Paskaita 12

Kodavimo ← Šifravimo teorijos elementai

Ap. ~~Kodavimo~~ Šifravimo schemą (kriptosistemą) nedidelio rinkinį (P, C, K, E, D)

1. P – galimų nešiotojų pranešimų (tekstų) aibė (plaintext space)
2. C – šifruotų pranešimų aibė (ciphertext space)
3. K – raktų aibė. (Key space).
   Simetriniuose kriptografiniuose algoritmuose garantuoja rakto slaptumas
4. E – šifravimo algoritmų (funkcijų) aibė / šeima, priklausanti nuo k:

$$E = \{ E_k : k \in K \}$$

$$E_k : P \to C$$

encryption functions

5. $\mathcal{D} = \{ D_k : k \in K \}$

$D_k : C \to P$

dešifravimo funkcijos (decryption functions).

6. $\forall e \in K \; \exists d \in K$ tokį, kad

$D_d(E_e(p)) = p, \; \forall p \in P.$

Pvz. Cezario šifras (Caesar cipher).
(arba rot cipher).

A	B	C	...	Z
0	1	2	...	25

$\Sigma = \{A, B, \ldots, Z\}$ abecelė

$\forall e \in \mathbb{Z}_{26}$ (lickams modulio 26 grupė!)

$E_e : \Sigma \to \Sigma \quad x \to (x+e) \bmod 26.$

Analogiškai

$D_d : \Sigma \to \Sigma \quad x \to (x-d) \bmod 26.$

$\forall e \Rightarrow d = e.$ $\boxed{D_d = E_{-e}}$

Pav. c = 5

CRYPTOGRAPHY
HWDUYTLWFUMD

Raktų aibė K turi tik 26 elementus, todėl lengva perrinkti visus variantus (nulaužti kodą).

Pav. 2. Vigenerė šifras

Papildomas raktas - žodis, kurio naudojamas parenkant e raktą

KAUNAS
e 10 0 20 13 0 18

KIRVIS
e 10 8 17 21 8 18

CRYPTOGRAPHY
10 0 20 13 0 18 10 0 20 13 0 18
R T R H

C R Y P T O G R A P H Y
10 8 17 21 8 18 10 8 17 21 8 18
M Z P K B G Q Z R K P Q

Kaip dešifruoti vigenere šifrą?

Ap. Jeigu e dešifravimo raktas $d = e$ arba galime lengvai apskaičiuoti $d = g(e)$, tai tokia kriptosistema vadinama simetrine.

Tada simetrinės sistemos slaptumo problema tampa saugaus rakto pasikeitimas tarp dviejų dalyvių (Alice ir Bob).

Ap. Asimetrinėje sistemoje žinodami e (tai viešoji informacija), negalime apskaičiuoti d.

Visi gali užšifruoti laiškus Bobui bet tik Bobas gali juos perskaityti.

Tai viešojo rakto kriptosistema.

Vienas iš dėstytojų išsakė ir buvo sukurti tokias sistemas / algoritmus. Buvo net premijuojamas, ar tokia sistema gali egzistuoti.

Kalbų teorija

Def. Baigtinę netuščią aibę Σ vadiname **alfabetu**. Alfabeto ilgiu yra laikomas Σ elementų (|Σ|) skaičius (elementus vadiname simboliais arba raidėmis).

Pav. 1 $\Sigma = \{A, B, \dots, Z\}$. $|\Sigma| = 26$.

Ilgis 26.

Pav. 2 $\Sigma = \{0, 1\}$. Ilgis 2. $|\Sigma| = 2$

Pav. 3 ASCII simbolių lentelė.

Simboliai sunumeruoti $\{0, 1, \dots, 127\}$.

Ilgis 128. (7 bitai). (8 bitai - išplėsta lentelė)

Numeracija: $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$.

Iš simbolių galime sudaryti baigtinio ilgio seką. Pavyzdžiui

(2, 3, 1, 2, 3) (arba 23123)

jei žinome, kad simbolius yra nenaturalieji

Taip pat nagrinėjame ir tuščią seką, kurią žymėsime ~~XXX~~ ε (arba ( )).

Def. Tegul Σ yra alfabetas

1. Žodžiu (a word) arba *struna* iš Σ vadiname šio alfabeto ~~bet~~ elementų baigtinę seką (įskaitant ir tuščią seką, kurią žymėsime ε).
2. Žodžio $\vec{w}$ ilgiu vadiname jo komponenčių skaičių (žymėsime $|\vec{w}|$).

$|\varepsilon| = 0$.

3. Visų žodžių, kuriuos galime sudaryti iš Σ (įskaitant ir ε) aibę yra žymima Σ^*.

4. Jei $\vec{v}, \vec{w} \in \Sigma^*$, tai $\vec{v}\vec{w} = \vec{v} \circ \vec{w}$ yra naujas žodis, kurį gaunamas sujungę $\vec{v}$ ir $\vec{w}$. (įvedame operaciją $\circ$ - ar ji asociatyvi? komutatyvi?)

COCA
COLA
$\Rightarrow$ COCACOLA

$$\vec{v} \circ \varepsilon = \varepsilon \circ \vec{v} = \vec{v}$$

5. Jeigu $n \in \mathbb{N}$, tai Σ^n yra aibė žodžių, kurių ilgis yra lygus n. ($\vec{w} \in \Sigma^n \Rightarrow |\vec{w}| = n$)

Uždav. $(\Sigma^*, \circ)$ yra monoidas.

Neutralus jo elementas $\varepsilon \in \Sigma^*$.

(Monoidas - pusgrupė, kuri turi neutralų elementą!)

Def. Tegul X yra aibė. Keitiniu (perstata) (permutation) vadiname bijekciją (abipus vienareikšmį) atvaizdavimą $f: X \to X$. Visų aibės X keitinių aibę žymėsime $S(X)$.

Keitinys - perstata

Pav. $X = \{0, 1, 2, 3, 4\}$.

Keitinys visada gali būti atvaizduotas taip: (čia pateikiame konkretų keitinį $\in S(X)$)

$$X_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 & 0 \end{pmatrix}$$

T. Lengva patikrinti, kad $S(X)$ kartu su operacija $\circ$ yra grupė (turi simetrinių elementų)

$$X_1' = \begin{pmatrix} 1 & 3 & 2 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 2 & 1 & 3 \end{pmatrix}$$

Bendruoju atveju ši grupė nėra komutatyvi (pateikti pvz.)

$X_1 = (1, 3, 2, 4, 0)$. Raskite simetrinį X_1'.

Def. $n \in \mathbb{N}$, tai S_n yra visų aibės $\{1, 2, \dots, n\}$ keitinių grupė.

Pvz. S_2 turi du elementus

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

T. $|S_n| = n!$

Perstatos (bijekcinicai keitiniai)

Apibrėžiame perstatą (ilgio d).

$\pi : \{0, 1, \dots, d-1\} \to \{0, 1, \dots, d-1\}$

Turime tekstą, kurį norime užšifruoti (pranešimą)

$$P = P_0 P_1 \dots P_{d-1} P_d P_{d+1} \dots P_{2d-1} \dots$$

Užšifruotas pranešimas

$$C = P_{\pi(0)} P_{\pi(1)} \dots P_{\pi(d-1)} P_{d+\pi(0)} P_{d+\pi(1)} \dots P_{d+\pi(d-1)} \dots$$

Nagrinėkime pavyzdį

MTM STUDENTAI GERAI PASIRUOŠĖ EGZA

Imkime keitinį

$d = 6$, $\pi = (1, 4, 0, 5, 2, 3)$

Turime raktą $k = (d, \pi)$.

Patogu transformaciją atvaizduoti matricine forma:

a) Perrašome kaip 6 stulpelių matricą

0	1	2	3	4	5
M	T	M	S	T	U
D	E	N	T	A	I
G	E	R	A	I	P
A	S	I	R	U	O
Š	È	E	G	Ž	A

$\longrightarrow$

1	4	0	5	2	3
T	T	M	U	M	S
E	A	D	I	N	T
E	I	G	P	R	A
S	U	A	O	I	R
È	Ž	Š	A	E	G

Skaitome tekstą eilutemis:

C = TTMUMSEADINTEIGPRASUAOIRÈŽŠ AEG.

---

b) Dešifravimo žingsnis

Randame simetrinę perstatą

$$\begin{pmatrix} 0&1&2&3&4&5 \\ 1&4&0&5&2&3 \end{pmatrix}' = \begin{pmatrix} 1&4&0&5&2&3 \\ 0&1&2&3&4&5 \end{pmatrix}$$

$$= \begin{pmatrix} 0&1&2&3&4&5 \\ 2&0&4&5&1&3 \end{pmatrix}$$

0	1	2	3	4	5
T	T	M	U	M	S
E	A	D	I	N	T
E	I	G	P	R	A
S	U	A	O	I	R
È	Ž	Š	A	E	G

→

2	0	4	5	1	3
M	T	M	S	T	U
D	E	N	T	A	I
G	E	R	A	I	P
A	S	I	R	U	O
Š	È	E	G	Ž	A

TRANSPOSITION šifras

Po užrašymo (pertvarkymo) į matricą formuojamas perstata nurodo informacijos skaitymo stulpelių eiliškumą.

$d = 5$, $\bar{\pi} = (4, 3, 2, 1, 0)$ (KRYPTOS atvejis)

0	1	2	3	4
M	T	M	S	T
U	D	E	N	T
A	I	G	E	R
A	I	P	A	S
I	R	U	O	S
È	E	G	Ž	A
M	I			

(1-y nebaigtinai eilutei užpild. dažnai ieškimo matrica)

C = TTRSŠASNEAOZME GPUGTDIIREIMUA AIÈM

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix}$$

Dešifravimas, kai nežinome raktо.

1. Cezario (ROT) šifras.

$$E_k(p) = p + k \pmod n$$

$n = 26$ – abecelės ilgis

Kadangi ta pati raidė p_j visada atvaizduojama į tą pačią šifruoto teksto raidę c_j, tai šifruoto teksto dažnių lentelė sutampa su pradinės abecelės dažnių lentele.

2. Vigenere šifras

Jeigu nustatomas rakto ilgis r, tai visas tekstas dalijamas į r dalių

$$(p_0, p_r, p_{2r}, \dots)$$
$$(p_1, p_{1+r}, p_{1+2r}, \dots)$$
$$(p_2, p_{2+r}, p_{2+2r}, \dots)$$

ir kiekvienas blokas dešifruojamas kaip ROT šifrą (remiantis dažnių lentele)

1 2 3 4 5 6 7 8 9 10.
D I D M I E S T I S

1 4 2 7 5 3 8 10 6 9.

Kaip generuojamos šis raktas?

Raktu generavimui dažnai naudojami prasmingi žodžiai, o tada randės užrašomos abecėlės tvarka

D D E I I I ...
1 2 3 4 5 6 ...

Kriptoanalizė

Kirckhoffo principas: priešininko žinios apie kriptosistemą viską, išskyrus raktą.

Taigi tikslas: rasti dešifravimo raktą (taip pat ir perskaityti slaptus pranešimus).

- ciphertext-only attack.
  (pavienis šifruotų atakų), kai žinome šifruotą tekstą arba.
- known-plaintext attack
  žinome: pradinių tekstų P_j ir šifruotų tekstų C_j, $j = 1, 2, \ldots, M$.

- pasirinkty teksto - šifro poros ataka.

  Kriptoanalitikas pats pasirenka pradinius tekstus ir turi galimybę gauti šifruotus tekstus

- ~~akademinis interesas~~

  Pasirinkty šifro ataka (chosen-ciphertext attack).

  Šifruotus tekstus pasirenka kriptoanalitikas ir jis gauna atitinkamus pradinius tekstus.

  (turi dešifravimo įrenginį, pvz. ENIGMA)