College Cryptografie

Cursusjaar 2003

Monome-dinome systeem

29 januari 2003

Constante lengte crypto-elementen → eenvoudig op te delen

Tegenmaatregelen:

- introductie van *nullen met andere lengte*
- *variable lengte* van de crypto-elementen

Voorbeeld 2-cijferige codering met 1-cijferige 0 als null

1. .. 18 15 11 34 37 11 29 32 19 23 23 17 ..
2. .. 18105 11343 71129 32190 23231 7 ..
3. .. 18151 01343 71129 32192 32031 7 ..
4. .. 18151 13437 10129 32192 30231 7 ..

Variatie: reeksen beginnend en eindigend met null-merk
voorbeeld .. 18105 72105 11343 71129 32190 02323 17 ..

Zwakke punt: overeenkomstige teksten verraden de nullen

Crypto-elementen 1 of 2 cijfers/letters

voorbeelden

T H I S I S S E C R E T .

3 05 02 9 02 9 9 5 01 4 5 3 16

30502 90299 50145 316

T H I S I S S E C R E T .

W MR MS CU MS CU CU V AX Y V W EW

WMRMS CUMSC UCUVA XYVWE W

straddling checkerboard

	0	1	8	3	4	5	2	9	7	6
				T	R	E	A	S	O	N
0	B	C	D	F	G	H	I	J	K	L
1	M	P	Q	U	V	W	X	Y	Z	.
8	0	1	2	3	4	5	6	7	8	9

- kolomcoördinaten gepermuteerd, sleutelwoord in toprij
- extra substituenten voor leestekens, cijfers
- ETA0.. in toprij comprimeert cryptogram

Sleutelconstructie

	0	1	8	3	4	5	2	9	7	6
	E	T	N	R	O	A	I	S		
7	B	C	D	F	G	H	J	K	L	M
6	P	Q	U	V	W	X	Y	Z	(	)

	0	1	8	3	4
	A	E	I	O	U
5	B	C	D	F	G
2	H	K	L	M	N
9	P	Q	R	S	T
7	V	W	X	Y	Z

Varianten - 1

	0	1	8	3	4	5
2	A	B	C	D	E	F
9	G	H	I	J	K	L
7	M	N	O	P	Q	R
62	S	T	U	V	W	X
69	Y	Z	0	1	2	3
67	4	5	6	7	8	9

monome-dinome-trinome

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

letter-bigram

Varianten - 2

1. identificeer rij-coördinaten
2. los de resulterende monoalfabetische substitutie op
3. reconstrueer de sleutel (zo mogelijk)

Hulpmiddelen

- monome-telling hoog $\stackrel{?}{\rightarrow}$ dinome-coördinaten
- bigram-telling veel contacten$\stackrel{?}{\rightarrow}$ dinome-coördinaten
- `..4444..` dan 4 een dinome-kandidaat
- herhalingen wijzen op letterscheiding
- monome-dinome identificatie geeft redelijke frequenties

		0	1	2	3	4	5	6	7	8	9
0	𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸//	2	2	5	–	6	2	2	7	2	14
1	𝍸𝍸	3	–	5	–	–	1	–	1	–	–
2	𝍸𝍸𝍸𝍸𝍸////	6	2	1	–	7	1	–	2	1	9
3		–	–	–	–	–	–	–	–	–	–
4	𝍸𝍸////	10	–	1	–	–	–	–	2	1	–
5	𝍸////	2	–	2	–	–	1	1	3	–	–
6	𝍸///	4	1	–	–	–	1	–	1	–	–
7	𝍸𝍸𝍸𝍸/	5	1	8	–	1	3	3	–	–	–
8	///	–	2	1	–	–	–	–	1	–	–
9	𝍸𝍸𝍸𝍸///	10	2	5	–	–	–	2	4	–	–

Eenvoudig voorbeeld

		0	1	2	3	4	5	6	7	8	9
0	𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸	2	2	5	-	6	2	2	7	2	14
1	𝍸𝍸𝍸	3	-	5	-	-	1	-	1	-	-
2	𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸	6	2	1	-	7	1	-	2	1	9
3		-	-	-	-	-	-	-	-	-	-
4	𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸	10	-	1	-	-	-	-	2	1	-
5	𝍸𝍸𝍸𝍸𝍸𝍸𝍸	2	-	2	-	-	1	1	3	-	-
6	𝍸𝍸𝍸𝍸𝍸𝍸	4	1	-	-	-	1	-	1	-	-
7	𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸	5	1	8	-	1	3	3	-	-	-
8	𝍸𝍸𝍸	-	2	1	-	-	-	-	1	-	-
9	𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸𝍸	10	2	5	-	-	-	2	4	-	-

dinome-coördinaten 0 en 2

Eenvoudig voorbeeld

	0	1	2	3	4	5	6	7	8	9
-		7		-	1	6	6	12	1	1
0	1	1	5	-	6	2	2	7	2	13
2	2	2	-	-	7	1	-	2	1	9

decompositie

	9	1	6	4	5	8	7	3	0	2
-	V	E	R	M	O	U	T	H		
0	A	B	C	D	F	G	I	J	K	L
2	N	P	Q	S	W	X	Y	Z	.	?

oplossing

Oplossing

		0	1	2	3	4	5	6	7	8	9
0	𝍸𝍸𝍸IIII	1	1	–	1	4	7	1	1	1	2
1	𝍸𝍸𝍸𝍸𝍸𝍸	3	1	11	1	–	1	2	3	3	5
2	𝍸𝍸𝍸𝍸𝍸𝍸II	2	7	2	3	3	2	1	9	1	3
3	𝍸III	–	1	1	–	–	3	–	1	1	1
4	𝍸𝍸𝍸III	1	1	3	–	1	9	–	6	5	2
5	𝍸𝍸𝍸𝍸𝍸𝍸I	2	3	2	–	3	9	–	6	5	2
6	𝍸II	–	–	3	1	–	1	–	1	–	1
7	𝍸𝍸𝍸𝍸𝍸𝍸𝍸I	7	10	7	2	2	1	1	3	2	1
8	𝍸𝍸III	1	3	3	–	1	–	–	3	–	1
9	𝍸𝍸𝍸I	2	3	–	–	4	4	1	2	–	–

Minder eenvoudig voorbeeld

		0	1	2	3	4	5	6	7	8	9
0	𝍸𝍸𝍸	1	1	–	1	4	7	1	1	1	2
1	𝍸𝍸𝍸𝍸𝍸𝍸	3	1	11	1	–	1	2	3	3	5
2	𝍸𝍸𝍸𝍸𝍸𝍸𝍸	2	7	2	3	3	2	1	9	1	3
3	𝍸𝍸	–	1	1	–	–	3	–	1	1	1
4	𝍸𝍸𝍸𝍸	1	1	3	–	1	9	–	6	5	2
5	𝍸𝍸𝍸𝍸𝍸𝍸	2	3	2	–	3	9	–	6	5	2
6	𝍸	–	–	3	1	–	1	–	1	–	1
7	𝍸𝍸𝍸𝍸𝍸𝍸𝍸	7	10	7	2	2	1	1	3	2	1
8	𝍸𝍸𝍸	1	3	3	–	1	–	–	3	–	1
9	𝍸𝍸𝍸	2	3	–	–	4	4	1	2	–	–

Best

7–2–1–5

Onderzoek

a. 1, 7

b. 2, 7

c. 5, 7

d. 1, 2, 7

e. 1, 5, 7

f. 2, 5, 7

g. 1, 2, 5, 7

Minder eenvoudig voorbeeld

	0	1	2	3	4	5	6	7	8	9
-	9		17	6	16	31	4		10	13
1	3	1	8	-	-	-	2	2	1	2
7	7	9	7	2	2	-	1	2	2	1

(a)

	0	1	2	3	4	5	6	7	8	9
-	15	18		5	16	30	5		11	12
2	1	6	2	1	-	1	1	8	1	3
7	3	6	6	2	2	-	1	3	1	1

(b)

	0	1	2	3	4	5	6	7	8	9
-	13			4	15	29	3		10	10
1	2	1	6	-	-	-	2	3	1	3
2	-	4	1	2	1	2	1	6	1	2
7	4	7	5	2	2	-	1	2	1	1

(d)

	0	1	2	3	4	5	6	7	8	9
-	9		16	16	13		5		4	13
1	3	-	9	-	-	1	1	2	3	1
5	-	3	2	-	3	6	-	4	5	1
7	7	7	5	2	2	-	1	2	1	1

(e)

Enkele decomposities

Cumulatieve tabel hoogste tellingen in %

	a	b	c	d	e	f	g	Engels
1	19.6	18.6	15.9	19.7	11.6	12.2	9.3	13.0
2	30.4	29.8	29.3	29.9	21.0	22.3	18.6	22.2
3	45.0	39.8	38.2	38.8	30.4	30.9	26.6	30.2
4	48.7	49.1	46.5	45.6	37.0	38.8	31.8	37.8
5	55.1	56.5	54.1	52.4	43.5	44.6	36.4	45.3
6	60.8	63.4	58.6	57.1	48.6	50.4	40.3	52.7

Cumulatieve tabel hoogste tellingen in %

	a	b	c	d	e	f	g	Engels
1	19.6	18.6	15.9	19.7	11.6	12.2	9.3	13.0
2	30.4	29.8	29.3	29.9	21.0	22.3	18.6	22.2
3	45.0	39.8	38.2	38.8	30.4	30.9	26.6	30.2
4	48.7	49.1	46.5	45.6	37.0	38.8	31.8	37.8
5	55.1	56.5	54.1	52.4	43.5	44.6	36.4	45.3
6	60.8	63.4	58.6	57.1	48.6	50.4	40.3	52.7