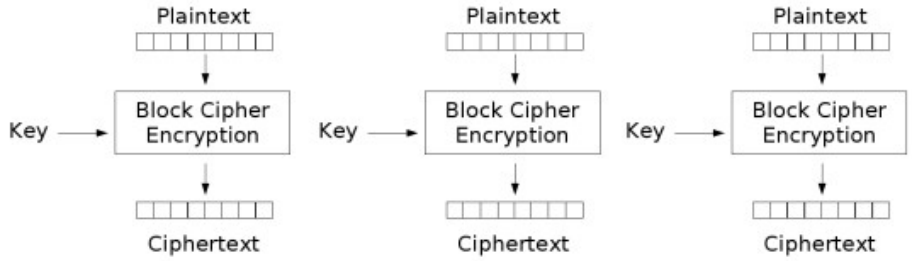
Round		δ
9	c11bfc09887fbc6c 548f1de471f64dfd	34
10	887fbc6c600f7e8b 71f64dfd4279876c	36
11	600f7e8bf596506e 4279876c399fdc0d	32
12	f596506e738538b8 399fdc0d6d208dbb	28
13	738538b8c6a62c4e 6d208dbbb9bdeeaa	33
14	c6a62c4e56b0bd75 b9bdeeaad2c3a56f	30
15	56b0bd7575e8fd8f d2c3a56f2765c1fb	33
16	75e8fd8f25896490 2765c1fb01263dc4	30
IP^{-1}	da02ce3a89ecac3b ee92b50606b62b0b	30

DES kriptoanalizė

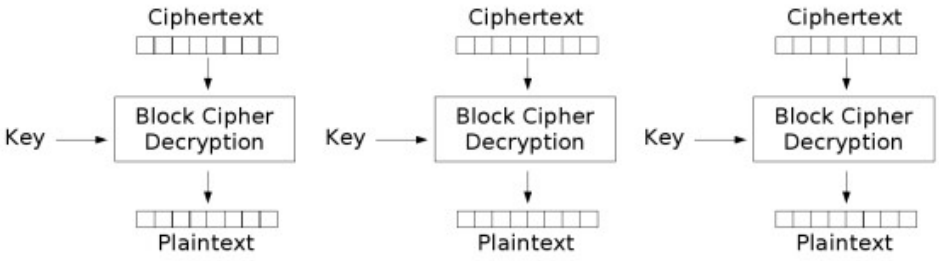
Skirtuminė (diferencialinė) kriptoanalizė 1990 :
turint 2^{47} pasirinktų teksto-šifro porų sėkmingai atakai reikia vidutiniškai 2^{47} operacijų.

Tiesinė kriptoanalizė 1993:
turint 2^{43} pasirinktų teksto-šifro porų sėkmingai atakai reikia vidutiniškai 2^{43} operacijų.

EBC režimas



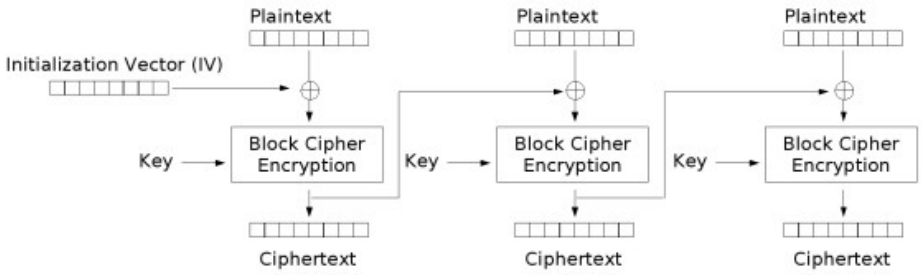
Electronic Codebook (ECB) mode encryption



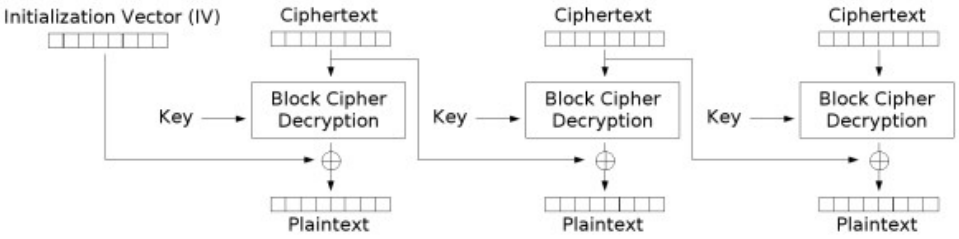
Electronic Codebook (ECB) mode decryption

Blokų pašalinimas, sukeitimas gali būti nepastebėtas...

Šifro blokų grandinės režimas (cipher block chaining mode CBC)

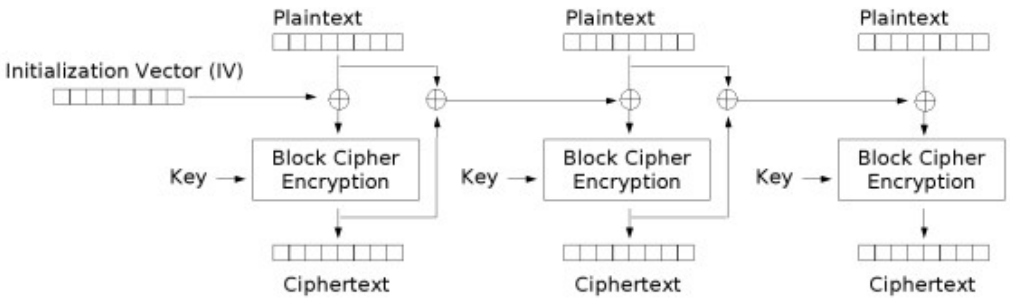


Cipher Block Chaining (CBC) mode encryption

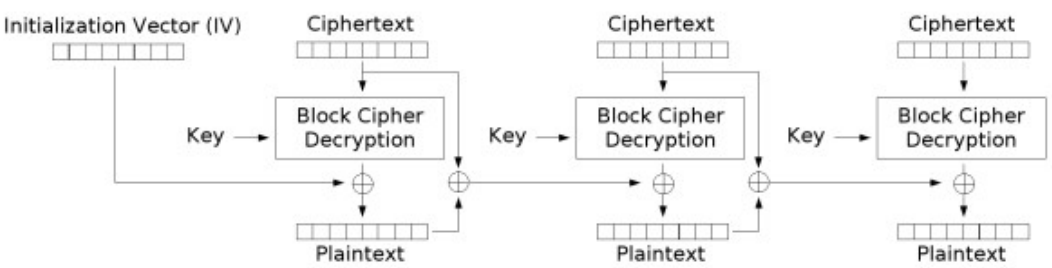


Cipher Block Chaining (CBC) mode decryption

Šifro blokų grandinės režimas (cipher block chaining mode CBC)

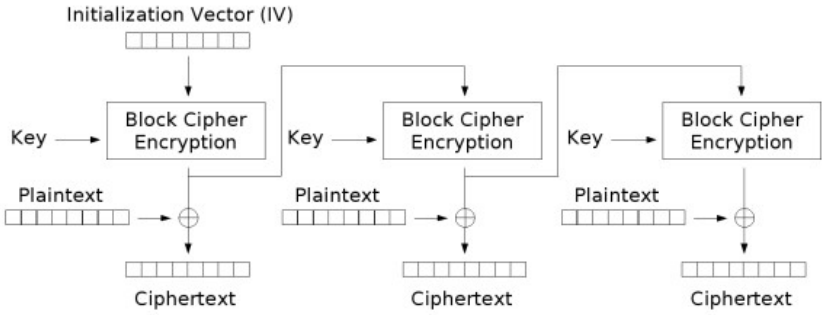


Propagating Cipher Block Chaining (PCBC) mode encryption

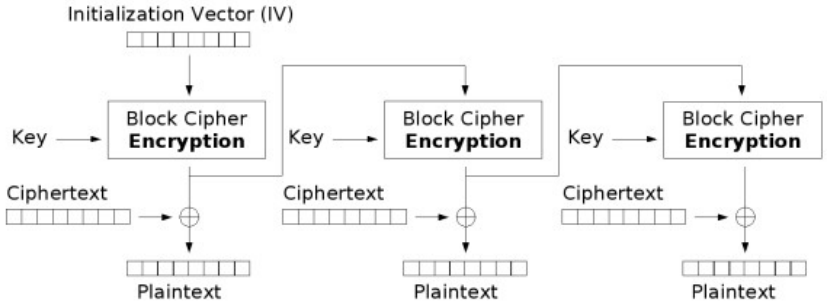


Propagating Cipher Block Chaining (PCBC) mode decryption

Išvesties grįžtamojo ryšio režimas (output feedback mode OFB

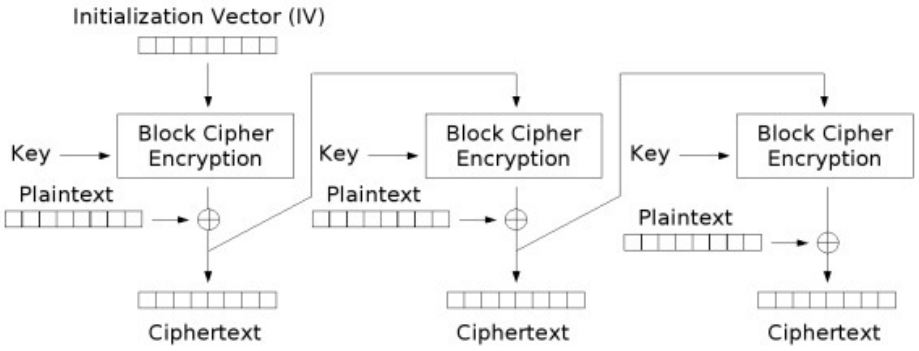


Output Feedback (OFB) mode encryption

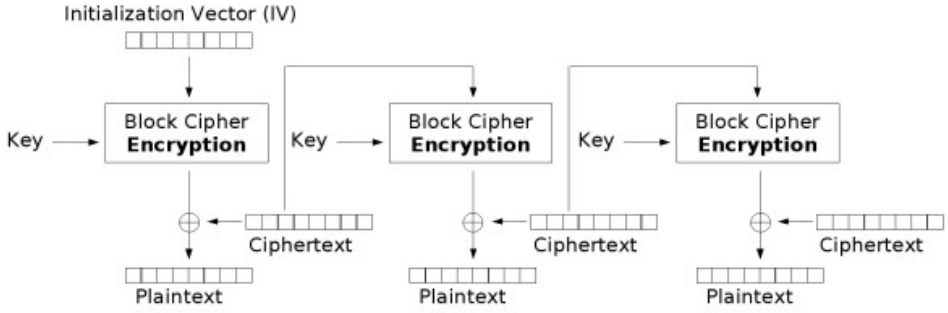


Output Feedback (OFB) mode decryption

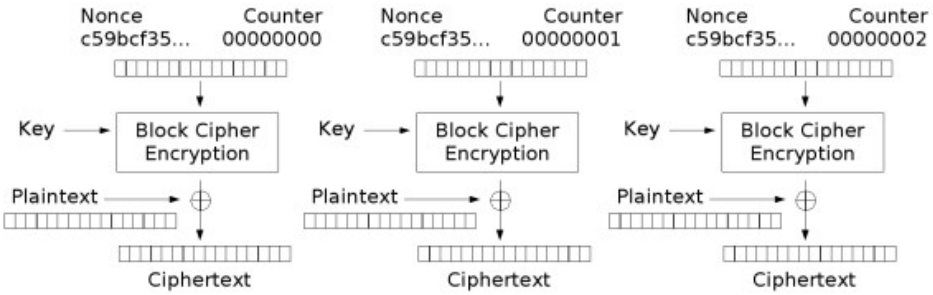
Šifrų grįžtamojo ryšio režimas (cipher feedback mode CFB)



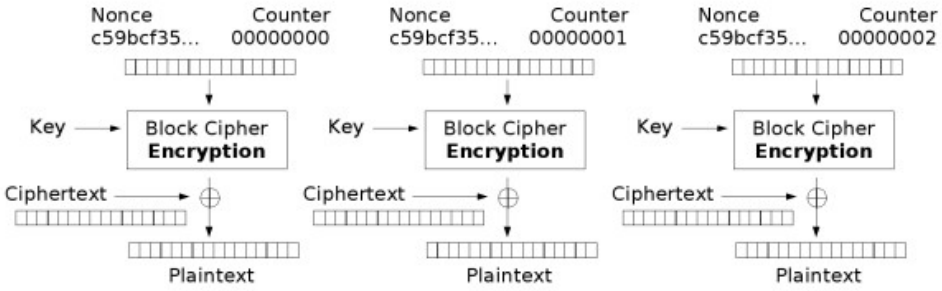
Cipher Feedback (CFB) mode encryption



Skaitliuko režimas (counter mode CTR)



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Trigubas DES

DES: $M \mapsto C = e(M|K), M \in \mathcal{B}^{64}, K \in \mathcal{B}^{56}, \mathcal{B} = \{0, 1\}$.

Trigubas DES:
$M \mapsto C = e(d(e(M|K_1)|K_2)|K_3), M \in \mathcal{B}^{64}, K_i \in \mathcal{B}^{56}$.

DES chronologija

1973-05-15	NBS skelbia pirmąjį pranešimą dėl šifravimo standarto konkurso
1974-08-27	NBS skelbia antrąjį pranešimą dėl šifravimo standarto konkurso
1975-03-17	DES struktūra paskelbta Federaliniame registre komentavimui
1976-08	Pirmoji darbinė DES konferencija
1976-09	Antroji darbinė konferencija, matematinių DES pagrindų aptarimas
1976-11	DES patvirtinta standartu
1977-01-11	DES paskelbta standartu FIPS PUB 46
1983	DES pakartotinai patvirtinta standartu
1988-01-22	DES patvirtinta atnaujintu standartu FIPS 46-1
1992	Bihamas ir Shamiras paskelbė pirmos teorinės atakos, reikalaujančios mažiau išteklių negu perranka aprašą: skirtuminę ataką. Atakai reikia 2^{47} teksto-šifro porų.
1993-12-30	DES pakartotinai patvirtinta atnaujintu standartu FIPS 46-2

DES chronologija

1994	Pirmojo eksperimentinė DES ataka naudojant tiesinę kriptoanalizę.
1999-01	Specialus kompiuteris (Deep Crack) rado DES raktą per 56 valandas.
1999-10-25	DES ketvirtą kartą patvirtinta standrrtu FIPS 46-3, kuris rekomenduoja naudoti trigubą DES.
2001-11-26	Pažangus šifravimo standartas (Advanced Encryption Standard) paskelbtas FIPS 197 dokumente.
2002-05-24	AES standartas įsigalioja.
2004-07-26	Standartas FIPS 46-3 atšaukiamas.

Trigubas DES

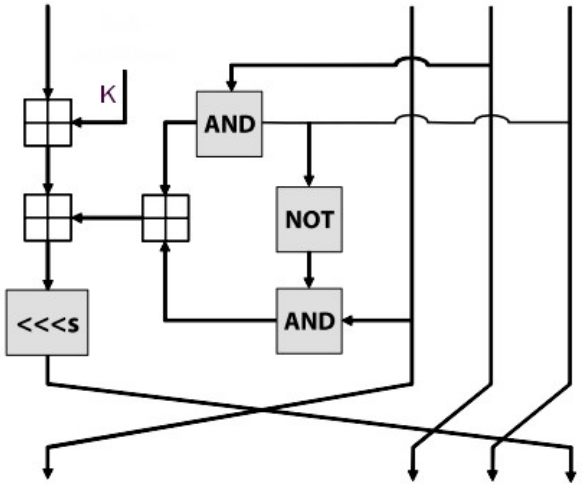
DES: $M \mapsto C = e(M|K), M \in \mathcal{B}^{64}, K \in \mathcal{B}^{56}, \mathcal{B} = \{0, 1\}$.

Dvigubas DES $M \mapsto C = e(e(M|K_1)|K_2)$ nėra saugesnis už DES. „Susitikimo pusiaukelėje“ ataka (meet-in-the-middle attack): turint teksto ir šifro porą $M, C = e(e(M|K_1)|K_2)$ lyginami du sąrašai:

$$[e(M|K) : K \in \mathcal{K}], \quad [d(C|K) : K \in \mathcal{K}].$$

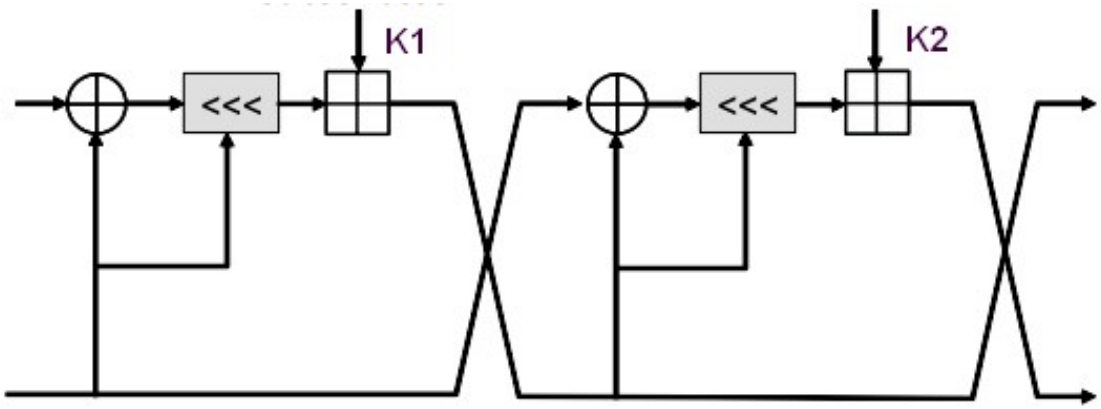
Trigubas DES:
$M \mapsto C = e(d(e(M|K_1)|K_2)|K_3), M \in \mathcal{B}^{64}, K_i \in \mathcal{B}^{56}$.

Feistelio variacijos: RC2 (Rivest Cipher)



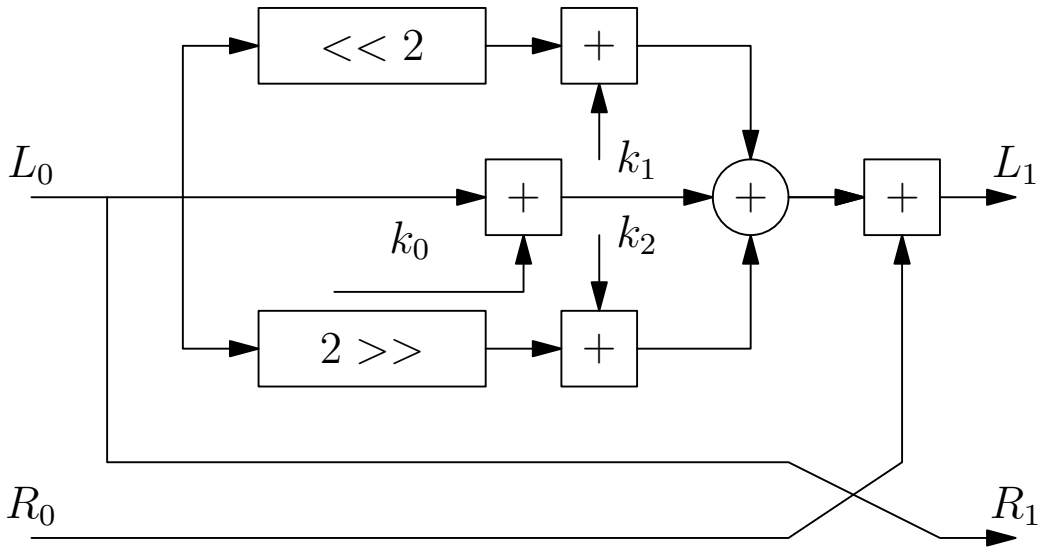
R. Rivest (1987), blokų ilgiai =64, $K_0, K_1, \ldots, K_{63}$ – iteracijų raktai (16 bitų); 18 iteracijų; K_m, m priklauso nuo dešiniojo bloko iteracijoje.

Feistelio variacijos: RC5 (Rivest Cipher)



R. Rivest (1995) blokų ilgiai =32, 64, 128, rakto ilgis =8m, iteracijų skaičius=1, . . . , 255; ciklinių postūmių ilgia priklauso nuo mažiausių reikšminių bitų.

Feistelio variacijos: TEA (Tiny Encryption Algorithm)



D. Wheeler, R. Needham (1994), bloko ilgis =64, rakto ilgis=128, 64 iteracijos.

AES (Advanced Encryption Standard) konkursas

1997 m. JAV Nacionalinis standartų ir technologijos institutas (National Institute of Standards and Technology NIST) paskelbė konkursą naujam kriptografijos standartui sukurti.

Gauta 15 pasiūlymų.
Finalininkai: MARS, RC6, Rijndael, Serpent ir Twofish.

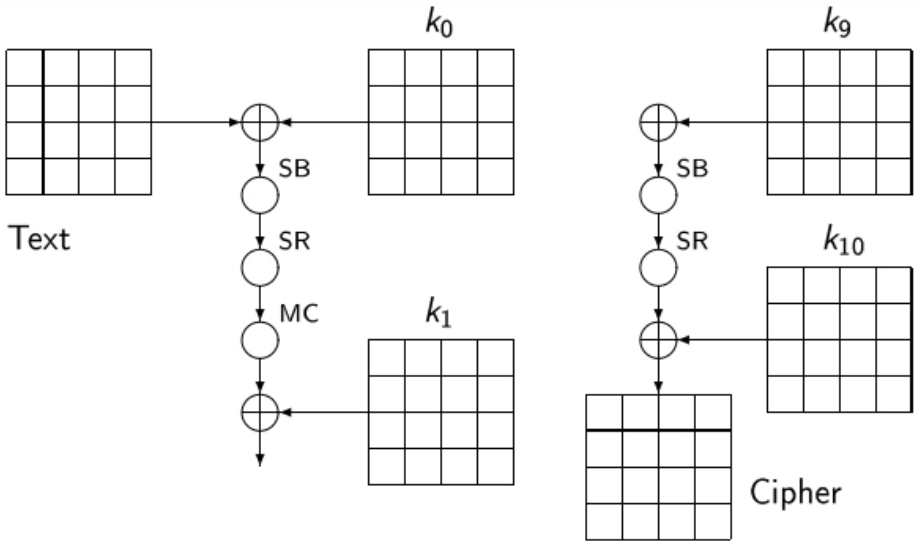
Nugalėjo Rijndael.

SQUARE schema

Pranešimas užrašomas matrica

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	s_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

Bendra AES schema



AES-128 sudaro 10 iteracijų. Kiekvienai iteracijai sukuriamas dalinis raktas.

Transformacijos: baitų keitinys (substitution of bytes SB), eilučių postūmis (shift rows SR), stulpelių sumaišymas (mix columns MC) ir sudėtis su daliniu raktu.

Srautiniai šifrai

Srautiniai šifrai

Pranešimas $M = m_1 m_2 \ldots$ – bitų eilutė.
Sukuriamas rakto srautas $K = x_1 x_2 \ldots$ ir M šifruojama:

$$C = e(M|K) = c_1 c_2 \ldots, \quad c_i = m_i \oplus x_i, \ i = 1, 2, \ldots$$

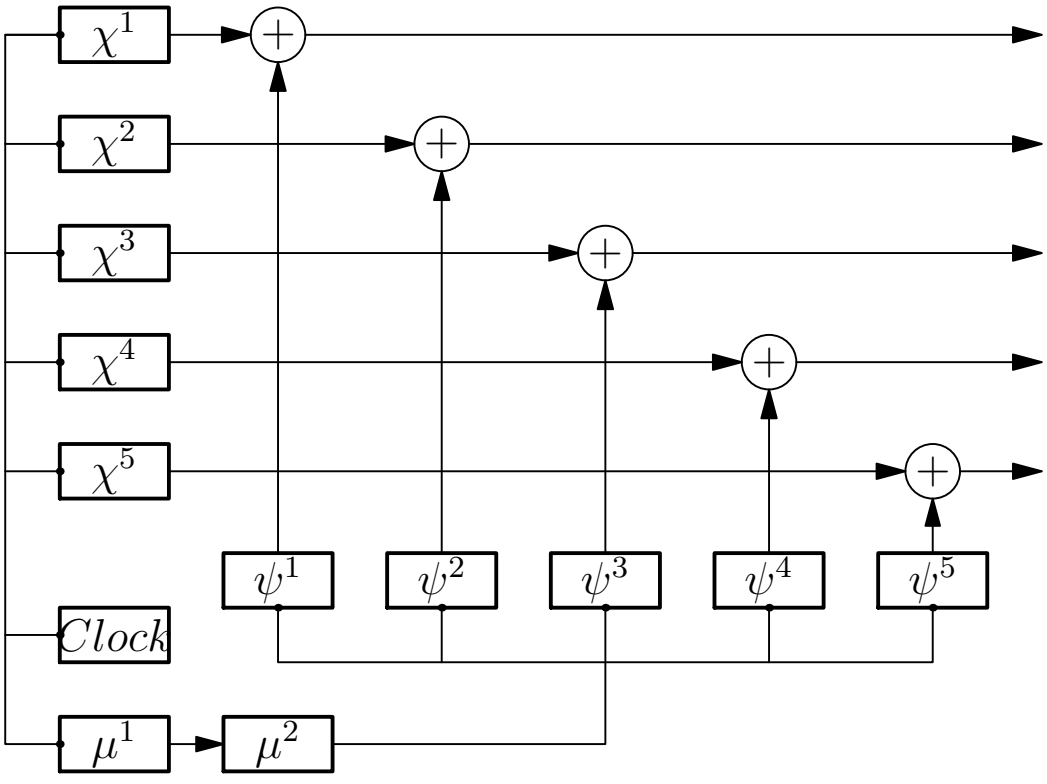
Dešifravimas – XOR operacija su tuo pačiu rakto srautu:

$$M = d(C|K) = m_1 m_2 \ldots, \quad m_i = c_i \oplus x_i, \ i = 1, 2, \ldots$$

Trūkumas: jei tas pats rakto srautas naudotas du kartus šifruojant $M_1 \neq M_2$, tai $M_1 \oplus M_2 = C_1 \oplus C_2$.

Lorenzo srautinis šifras

Vokiečių naudotas Antrajame pasauliniame kare strategiškai svarbiai informacijai šifruoti.



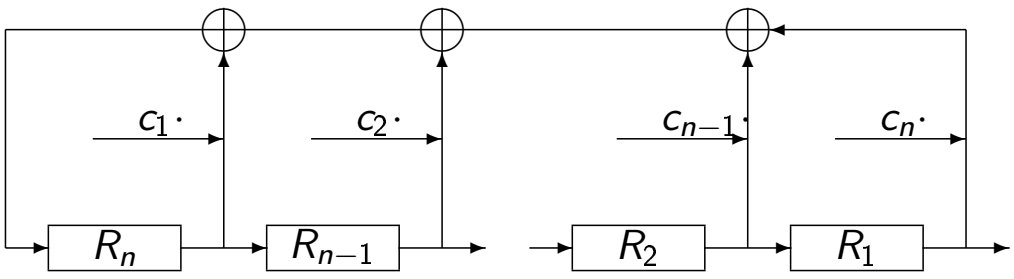
Lorenzo srautinis šifras

Poslinkio funkcija: $rot(a_1, \ldots, a_n) = (a_n, a_1, \ldots, a_{n-1})$. Registrų χ^j, ψ^j, μ^j ilgiai $41, 31, 29, 26, 23, 43, 47, 51, 53, 59, 61, 37$. Registrų padėtys žingsnyje t pažymėtos $\chi^j(t), \psi^j(t), \mu^j(t)$, paskutinis bitas įrašomas į rakto srautą. $m_1(t), m_2(t)$ yra μ^1, μ^2 generuoti bitai. Matematinis veikimo aprašymas:

$$\begin{aligned} \chi^j(t+1) &= rot(\chi^j(t)), \qquad \mu^1(t+1) = rot(\mu^1(t)), \\ \mu^2(t+1) &= rot^{m_1(t)}(\mu^2(t)), \quad \psi^j(t+1) = rot^{m_2(t)}(\psi^j(t)). \end{aligned}$$

Kiekviename žingsnyje generuojami 5 rakto srauto bitai.

Tiesiniai grįžtamojo ryšio registrai (linear feedback shift registers)



Kiekvienas ciklas sukuria vieną rakto srauto bitą. Registrų reikšmių atnaujinimas: R_n siunčiama į R_{n-1}, ... R_2 siunčiama į R_1, nauja R_n reikšmė yra tiesinė senų reikšmių $R_1, \ldots, R_n$ kombinacija.

Tiesiniai grįžtamojo ryšio registrai

Tegu

$$x(t) = \langle x_1(t), \ldots, x_n(t) \rangle$$

registrų reikšmių žingsnyje t vektorius. Tada

$$\begin{aligned} x_i(t+1) &= x_{i+1}(t), \quad 1 \leqslant i \leqslant n-1, \\ x_n(t+1) &\equiv c_1 x_n(t) + \cdots + c_n x_1(t) \pmod 2, \end{aligned}$$

čia $c_i \in \{0, 1\}$, $1 \leqslant i \leqslant n$. Konstanta $c_n \neq 0$; jei $c_n = 0$ paskutinį registrą būtų galima pašalinti.

Periodinės sekos

Apibrėžimas. Seka $\{y_i\}$ $(i = 0, 1, \ldots)$ vadinama periodine, jei egzistuoja natūralusis skaičius p, kad kai $i \geqslant 0$ teisinga lygybė $y_{i+p} = y_i$. Mažiausias skaičius p, kuriam teisinga ši sąlyga vadinamas sekos periodu.

Teorema. n tiesinių registrų seka generuoja periodinį ne didesnio kaip $2^n - 1$ periodo bitų srautą.

Primityvieji daugianariai

Apibrėžimas. n-tojo laipsnio daugianaris $f(x) \in \mathbb{F}_2[x]$ vadinamas primityviuoju, jeigu jis yra neskaidus ir nedalija daugianarių $x^d + 1$, kai $d < 2^n - 1$.

Egzistuoja bet kokio laipsnio primityvieji daugianariai!

Maksimalaus periodo sekos

Apibrėžimas. Daugianaris

$$P_n(x) = 1 + c_1 x + \cdots + c_n x^n, \ c_n \neq 0,$$

vadinamas charakteringuoju tiesinių registrų sistemos daugianariu.

Teorema. Tiesinių registrų sistemos generuoto srauto periodas yra maksimalus (lygus $2^n - 1$) tada ir tik tada, kai sistemos charakteringasis daugianaris yra primityvus.

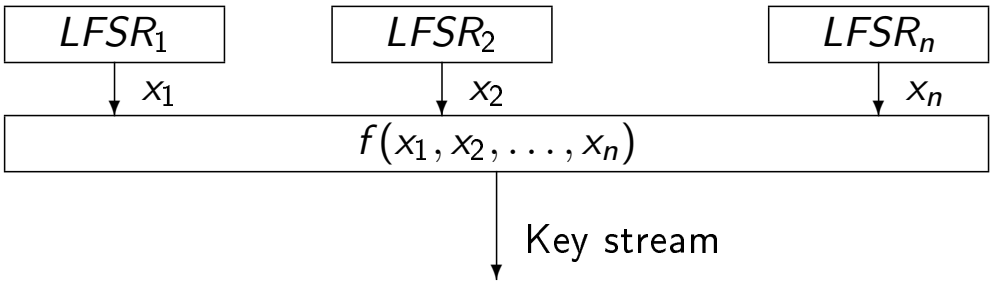
Primityvūs daugianariai

n	Polynomial	$2^n - 1$
2	$x^2 + x + 1$	3
3	$x^3 + x^2 + 1$	7
4	$x^4 + x^3 + 1$	15
5	$x^5 + x^3 + 1$	31
6	$x^6 + x^5 + 1$	63
7	$x^7 + x^6 + 1$	127
8	$x^8 + x^6 + x^5 + x^4 + 1$	255
9	$x^9 + x^5 + 1$	511
10	$x^{10} + x^7 + 1$	1023
11	$x^{11} + x^9 + 1$	2047
18	$x^{18} + x^{11} + 1$	262143

Srautinių šifrų kriptoanalizė

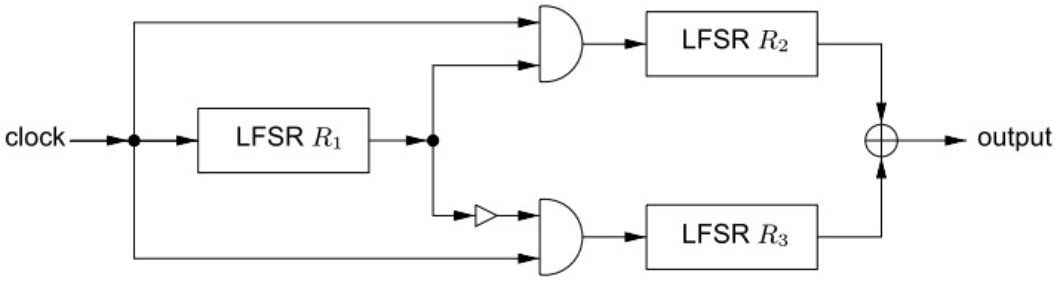
Jeigu srautinio šifro raktų srautas yra generuotas tiesinių registrų sistema, šifrą galima įveikti teksto-šifro poros ataka.

Tiesinių registrų sistemų kombinavimas



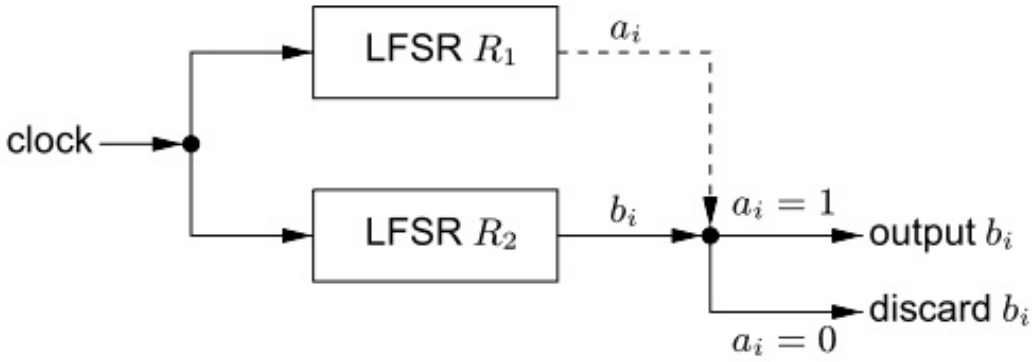
Funkcija f pašalina tiesiškumą.

Tiesinių registrų sistemų kombinavimas



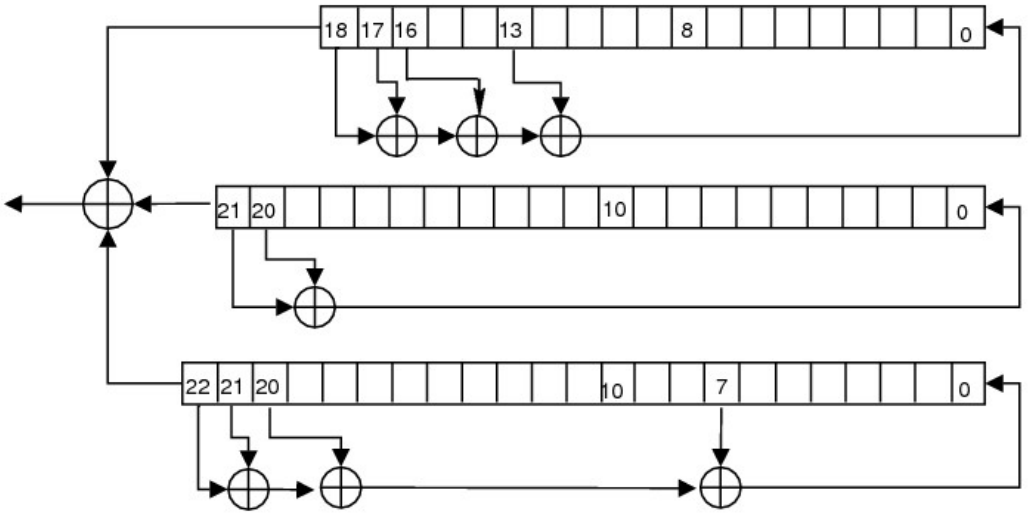
Žingsnių valdymo generatorius

Tiesinių registrų sistemų kombinavimas



Srauto retinimo generatorius

A5/1



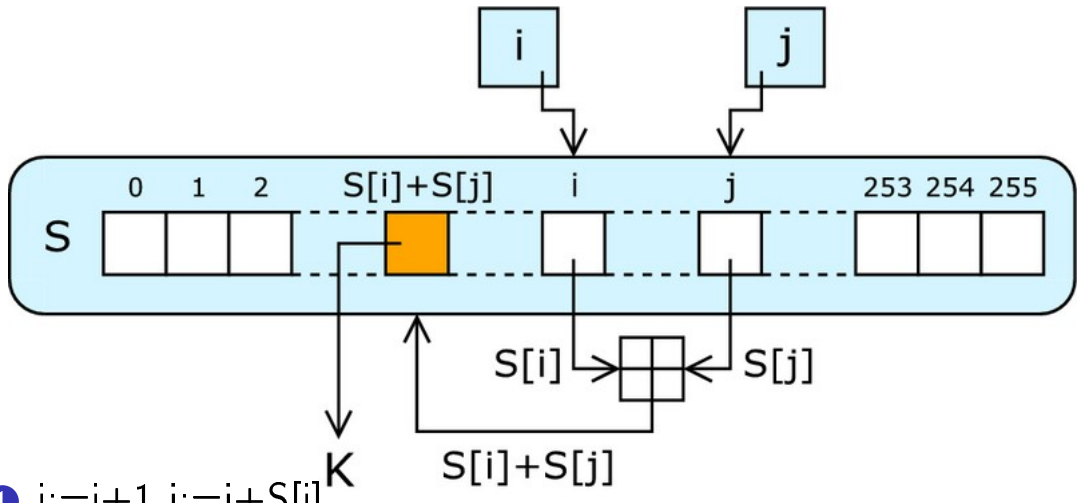
A5/1 naudojamas pokalbiams mobiliaisiais telefonais šifruoti.

RC4

Raktas: l baitų $K[0], \ldots, K[l-1]$ seka.
Inicializacija:

1. j:=0
2. for i= 0 to 255 do
3. S[i]:=i end
4. for i= 0 to 255 do
5. j:=j+S[i+K[i mod l]]
6. S[i]<->S[j] end i:=0 j:=0

RC4 šifravimass



1. i:=i+1 j:=j+S[i]
2. S[i]<->S[j]

$S[S[i] + S[j]] \mapsto$ key stream

Statistiniai testai

Statistiniai testai taikomi vertinant pseudoatsitiktinių bitų generatorius.
Tegu $X_1, X_2, \ldots$ yra nepriklausomi atsitiktiniai dydžiai, su vienodomis tikimybėmis įgyjantys reikšmes $\{0, 1\}$. Jų reikšmių seka – tikras atsitiktinių bitų srautas.

Problema

Turime bitų srautą $x = x_1 x_2 \ldots x_n$.

Reikia priimti vieną iš dviejų hipotezių:

H_0 : x **yra tipinė dydžių** $X_1, \ldots, X_n$, generuota seka;
H_1 : x **nėra tipinė dydžių** $X_1, \ldots, X_n$ generuota seka.

Viešojo rakto kriptografijos matematiniai pagrindai

Euklido algoritmas bendram didžiausiam dalikliui rasti

$$
\begin{aligned}
a &= q_0 b + r_0, && 0 < r_0 < b,\\
b &= q_1 r_0 + r_1, && 0 < r_1 < r_0,\\
r_0 &= q_2 r_1 + r_2, && 0 < r_2 < r_1,\\
&\cdots\cdots\cdots\\
r_{n-2} &= q_n r_{n-1} + r_n, && 0 < r_n < r_{n-1},\\
r_{n-1} &= q_{n+1} r_n,\\
r_n &= (a, b).
\end{aligned}
$$

Bendrojo didžiausio daliklio išraiška

$$
\begin{aligned}
(a, b) &= r_{n-2} + (-q_n) r_{n-1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
(a, b) &= u r_{k-2} + v r_{k-1},\\
(a, b) &= v r_{k-3} + (u - v q_{k-1}) r_{k-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
(a, b) &= xa + yb.
\end{aligned}
$$

Bendrojo didžiausio daliklio išraiška

r_{i-1}, r_i	q_i	u_{i-1}, u_i
a, b		x, y
b, r_0	q_0	
r_0, r_1	q_1	
r_1, r_2	q_2	
$\ldots$	$\ldots$	
r_{k-2}, r_{k-1}	q_{k-1}	$v; u - vq_k.$
r_{k-1}, r_k	q_k	$u; v$
$\ldots$	$\ldots$	
r_{n-2}, r_{n-1}	q_{n-1}	$1; -q_n$
r_{n-1}, r_n	q_n	

Pavyzdys

$57; 10$		$3; -17$
$10; 7$	5	$-2; 3$
$7; 3$	1	$1; -2$
$3; 1$	2	

$$(57, 10) = 3 \cdot 57 + (-17) \cdot 10$$

Eulerio funkcija

Apibrėžimas. Funkcija

$$\varphi(n) = |\{m : 1 \leqslant m < n, (m, n) = 1\}|$$

vadinama Eulerio funkcija.

Funkcijos $\varphi(n)$ savybės

Teorema. Jei $(m, n) = 1$, tai

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Teorema.

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Svarbios teoremos

Teorema. (Fermat) Jei $(a, n) = 1$, tai $a^{\varphi(n)} - 1 = tn$, t. y. $a^{\varphi(n)} - 1$ dalijasi iš n.

Teorema. (Euler) Jei p pirminis, $(a, p) = 1$, tai $a^{p-1} - 1$ dalijasi iš p.

$\mathbb{Z}_n, \mathbb{Z}_n^*$

$$\begin{aligned} \mathbb{Z}_n &= \{0, 1, 2, \ldots, n-1\}, \\ \mathbb{Z}_n^* &= \{a : a \in \mathbb{Z}_n, (a, n) = 1\}, \\ \mathbb{Z}_p^* &= \{1, 2, \ldots, p-1\}, \quad \text{jei } p \text{ pirminis skaičius.} \end{aligned}$$

Sudėtis ir daugyba aibėje $\mathbb{Z}_n$
Jei $a - b$ dalijasi iš n, žymime

$$a \equiv b \pmod{n}$$

Šis sąryšis vadinamas lyginiu.
Lyginių savybės (beveik) tos pačios kaip lygybių savybės!

Svarbios teoremos

Teorema. (Fermat) Jei $(a, n) = 1$, tai $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Teorema. (Euler)Jei p pirminis ir $(a, p) = 1$, tai $a^{p-1} \equiv 1 \pmod{p}$.

Grupės, žiedai, kūnai

$\mathbb{Z}_n$ su sudėties ir daugybos moduliu n veiksmais sudaro žiedą.

Atvirkštinis elementas a^{-1} egzistuoja tada ir tik tada, kai $a \in \mathbb{Z}_n^*$!

Atvirkštinį elementą galima rasti išplėstiniu Euklido algoritmu.

Aibė $\mathbb{Z}_n^*$ su daugybos veiksmu sudaro grupę.

Jei p yra pirminis, tai $\mathbb{Z}_p$ yra kūnas.

Kinų liekanų teorema

Duoti skaičiai $y_1, y_2, \ldots, y_k, n_1, n_2, \ldots, n_k$. Reikia rasti skaičių y, kad

$$y \equiv y_1 \pmod{n_1}, y \equiv y_2 \pmod{n_2}, \ldots, y \equiv y_k \pmod{n_k}.$$

Teorema. Tegu $n_1, n_2, \ldots, n_k$ tarpusavyje pirminiai skaičiai, $y_1, y_2, \ldots, y_k$ bet kokie skaičiai. Tegu $n = n_1 n_2 \cdots n_k, m_i = n/n_i$, o $d_i m_i \equiv 1 \pmod{n_i}$. Tada skaičius

$$y = y_1 d_1 m_1 + y_2 d_2 m_2 + \ldots + y_k d_k m_k$$

tenkina visus lyginius $y \equiv y_i \pmod{n_i}$.

Kėlimo kvadratu algoritmas

$$\begin{aligned} 31 &= 1 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4, \\ 10^{31} &= 10^1 \cdot 10^2 \cdot (10^2)^2 \cdot ((10^2)^2)^2 \cdot (((10^2)^2)^2)^2, \end{aligned}$$

$$\begin{aligned} &10^2 \equiv 7 \pmod{31}, \quad 7^2 \equiv 18 \pmod{31}, \\ &18^2 \equiv 14 \pmod{31}, \quad 14^2 \equiv 10 \pmod{31}, \\ &10^{31} \equiv 10 \cdot 7 \cdot 18 \cdot 14 \cdot 10 \pmod{31} \equiv 25 \pmod{31}. \end{aligned}$$

Ciklinė grupė $\mathbb{Z}_p^*$

Tegu p yra pirminis skaičius. Tada bet kokiam $a, (a,p) = 1$ $a^{p-1} \equiv 1 \pmod{p}$, t. y. $a^{p-1} = 1$ kūne $\mathbb{Z}_p$.

Egzistuoja $g \in \mathbb{Z}_p$, kad

$$\{g^0, g^1, \ldots, g^{p-2}\} = \mathbb{Z}_p^*.$$

Elementas g vadinamas generuojančiu elementu (arba primityviąja vieneto šaknimi moduliu p).

Teorema. Elementas g yra generuojantis elementas mod p tada ir tik tada, kai visiems netrivialiesiems dalikliams $d|p-1$ $g^d \not\equiv 1 \pmod{p}$.

Diskretusis logaritmas

Apibrėžimas. Tegu p pirminis skaičius ir $g \in \mathbb{Z}_p^*$ generuojantis elementas. Tada kiekvienam $x \in \mathbb{Z}_p^*$ egzistuoja vienintelis $y \in \mathbb{Z}_{p-1}$, kad

$$x = g^y \ (t.y.\ x \equiv g^y \pmod{p}).$$

Elementas y vadinamas diskrečiuoju x logaritmu moduliu p ir žymimas $y = \log_g x$.

Kvadratiniai lyginiai

Apibrėžimas. Elementas a is vadinamas kvadratine liekana mod n, jeigu egzistuoja x, kad $x^2 \equiv a \pmod{n}$.

Jei n yra pirminis skaičius, lyginio $x^2 \equiv a \pmod{n}$ sprendinių egzistavimas tiriamas naudojant Legendre symbolį.

Legendre simbolis

Apibrėžimas. Tegu q yra pirminis skaičius, Legendre symbolis apibrėžiamas taip:

$$\left(\frac{a}{q}\right) = \begin{cases} 0, & \text{jei } a \equiv 0 \pmod{q}, \\ 1, & \text{jei } x^2 \equiv a \pmod{q} \text{ turi sprendinį}, \\ -1, & \text{jei } x^2 \equiv a \pmod{q} \text{ neturi sprendinių}. \end{cases}$$

Savybės

Teorema.

$$\left(\frac{a^2}{q}\right) = 1, \quad \left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right),$$
$$\left(\frac{a}{q}\right) \equiv a^{(q-1)/2} \pmod{q}, \quad \left(\frac{a+kq}{q}\right) = \left(\frac{a}{q}\right),$$
$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}, \quad \left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8}.$$

Gauso dėsnis

Teorema. Jei p, q du skirtingi pirminiai skaičiai, tai

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Svarbus atskiras atvejis

Teorema. Tegu p yra pirminis skaičius, $p \equiv 3 \pmod 4$, ir su a $x^2 \equiv a \pmod p$ turi sprendinį. Tada vienas iš sprendinių yra

$$x_0 \equiv a^{\frac{p+1}{4}} \pmod p.$$

Viešojo rakto kriptografija

Kuprinės uždavinys

ID: natūraliųjų skaičių (svorių) rinkinys $W = \{w_1, w_2, \ldots, w_n\}$, natūralusis skaičius w.
Q: Ar yra tokie $x_i \in \{0, 1\}$, kad

$$w = x_1 w_1 + x_2 w_2 + \cdots + x_n w_n?$$

Ar svorio w kuprinę galima sudėti iš duotų svorių?

Sparčiai didėjantys svoriai

Apibrėžimas. Sakysime, kad svoriai $w_1, w_2, \ldots, w_n$ sparčiai didėja, jei visiems $i > 1$ teisinga nelygybė

$$w_1 + w_2 + \cdots + w_{i-1} < w_i.$$

Teorema. Jeigu sistemą $W = \{w_1, w_2, \ldots, w_n\}$ sudaro sparčiai didėjantys svoriai, tai kuprinės uždavinys sprendžiamas polinominio laiko algoritmu.

Kuprinės uždavinio sprendimas

Tegu v yra duotasis svoris. Ieškome išraiškos

$$v = x_1 w_1 + x_2 w_2 + \cdots + x_n w_n, \quad x_i \in \{0, 1\}.$$

Kodas:

- 1. $w := v, j := n$;
- 2. jei $w \geqslant w_j$, tai $x_j = 1$; jei $w < w_j$, tai $x_j = 0$; $w := w - x_j w_j$;
- 3. jei $w = 0$, išraišką suradome; jei $w \neq 0, j = 0$, išraiškos nėra; kitais atvejais kartojame 2 žingsnį.

Kuprinės ir šifrai

Su svorių sistema $W = \{w_1, w_2, \ldots, w_n\}$ galime šifruoti dvejetainę eilutę:

$$x_1 x_2 \ldots x_n \to c = x_1 w_1 + x_2 w_2 + \cdots + x_n w_n.$$

Kaip šią idėją paversti tikra kriptosistema?

1976 m. sprendimą rado Merkle ir Hellman.

Merkle-Hellmano kuprinės kriptosistema

Pranešimų aibė $\mathcal{M} = \{0,1\}^n$, šifrų aibė $\mathcal{C} \subset \mathbb{N}$.

Privatusis raktas: $K_p = \langle W, s\rangle$, čia $W = \langle w_1, w_2, \ldots, w_n\rangle$ – sparčiai didėjančių svorių sistema;
$w_1 + w_2 + \cdots + w_n < p, \quad (s,p) = 1.$

Viešasis raktas: $K_v = \langle v_1, v_2, \ldots, v_n\rangle$, $v_i \equiv w_i s^{-1} \pmod{p}$ (sugadinti sparčiai didėjantys svoriai).

Šifravimas: $C = e(m_1 m_2 \ldots m_n | K_v) = m_1 v_1 + \cdots + m_n v_n.$

Dešifravimas: $C_1 \equiv Cs \pmod{p}$, $C_1 = m_1 w_1 + \cdots + m_n w_n$, $m_1 \ldots m_n = d(C|K_p)$.

Kuprinės kriptosistema

Kuprinės kriptosistema yra matematiškai įveikta!

RSA

Ronald Rivest, Adi Shamir, Leonard Adleman

RSA kriptosistema

Pranešimų ir šifrų aibė: $\mathcal{M} = \mathcal{C} = \mathbb{Z}_n,\ n = pq,\ p, q$ yra pirminiai skaičiai.

Privatus raktas: $K_p = \langle d \rangle,\ (d, \varphi(n)) = 1, \varphi(n) = (p-1)(q-1).$

Viešas raktas: $K_v = \langle n, e \rangle,\ ed \equiv 1 \pmod{\varphi(n)}.$

Šifravimas: $C = e(M|K_v) \equiv M^e \pmod{n}.$

Dešifravimas: $M = d(C|K_p) \equiv C^d \pmod{n}.$

Dešifravimo pagreitinimas naudojant kinų liekanų teoremą: skaičiuoti
$M_1 = d(C|K_p) \equiv C^d \pmod{p}, M_2 = d(C|K_p) \equiv C^d \pmod{q}$ ir taikant kinų liekanų teoremą rasti M.

RSA hipotezė

RSA kriptoanalizės uždavinys ekvivalentus skaičių skaidymo uždaviniui.

Skaičių skaidymo daugikliais uždavinio sudėtingumas

The RSA-155 Challenge

Zürcher Hochschule Winterthur

- **The Effort**
  - 512 bit number (155 decimal digits)
  - factored on August 22, 1999 after 7 months of cracking
  - 300 workstations and Pentium PCs, 1 Cray supercomputer

```
109417386415705274218097073220403576120
037329454492059909138421314763499842889
347847179972578912673324976257528997818
337970765372440271467435315933543338 97
=
102639592829741105772054196573991675900
716567808038066803341933521790711307779
*
106603488380168454820927220360012878679
207958575989291522270608237193062808643
```

RSA saugumas : maži raktai

Teorema. Tegu $K_v = \langle n, e \rangle, K_p = \langle d \rangle$ yra RSA raktai, ir p, q, d tenkina sąlygą

$$q < p < 2q, \quad d < \frac{1}{3} n^{\frac{1}{4}}.$$

Tada privatus raktas gali būti rastas iš viešojo polinominiu algoritmu.

RSA saugumas

Teorema. Tegu $K_v = \langle n, e \rangle$, ir $K_p = \langle d \rangle$ yra žinomi RSA raktai. Naudojantis raktais n gali būti išskaidytas tikimybiniu polinominiu algoritmu.

RSA saugumas: modulio skaidymas

Išskaidysime n naudodami e, d. Išreiškiame:
$ed - 1 = 2^s t, \quad (2, t) = 1$. Pasirenkame $a, (a, n) = 1$, ir skaičiuojame:

$$a_0 \equiv a^t \pmod{n}, \quad a_1 \equiv a_0^2 \pmod{n}, \quad \ldots \quad a_i \equiv a_{i-1}^2 \pmod{n}, \ldots$$

Laukiame a_j lygaus 1. Tegu v yra mažiausias indeksas, kad

$$a_{v-1} \not\equiv 1 \pmod{n}, \quad a_v \equiv 1 \pmod{n}.$$

$$a_v \equiv a^{2^v t} \equiv a_{v-1}^2 \pmod{n}, \quad a_v - 1 \equiv (a_{v-1} - 1)(a_{v-1} + 1) \equiv 0 \pmod{n}.$$

Sandauga $(a_{v-1} - 1)(a_{v-1} + 1)$ dalijasi iš n; jei nei vienas iš daugiklių nesidalija iš n, tai vienas jų dalijasi iš p, kitas iš q. Naudojantis Euklido algoritmu gauname:

$$p = (a_{v-1} - 1, n), \quad q = (a_{v-1} + 1, n).$$

Rabino kriptosistema: raktai

Privatusis raktas. $K_{pr} = \langle p, q \rangle$, p, q – pirminiai skaičiai,
$p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$.

Viešasis rakta. $K_v = \langle n \rangle, n = pq$.

Šifravimas ir dešifravimas

Šifravimas. Pranešimai paverčiami skaičiais $m \in \mathbb{Z}_n$,

$$c = e(m|K_v) \equiv m^2 \pmod{n}.$$

Dešifravimas.

$$\begin{aligned} &m_1 \equiv c^{\frac{p+1}{4}} \pmod{p}, \quad m_2 \equiv c^{\frac{q+1}{4}} \pmod{q}, \\ &uq \equiv 1 \pmod{p}, \quad vp \equiv 1 \pmod{q}, \\ &m \equiv \pm m_1 uq \pm m_2 vp \pmod{n} \end{aligned}$$

Viena iš keturių reikšmių – iššifruotas pranešimas.

Diskrečiojo logaritmo apibrėžimas

Apibrėžimas. Tegu p – pirminis skaičius, g – generuojantis $\mathbb{Z}_p^*$ elementas. Tegu $a \in \mathbb{Z}_p^*$ ir

$$g^x = a, \quad 0 \leq x \leqslant p-2.$$

Tada x vadinamas a diskrečiuoju logaritmu pagrindu g, $x = \log_g a$.

Kūdikio-milžino žingsnių algoritmas

Autorius Daniel Shanks.

Tegu p pirminis skaičius, $m = \lceil \sqrt{p-1} \rceil$, g – generuojantis elementas mod p.
Jei $y = \log_g x$, tai

$$y = mj + i, \quad 0 \leqslant j < m, \ 0 \leq i < m.$$

Kūdikio-milžino žingsnių algoritmas

Pasiruošimas. Apskaičiuojami lentelės nariai

$$L_1 : \quad \langle j, g^{mj} (\mathrm{mod}\ p) \rangle, \quad 0 \leq j < m.$$

Skaičiuojamas logartimas. Tegu x duotas skaičius, skaičiuojame

$$L_2 : \quad \langle i, xg^{-i} (\mathrm{mod}\ p) \rangle, \quad 0 \leq i < m.$$

Lentelėse L_1, L_2 randame eilutes su vienodomis komponentėmis: $\langle j, y \rangle \in L_1, \langle i, y \rangle \in L_2$. Tada:

$$g^{mj} = xg^{-i}, \quad x = g^{mj+i}, \quad \log_g x \equiv mj + i \ (\mathrm{mod}\ p-1).$$

ElGamalio kriptosistema

Raktai. Tegu p pirminis skaičius, g generuojantis elementas mod p, $0 < a \leq p-1$.

$$K_v = \langle p, g, \beta \rangle, \quad \beta \equiv g^a \pmod{p}, \quad K_p = \langle a \rangle.$$

Šifravimas. Pranešimų aibė $\mathcal{M} = \mathbb{Z}_p^*$. Pasirenkame $k \in \mathbb{Z}_p^*$, šifruojame M taip:

$$C_1 \equiv g^k \pmod{p}, C_2 \equiv M\beta^k \pmod{p}$$
$$e(M, K_v) = \langle C_1, C_2 \rangle = C.$$

Dešifravimas. Šifras $C = \langle C_1, C_2 \rangle$ dešifruojamas taip:

$$M = d(C, K_p) \equiv C_2 (C_1^a)^{-1} \pmod{p}.$$

Skaitmeninių parašų schemos

Skaitmeninio parašo schema: pranešimų aibė $\mathcal{M}$, parašų aibė $\mathcal{P}$, raktų $K = \langle K_{pb}, K_{pr} \rangle$ aibė $\mathcal{K}$ ir algoritmų šeimos:

$$\begin{aligned} sig(\cdot|K_{pr}) &: \mathcal{M} \to \mathcal{P}, \\ ver(\cdot|K_{pb}) &: \mathcal{M} \times \mathcal{P} \to \{0,1\}. \end{aligned}$$

Jeigu $y \in \mathcal{P}$ siunčiamas kaip $x \in \mathcal{M}$ parašas, tai jis priimamas, jei $ver(x, y|K_{pb}) = 1$, ir atmetamas, jei $ver(x, y|K_{pb}) = 0$.
Teisingai sudarytas parašas visada priimamas:

$$ver(x, sig(x|K_{pr})|K_{pb}) = 1.$$

Skaitmeninių parašų naudojimas

Skaitmeniniai parašai naudojami:

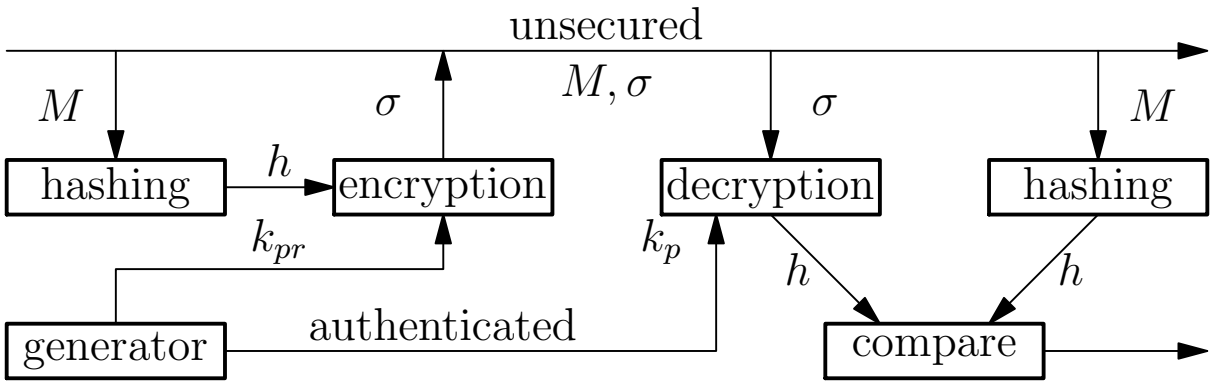
1. duomenų prieigos kopntrolei;
2. vartotojams autentifikuojantis sistemos atžvilgiu;
3. vartotojams autentifikuojant duomenis;
4. pasirašant tikrus dokumentus.

Skaitmeninių parašų schemų atakos

1. Visiškas sužlugdymas: privatus raktas randamas iš viešojo.
2. Universali klastotė: nustatomas algoritmas, sukuriantis bet koio pranešimo galiojantį parašą naudojantis tik viešuoju raktu.
3. Selektyvi klastotė: nenaudodamas viešojo rakto priešininkas gali sukurti tam tikrus pranešimus ir galiojančius jų parašus.
4. Egzistencinė klastotė: naudodamasis viešuoju raktu priešininkas gali sukurti pranešimą ir galiojantį jo parašą.

Kriptosistemos ir skaitmeninių parašų schemos

Beveik visas viešojo rakto kriptosistemas galima paversti skaitmeninių parašų schemomis; pasirašymas – šifravimas, parašo tikrinimas – dešifravimas.



RSA skaitmeninis parašas

Pranešimų aibė $\mathbb{Z}_n$, $n = pq$, p, q – dideli pirminiai skaičiai.

Privatus pasirašymo raktas: $K_{pr} = \langle d \rangle$, $(d, \varphi(n)) = 1$.
Viešasis parašų tikrinimo raktas : $K_{pb} = \langle n, d \rangle$,
$ed \equiv 1 \pmod{\varphi(n)}$.

Pasirašymas: pranešimas $x \in \mathbb{Z}_n$, parašas $y \equiv x^d \pmod{n}$.

Tikrinimas: Parašas priimamas, jei $y^e \equiv x \pmod{n}$.
Pranešimą galime atkurti iš jo parašo!

Aklas RSA parašas

B nori gauti pranešimo m parašą neatskleisdamas paties pranešimo.
Tegu $K_{pb,A} = \langle e_A, n_A \rangle$ ir $K_{pr,A} = \langle d_A \rangle$ yra vartotojo A RSA raktai.
B renkasi bet kokį $r, (r, n) = 1$ ir skaičiuoja

$$x \equiv r^{e_A} m \pmod{n_A}$$

bei siunčia, kad A pasirašytų.
A pasirašo ir siunčia B parašą

$$z = sig(x|K_{pr,A}) \equiv x^{d_A} \pmod{n_A}.$$

B skaičiuoja reikiamo pranešimo parašą:

$$y \equiv r^{-1} z \equiv r^{-1} x^{d_A} \equiv r^{-1} (r^{e_A} m)^{d_A} \equiv m^{d_A} \bmod n_A.$$

Skaičius $y = sig(m|K_{pr,A})$ yra tinkamas pranešimo m parašas.

ElGamalio skaitmeninis parašas

Pranešimų aibė $\mathcal{M} = \mathbb{F}_p^*$, čia p didelis pirminis skaičius; parašų aibė $\mathcal{P} = \mathbb{F}_p^* \times \mathbb{Z}_{p-1}$.
Privatusis raktas: $K_{pr} = \langle a \rangle, a \in \mathbb{Z}_{p-1}$.
Viešasis raktas: $K_{pb} = \langle p, \alpha, \beta \rangle$, čia α genruojantis elementas, $\beta \equiv \alpha^a \pmod{p}$.
Pasirašymas: pasirenkamas atsitiktinis skaičius $k, (k, p-1) = 1$, tada:

$$\gamma \equiv \alpha^k \pmod{p}, \delta \equiv (x - a\gamma) k^{-1} \pmod{(p-1)},$$
$$\langle \gamma, \delta \rangle = sig(x|K_{pr}).$$

Parašo tikrinimas: parašas priimamas tada ir tik tada, kai $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$.

ElGamalio skaitmeninio parašo saugumas

Jeigu du skirtingi pranešimai buvo pasirašyti su ta pačia k reikšme, privatusis raktas gali būti surastas naudojantis parašais:

$$sig(x_1|K_{pr}) = \langle \gamma, \delta_1 \rangle, \quad sig(x_2|K_{pr}) = \langle \gamma, \delta_2 \rangle.$$

Schnorro skaitmeninis parašas

Pranešimų aibė $\mathcal{M} = \mathbb{F}_q$, čia q yra pirminis $p-1$ daliklis; p yra didelis pirminis skaičius.
Privatusis raktas: $K_{pr} = \langle a \rangle, 0 < a < q-1$.
Viešasis raktas: $K_{pb} = \langle p, q, \alpha, \beta \rangle$, $\alpha \in \mathbb{F}_p$ yra q-osios eilės elementas $\beta \equiv \alpha^{-a} \pmod{p}$.

Pasirašymas: pranešimas x; pasirinkus $0 \leq r < q-1$, skaičiuojame: $\gamma \equiv \alpha^r \pmod{p}, \delta \equiv r + ax \pmod{q}, sig(x|K_{pr}) = \langle \gamma, \delta \rangle$.

Parašo tikrinimas: x pranešimo parašas $sig(x|K_{pr}) = \langle \gamma, \delta \rangle$ priimamas tada ir tik tada, kai $\alpha^\delta \beta^x \equiv \gamma \pmod{p}$.

DSA (Digital Signature Algorithm)

Pranešimų aibė $\mathcal{M} = \mathbb{F}_p^*$, parašų aibė – $\mathcal{P} = \mathbb{F}_q \times \mathbb{F}_q$, čia q yra pirminis $p-1$ daliklis; p didelis pirminis skaičius.
Privatusis raktas: $K_{pr} = \langle a \rangle,\ 0 < a < q-1$.
Viešasis raktas: $K_{pb} = \langle p, q, \alpha, \beta \rangle$, $\alpha \in \mathbb{F}_p$ yra q-osios eilės elementas, t.y. $\beta \equiv \alpha^a \pmod{p}$.
Pasirašymas: pasirenkamas atsitiktinis $k \in \mathbb{F}_q^*$ ir skaičiuojama:
$sig(x|K_{pr}) = \langle \gamma, \delta \rangle$,

$$\gamma \equiv \alpha^k (\mathrm{mod}\ p) \pmod{q},\ \delta \equiv (x + a\gamma)k^{-1} \pmod{q}.$$

Turi būti patenkinta sąlyga $(\delta, q) = 1$.
Parašo tikrinimas: parašas priimamas tada ir tik tada, kai

$$\alpha^{e_1}\beta^{e_2} (\mathrm{mod}\ p) \equiv \gamma \pmod{q},$$
$$e_1 \equiv x\delta^{-1} \pmod{q}, e_2 \equiv \gamma\delta^{-1} \pmod{q}.$$

Paslapties dalijimo schemos

Kai visų dalyvavimas būtinas

Paslaptis – dvejetainė eilutė $S \in \{0,1\}^m$ – turi būti padalyta taip, kad tik visi dalyviai kartu galėtų ją atkurti.
Dalintojas pasirenka atsitiktines eilutes $S_1, \cdots, S_{n-1} \in \{0,1\}^m$ ir suranda

$$S_n = S \oplus S_1 \oplus S_2 \oplus \cdots \oplus S_{n-1}.$$

Dalyviui D_i saugiu kanalu perduodama jo paslapties dalis S_i.

Paslapties atkūrimas:

$$S = S_1 \oplus S_2 \oplus \cdots \oplus S_{m-1} \oplus S_n.$$

Shamiro paslapties dalijimo schema

Tegu n yra dalyvių skaičius, $m > n$ didelis skaičius, paslaptis – skaičius $S \in \mathbb{Z}_m$. Dalytojas D pasirenka $S_1, S_2, \ldots, S_{n-1} \in \mathbb{Z}_m$ atsitiktinai ir randa

$$S_n \equiv S - S_1 - S_2 - \cdots - S_{n-1} \pmod{m}.$$

Dalyviui D_i įteikiama jo paslapties dalis S_i. Paslapties atkūrimas:

$$S \equiv S_1 + S_2 + \cdots + S_n \pmod{m}.$$

Paslapties dalijimo schema su slenksčiu

Apibrėžimas. Tegu S yra paslaptis ir $S_1, S_2, \ldots, S_n$ jos dalys, įteiktos dalyviams $D_1, D_2, \ldots, D_n$. Sakysime, kad paslaptis padalyta su slenksčiu t $(1 \leqslant t \leqslant n)$, jei S gali būti atkurta iš ne mažiau kaip t paslapties dalių.

Shamiro paslapties dalijimo schema su slenksčiu

Dalytojas parenka didelį pirminį p, $p > n$, atsitiktinai parenka skaičius $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p$ ir įteikia dalyviui D_i jo skaičių $x_i (i = 1, 2, \ldots, n)$; šie skaičiai nebūtinai laikomi paslaptyje.
Paslaptis yra skaičius $S \in \mathbb{Z}_p$.
Dalytojas parenka skaičiuis $a_1, a_2, \ldots, a_{t-1} \in \mathbb{Z}_p, a_{t-1} \neq 0$ ir sudaro daugianarį

$$a(x) = S + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \in \mathbb{Z}_p[x].$$

Dalyvio D_i, paslapties dalis yra $S_i \equiv a(x_i) \pmod{p}$.

Shamiro paslapties dalijimo schema su slenksčiu

Paslaptis S gali būti atkurta iš bet kokio t paslapties dalių rinkinio $S_{i_1}, S_{i_2}, \ldots, S_{i_t}$:

$$
\begin{aligned}
&S + a_1 x_{i_1} + a_2 x_{i_1}^2 + \cdots + a_{t-1} x_{i_1}^{t-1} = S_{i_1}, \\
&S + a_1 x_{i_2} + a_2 x_{i_2}^2 + \cdots + a_{t-1} x_{i_2}^{t-1} = S_{i_2}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&S + a_1 x_{i_t} + a_2 x_{i_t}^2 + \cdots + a_{t-1} x_{i_t}^{t-1} = S_{i_t}
\end{aligned}
$$

Shamiro paslapties dalijimo schema su slenksčiu

Paslapties dalijimas: Dalytojas D, dalyviai $D_1, D_2, \ldots, D_n$. D pasirenka pirminį p, skirtingus $x_1, x_2, \ldots, x_n \in \mathbb{Z}_p$ ir įteikia D_i skaičius x_i. Skaičius p yra viešas, paslaptis yra skaičius $S \in \mathbb{Z}_p$. D parenka $a_1, a_2, \cdots, a_{t-1}$ atsitiktinai, $a_{t-1} \neq 0$, sudaro daugianrį

$$a(x) = S + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1},$$

įteikia dalyviui D_i jo paslapties dalį $S_i \equiv a(x_i) \pmod{p}$.
Paslapties atkūrimas: t dalyvių $D_{i_1}, D_{i_2}, \ldots, D_{i_t}$ atkuria paslaptį iš savo dalių:

$$S \equiv \sum_{i=1}^{t} S_{i_j} \prod_{\substack{1 \leqslant k \leqslant t \\ k \neq j}} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \pmod{p}.$$