How the Dutch broke the Japanese Blue Code in the late 1930s

Joost Rijneveld

Supervisor:
Bart Jacobs

Radboud University Nijmegen

Historic context (1933-1938)

Japanese expansionism, threatened Dutch Indies
(Second Sino-Japanese war, 1937)

Johannes Frans Willem Nuboer

Set up *Department 1: Intelligence* in Batavia

Filed monthly reports on gathered intelligence
- Press information, diplomatic intel
- Photographs of Japanese ships
- **Naval telegrams**

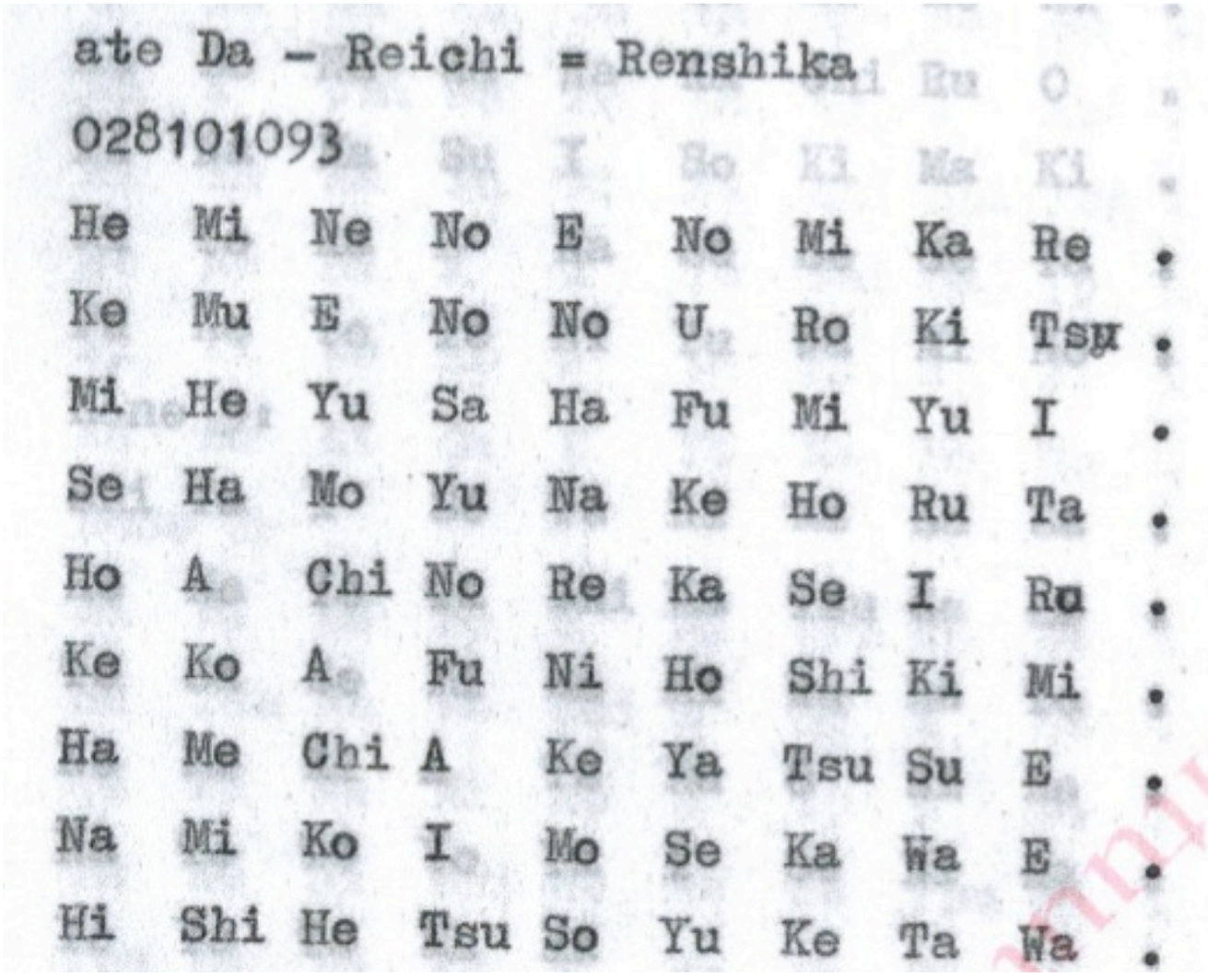
Memoirs and notes of Nuboer form the basis of the material for this thesis

Research Question

How did the Japanese naval crypto-systems work, and how were the cryptographers of the Dutch Indies Navy able to break the systems?

Japanese telegrams

44-symbol Kana alphabet (using Wabun Morse code)

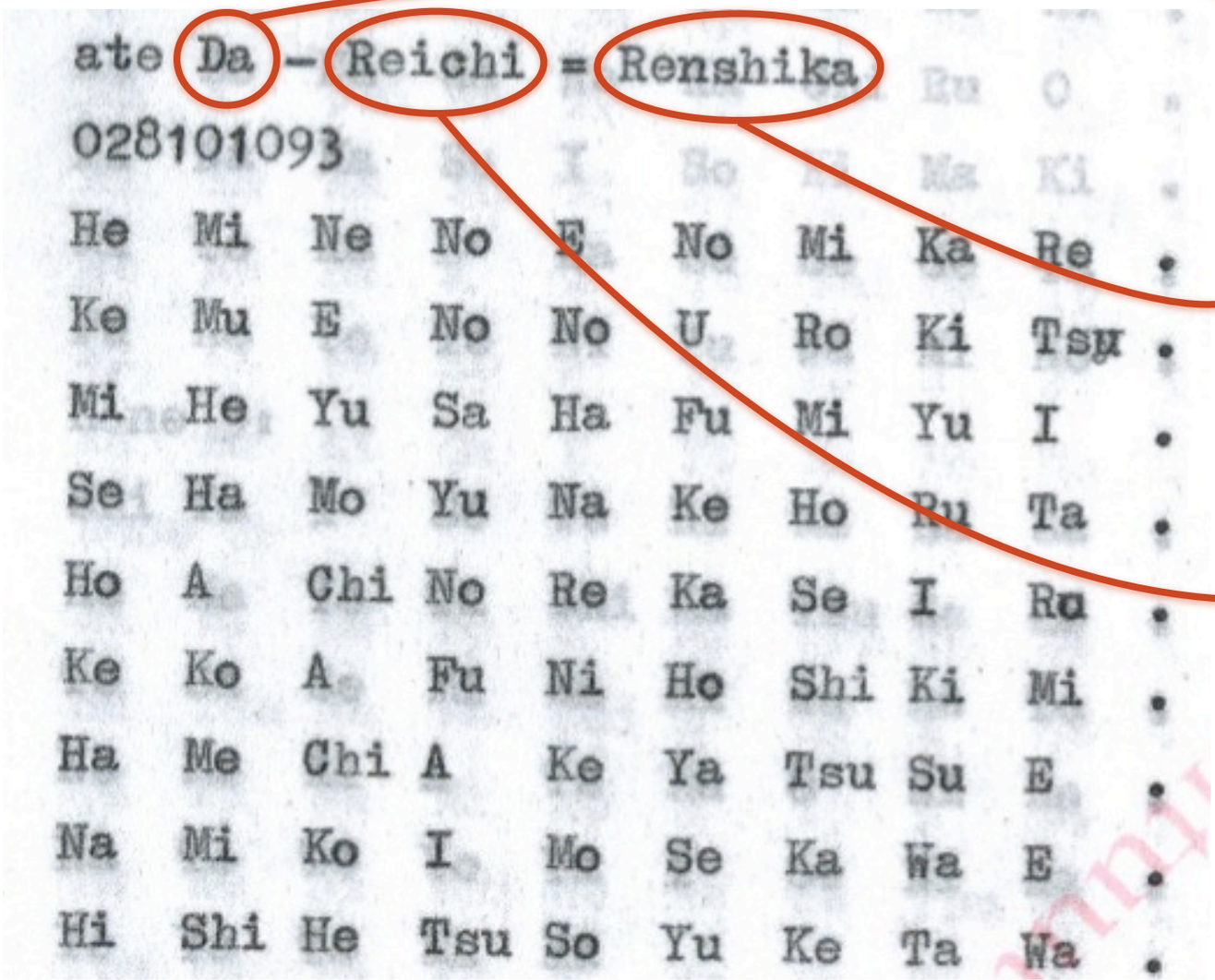


ate Da - Reichi = Renshika
028101093

He	Mi	Ne	No	E	No	Mi	Ka	Re	.
Ke	Mu	E	No	No	U	Ro	Ki	Tsu	.
Mi	He	Yu	Sa	Ha	Fu	Mi	Yu	I	.
Se	Ha	Mo	Yu	Na	Ke	Ho	Ru	Ta	.
Ho	A	Chi	No	Re	Ka	Se	I	Ru	.
Ke	Ko	A	Fu	Ni	Ho	Shi	Ki	Mi	.
Ha	Me	Chi	A	Ke	Ya	Tsu	Su	E	.
Na	Mi	Ko	I	Mo	Se	Ka	Wa	E	.
Hi	Shi	He	Tsu	So	Yu	Ke	Ta	Wa	.

Japanese telegrams

44-symbol Kana alphabet (using Wabun Morse code)


ate Da - Reichi = Renshika
028101093
He Mi Ne No E No Mi Ka Re .
Ke Mu E No No U Ro Ki Tsu .
Mi He Yu Sa Ha Fu Mi Yu I .
Se Ha Mo Yu Na Ke Ho Ru Ta .
Ho A Chi No Re Ka Se I Ru .
Ke Ko A Fu Ni Ho Shi Ki Mi .
Ha Me Chi A Ke Ya Tsu Su E .
Na Mi Ko I Mo Se Ka Wa E .
Hi Shi He Tsu So Yu Ke Ta Wa .

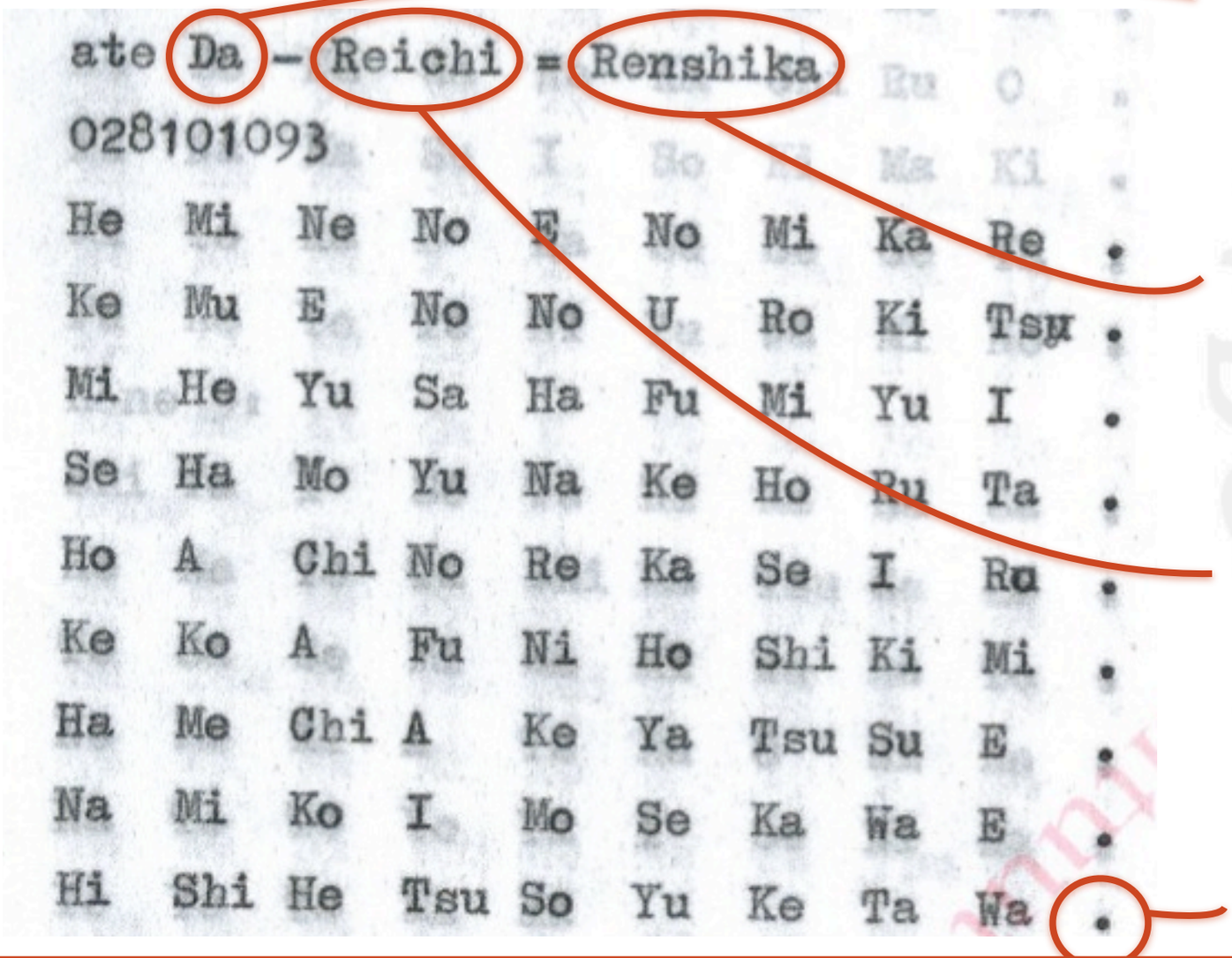
‘To’
Chief of the Naval staff

‘From’
Commander of the training squadron

‘CC’
Commander in Chief of the combined fleet

Japanese telegrams

44-symbol Kana alphabet (using Wabun Morse code)



‘To’
Chief of the Naval staff

‘From’
Commander of the training squadron

‘CC’
Commander in Chief of the combined fleet

‘.’ code

The ‘.’ codebook

Codebook cipher: one-to-one map of code strings to plaintext strings

Build up using 4 Kana-symbol code groups

Fourth symbol is a ‘checksum’, $44^3 = 85.184$ codes

```
So    Ra    To    (He)
32 + 24 + 37      = 93
(93 - 1) mod 44 = 4
```

Represents *Destroyer Minazuki*

Kure Maritime Museum

Breaking the '.' code cipher

Codebook should not be used without further encryption

'Simple' transposition cipher:
permutation of columns

Original cipher was replaced in summer 1935

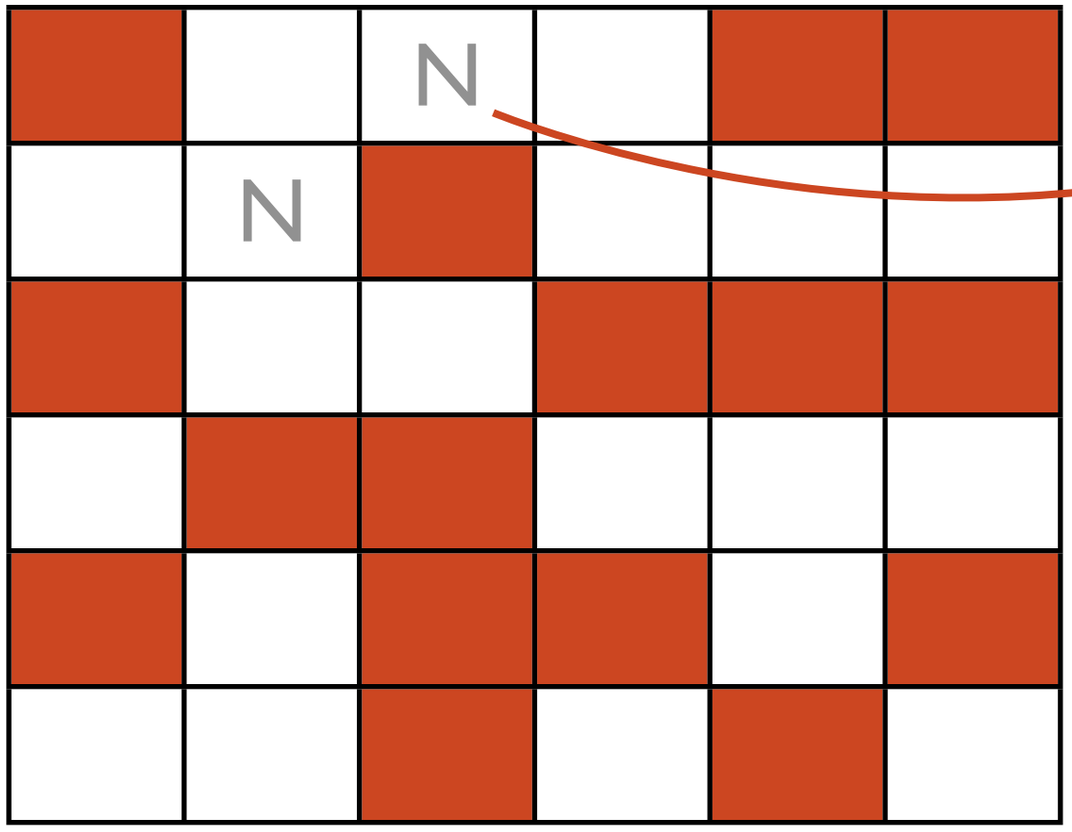
New, more complicated cipher:
complicated figure, nulls and blanks
permutation of columns
reading vertically

Keys changed often
15 permutations cycled, one per day
2 figures in use (even / odd months)

The second '.' code cipher

Plaintext: *Two can keep a secret if one is dead*

Permutation: `2-5-1-6-3-4`



The second '.' code cipher

Plaintext: *Two can keep a secret if one is dead*

Permutation: `2–5–1–6–3–4`

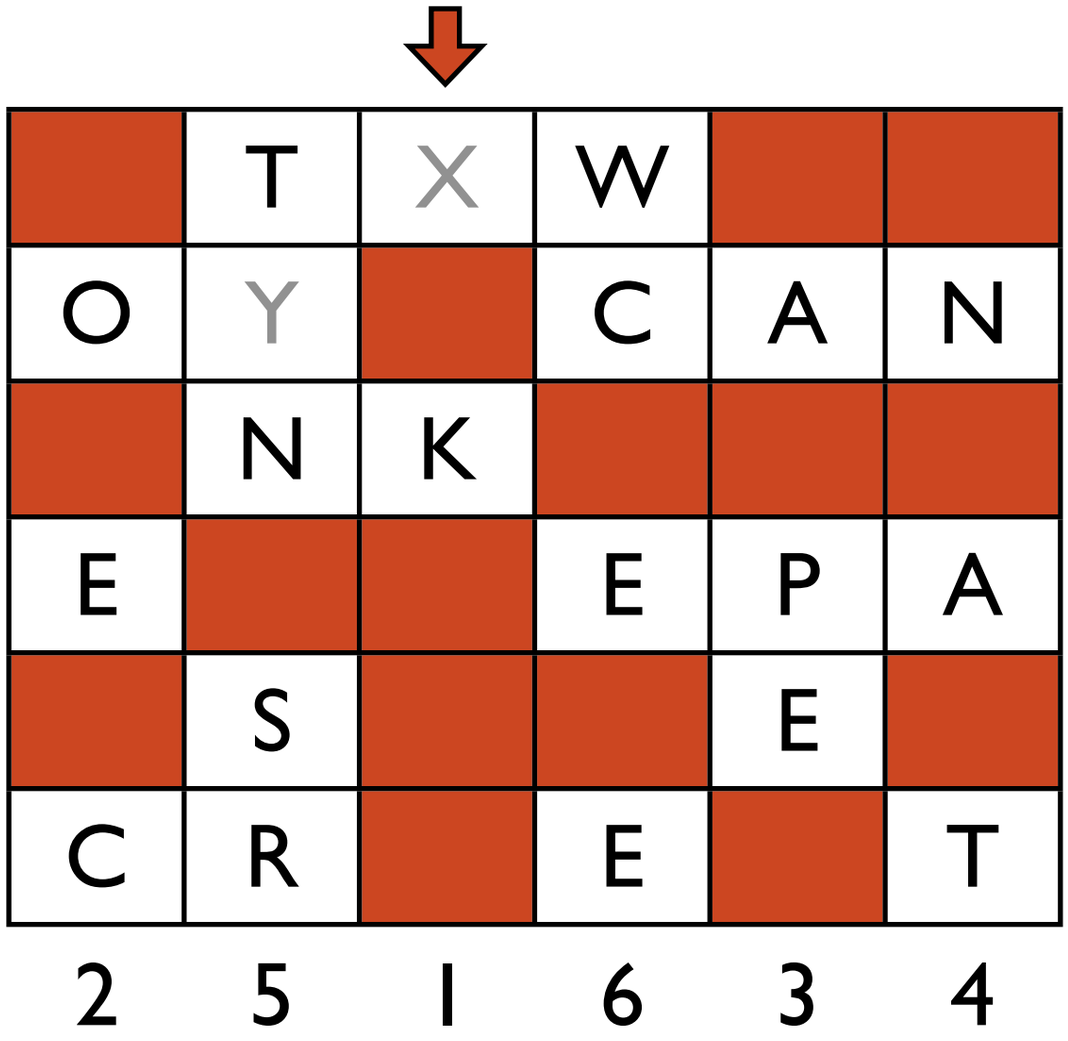
	T	N	W		
O	N		C	A	N
	N	K			
E			E	P	A
	S			E	
C	R		E		T

	I	N	F		
O	N		N	E	I
	S	D			
E			A	D	

The second '.' code cipher

	T	X	W		
O	Y		C	A	N
	N	K			
E			E	P	A
	S			E	
C	R		E		T
2	5	1	6	3	4

The second '.' code cipher



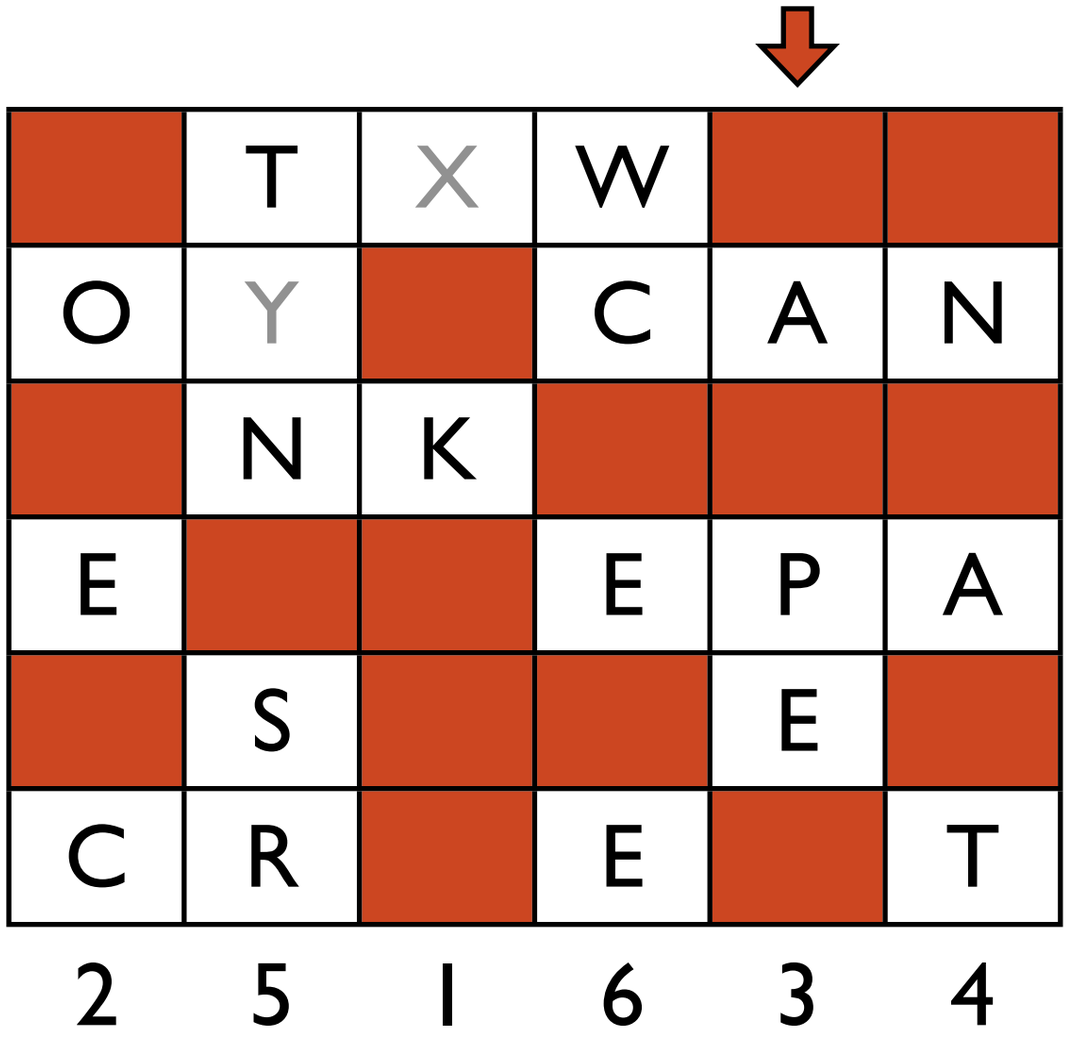
XK

The second '.' code cipher

	T	X	W		
O	Y		C	A	N
	N	K			
E			E	P	A
	S			E	
C	R		E		T
2	5	1	6	3	4

XK OEC

The second '.' code cipher



XK OEC APE

The second '.' code cipher

	T	X	W		
O	Y		C	A	N
	N	K			
E			E	P	A
	S			E	
C	R		E		T
2	5	1	6	3	4

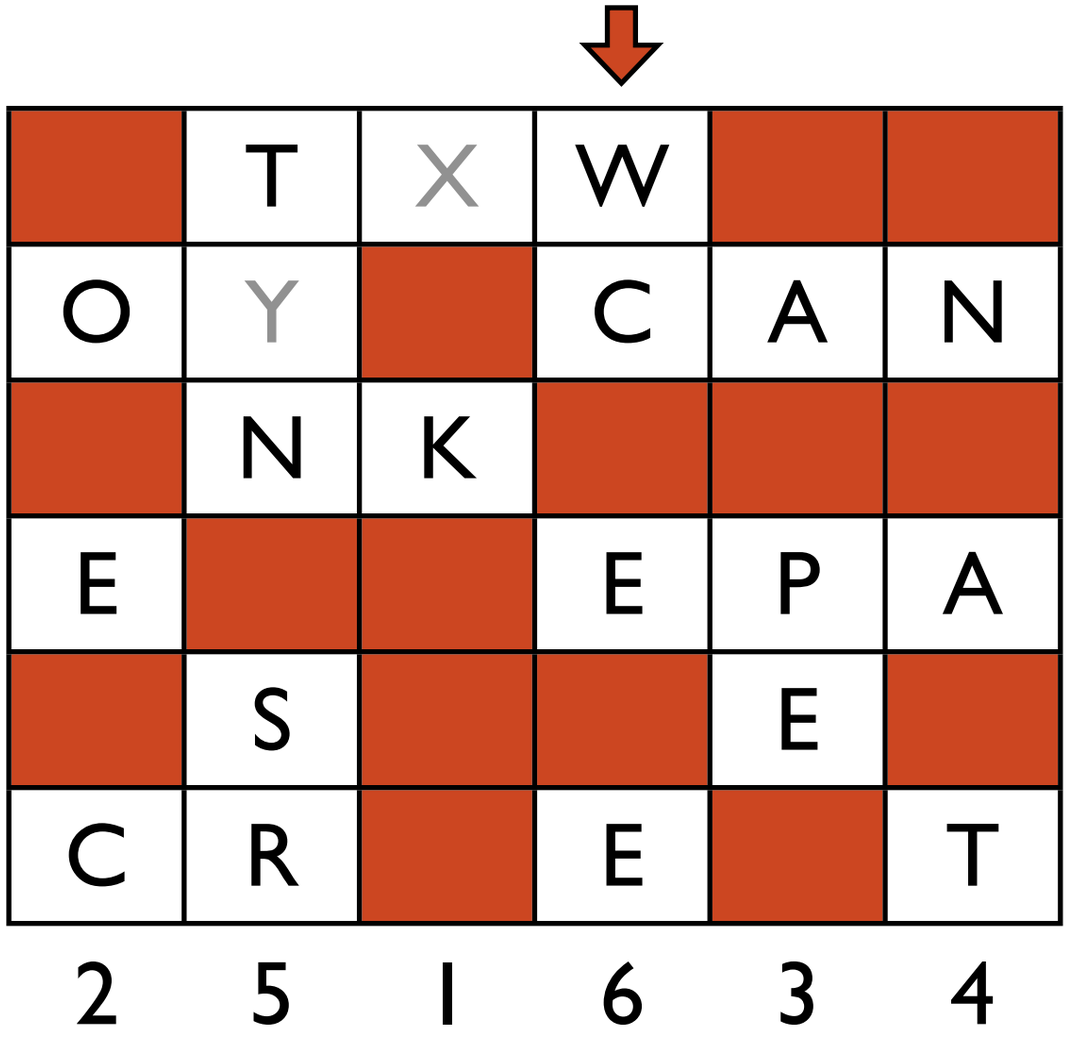
XK OEC APE NAT

The second '.' code cipher

	T	X	W		
O	Y		C	A	N
	N	K			
E			E	P	A
	S			E	
C	R		E		T
2	5	1	6	3	4

XK OEC APE NAT TYNSR

The second '.' code cipher



XK OEC APE NAT TYNSR WCEE

Ciphertext:
XKOECAPENATTYNSRWCEE

Decryption is analogous, but leave out X and Y

Breaking the second ‘.’ code cipher

Finding the figure is *really, really difficult!*

Breaking the second '.' code cipher

Step 1: Finding the separated columns in the ciphertext

0082:	Ho	Ru	Na	Re	A	He	Wi	U	Ta	Ta	Mu	Ri	Wi	Mo	Ma	Ra	Ku	No	Ni	U
0083:	Mo	Ke	Na	Sa	A	E	Wi	Na	Wi	Wi	Te	Shi	Su	Tsu	U	A	Ni	Ku	Ki	Yo
0075:	Ho	Ho	Ru	Wi	So	A	Ku	He	Te	Yo	Wi	To	Na	No	Ra	So	A	I	Na	Ko
0077:	Ho	Ma	Na	Ni	So	E	He	Tsu	Na	Yo	Wi	To	O	No	He	Ri	E	I	Ne	Ko
0078:	Ho	Ku	Na	Sa	Sa	E	E	Tsu	Na	Yo	Wi	Tsu	I	No	Ra	Ke	E	A	O	Ko
0081:	Ho	Wi	Ra	Sa	Sa	A	E	Tsu	Na	U	Wi	Ya	Mi	Ri	Ra	So	A	Ko	O	Ku
0076:	Ho	To	Na	Sa	Ta	Sa	A	Ku	Tsu	Na	Yo	Wi	Ya	Wi	Chi	No	He	U	A	Ko
0079:	Ho	Wi	Na	Sa	Wi	So	E	E	Ra	Na	Yo	Wi	Ni	Chi	Re	No	He	O	A	Ne
0084:	Mo	Te	Ta	Sa	Ma	So	A	E	Tsu	Na	Wi	Wi	He	Chi	Ho	Su	He	Ru	A	I

Table 6.3: Connecting identical symbols. Completed in appendix G

Breaking the second '.' code cipher

Step 2: Finding the permutation

0082:	Ho	Ru	Na	Re	A	He	Wi	U	Ta	Ta	Mu	Ri	Wi	Mo	Ma	Ra	Ku	No	Ni	U
0083:	Mo	Ke	Na	Sa	A	E	Wi	Na	Wi	Wi	Te	Shi	Su	Tsu	U	A	Ni	Ku	Ki	Yo
0075:	Ho	Ho	Ru	Wi	So	A	Ku	He	Te	Yo	Wi	To	Na	No	Ra	So	A	I	Na	Ko
0077:	Ho	Ma	Na	Ni	So	E	He	Tsu	Na	Yo	Wi	To	O	No	He	Ri	E	I	Ne	Ko
0078:	Ho	Ku	Na	Sa	Sa	E	E	Tsu	Na	Yo	Wi	Tsu	I	No	Ra	Ke	E	A	O	Ko
0081:	Ho	Wi	Ra	Sa	Sa	A	E	Tsu	Na	U	Wi	Ya	Mi	Ri	Ra	So	A	Ko	O	Ku
0076:	Ho	To	Na	Sa	Ta	Sa	A	Ku	Tsu	Na	Yo	Wi	Ya	Wi	Chi	No	He	U	A	Ko
0079:	Ho	Wi	Na	Sa	Wi	So	E	E	Ra	Na	Yo	Wi	Ni	Chi	Re	No	He	O	A	Ne
0084:	Mo	Te	Ta	Sa	Ma	So	A	E	Tsu	Na	Wi	Wi	He	Chi	Ho	Su	He	Ru	A	I

Table 6.4: Marking appended symbols. Completed in appendix G

Form code groups with the appended symbols

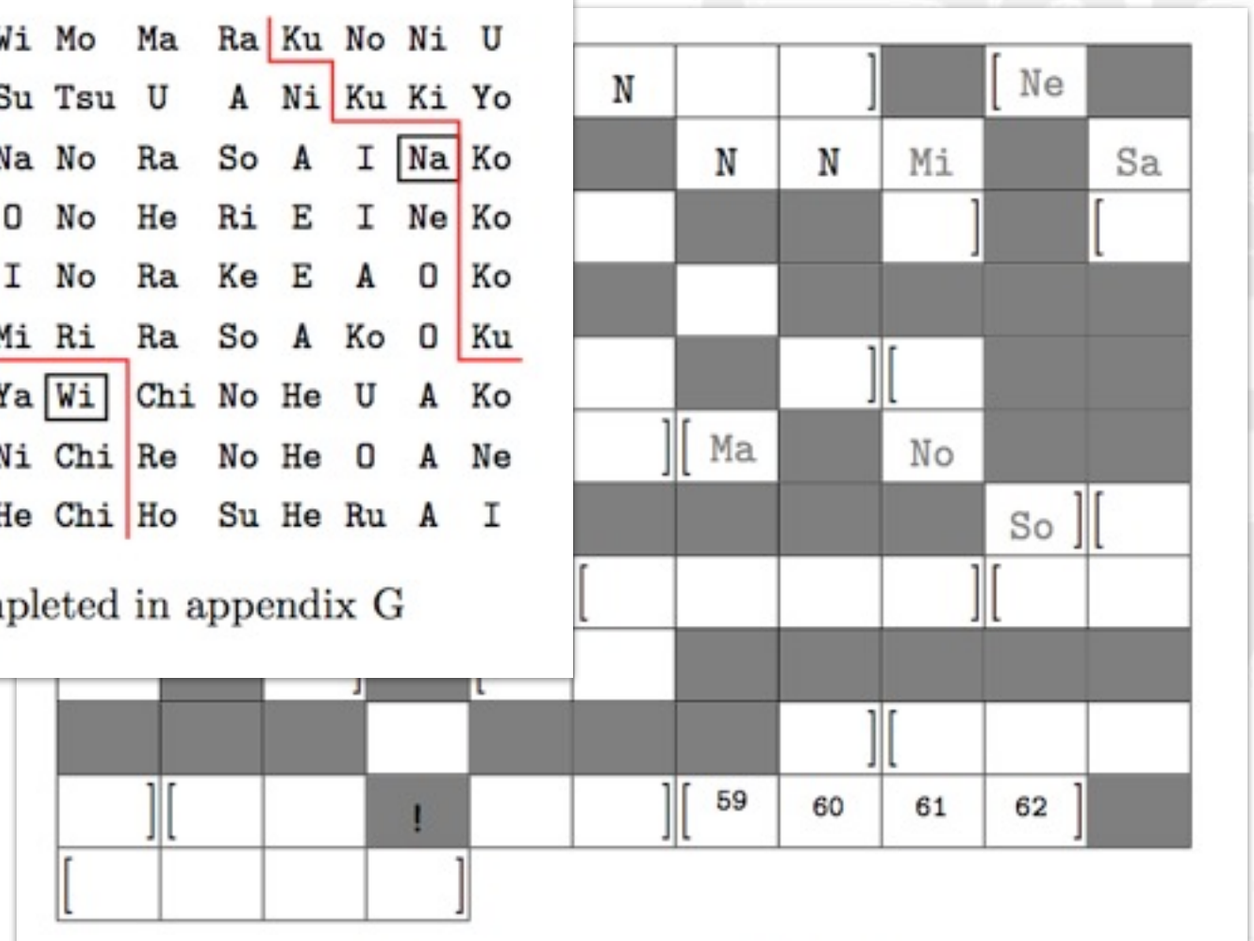


Table 6.6: Encryption figure (November 1935)

Breaking the second '.' code cipher

Step 3: Finding the figure

10	8	6	7	2	9	5	1	3	11	4
Ru	Mu	Mi	Ne	Sa	I	Ko	Ho	Yo	Re	Chi
Yo	Ko	Ri	So	A	Ne	Ku	To	Wi	Mi	No
Ro	Na	A	He	Ku	Yu	To	Na	Ya	Ku	He
Ma	Wa	No	Wi	Tsu	Ha	A	Sa	Wi	Tsu	U
Ha	Ke	No	Na	Na	No	Wa	Ta		Ki	A
He	Wi	He			Na	Ma			A	Ko
		No			Ru	Ra			No	Ne

Table 6.5: Telegram 0076 in re-ordered columns

Breaking the second ‘.’ code cipher

Finding a new permutation is still difficult, but *much easier*

(recall: this permutation changed *every day*)

Breaking the second '.' code cipher

Step 1: locate a common code group: `Mi I Wa (Na)`

Ki	A	Ni	Hi	Ho	A	Ta	Na	Mi	So	Ma	Ke	Hi	Se	Hi	Re	Se	Ki
Mu	Shi	Ru	Ha	Wa	Yu	Se	Wa	Hi	Na	E	A	I	Ya	Ni	Mo	O	A
E	Ku	Me	Shi	Ma	No	Na	Tsu	E	Ya	A	Ru	So	Te	So	Sa	Na	O
Mi	Mi	Ru	A	Ya	Ra	Na	Ta	Na	Sa	Ru	Wi	Ho	Ni	Fu	Ro	Fu	Yu
Me	He	He	Mi	Ro	Shi	Se	A	A	Ri	Ma	Sa	Ho	Yo	Mo	No	I	Mo

Ri	Ni	Me	Shi	Ra	Tsu	Ri	Me	Ri	Ke	Te	Ru	Ya	Ki	Ka	Ha	Te	Mi
Ki	Me	Mi	Tsu	Ta	Me	Me	Ha	Ko	Ki	Ha	Ne	Na	Tsu	Ko	E	I	I
Ko	Tsu	Tsu	Wa	To	U	Tsu	Re	Ho	Mu	Ha	Me	Ra	Ni	I	Ra	Yu	Ma
Mo	Mo	Yo	Ru	Ne	Me	Ke	U	Re	Ka	Yo	Yu	Sa	Mo	Ho	Se	Mo	Re
Ri	Re	Na	Ru	Ho	Ho	Mo	Ma	Ki	Ka	Ho	So	Wa	Se	Hi	Ka	Ro	Ne

Table 6.12: Ninety symbol prefix of 304001200

Breaking the second '.' code cipher

Step 2: fitting the group in the figure

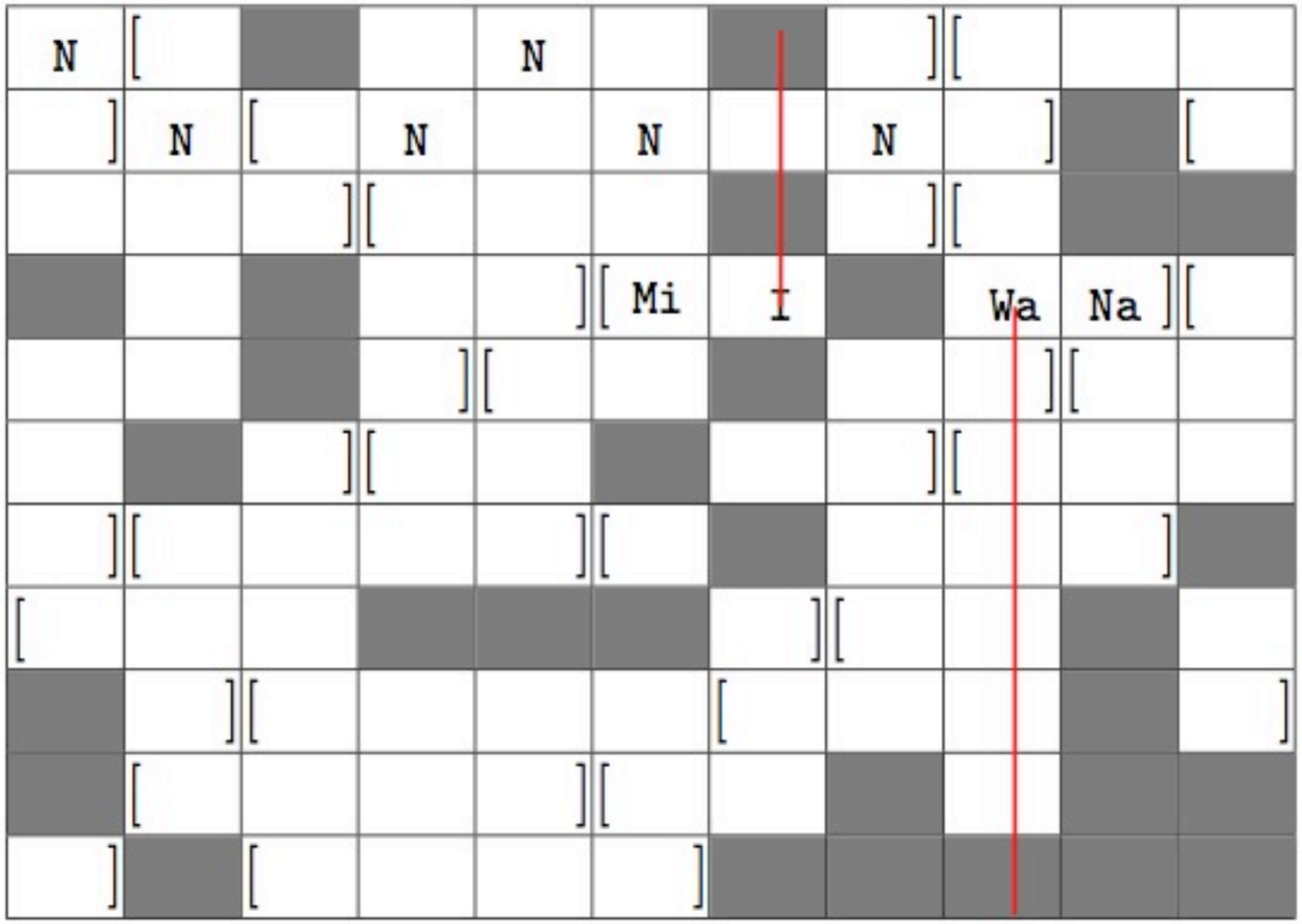


Table 6.13: The distance between `Wa` and `I` is 8

Breaking the second '.' code cipher

Step 3: deducing the column content

N	[			N	Na		]	[	Shi	Ta	
]	N	[	N		O	A	N		Ru]		[
		]	[		Mi		]	[	Ha		
				]	[	Mi	I		Wa	Na	[
			]	[		Ru			Yu]	[	Sa
		]	[			Ya	]	[	Se	Ru	
	]	[			]	[	A			Wa	Wi]
[							Ni]	[		Hi	
		]	[			Ya]	[	Mo		Na	]
	[				]	[	Ra	O		E	
]		[				Na]					

Table 6.14: Filling columns six, seven, nine and ten

Ki	A	Ni	Hi	Ho	A	Ta	Na	Mi	So	M
Mu	[Shi	Ru	Ha	Wa	Yu	Se	Wa	Hi	Na	
E	Ku	Me	Shi	Ma	No	Na	Tsu	E	Ya	A
Mi	Mi	Ru	A	Ya	Ra	Na]	[Ta	Na	Sa	Ru
Me	He	He	Mi	Ro	Shi	Se	A	A	Ri	Ma

Ru	So	Te	So	Sa	[Na
Wi]	Ho	Ni	Fu	Ro	Fu
Sa	Ho	Yo	Mo	No	I

U
Yu
Mo

The American effort: Blue Code

Also working on Japanese codes

Worked on Red Book, obtained by '*practical cryptanalysis'* and solved by Agnes Meyer Driscoll in 1928

Blue Book solved in 1933 by Safford, Dyer and Driscoll

Aided by an IBM tabulating machine

"... their success had followed what was possibly the ***most difficult cryptanalytic task ever undertaken*** *by the United States* ***up to that time.****"* (Parker, 1994)

"Driscoll's work in solving the system may have been even more brilliant than the Army's subsequent solution of the Purple machine." (Parker, 1994)

The American effort: Blue Code

Cipher consisted of a grid, Kana symbols were written from left to right and read off from top to bottom

Transposition changed daily

“It employed a relatively ***sophisticated columnar transposition*** *involving both* ***nulls and blanks****. The garble table, or differential feature, reduced the number of code groups to* ***85,184,*** *nearly the same as the Red book.”* (Pelletier, 1996)

Discontinued in 1939: timeframe matches the ‘.’ code

Conclusions

Nuboer worked on several systems, ‘.’ was most important

Wartime results:
- Clear overview of Japanese threat
- Allowed for early Shanghai evacuation

Explored two ciphers of the ‘.’ code
- Second cipher was much more sophisticated

Most likely the same code as the Blue Code / Blue Book
- Future research possible

Implementation of ‘finding the permutation’ found several keys:
- `github.com/joostrijneveld/blue-code-permutations`

Discussion

Questions?