Cursus Cryptografie

Hagelin

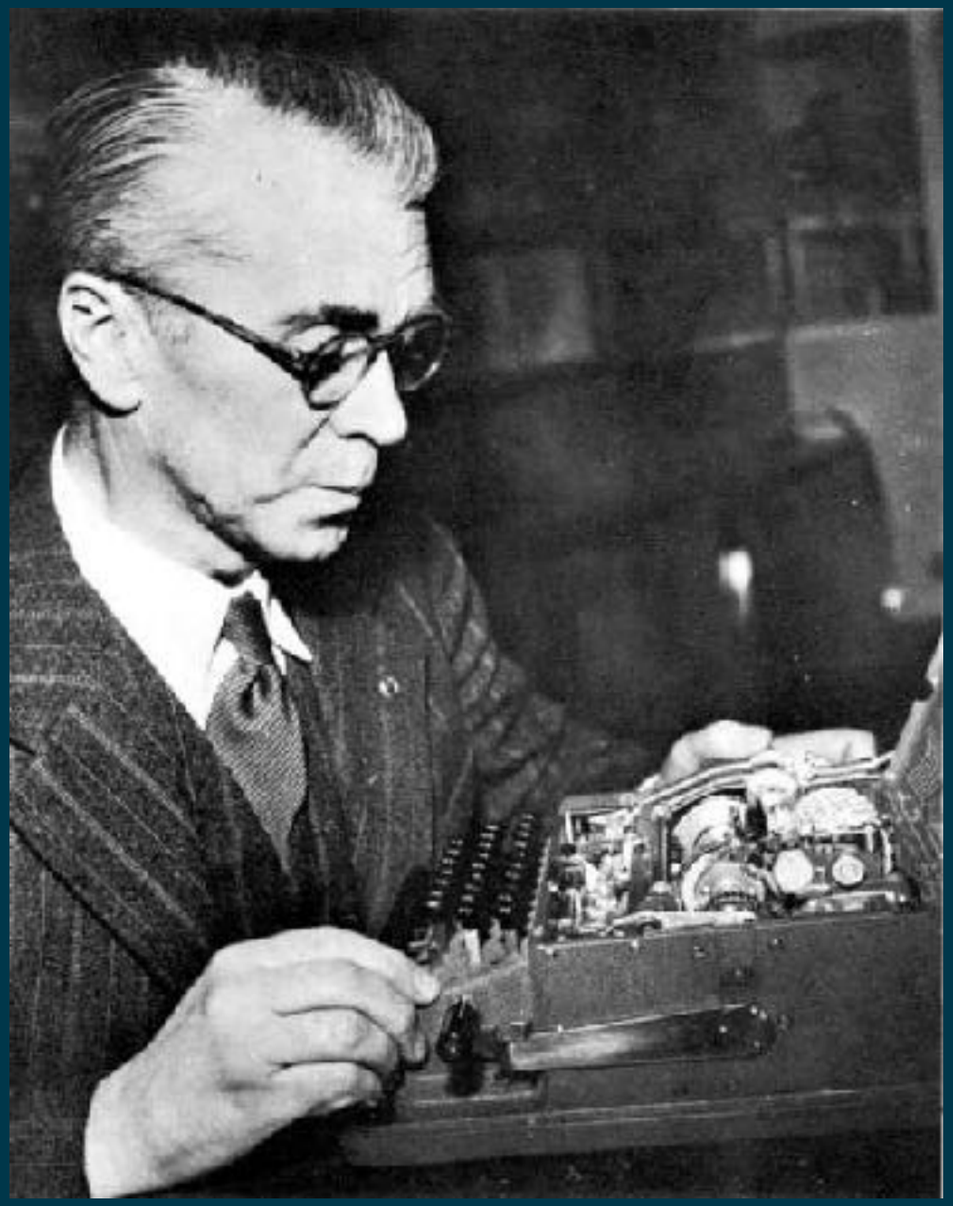
16-03-2016

Onderwerpen

- Boris Hagelin
- modellen
- werking
- cryptoanalyse
  - stagger
  - pinwielstatistiek: de practicum oefening
  - differencing

Boris Caesar Wilhelm Hagelin

- 1892–1983
  geboren in de Kaukasus
  zoon van Zweeds diplomaat
- studie werktuigbouwkunde in Sint Petersburg en Stockholm
- in 1922 voor de familie in dienst bij firma Aktiebolaget Cryptograph van Arvid Damm
- begin WW2 naar Amerika
- later Crypto Aktiengesellschaft in Zug, Zwitserland



Modellen

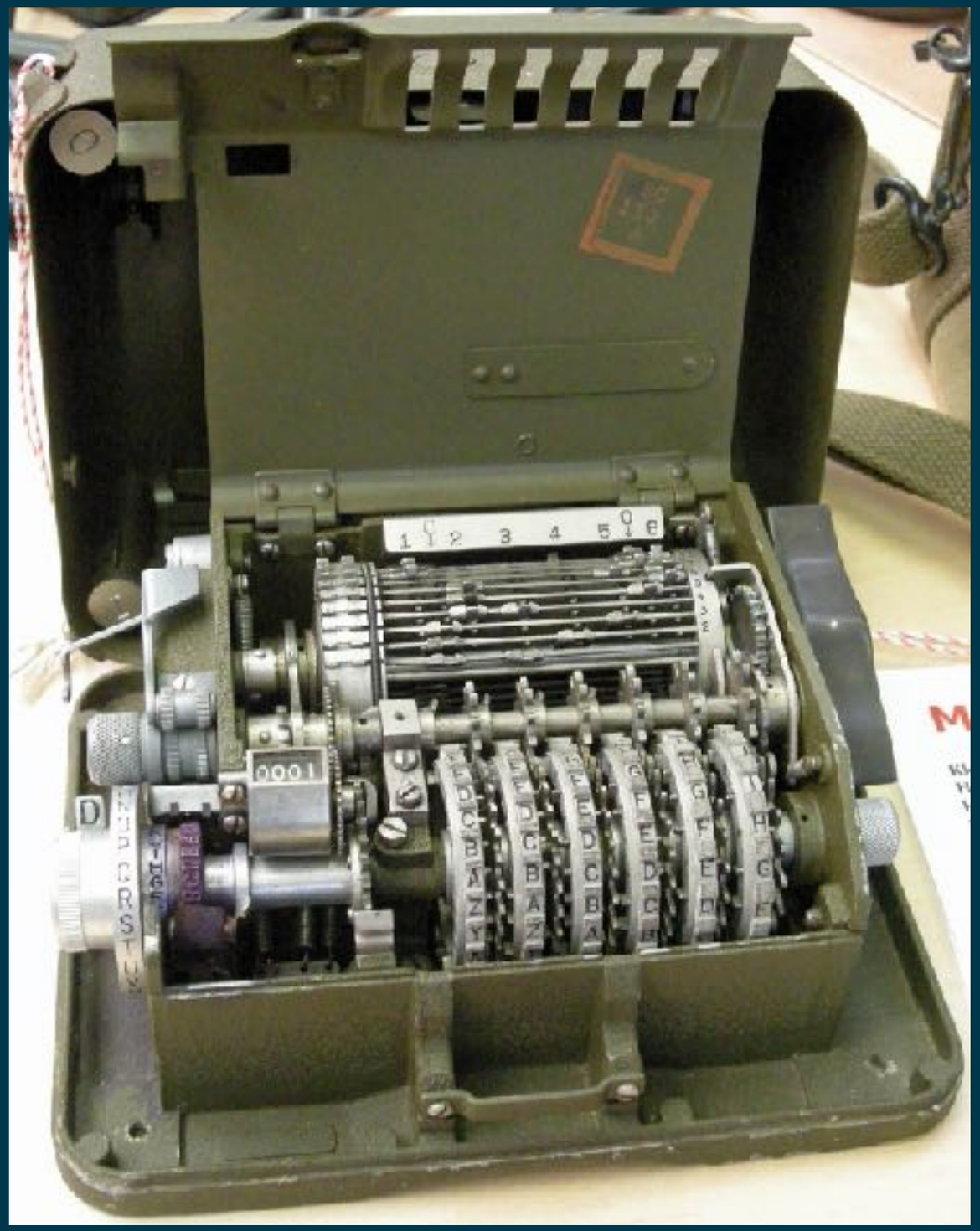
- B21 voor Zweedse leger met Damm halfrotor
- C35 eerste van de C-serie, op Frans verzoek 25,23,21,19,17 wiel, 25 lineaal 10,8,4,2,1
- C38 en voor US-Army M209 26,25,23,21,19,17 wiel, 27 linealen met 2 ruiters
- C52X permuteerbaar alfabet 47,46,43,42,41,38,34,31,29,26,25 wiel onregelmatig stappenpatroon
- CD57 40 linealen, geen overlap

Model B21

- fractionerend systeem
- gebruikt door Nederland
- 1939 Friedman cryptoanalyse: *Analysis of the Hagelin Cryptograph Type-B211*
- Joseph Petersen, vriend van Nederlandse cryptoanalist Verkuyl, geeft die publicatie aan Nederland
  NSA: “Betrayer of the Trust”

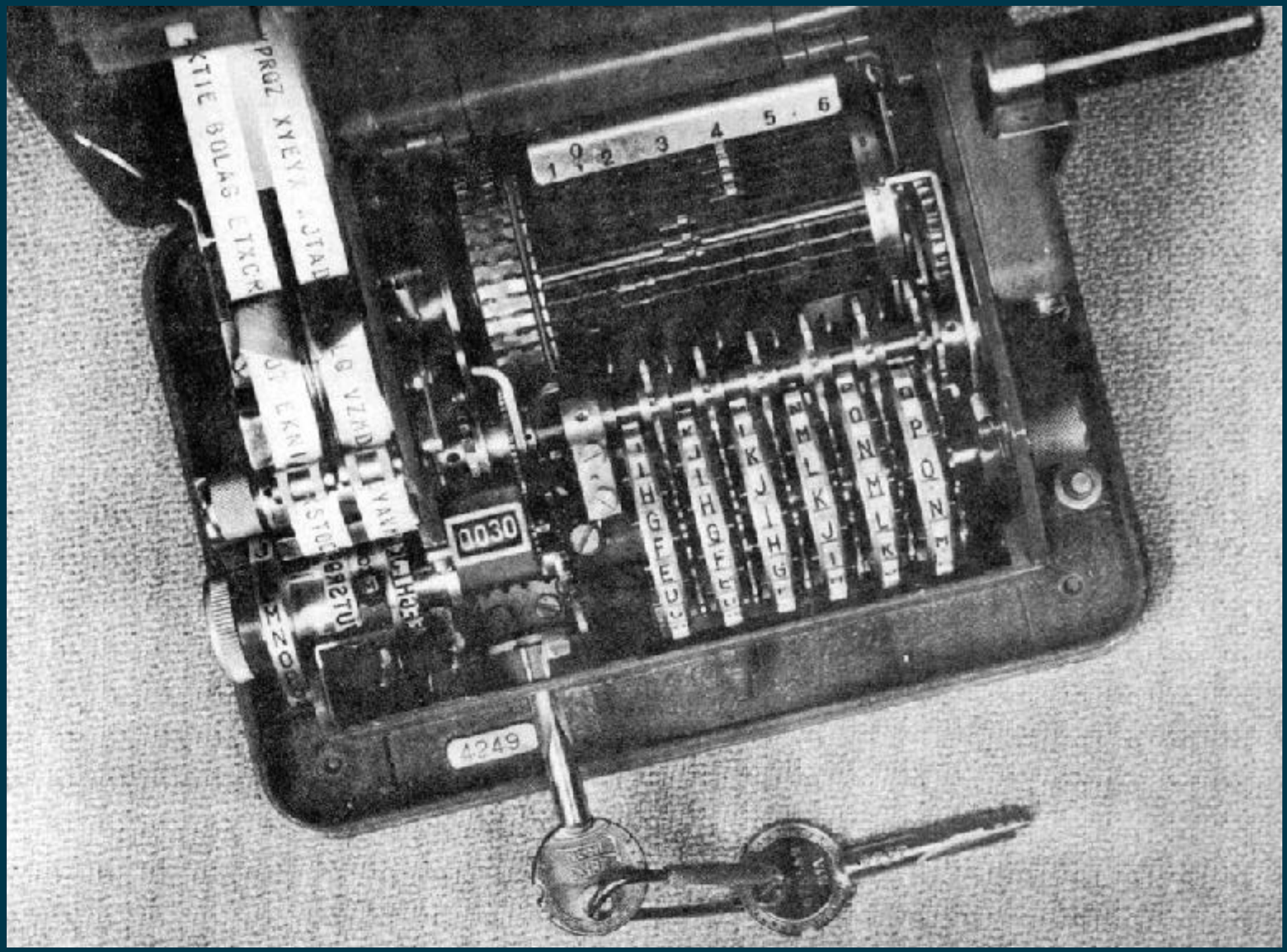
Model C52X

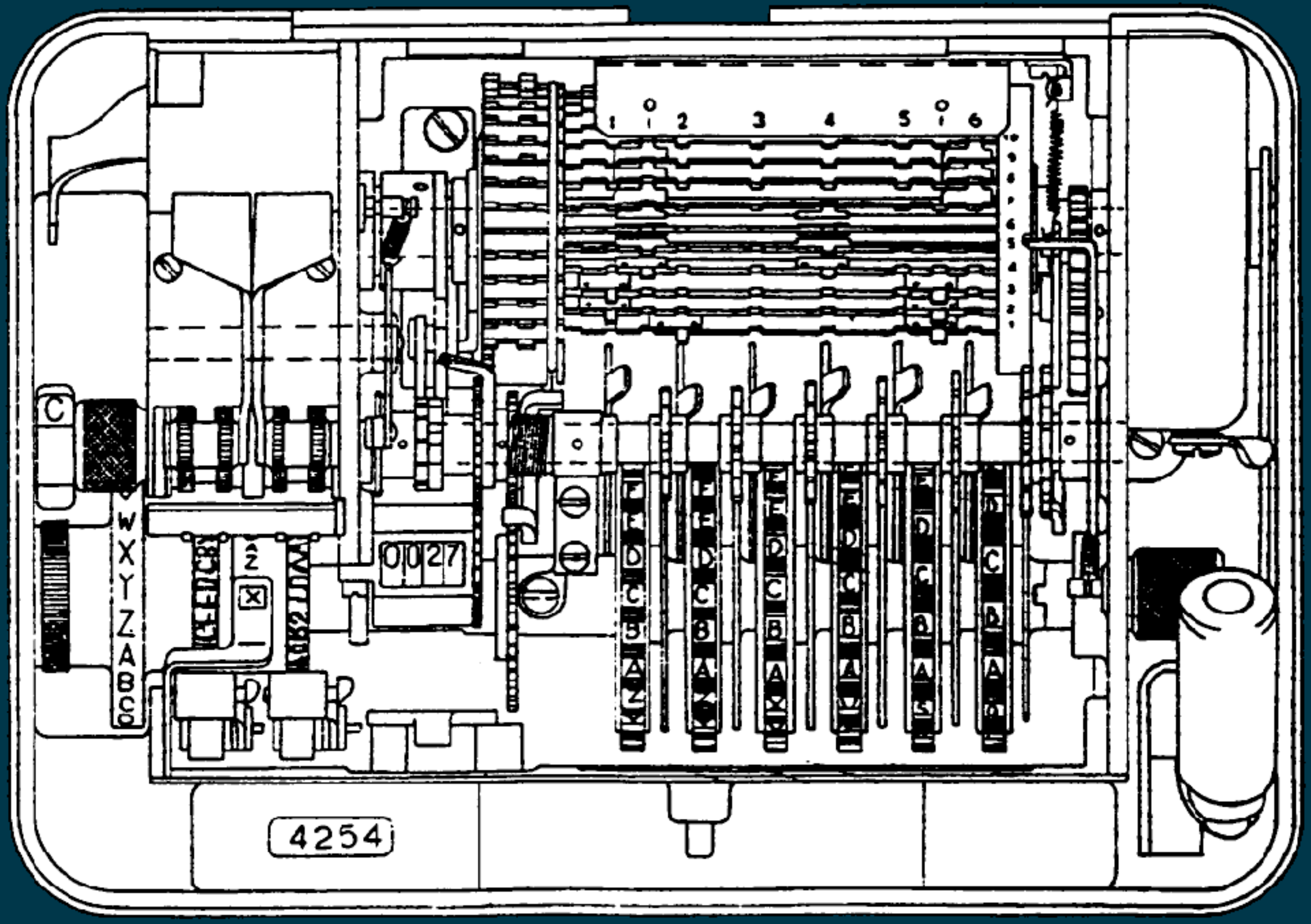
Model M209



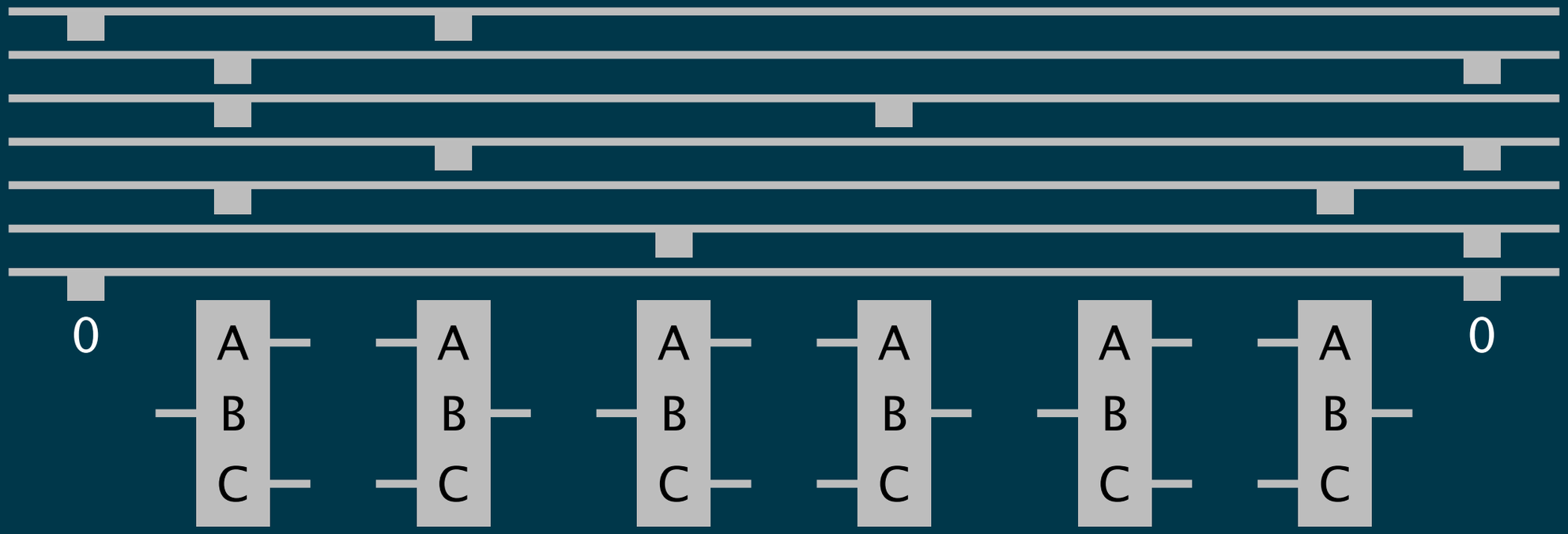
US-army divisie en lager
140.000+ gemaakt
van Operation Torch 1942
tot Koreaanse oorlog 1950-1953

Constructie M209




1
2
3
4
5
6
WXYZABC
0027
4254

Werking



- 6 wielen met resp. 26, 25, 23, 21, 19, 17 pinnen
- kooi van 27 linealen met elk 2 verplaatsbare ruiters
- aantal actieve linealen bepaalt Beaufort sleutel
  overlap telt slechts eenmaal
- alle wielen draaien 1 stap per vercijfering

Voorbeeld vercijfering

Beaufort-tabel

```
      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
   4  D 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
```

	ruiters: 17-wiel 4 19-wiel 7 21-wiel 5 overlap 17 en 19-wiel 1																							
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
17	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
19	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
21	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
kick	7	12	0	4	10	0	15	4	0	0	0	15	7	10	4	0	9	0	7	7	15	4	5	10	4
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

Parameters M209 & C38

- periode 26x25x23x21x19x17 = 101.405.850
- pinposities 26+25+23+21+19+17 = 131
- linealen 27 met 1 + 6 + 15 = 22 bezettingen
- startposities 101.405.850
- C38 slide met 26 posities, M209 heeft vaste slide A=Z
  vergelijk in syllabus Beaufort met M209-tabel !
- presentatie 5 lettergroepen Z/X = spatie
- aparte stand voor vercijferen van codegroepen

Cryptoanalyse

- analyse sleutelstroom
  - classificeer pinnen uit kick-statistiek
  - kick-verschillen als overlap afwezig
  - kick-verschillen uit gemeenschappelijke klaartekst
- sleutelstroom te vinden uit
  - known-plaintext
  - stagger
  - Kerckhoffs' superpositie
- frequentiestatistiek van de cijfertext
  - pinnen classificeren als aan/uit

Stagger - Beaufort

```
EXAMPLEOFSTAGGERS klaartekst-1
BRYGYEIRBKPITSQBD cryptogram-1

EXAMPLEOFASTAGGER klaartekst-2
BRYGYEIRBCQPZSOOE cryptogram-2
```

1. K1 is dezelfde letter als Q2
2. veronderstel K1 = A dus Q2 = A
3. sleutel voor Q2 dan Q
4. sleutel Q ontcijfert P1 = B
5. dus ook P2 = B dan sleutel Q
6. sleutel Q ontcijfert I1 = I enz.
7. goede oplossing uit Caesar shift:

```
ABIOOMZAQBCI
BCJPPNABRCDJ
     ...
STAGGERSITUA
     ...
```

Kerckhoffs' superpositie

Als cryptogrammen in diepte onder elkaar liggen
hebben letters in elke kolom dezelfde substitutie en
heeft elke kolom een *monoalfabetische* distributie

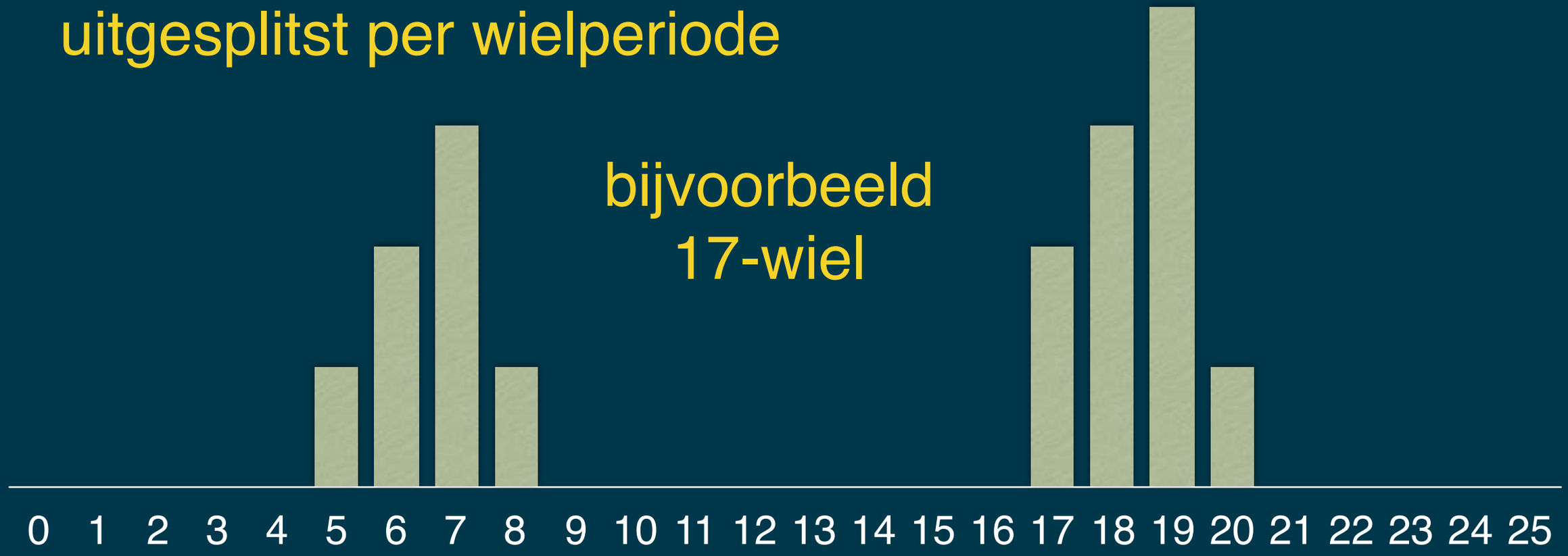
indicaties voor diepte:

- hoog aantal coïncidenties
- herhalingen van enige lengte
  vast verschil bij verschillende slide C38
- kennis van het indicatorsysteem

Oplossen van de Kerckhoffs' superpositie geeft klaartekst
dus *known-plaintext* en dus de *sleutelstroom*

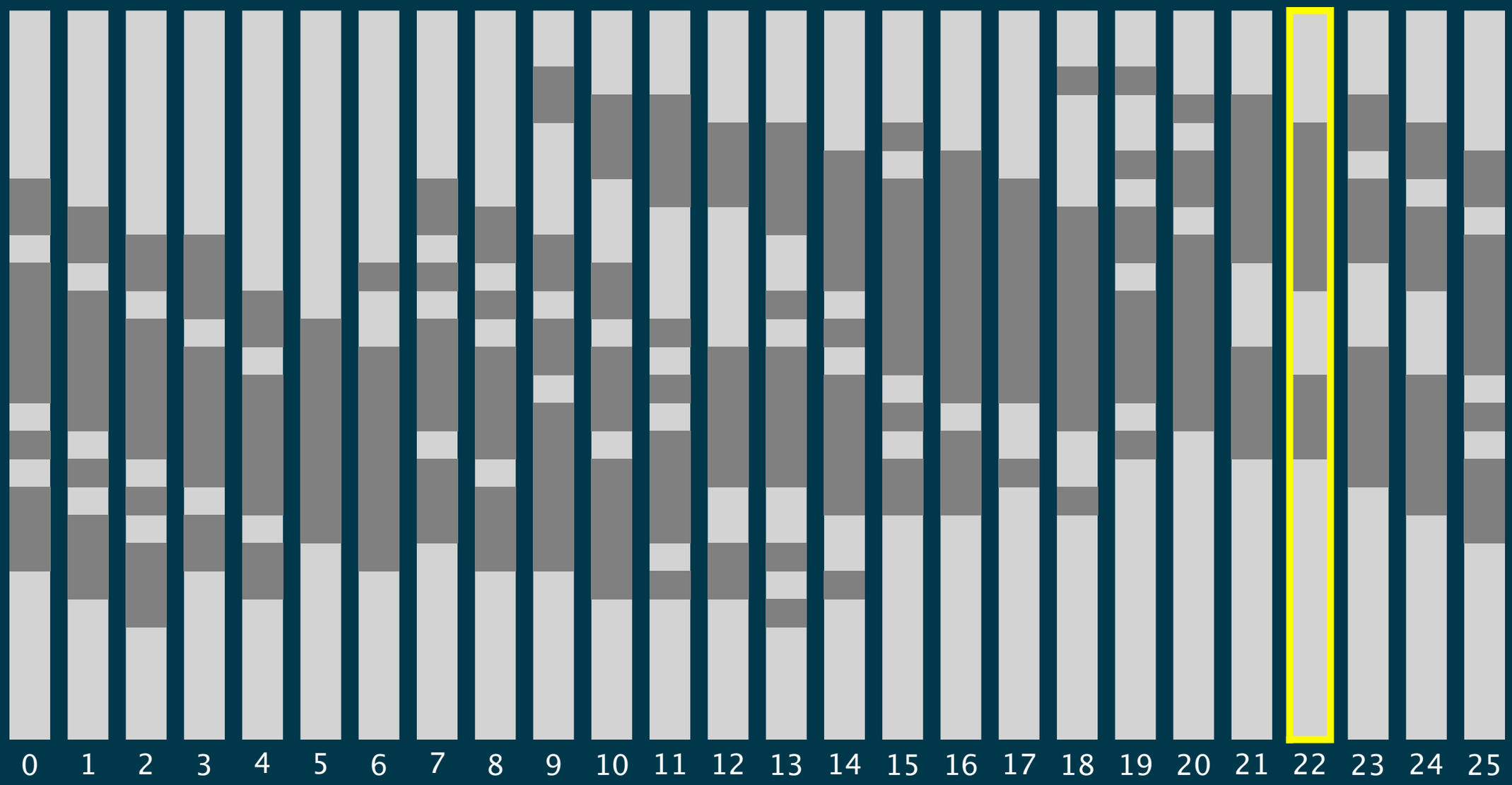
Bimodale pinstatistiek

aantal van elke gemiddelde kick
uitgesplitst per wielperiode



Links wielen met inactieve pin, rechts met actieve pin

Bepaling slide



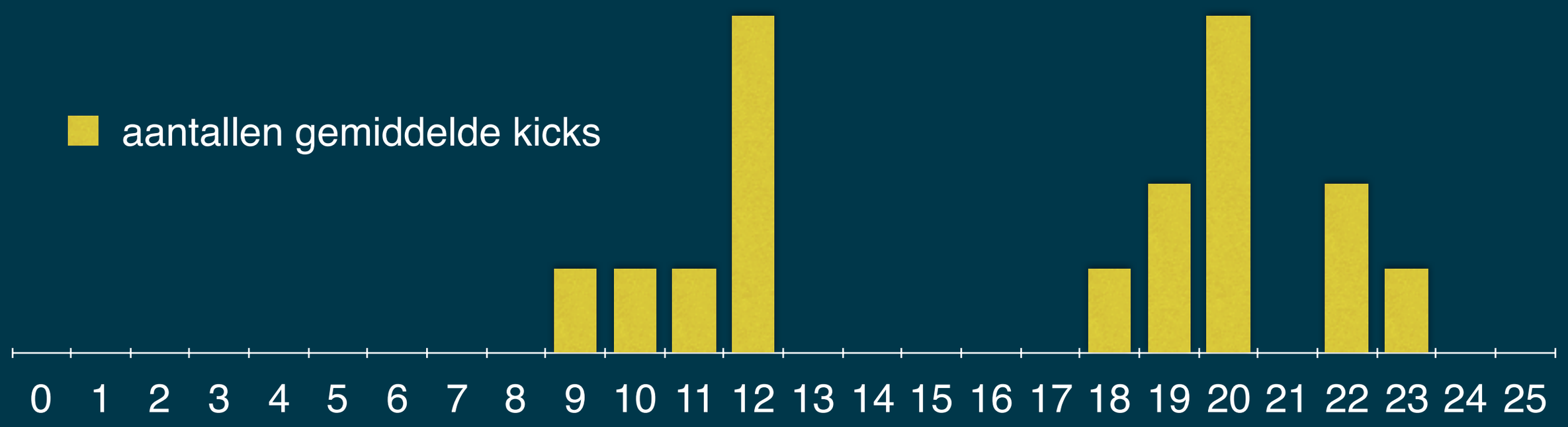
verkeerde slide → uitgesmeerde pinstatistiek

17-wiel

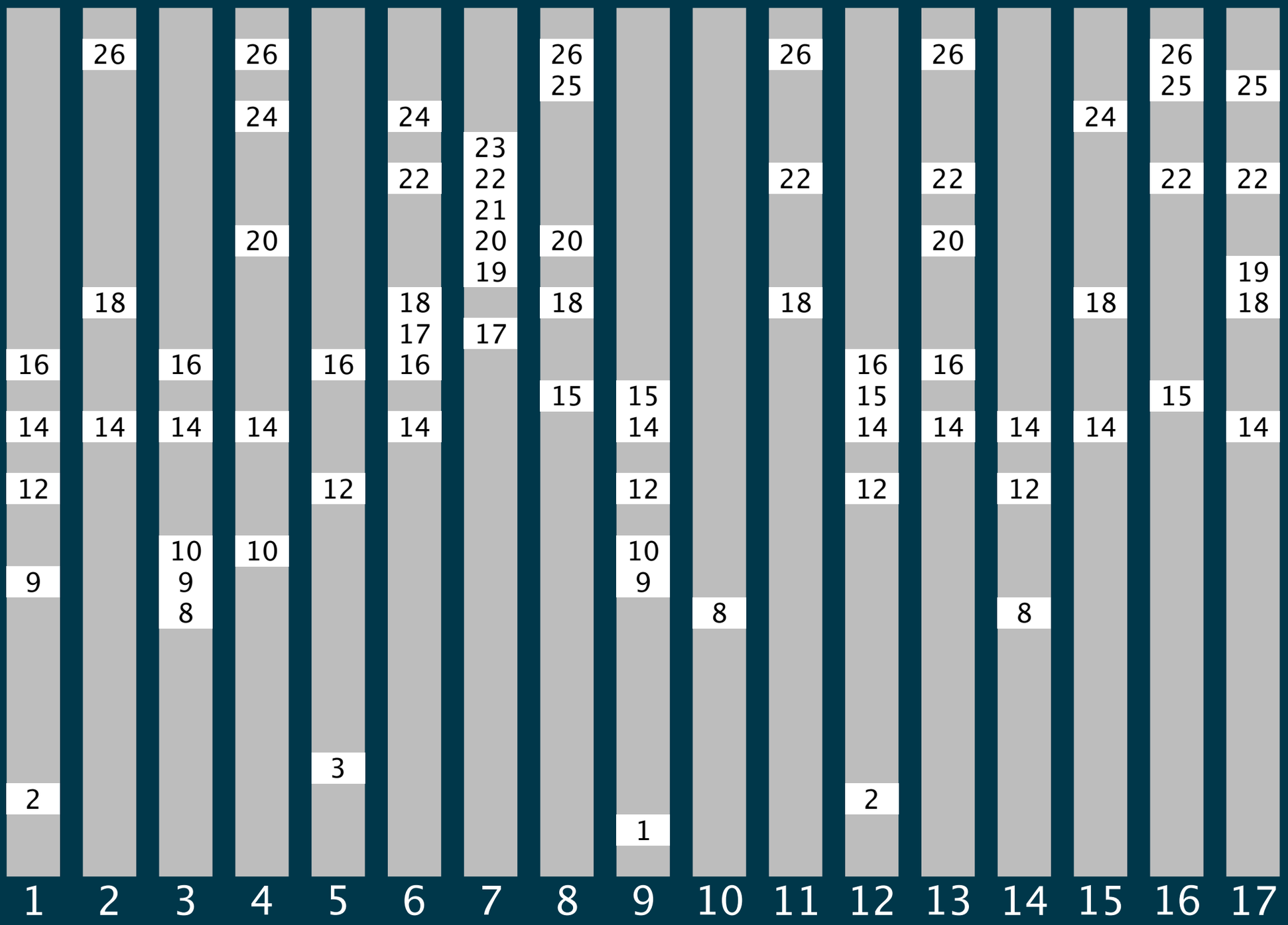
pinpositie	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
kick	9	18	10	24	3	24	21	15	15	12	18	14	14	12	14	26	19
kick	16	18	14	26	12	18	20	25	1	14	26	2	26	14	14	25	14
kick	12	14	14	26	12	16	22	26	10	8	21	16	16	12	24	15	22
kick	14	14	8	14	16	17	19	25	9	8	22	12	22	8	24	22	18
kick	16	18	8	20	12	14	23	18	10	8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

0 of 26

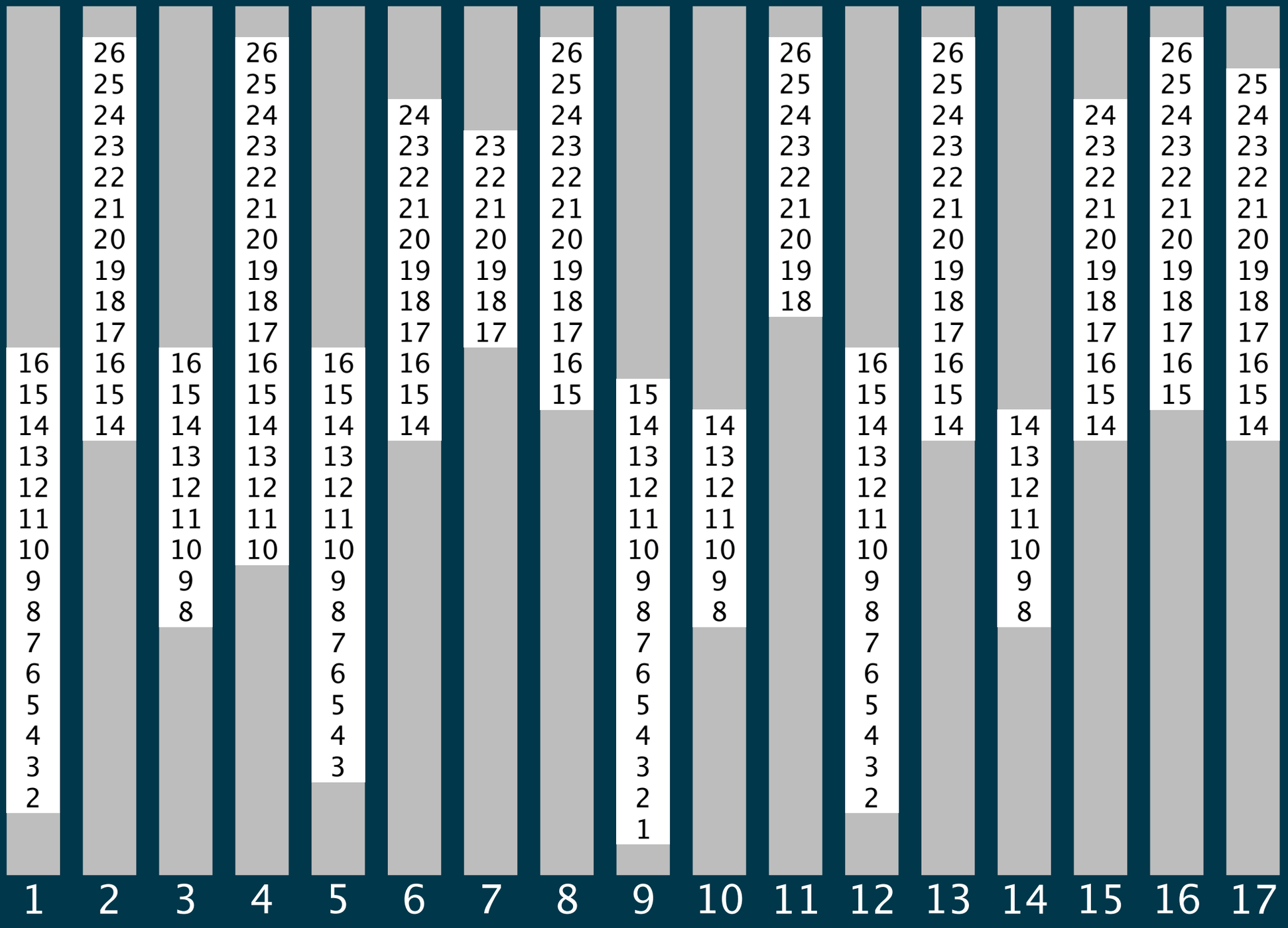
1 of 27



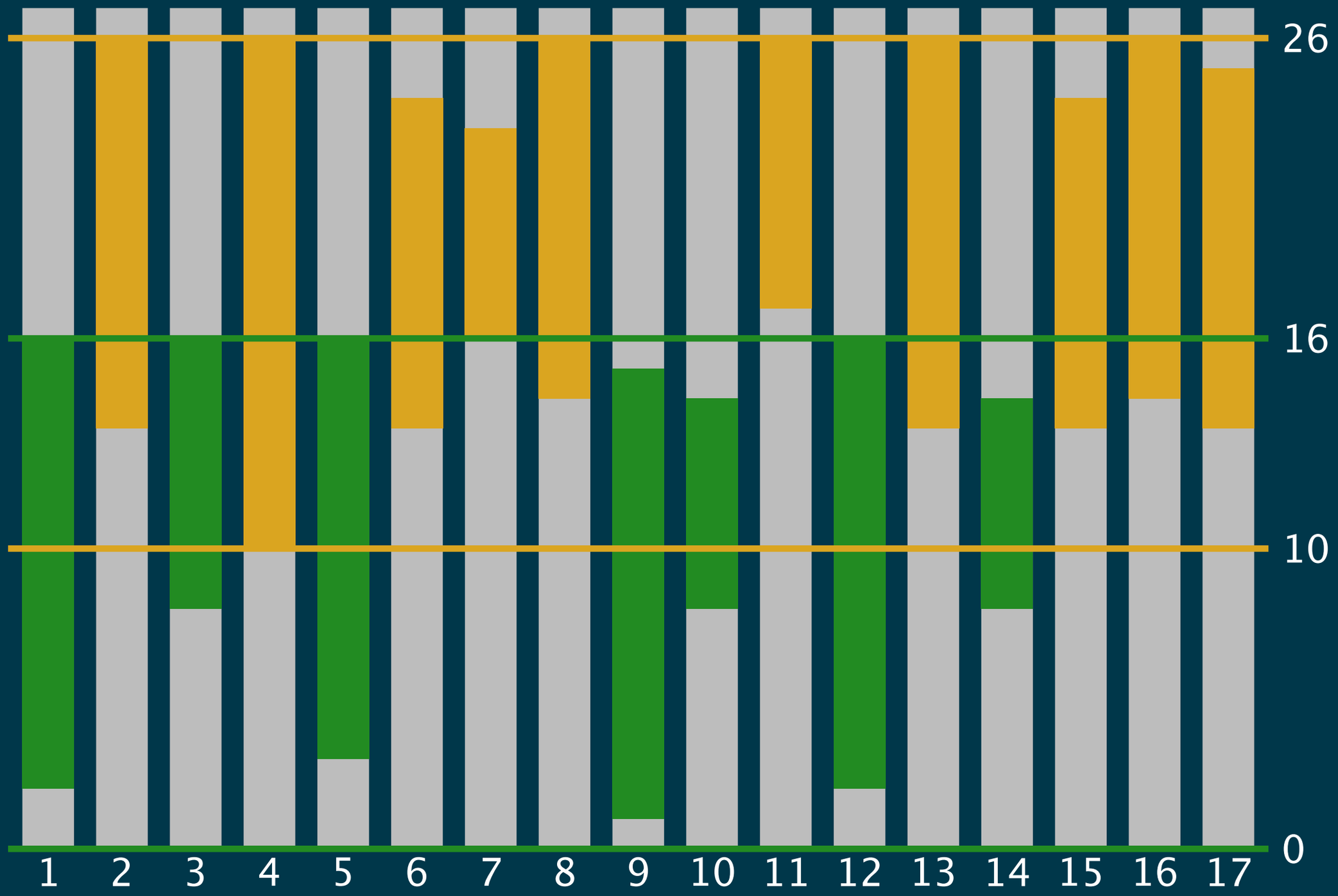
Kicks per pin



Kicks range

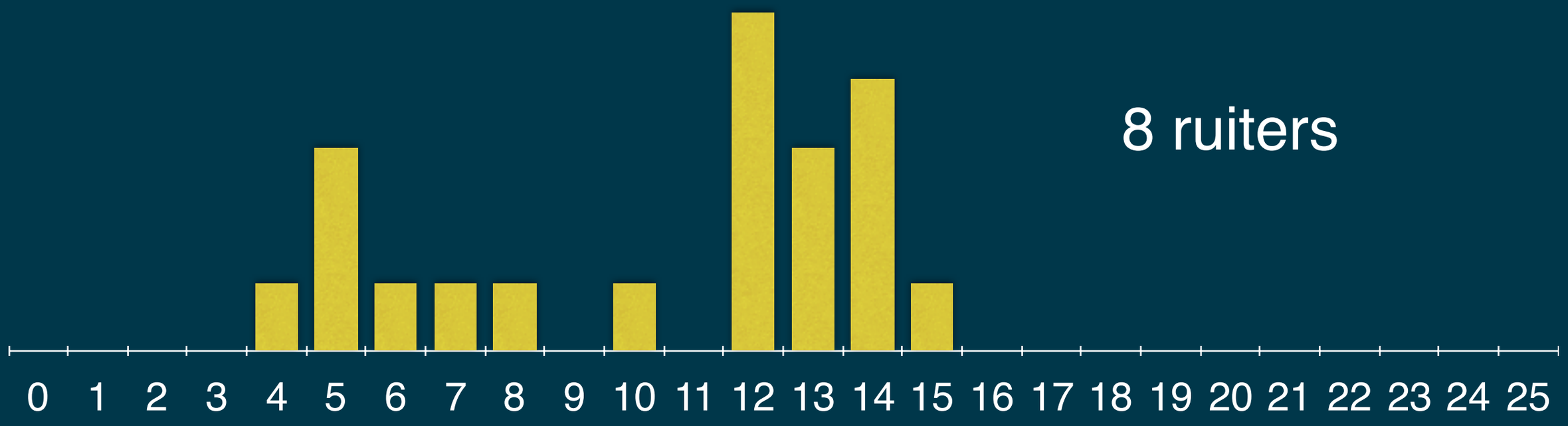

1: 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2
2: 26 25 24 23 22 21 20 19 18 17 16 15 14
3: 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8
4: 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10
5: 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3
6: 24 23 22 21 20 19 18 17 16 15 14
7: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

Pinnen en 10 ruiters



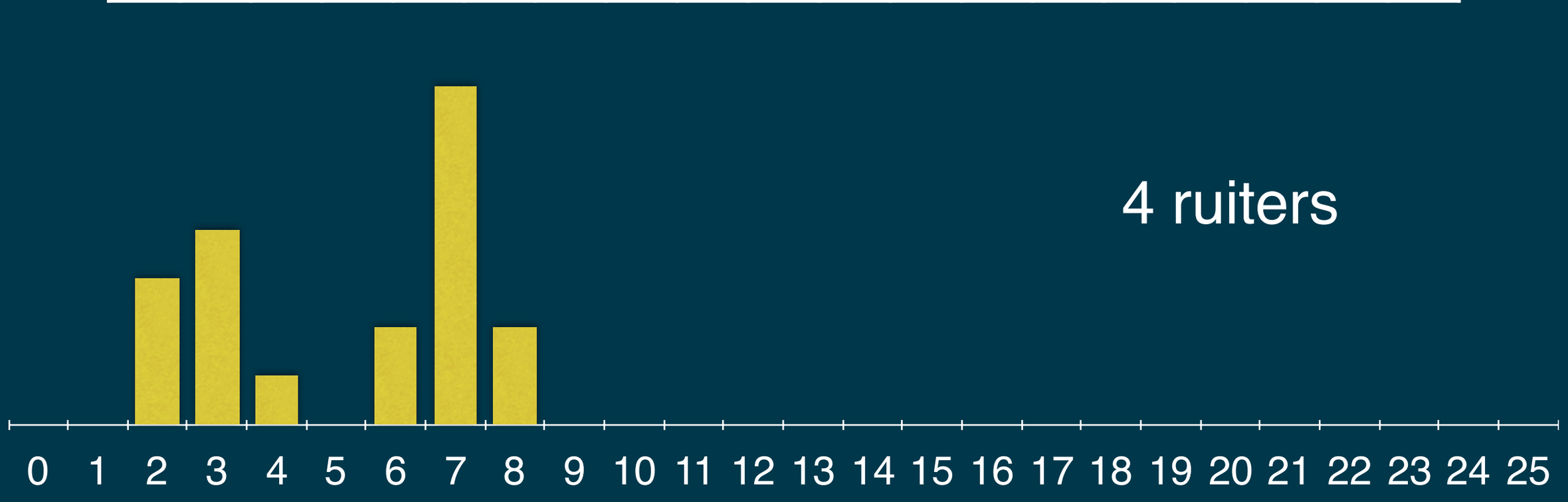
21-wiel na aftrek 17-wiel

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												
8	0	8	8	0	8	8	0	8	8	0	8	0	8	0	8	8	8	0	8	8



19-wiel na aftrek 21-wiel

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	4	0	4	0	4	0	4	4	0	4	4	0	4	0	4	0	4	4



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							

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							

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							

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							

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							

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							

Differencing

Geen overlap tussen ruiters
26+25+23+21+19+17 = 131 sleutelwaarden bekend
→ reconstructie mogelijk

verschillen $kick_i$ - $kick_{i+26}$ elimineert 26-wiel
dan verschillen $kick_i$ - $kick_{i+25}$ elimineert 25-wiel
dan verschillen $kick_i$ - $kick_{i+23}$ elimineert 23-wiel
dan verschillen $kick_i$ - $kick_{i+21}$ elimineert 21-wiel
dan verschillen $kick_i$ - $kick_{i+19}$ elimineert 19-wiel

resteren veelvouden modulo 26 van 17-wiel kick
bereken daaruit 17-wiel kick

Voorbeeld 17-wiel

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Δ^{26}	12	0	0	14	20	4	16	20	6	8	12	20	18	14	20	4	20
Δ^{25}	20	0	8	0	8	12	14	8	24	14	18	6	6	12	14	24	20
Δ^{23}	20	6	8	20	0	6	0	20	18	20	12	12	20	6	20	6	14
Δ^{21}	14	0	20	0	6	6	20	20	12	6	6	0	20	0	20	12	20
Δ^{19}	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

kicks 6+12 onmogelijk en kicks 0 of 20 onwaarschijnlijk

Klaartekst eliminatie

Δ^{26} t/m Δ^{17} → verschillen klaartekst															
..	13	18	18	13	3	5	13	15	..						
..	12	17	20	25	11	14	13	18	18	13	3	5	13	15	..

- bepaal de herhaling en leg in diepte
- verschillen in diepte elimineert de klaartekst
- reconstrueer kick-verschillen tot
  0, kick1, -kick2, kick1-kick2
- selecteer hieruit de goede oplossing