Automataelméleti alapú adatfolyam titkosító

Prof. Dr. Dömösi Pál Béla és Dr. Habil. Horváth Géza

T.E.L.L. Software Hungaria Kft.

véges automata

Definíció

Az $A = (Q, T, \delta)$ hármast kimenőjel nélküli, determinisztikus véges automatának nevezzük, ahol:

- *Q - belső állapotok (véges nemüres halmaz),*
- *T - bemenő jelek (véges nemüres ábécé),*
- *δ - átmenetfüggvény: $Q \times T \rightarrow Q$.*

példa

Példa: Determinisztikus véges automata

$$A = (\{a, b, c\}, \{1, 2, 3\}, \delta)$$

δ	a	b	c
1	c	b	a
2	a	c	b
3	b	a	c

titkosítás véges automatával

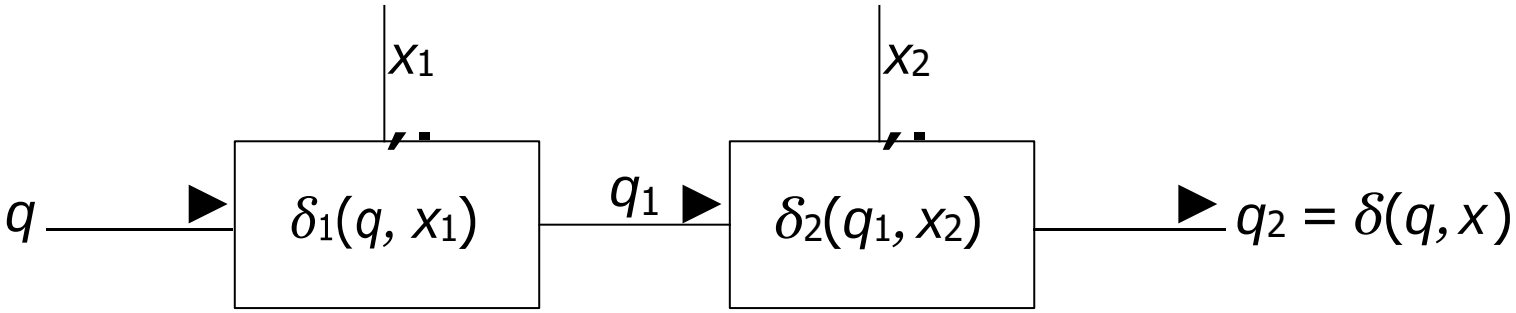
$$A = (\{a, b, c\}, \{1, 2, 3\}, \delta)$$

δ	a	b	c
1	c	b	a
2	a	c	b
3	b	a	c

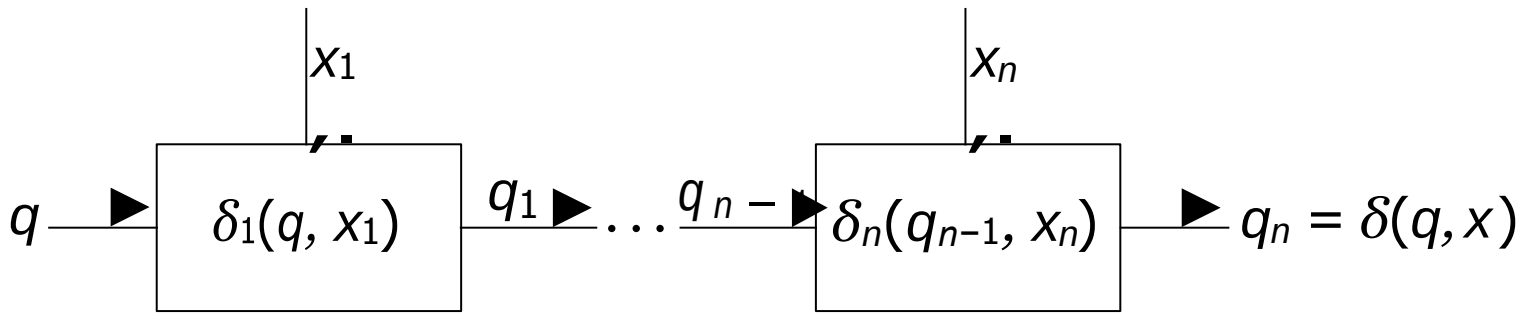
- az állapothalmaz megegyezik a nyílt és a titkos szöveg ábécével $\{a, b, c\}$
- a bemenő jelek álvéletlen számok $\{1, 2, 3\}$
- minden sor az állapothalmaz egy permutációja

nyílt szöveg:	a	b	b	a	b	a	b	a
álvéletlenszámok:	1	2	1	2	3	1	3	3
titkosított szöveg:	c	c	b	a	a	c	a	b

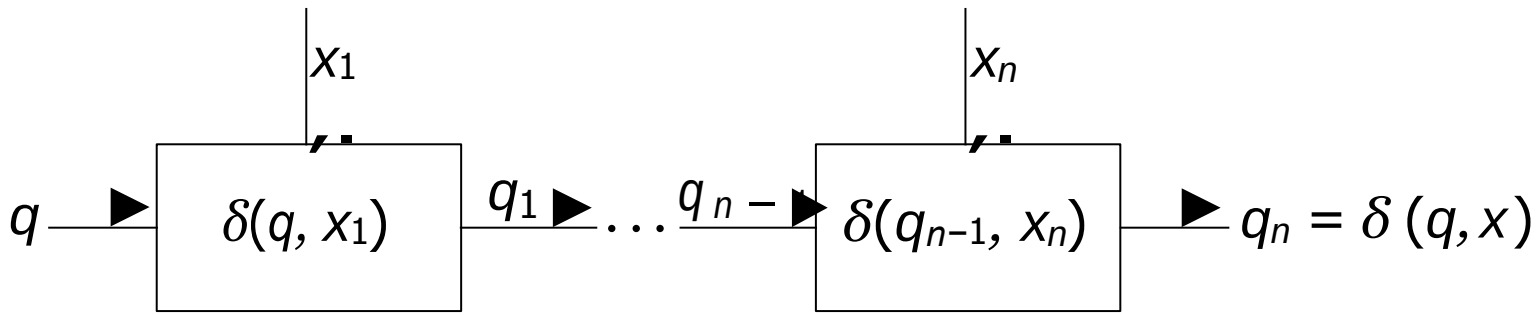
automaták temporális szorzata



általánosított temporális szorzat



az általunk használt temporális szorzat



példa

Példa: $A = (Q, X, \delta)$, $A^{-1} = (Q, X, \delta^{-1})$, $Q = X = \{0, 1, 2, 3\}$

δ	0	1	2	3
0	1	2	3	0
1	2	0	1	3
2	3	1	0	2
3	0	3	2	1

δ^{-1}	0	1	2	3
0	3	0	1	2
1	1	2	0	3
2	2	1	3	0
3	0	3	2	1

- az állapothalmaz megegyezik a nyílt és a titkos szöveg ábécével $\{0, 1, 2, 3\}$
- a bemenő jelek álvéletlenszámok $\{0, 1, 2, 3\}$
- minden sor az állapothalmaz egy permutációja (latin négyzet használata ajánlott)

nyílt szöveg:	0	1	2	3
álvéletlenszámok:	11	21	30	31
titkos szöveg:	1	0	3	0

előnyök

- Az eljárás nem használ processzort igénylő műveletet, mindössze a memóriából olvas és a memóriába ír.
- Nem támadható ismert nyílt/titkos szövegpár alapú támadással. (XOR)
- A latin négyzetek nagy száma miatt a fél bájtokon történő (mindössze 16X16 méretű latin négyzetet igénylő) titkosítás is biztonságos, aminek a kulcsmérete csak 128 bájt.
- A felépítése egyszerű, ezért
  - könnyű megérteni,
  - könnyű leprogramozni,
  - könnyű célhardvert készíteni hozzá.
- P. Dömösi, G. Horváth: A Novel Stream Cipher Based on Deterministic Finite Automata, *Proceedings of the Ninth Workshop on Non-Classical Models of Automata and Applications (NCMA 2017) Short Papers*, (2017), 11-16.

helyettesítéses kiptorendszer

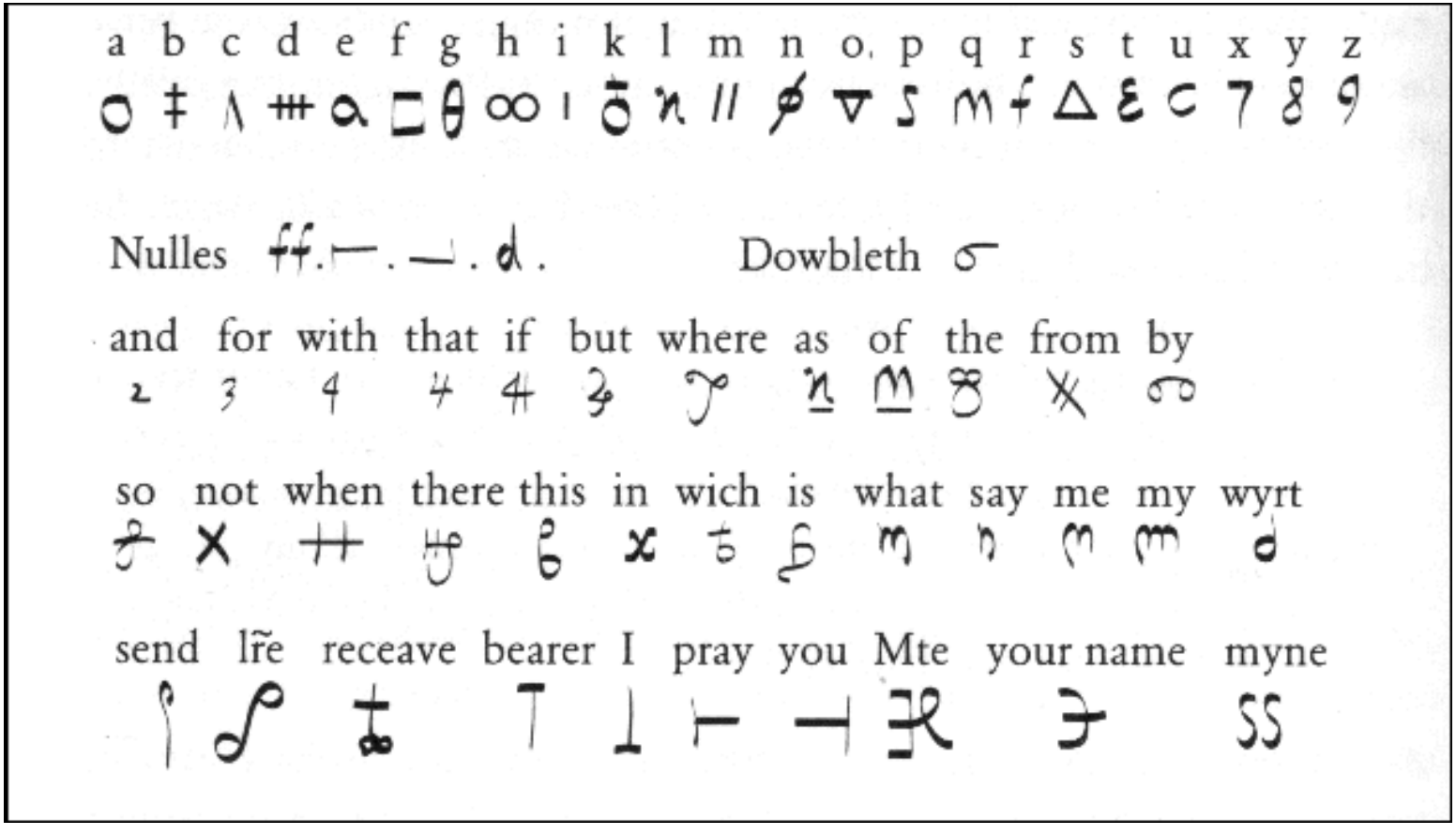
kulcs: a permutáció

titkosítás/visszafejtés:

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

támadás: gyakoriságelemzés

Stuart Mária kód



titkosítás

1. Legyen $p_1 \dots p_k$ a nyílt szöveg, ahol $p_1, \dots, p_k \in Q$.
2. Legyenek továbbá $r_1, \dots, r_k \in X^+$ az álvéletlenszám generátor által generált számok. (Ezen álvéletlenszámok mérete egységesen $|r_1|, \dots, |r_k| = n$ valamely n számra.)
3. A titkos szöveg azon $c_1 \cdots c_k \in Q^+$ szó lesz, melyre

$$c_1 = \overrightarrow{\delta}(p_1, r_1), \dots, c_k = \overrightarrow{\delta}(p_k, r_k).$$

visszafejtés

1. Legyen $c_1 \dots c_k$ a titkos szöveg, ahol $c_1, \dots, c_k \in Q$.
2. Legyenek $r_1, \dots, r_k \in X^+$ az álvéletlenszám generátor által generált számok.
3. A visszafejtett szöveg azon $p_1 \cdots p_k \in Q^+$ szó lesz, melyre

$$\overrightarrow{p_1 = \delta^{-1}(c_1, (r_1)^R)}, \dots \overrightarrow{p_k = \delta^{-1}(c_k, (r_k)^R)},$$

ahol $(r_i)^R$ a r_i szó inverze.