Cursus Cryptografie

Monome-dinome

16-02-2017

Probleemstelling

- crypto elementen hebben constante lengte
  - *cryptogram eenvoudig op te delen*
- tegenmaatregelen
  - *gebruik nullen*
  - *crypto elementen van variabele lengte*

Voorbeeld nullen

.. 1815 1134 3711 2932 1923 2317 ..

.. 1810 5113 4371 1293 2190 2323 17 ..

.. 1815 1134 3071 1293 2192 3203 17 ..

.. 1815 1134 3710 1293 2192 3023 17 ..

maar: tekstherhalingen verraden de nullen

Variant: reeksen met nul-markering

.. 1805 7210 1511 3437 1129 3210 3092 3231 7 ..

Monome-dinome schema

crypto elementen van verschillende lengte gebruiken

cijfers

D I T I S G E H E I M

33 03 4 03 8 32 2 01 2 03 36

33034 03832 20120 336

letters

D I T I S G E H E I M

AA QA K QA M AC T QK T QA QX

AAQAK QAMAC TQKTQ AQX

Straddling Checkerboard

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

- T=3, B=00, F=03, M=10, U=13, 0=80
- kolomcoördinaten gepermuteerd
- sleutelwoord in toprij
- ruimte voor cijfers, leestekens
- etao… in toprij comprimeert cryptogram

Varianten

	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

6 als nul te gebruiken

Monome-dinome-trinome

	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
67	Y	Z	0	1	2	3
69	4	5	6	7	8	9

Bigram

			Q V	R W	S X	T Y	U Z
			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	•	$	(	)

Veel homofone combinaties mogelijk

Cryptoanalyse

1. identificeer dinome-coördinaten
2. los monoalfabetische substitutie op
3. reconstrueer zo mogelijk sleutel

Vuistregels:

- telling hoog → dinome coördinaat ?
- veel verschillende contacten → dinome coördinaat ?
- —4444— dinome coördinaat 4 ?
- herhalingen → letterscheiding
- monome-dinome splitsing geeft goede frequenties

Voorbeeld - 1

		0	1	2	3	4	5	6	7	8	9
0	42	2	2	5	-	6	2	2	7	2	14
1	10	3	-	5	-	-	1	-	1	-	-
2	29	6	2	1	-	7	1	-	2	1	9
3	0	-	-	-	-	-	-	-	-	-	-
4	14	10	-	1	-	-	-	-	2	1	-
5	9	2	-	2	-	-	1	1	3	-	-
6	7	4	1	-	-	-	1	-	1	-	-
7	21	5	1	8	-	1	3	3	-	-	-
8	4	-	2	1	-	-	-	-	1	-	-
9	23	10	2	5	-	-	-	2	4	-	-

Dinome kandidaten

		0	1	2	3	4	5	6	7	8	9	
0	42	2	2	5	-	6	2	2	7	2	14	← dinome
1	10	3	-	5	-	-	1	-	1	-	-	
2	29	6	2	1	-	7	1	-	2	1	9	← dinome
3	0	-	-	-	-	-	-	-	-	-	-	
4	14	10	-	1	-	-	-	-	2	1	-	
5	9	2	-	2	-	-	1	1	3	-	-	
6	7	4	1	-	-	-	1	-	1	-	-	
7	21	5	1	8	-	1	3	3	-	-	-	
8	4	-	2	1	-	-	-	-	1	-	-	
9	23	10	2	5	-	-	-	2	4	-	-	

Decompositie

	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

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

Voorbeeld - 2

		0	1	2	3	4	5	6	7	8	9
0	19	1	1	-	1	4	7	1	1	1	2
1	30	3	1	11	1	-	1	2	3	3	5
2	32	2	7	2	3	3	2	1	9	1	3
3	8	-	1	1	-	-	3	-	1	1	1
4	18	1	3	3	-	1	9	-	6	5	2
5	31	2	3	2	-	3	9	-	6	5	2
6	7	-	-	3	1	-	1	-	1	-	1
7	36	7	10	7	2	2	1	1	3	2	1
8	13	1	3	3	-	1	-	-	3	-	1
9	16	2	3	-	-	4	4	1	2	-	-

Dinome kandidaten

		0	1	2	3	4	5	6	7	8	9
0	19	1	1	-	1	4	7	1	1	1	2
1	30	3	1	11	1	-	1	2	3	3	5
2	32	2	7	2	3	3	2	1	9	1	3
3	8	-	1	1	-	-	3	-	1	1	1
4	18	1	3	3	-	1	9	-	6	5	2
5	31	2	3	2	-	3	9	-	6	5	2
6	7	-	-	3	1	-	1	-	1	-	1
7	36	7	10	7	2	2	1	1	3	2	1
8	13	1	3	3	-	1	-	-	3	-	1
9	16	2	3	-	-	4	4	1	2	-	-

dinome = 7

overige kandidaten

1-2-5

<u>proberen</u>

1-7

2-7

5-7

1-2-7

1-5-7

2-5-7

1-2-5-7

Decomposities

	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

	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

	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

	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

Cumulatieve frequenties

	1-7	2-7	5-7	1-2-7	1-5-7	2-5-7	1-2-5-7	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