College Cryptografie

Cursusjaar 2003

Analyse Hagelin cryptograaf

4 maart 2003

Hagelin

Modellen

Werking

Cryptoanalyse

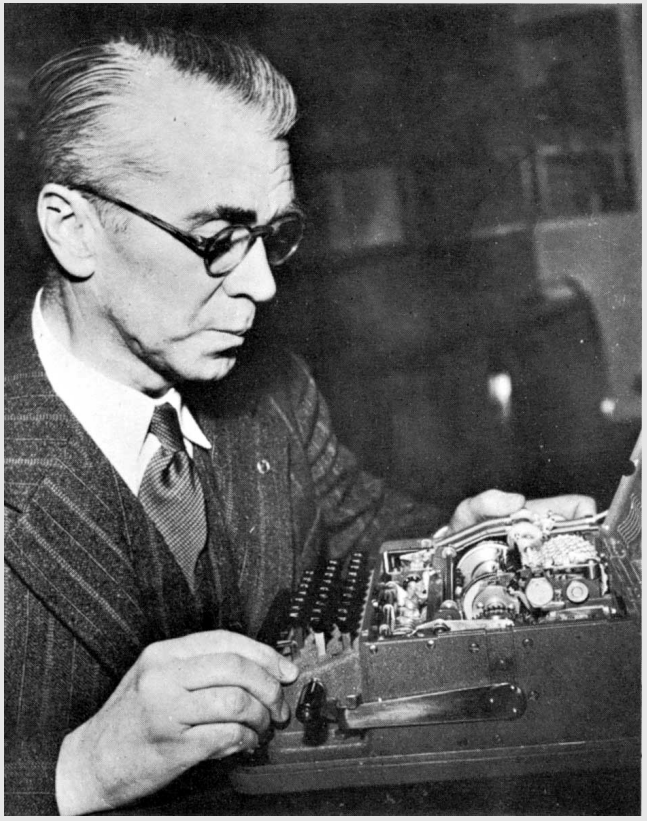
Stagger

Kerckhoffs superpositie

Sleutelstroom statistiek

Pinstatistiek

Differencing

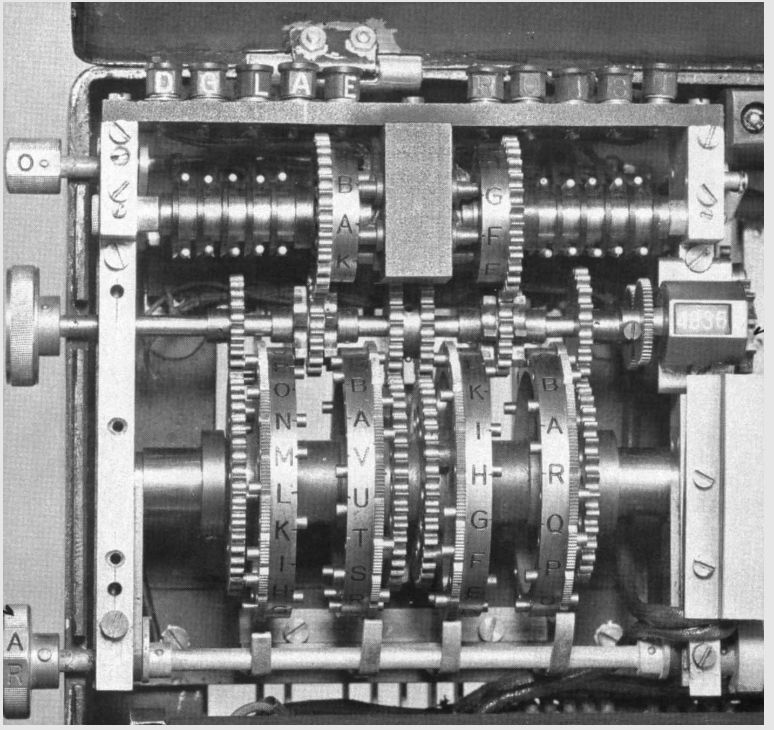


- Boris Caesar Wilhelm Hagelin
  geboren 1892 Kaukasus
  zoon Zweeds diplomaat
- studiewerktuigbouwkunde
  St Petersburg en Stockholm
- 1922 voor familie in dienst
  Aktiebolaget Cryptograph
  Arvid Damm
- later Zwitserland
  Crypto Aktiengesellschaft
- overleden 1983

Hagelin

- 1926 model B21
  voor Zweedse leger
- 1934 C-serie
  op Frans verzoek
- 1940 via Duitsland en
  Genua naar Amerika met
  prototypes model M209
- latere modellen C52, CD57

B211

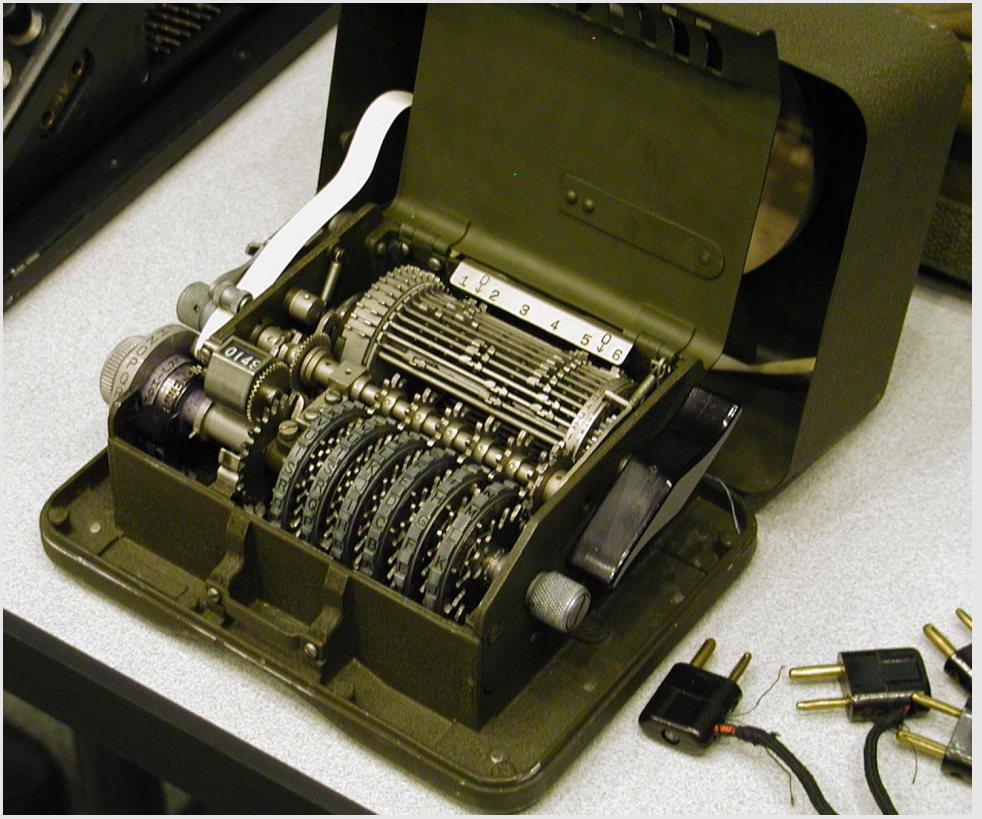


Modellen

- US-Army, WW2, model M209, divisie–bataljon, 140.000+
  voor het eerst operatie Torch, Noord-Afrika
- Italiaanse vloot, WW2, model C38
  sedert zomer 1941 gebroken door GCCS
  aanvallen vanaf Malta op konvooien naar Rommel's DAK
- Egypte 1950, ambassades
  van belang tijdens 5-daagse oorlog
- Nederland, model B211
  1954 NSA-cryptoanalist Joseph Peterson gearresteerd
  Analysis of the Hagelin Cryptograph Type B-211, 1939

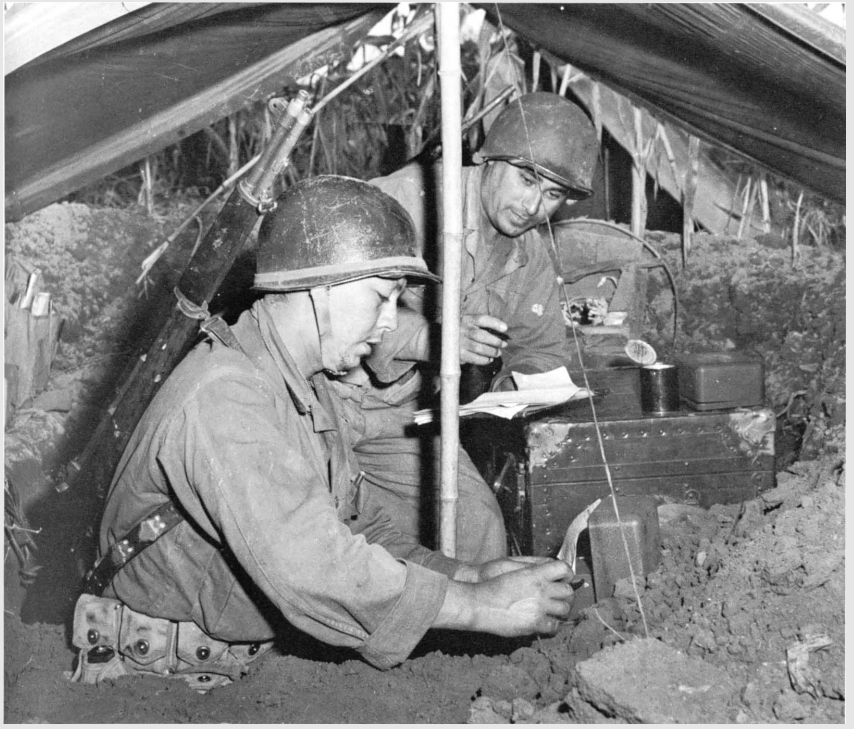
Gebruikers

model M-209



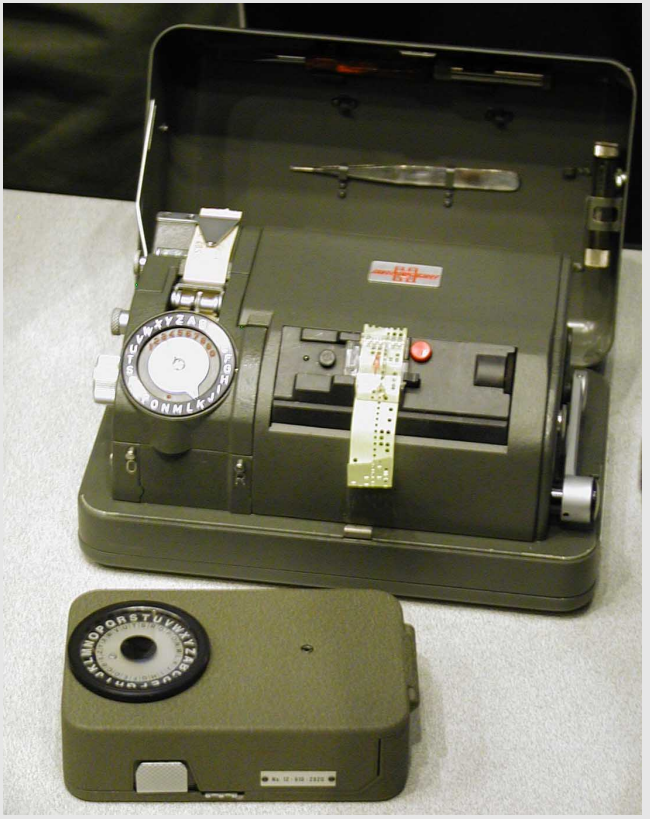
Illustraties

M209 in Koreaanse oorlog

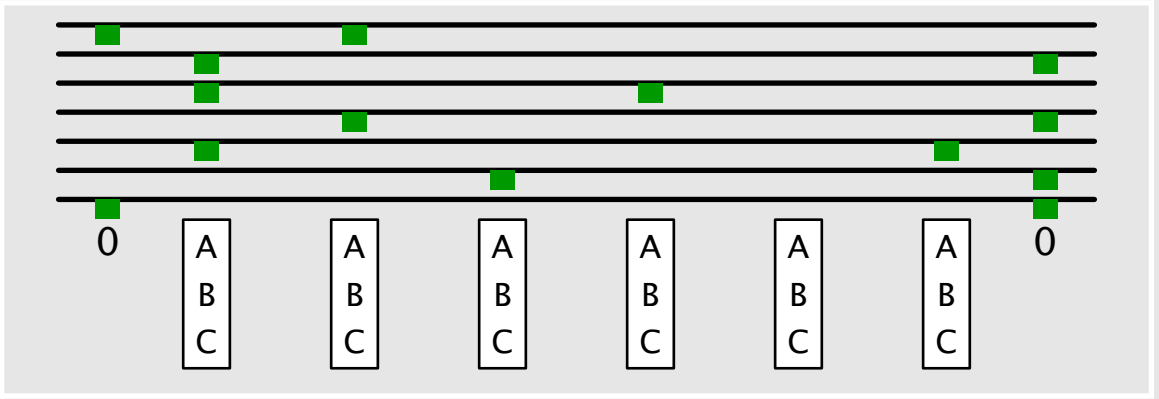


model CX52

pocketmodel CD57



Illustraties



- zes wielen met resp. 26, 25, 23, 21, 19, 17 pinposities
- kooi met 27 linealen elk met twee verplaatsbare ruiters
- tel aantal aktieve linealen bij rondgang kooi
- selecteer daarmee rij in Beaufort-tabel
- per vercijfering draait elk wiel één stap

Werking

	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
0,26	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
1,27	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
2	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
3	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D

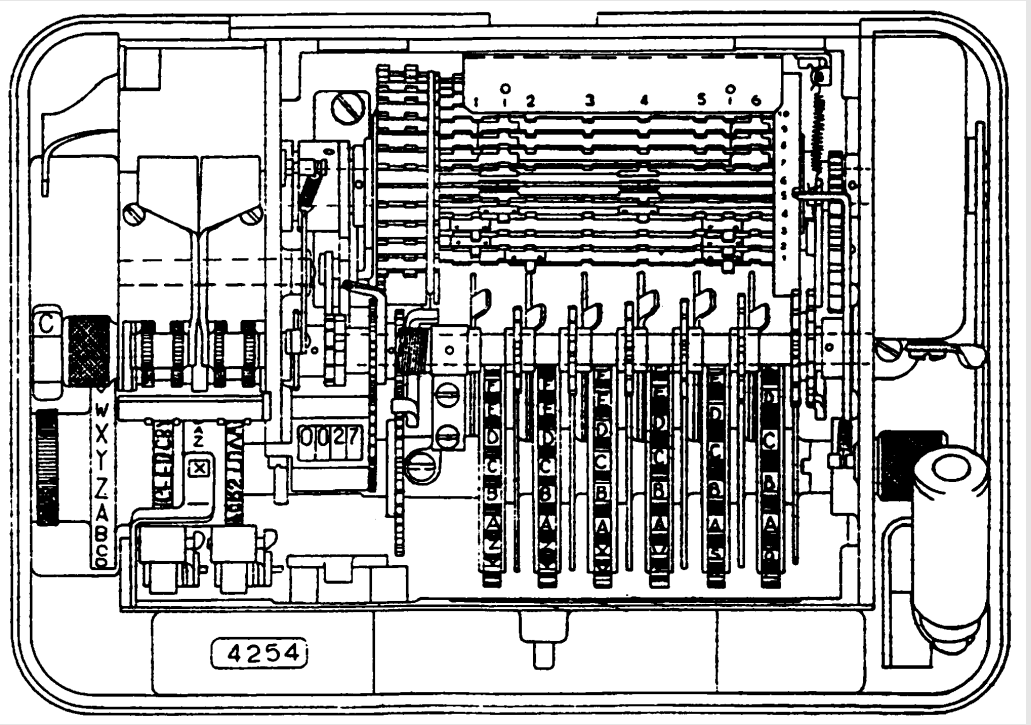
.....

	W1 = 17(4)	W2 = 19(7)	W3 = 21(5)	1 W1-W2 overlap

pt	V	O	O	R	B	E	E	L	D	V	A	N	E	E	N	H	A	G	E	L	I	N	B	O	O	D	S	C	H	A	P
W1	0	0	0	4	4	0	4	4	0	0	0	4	0	4	4	0	4	0	0	0	4	4	0	4	4	0	0	0	4	0	4
W2	7	7	0	0	7	0	7	0	0	0	0	7	7	7	0	0	0	0	7	7	7	0	0	7	0	7	0	0	0	0	7
W3	0	5	0	0	0	0	5	0	0	0	0	5	0	0	0	0	5	0	0	0	5	0	5	0	0	0	0	5	0	0	0
kick		1			1			1					1		1							1			1						1
	7	2	0	4	0	0	5	4	0	0	0	5	7	0	4	0	9	0	7	7	5	4	5	0	4	7	0	5	4	0	0
ct	L	X	L	M	I	V	K	S	W	E	Z	B	C	F	Q	S	I	T	C	V	G	Q	D	V	P	D	H	C	W	Z	U

Voorbeeld vercijfering

Model C38



Illustraties

- lengte periode $26 \times 25 \times 23 \times 21 \times 19 \times 17 = 101.405.850$
- $26 + 25 + 23 + 21 + 19 + 17 = 131$ pin posities
- 27 linealen met $1 + 6 + \binom{2}{6} = 22$ bezettingen
  nota bene: permutaties tussen de linealen ineffectief
- 101.405.850 startposities
- model C38: 26 relatieve posities pt–ct alfabet (*slide*)
  model M209: slide vast A–Z
- slechts 26 substituties ontstaan uit 64 pin patronen

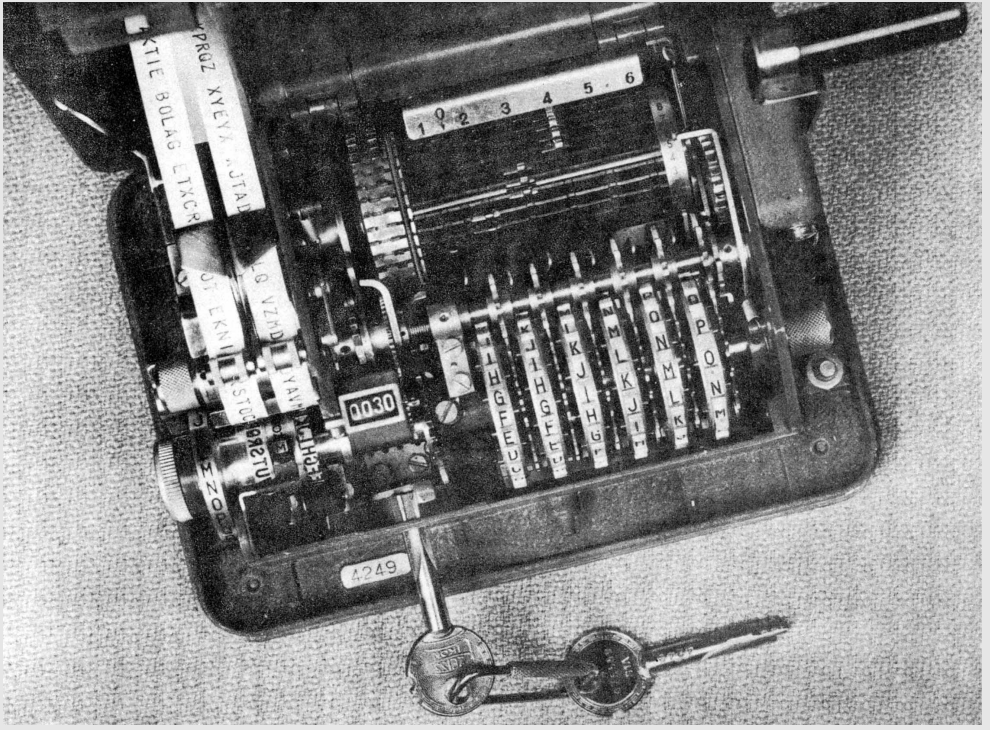
Parameters

```
26 ABCDEFGHIJKLMNOPQRSTUVWXYZ
   PQRSTUVWXYZABCDEFGHIJKLMNO
25 ABCDEFGHIJKLMNOPQRSTUVXYZ
   OPQRSTUVXYZABCDEFGHIJKLMN
23 ABCDEFGHIJKLMNOPQRSTUVX
   NOPQRSTUVXABCDEFGHIJKLM
21 ABCDEFGHIJKLMNOPQRSTU
   MNOPQRSTUABCDEFGHIJKL
19 ABCDEFGHIJKLMNOPQRS
   LMNOPQRSABCDEFGHIJK
17 ABCDEFGHIJKLMNOPQ
   KLMNOPQABCDEFGHIJ
```

drie standen

1. vercijfer → groepen van 5
2. ontcijfer → Z/X = spatie
3. coderen geen spatie

Model C38



Beaufort vercijfering: $C + P = K + S$

P = klaar, C = vercijferd, K = sleutel, S = slide

klaarletter naar printpositie, printpositie stationair

- slide = A, klaarletter E, beginstand

  ABCDEFGHIJKLMNOPQRSTUVWXYZ indicatorwiel

  AZYXWVUTSRQPONMLKJIHGFEDCB printwiel

- slide = A, E vercijferd met kick = 12

  OPQRSTUVWXYZABCDEFGHIJKLMN indicatorwiel

  MLKJIHGFEDCBAZYXWVUTSRQPON printwiel

- slide = H, E vercijferd met kick = 12

  OPQRSTUVWXYZABCDEFGHIJKLMN indicatorwiel

  TSRQPONMLKJIHGFEDCBAZYXWVU printwiel

Effect slide

- model B21
  fractionerend systeem gebaseerd op Damm halfrotor
- model C35
  5 wiel 25, 23, 21, 19, 17; 25 lineaal 10, 8, 4, 2, 1 ruiter
- model C38
  6 wiel 26, 25, 23, 21, 19, 17; 27 lineaal 2 ruiters
  M209 vaste alfabetringen op A=Z
- model C52
  6 wiel 47, 46, 43, 42, 41, 38, 34, 31, 29, 26, 25
  32 lineaal, onregelmatige stap
- model CD57
  40 lineaal geen overlap, permuteerbaar alfabet

Modellen

- known plaintext – analyse van de sleutelstroom
  - classificeer pinnen met kick statistiek
  - verschilberekening kick waarden (geen overlap)
- ciphertext-only analyse
  - classificeer pinnen met frequentie statistiek
  - verschilberekening met gemeenschappelijke klaartekst
- hoe vinden we een sleutelstroom?
  - uit bekende klaartekst
  - optreden van een *stagger*
  - overlappende sleutelstromen (*Kerckhoffs superpositie*)
  - partiële sleutel en klaartekst overlappingen
  - unique odd key (speciale pinsetting)

- known plaintext – analyse van de sleutelstroom
  - classificeer pinnen met kick statistiek
  - verschilberekening kick waarden (geen overlap)
- ciphertext-only analyse
  - classificeer pinnen met frequentie statistiek
  - verschilberekening met gemeenschappelijke klaartekst
- hoe vinden we een sleutelstroom?
  - uit bekende klaartekst
  - optreden van een *stagger*
  - overlappende sleutelstromen (*Kerckhoffs superpositie*)
  - partiële sleutel en klaartekst overlappingen
  - unique odd key (speciale pinsetting)

Hagelin oefening

Treedt op als berichten een letter in lengte verschillen

- EXAMPLEOFSTAGGERSITUATION — klaartekst 1
  EXAMPLEOFASTAGGERSITUATION — klaartekst 2
  GPZTOQNGHDJJAZVTWOGQBVTBTD — sleutelstroom
  BRYGYEIRBKPITSQBDFMVABKMF — cryptogram 1
  BRYGYEIRBCQPZSOOEVXWGUZSEP — cryptogram 2
- stel K1 = A → Q2 = A → sleutelletter = R → P1 = b enzovoorts
- inspecteer alle Caesar verschuivingen van deze 'ontcijfering'

  ABIOOMZAQBCIBQWV

  BCJPPNABRCDJCRXW

  ...

  STAGGERSITUATION

Zoek overlappende sleutelstromen en leg deze *in diepte*

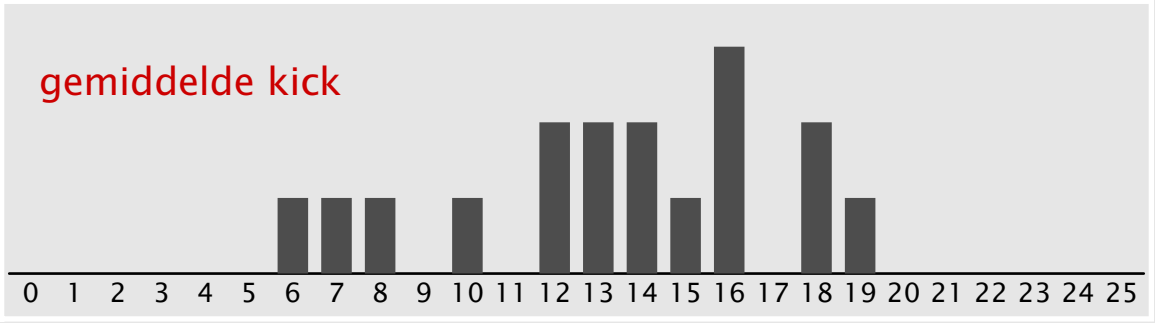
Als de cryptogrammen in diepte onder elkaar gelegd worden hebben de letters in elke kolom dezelfde substitutie gekregen heeft dus elke kolom een *monoalfabetische* distributie

Indicaties voor goede onderlinge positie

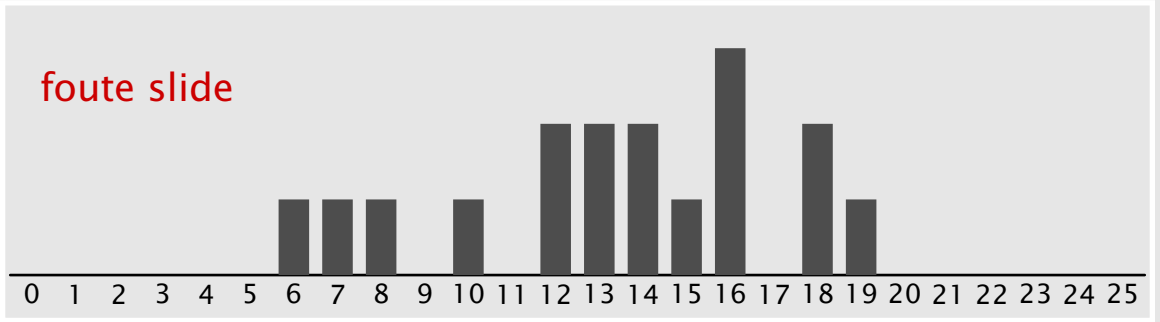
- hoog aantal coïncidenties
- herhalingen van enige lengte
- kennis van het indicatorsysteem voor beginstand
- Hagelin: verschillende slide *constant verschil* `A-C`, `B-D`, ...

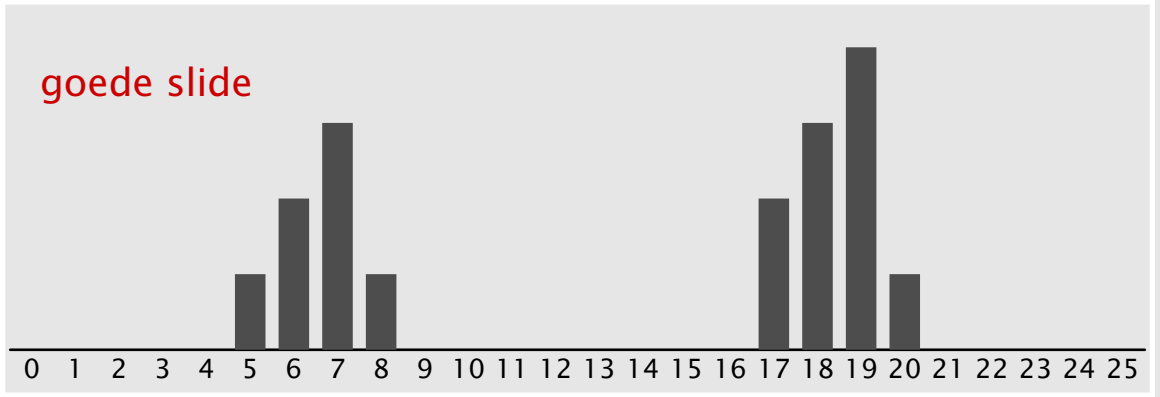
Kerckhoffs superpositie

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
5	14	6	20	25	20	17	11	11	8	14	10	10	8	10	22	15
12	14	5	22	8	14	16	21	23	10	22	24	22	10	10	21	10
8	10	10	22	8	12	18	22	6	4	17	12	12	8	20	11	17
10	10	10	10	12	13	15	21	5	4	18	8	18	4	20	18	14
12	14	4	16	8	10	19	14	6	4	18	11	16	4	14	22	21
24	22	12	6	12	18	13	16									
12	14	8	16	12	14	16	18	10	6	18	13	16	7	15	19	13



Sleutelstroom statistiek



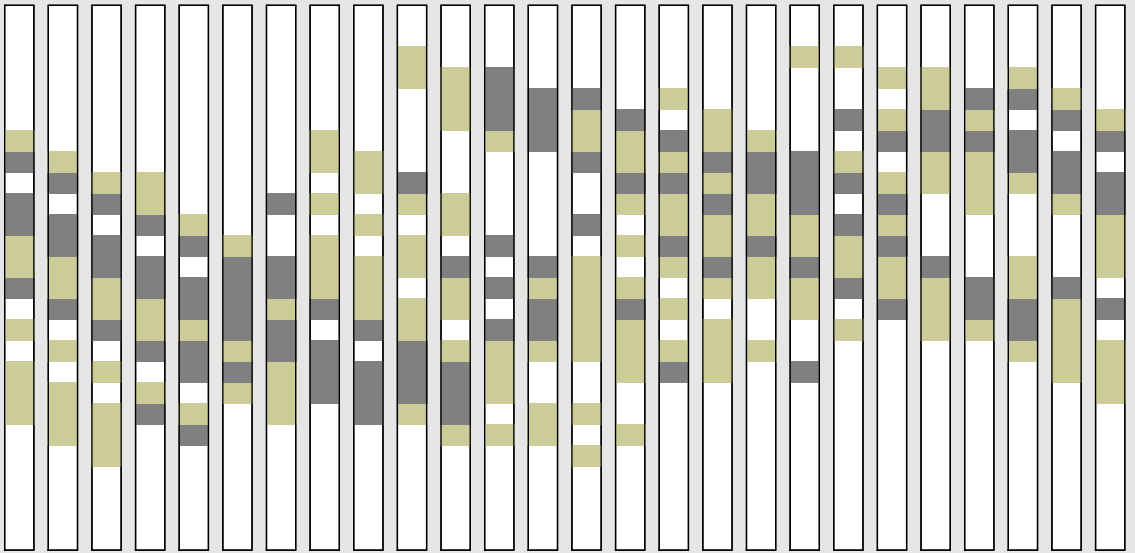


Bimodale statistiek

Bepaling instelling pinnen m.b.v. bimodale distributie kicks

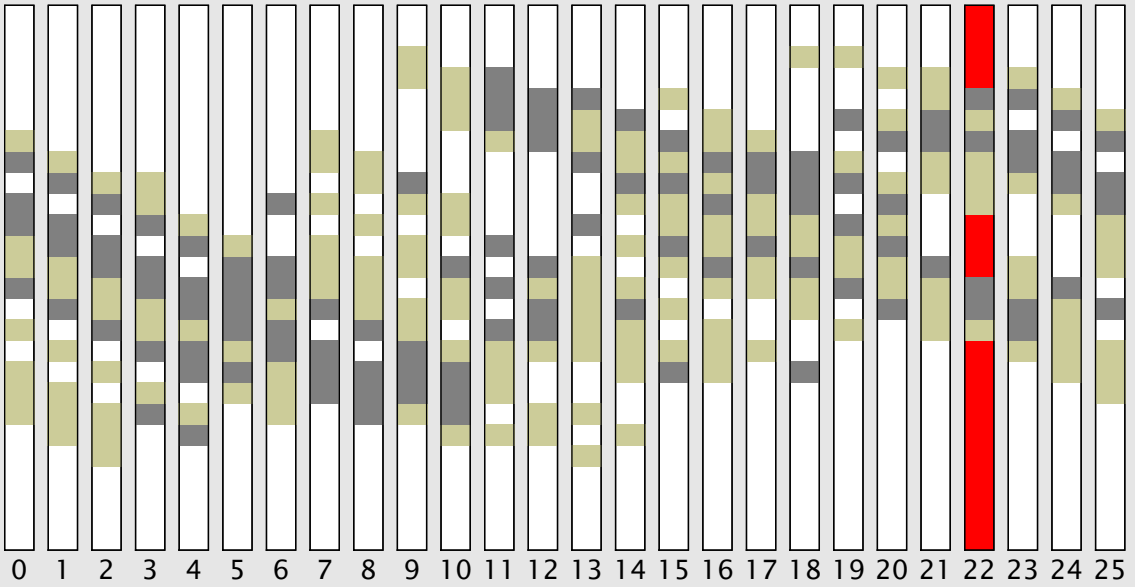
- bepaal letterdistributie modulo wielperiode
- overige wielen geven min of meer random bijdrage
- resulteert twee soorten distributie:
  - 0-pin rond gemiddelde waarde zonder kick
  - 1-pin rond gemiddelde waarde met kick
- match distributies van alle pinnen met elkaar
- twee groepen, onbekend welke 0 en welke 1
- uit statistisch model: paar duizend letters per bericht nodig

histogrammen kicks voor elke slide



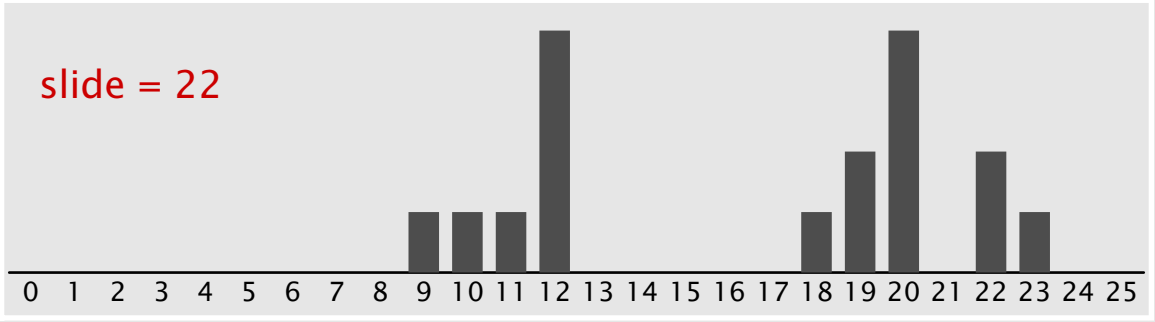
Slide bepalen

histogrammen kicks voor elke slide



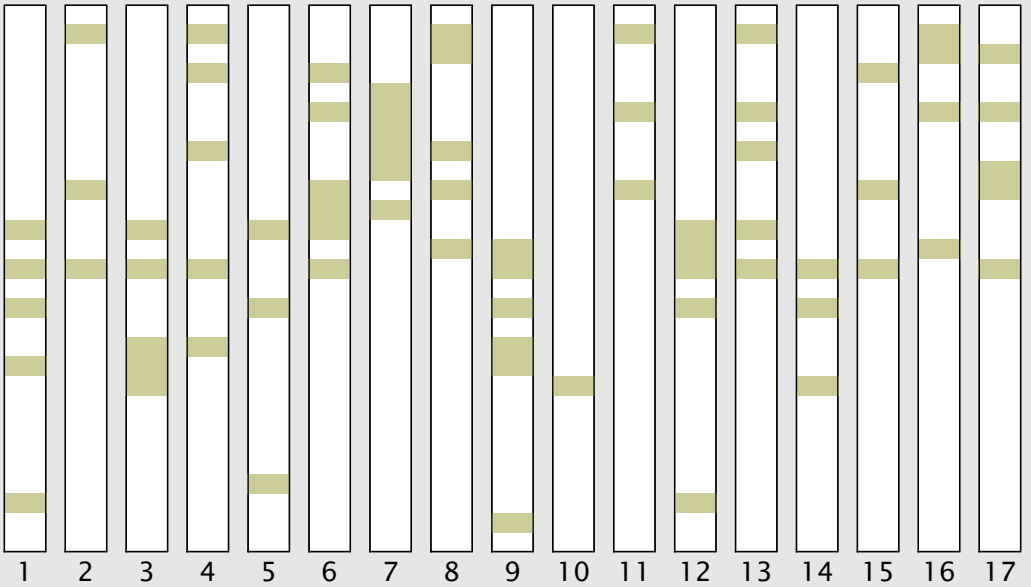
Slide bepalen

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



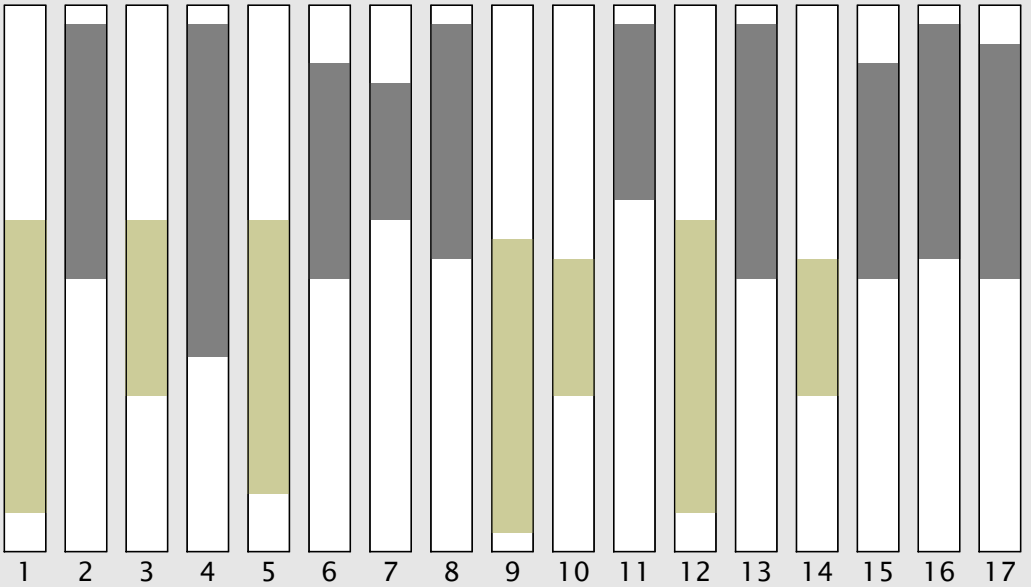
Statistiek 17 wiel

gevonden kicks

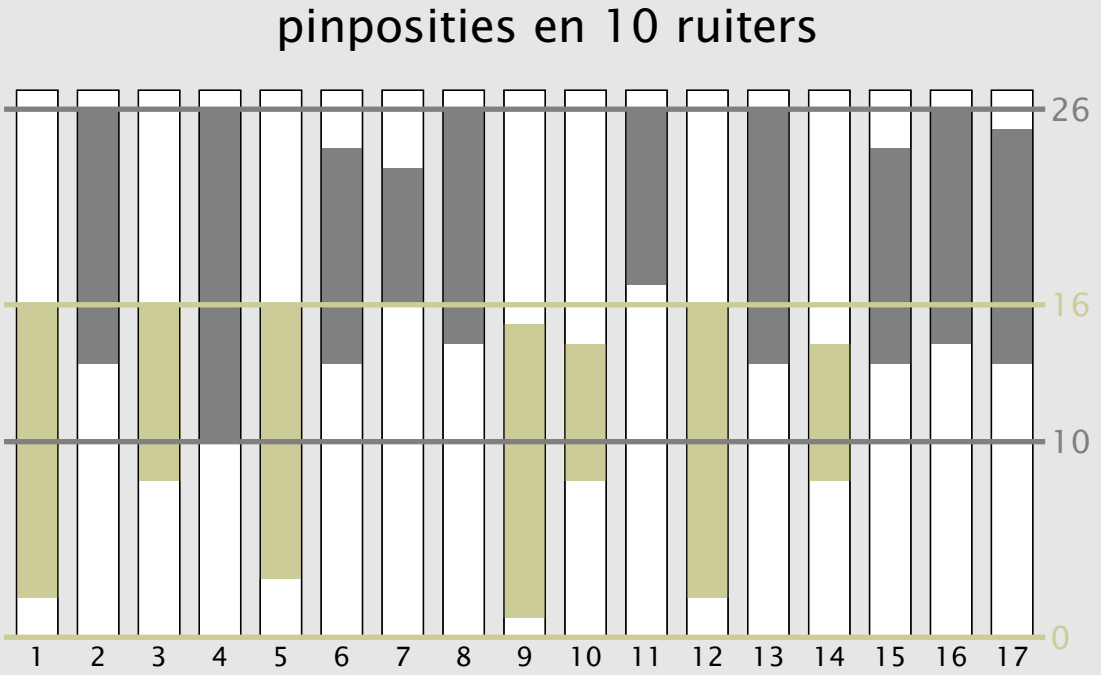


Statistiek 17 wiel

range van de gevonden kicks



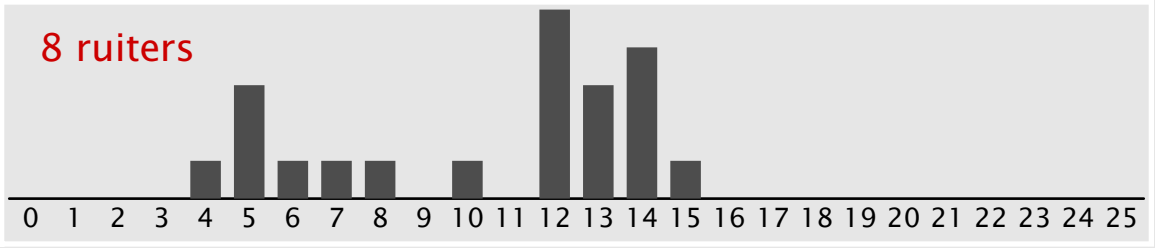
Statistiek 17 wiel



Statistiek 17 wiel

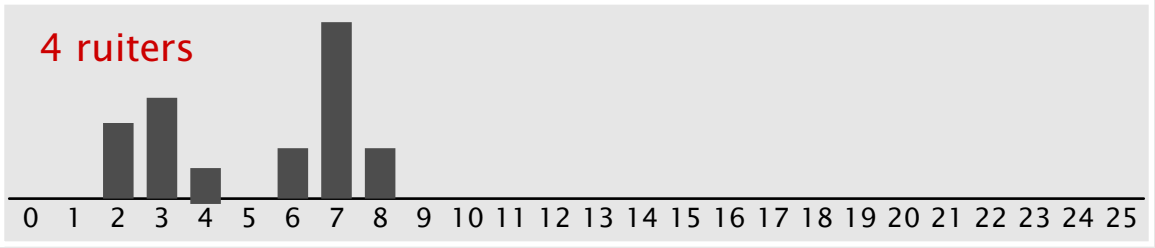
kicks 17 wiel verwijderd

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
9	8	10	14	3	14	11	5	15	12	8	14	4	12	4	16	9	16	8	9	16
12	8	10	15	1	14	16	2	16	14	4	15	4	12	4	14	16	12	6	12	16
10	8	11	16	6	12	14	6	11	14	4	14	4	16	7	9	15	9	8	12	12
12	8	14	12	8	16	8	8	10	12	4	13	8	10	8	12	15	10	8	8	16
15	2	16	16	0	16	12	7	10												
1	0	1	1	0	1	1	0	1	1	0	1	0	1	0	1	1	1	0	1	1



kicks 17 + 21 wiel verwijderd

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	8	2	6	3	6	3	5	7	4	8	6	4	4	4	8	1	8	8
1	8	4	8	2	7	1	6	8	2	8	6	4	7	4	4	4	7	8
4	6	4	8	2	8	3	8	6	4	6	5	3	6	4	6	4	8	7
1	7	1	8	4	4	4	8	6	4	8	8	0	8	2	4	4	5	8
2	8	4	7	2	8	0	8	7	2	8	8	0	8	4	7	2		
0	1	0	1	0	1	0	1	1	0	1	1	0	1	0	1	0	1	1



Statistiek 19 wiel

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Kicks 23-25-26

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
													0											
													0											
													0											
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
									0															
									0															
									0															
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
												0							0			0		
												0							0			0		
												0							0			0		
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
							0						0											
							0						0											
							0						0											
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Kick = 0

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0			0								0		0			0			0				0	
							0		0			0	0						0			0		
				0				0		0			0				0			0				
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
	0								0		0			0			0				0			0
							0		0			0	0						0			0		
					0				0		0			0				0			0			
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
							0		0			0			0				0			0		
							0		0			0	0						0			0		
						0				0		0			0				0			0		
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
					0		0			0			0				0							
							0		0			0	0											
							0				0		0			0								
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Completeer wielperiode

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0			0								0		0			0			0				0	
							0		0			0	0						0			0		
				0				0		0			0				0		1	0				
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
	0								0		0			0			0				0			0
							0		0		2	0	0	2					0		2	0		
					0				0		0			0				0			0			
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
							0		0			0			0				0			0		
							0		0			0	0		2				0			0		
						0	1		1	0		0			0				0			0		
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
					0		0			0			0				0							
							0		0			0	0											
							0				0		0			0								
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Bepaal nieuwe kicks

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0			0								0		0			0			0				0	
							0		0		2	0	0	2	2				0		2	0		
				0	1		1	0		0			0				0		1	0				
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
	0								0		0			0			0				0			0
							0		0		2	0	0	2	2				0		2	0		
					0	1		1	0		0			0				0		1	0			
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
							0		0			0			0				0			0		
							0		0		2	0	0	2	2				0		2	0		
						0	1		1	0		0			0				0		1	0		
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
					0		0			0			0				0							
							0		0		2	0	0		2									
							0	1		1	0		0			0								
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Completeer wielperiode

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0			0								0		0			0			0				0	
							0		0		2	0	0	2	2				0		2	0		
				0	1		1	0		0	?		0				0		1	0				
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
	0								0		0			0			0				0			0
							0		0		2	0	0	2	2				0		2	0		
					0	1		1	0		0			0				0		1	0			
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
							0		0			0			0				0		0	0		
							0		0		2	0	0	2	2				0		2	0		
						0	1		1	0		0			0				0		1	0		
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
					0		0			0			0				0							
							0		0		2	0	0		2									
							0	1		1	0		0			0								
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Overlap 25-26 wiel

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0		0	0		0		0				0		0			0			0				0	
0		2	2		2		0		0	2	2	0	0	2	2	0			0		2	0	2	
1				0	1		1	0		0			0			1	0		1	0				
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
0	0		0		0				0		0			0			0				0		0	0
0	2		2		2		0		0	2	2	0	0	2	2		2		0		2	0	2	0
1					0	1		1	0		0			0				0		1	0			1
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
	0		0				0		0			0			0				0		0	0		0
	2		2		2		0		0	2	2	0	0	2	2				0		2	0		0
						0	1		1	0		0			0				0		1	0		1
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
	0				0		0			0			0				0							
	2				2		0		0	2	2	0	0		2		2							
							0	1		1	0		0			0								
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Verdere uitwerking

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0		0	0		0		0				0		0			0			0				0	
0	2	2	2		2		0		0	2	2	0	0	2	2	0	2		0		2	0	2	0
1				0	1		1	0		0			0			1	0		1	0		1	1	
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
0	0		0		0				0		0			0			0				0		0	0
0	2	2	2		2		0		0	2	2	0	0	2	2	0	2		0		2	0	2	0
1	1				0	1		1	0		0			0			1	0		1	0		1	1
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
	0		0				0		0			0			0				0		0	0		0
0	2	2	2		2		0		0	2	2	0	0	2	2	0	2		0		2	0	2	0
	1	1				0	1		1	0		0			0			1	0		1	0		1
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
	0				0		0			0			0			3	0							
0	2	2	2		2		0		0	2	2	0	0		2	0	2							
1		1	1				0	1		1	0		0			0								
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Wiel 23 = 3

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0		0	0		0		0			3	0		0			0			0			3	0	
0	2	2	2		2		0		0	2	2	0	0	2	2	0	2		0		2	0	2	0
1				0	1		1	0		0			0			1	0		1	0		1	1	
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
0	0		0		0				0		0			0			0			3	0		0	0
0	2	2	2		2		0		0	2	2	0	0	2	2	0	2		0		2	0	2	0
1	1				0	1		1	0		0			0			1	0		1	0		1	1
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
	0		0				0		0			0			0			3	0		0	0		0
0	2	2	2		2		0		0	2	2	0	0	2	2	0	2		0		2	0	2	0
	1	1				0	1		1	0		0			0			1	0		1	0		1
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
	0				0		0			0			0			3	0							
0	2	2	2		2		0		0	2	2	0	0		2	0	2							
1		1	1				0	1		1	0		0			0								
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Overlap 23–25 wiel

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	3	0	0	3	0	3	0	3	3	3	0	3	0	3	3	0	3	3	0	3	3	3	0	3
0	2	2	2	0	2	0	0	0	0	2	2	0	0	2	2	0	2	1	0	1	2	0	2	0
1	0	1	1	0	1	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	1	1	0
1	4	2	2	3	2	3	1	3	4	4	2	4	0	4	4	1	4	4	1	4	4	4	2	3
0	0	3	0	3	0	3	3	3	0	3	0	3	3	0	3	3	0	3	3	3	0	3	0	0
0	2	2	2	0	2	0	0	0	0	2	2	0	0	2	2	0	2	1	0	1	2	0	2	0
1	1	0	1	1	0	1	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	1	1
1	2	4	2	4	2	4	3	4	0	4	2	4	4	2	4	4	2	4	3	4	2	4	2	1
3	0	3	0	3	3	3	0	3	0	3	3	0	3	3	0	3	3	3	0	3	0	0	3	0
0	2	2	2	0	2	0	0	0	0	2	2	0	0	2	2	0	2	1	0	1	2	0	2	0
0	1	1	0	1	1	0	1	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	1
3	2	4	2	4	4	3	1	3	1	4	4	0	4	4	2	4	4	4	0	4	2	0	4	1
3	0	3	3	3	0	3	0	3	3	0	3	3	0	3	3	3	0							
0	2	2	2	0	2	0	0	0	0	2	2	0	0	2	2	0	2							
1	0	1	1	0	1	1	0	1	0	1	0	1	0	1	1	0	1							
4	2	4	4	3	2	4	0	4	3	2	4	4	0	4	4	3	2							

Analyse compleet

Stel
- geen overlap tussen ruiters
- 26+25+23+21+19+17 = 131 sleutelwaarden bekend

Gevolg: reconstructie ruiters en pinnen mogelijk

- a_i = kick 26-wiel op positie i
  b_i = kick 25-wiel op positie i
  ...
  f_i = kick 17-wiel op positie i

- totale kick op positie i is
  $a_i + b_i + c_i + d_i + e_i + f_i$

- $kick_i = a_i + b_i + c_i + d_i + e_i + f_i$
  $kick_{i+26} = a_{i+26} + b_{i+26} + c_{i+26} + d_{i+26} + e_{i+26} + f_{i+26}$
- *verschil* $\Delta_i^1 = kick_i - kick_{i+26}$
  $= (a_i - a_{i+26}) + (b_i - b_{i+26}) + \cdots + (f_i - f_{i+26})$
- voor het 26-wiel geldt $a_i = a_{i+26}$ zodat
  $\Delta_i^1 = (b_i - b_{i+26}) + \cdots + (f_i - f_{i+26})$ eliminatie 26-wiel
- idem $\Delta^2 = \Delta_i^1 - \Delta_{i+25}^1$ eliminatie 25-wiel
- $\cdots$
- $\Delta^5 = \Delta_i^4 - \Delta_{i+19}^4$ veelvouden modulo 26 van kicks 17-wiel

Berekening kicks door terugwerken van

$$\Delta^5 \rightarrow \Delta^4 \rightarrow \Delta^3 \rightarrow \Delta^2 \rightarrow \Delta^1 \rightarrow kicks$$

voorbeeld reconstructie van 17-wiel kicks

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Δ^5	12	0	0	14	20	4	16	20	6	8	12	20	18	14	20	4	20
Δ^4	20	0	8	0	8	12	14	8	24	14	18	6	6	12	14	24	20
Δ^3	20	6	8	20	0	6	0	20	18	20	12	12	20	6	20	6	14
Δ^2	14	0	20	0	6	6	20	20	12	6	6	0	20	0	20	12	20
Δ^1	20	0	0	0	0	6	20	0	6	0	6	0	20	0	0	6	20
kicks	0	6	0	0	6	6	0	0	6	6	6	0	0	6	0	6	0

andere oplossingen: kicks 6,12 onmogelijk, kicks 0,20 onwaarschijnlijk

Soortgelijke procedure kan worden uitgevoerd met Δ^6 als men beschikt over twee stukken *gemeenschappelijke* klaartekst

constateer aan herhaling in de 6e verschillen

13	18	18	13	3	5	13	15	..	..	..	..	..	..	..
12	17	20	25	11	4	13	18	18	13	3	5	13	15	..

- leg in diepte: $\Delta_1^5 - \Delta_2^5$ elimineert klaartekst
- reconstrueer nu het *verschil* van de twee kick reeksen
- moet bevatten $0, kick_1, -kick_2, (kick_1 - kick_2)$
- selecteer de goede oplossing