UNIVERSITY OF AMSTERDAM

Jaap van Ginkel

Blue slides credit to: Hans van der Meer

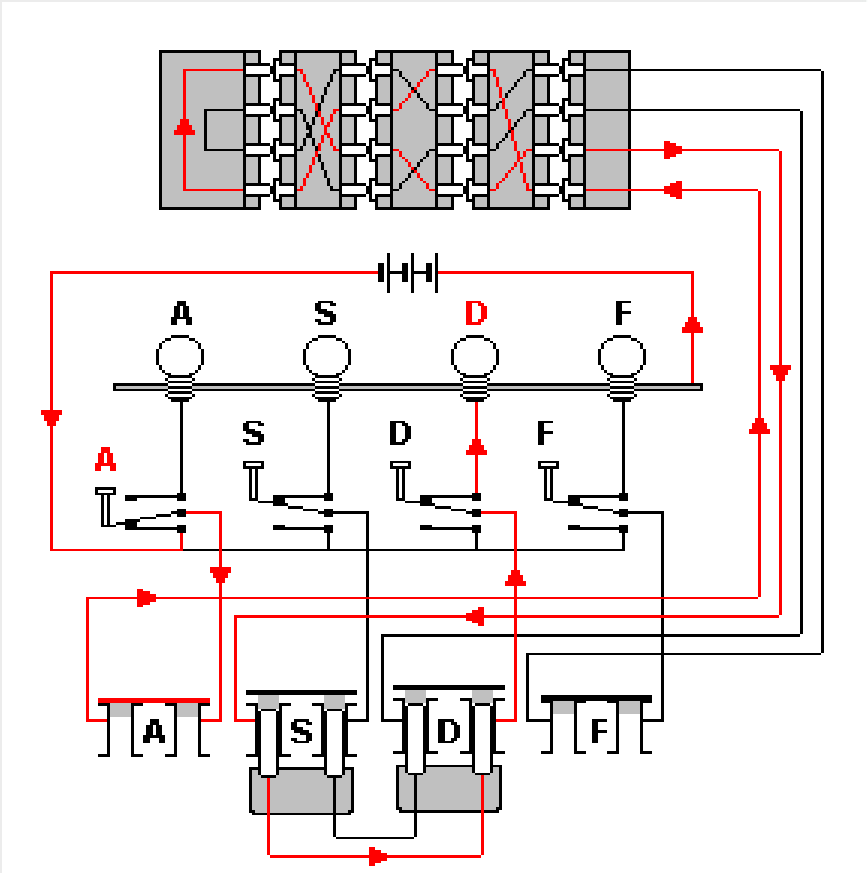
Enigma

September 5, 2024 Security of Systems and Networks

Enigma

- One of many rotor machines
- Well known from WWII
- Extensively documented many anecdotes
- Others:
  - Sigaba (United States)
  - Typex (Great Britain)
  - Lorenz SZ 40/42 (Germany)
  - Siemens and Halske T52 (Germany)
  - Fialka M-125 (Soviet)

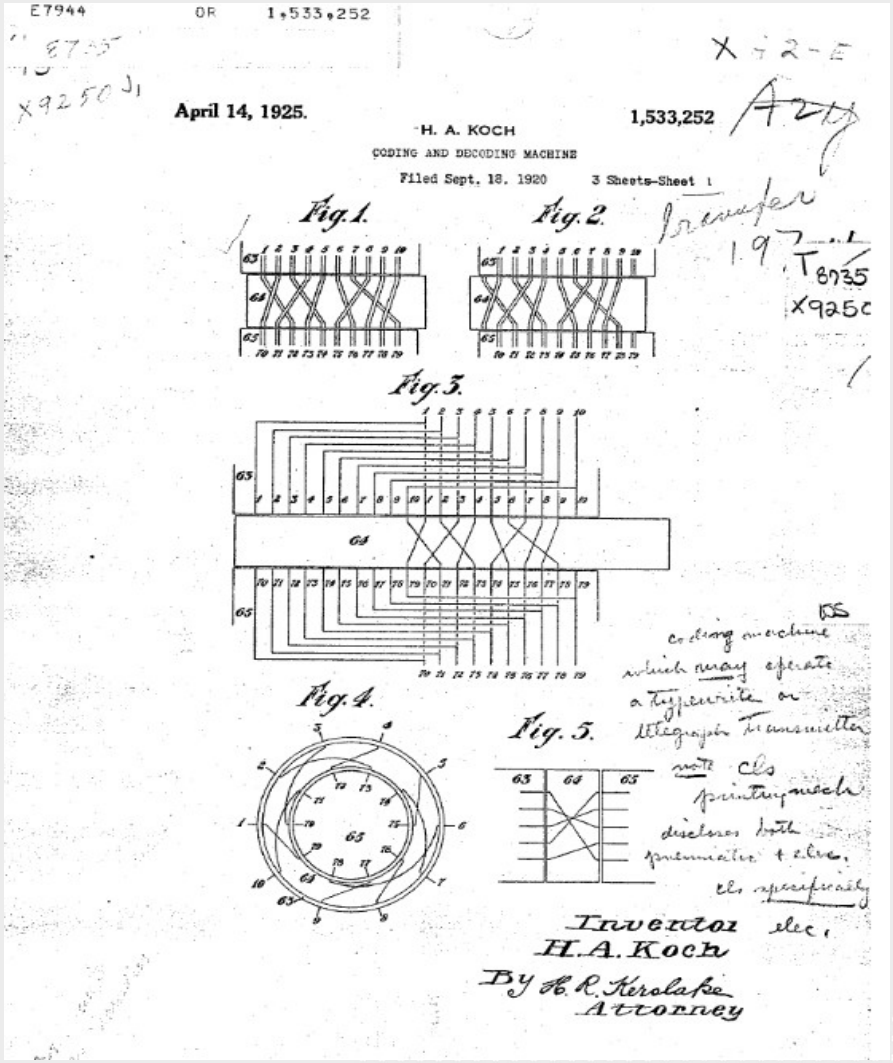
Enigma




Klappe schliessen
ENIGMA

1919 Patent

- Theo A. van Hengel
- R.P.C Spengler
- Patented by Koch
- Sold to Scherbius



E7944 OR 1,533,252

April 14, 1925. H. A. KOCH 1,533,252

CODING AND DECODING MACHINE

Filed Sept. 18, 1920 3 Sheets-Sheet 1

Fig. 1. Fig. 2.

Fig. 3.

Fig. 4. Fig. 5.

Inventor H. A. Koch

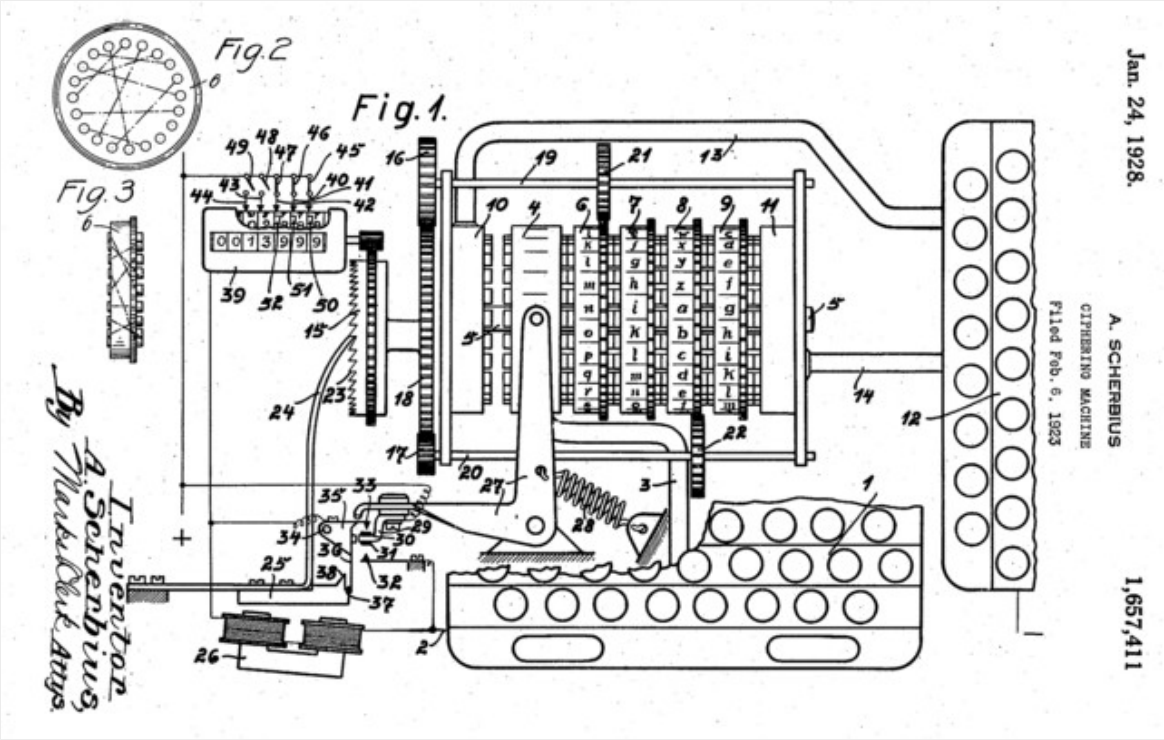
By H. R. Kerslake Attorney

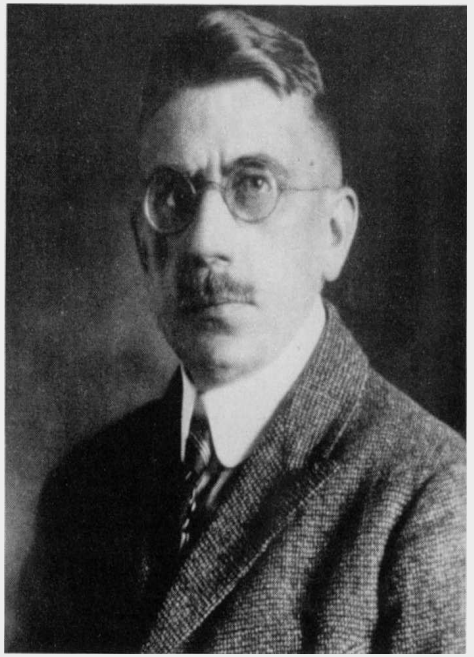
- 1915 Spengler en Van Hengel in N.O.Indië
- 1919 Koch patent
- 1920 Chiffriermaschinen AG
- 1923 Enigma-A
- 1926 Kriegsmarine Funkschlüssel-C
- 1928 Enigma in de Wehrmacht
- 1930 in Luftwaffe, Kriegsmarine, Abwehr

Van Hengel

1928 Patent

- Arthur Scherbius

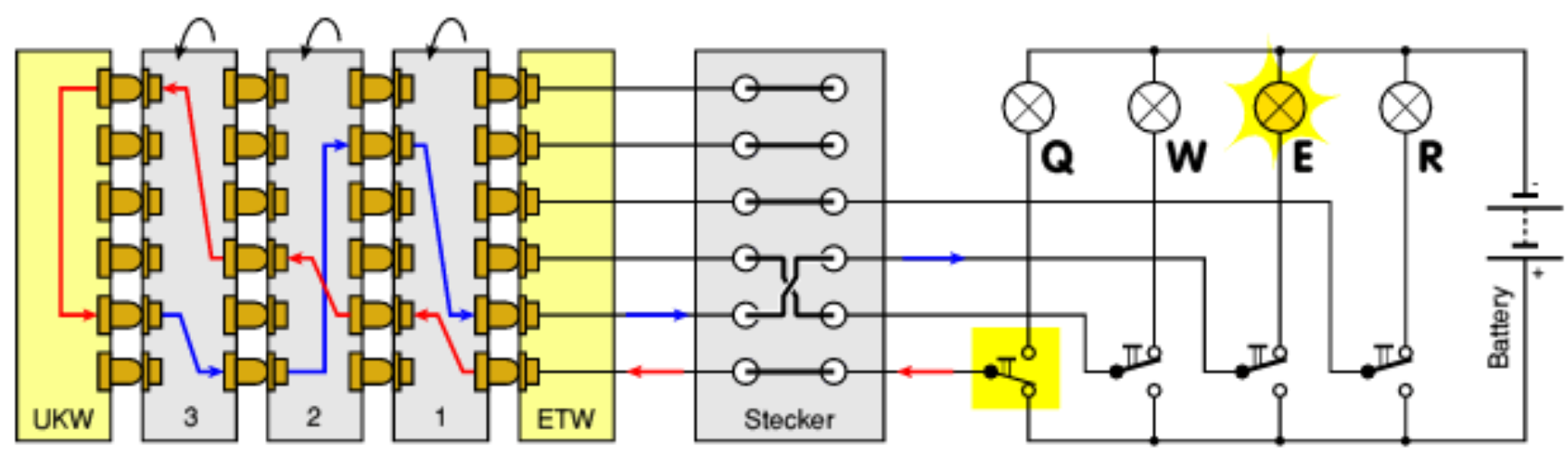


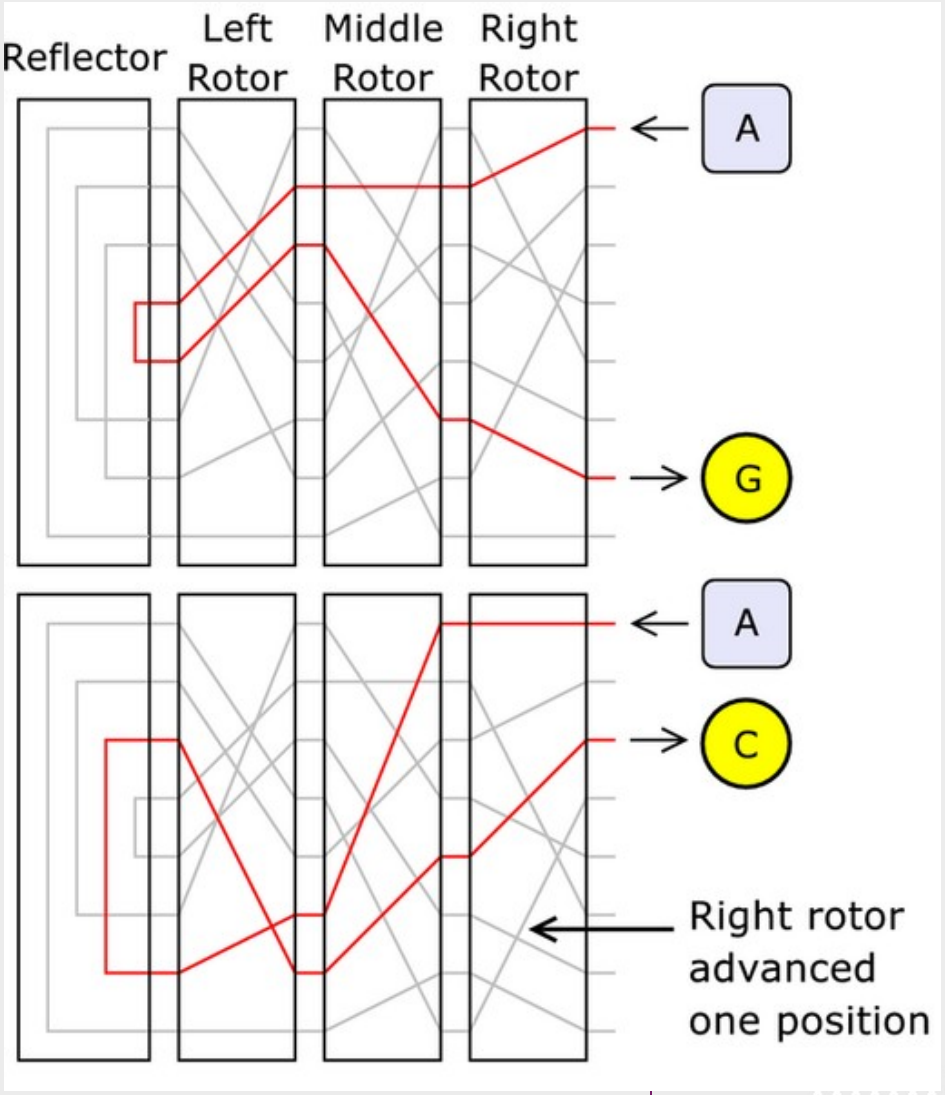


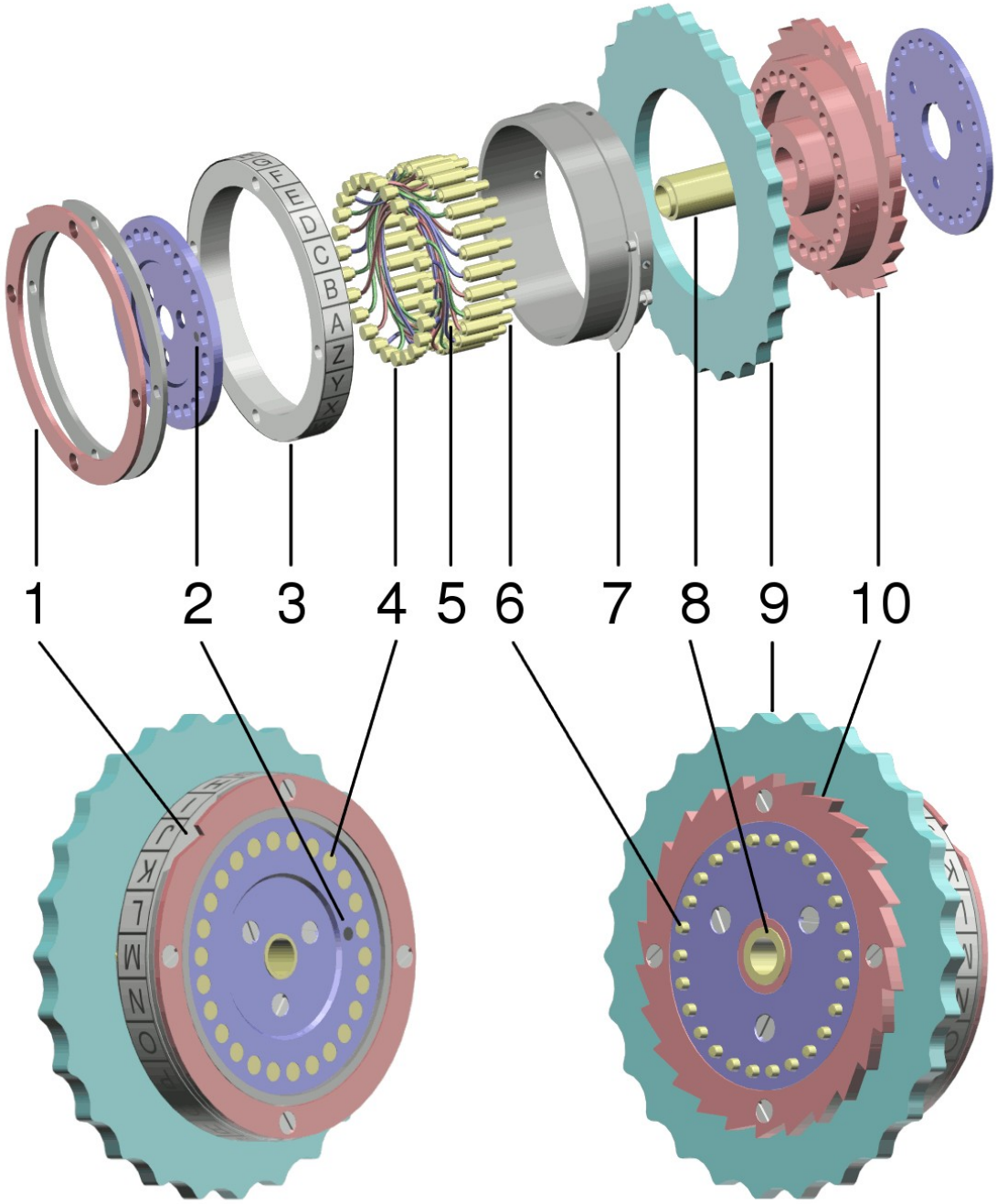
Arthur Scherbius

Enigma

- Poly alphabetic substitution cipher
- 3 wheels + reflector
- Long "period" 26 × 25 × 26 =16900
- Roughly $3*10^{114}$ possibilities
- Exhaustive search impossible
- Safe if principle and wiring would be known
  - At least that was intended...

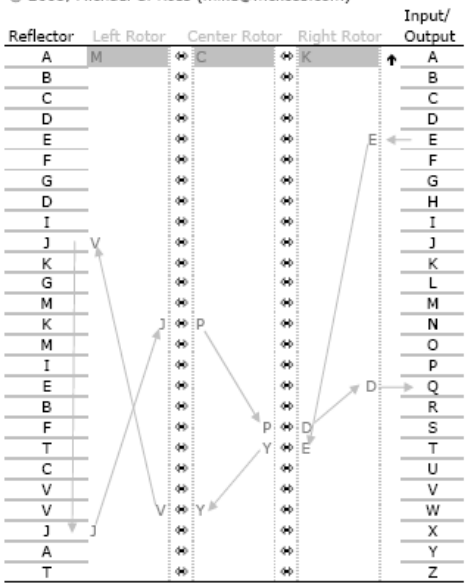

UKW
3
2
1
ETW
Stecker
Q
W
E
R
Battery


Reflector
Left Rotor
Middle Rotor
Right Rotor
A
G
A
C
Right rotor advanced one position


1
2
3
4
5
6
7
8
9
10

Enigma in Action

Paper Enigma Machine



Setup

1. Select left/center/right rotors.
2. Position initial wheel positions by sliding the indicated window letter up to the first row.

Operation

[Start at the input column at right, then work left to reflector, and then back to the right to the output column.]

1. If the ↑ notch appears in the window row, shift that rotor and the rotor to the left up one row (the Right Rotor is always shifted up one row before each letter is encoded/decoded).
2. Select letter to encode/decode in the Input column.
3. Read adjacent letter, *X*, in right hand column of the Right Rotor; select the letter *X* in the left hand column of the Rotor.
4. Repeat for Center Rotor.
5. Repeat for Left Rotor.
6. Read the adjacent letter, *R*, in the Reflector; select the *other* letter *R* in the Reflector.
7. Read adjacent letter, *Y*, in left hand column of the Left Rotor; select the letter *Y* in the right hand column of the Rotor.
8. Repeat for Center Rotor.
9. Repeat for Right Rotor.
10. Write down the adjacent letter, *Z*, in the output column.

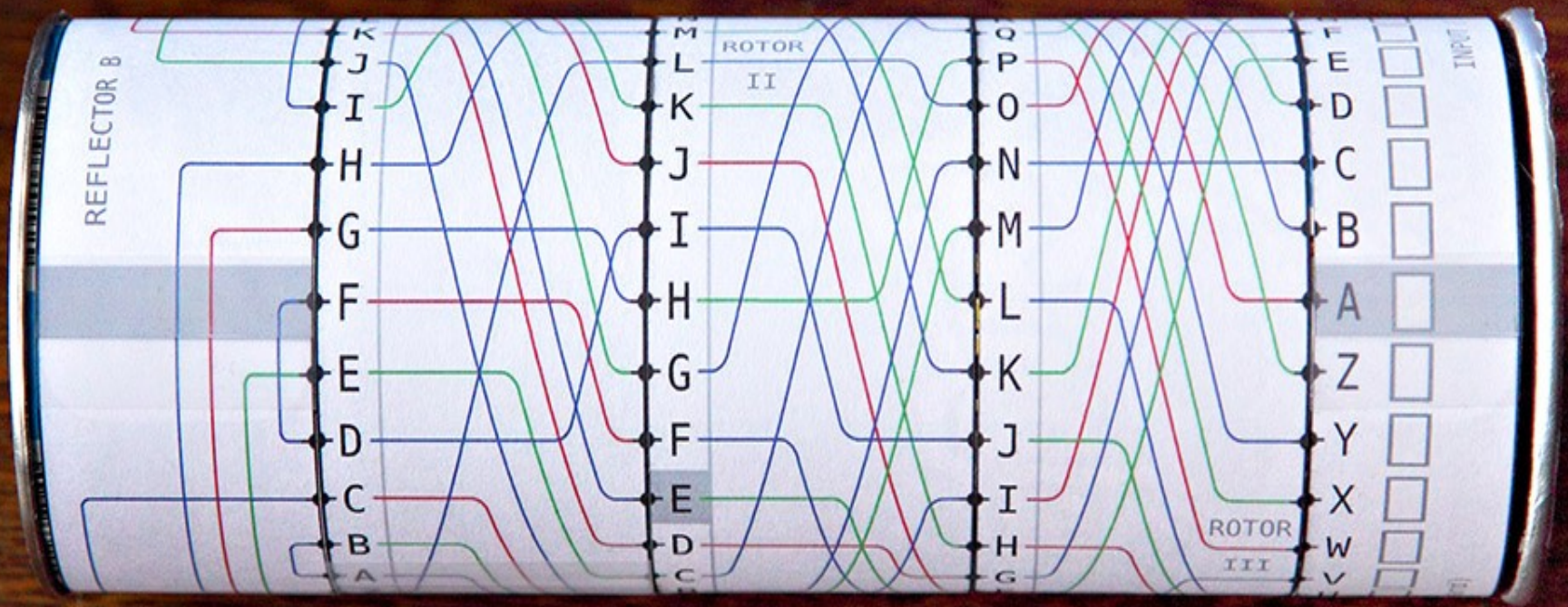
Repeat for each letter of the message.

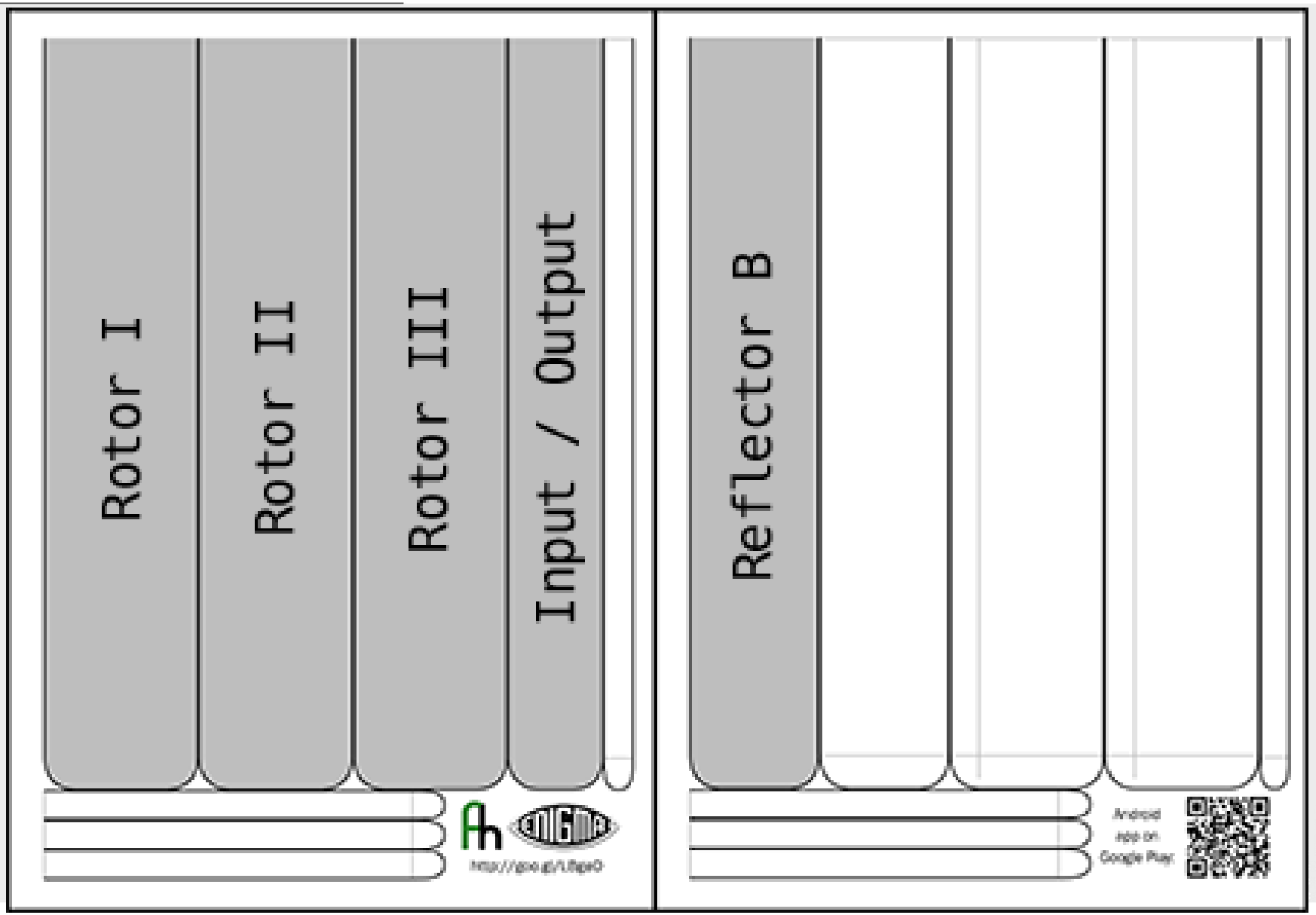
Example: Initial setting: I-II-III: MCK, Letter E encodes to Q.
Sample Message: QMJIDO MZWZJFJR

Rotor I		Rotor II		Rotor III	
A	E	A	A	A	B
B	K	B	J	B	D
C	M	C	D	C	F
D	F	D	K	D	H
E	L	E	S	E	J
F	G	F	I	F	L
G	D	G	R	G	C
H	Q	H	U	H	P
I	V	I	X	I	R
J	Z	J	B	J	T
K	N	K	L	K	X
L	T	L	H	L	V
M	O	M	W	M	Z
N	W	N	T	N	N
O	Y	O	M	O	Y
P	H	P	C	P	E
Q	X	Q	Q	Q	I
R	U	R	G	R	W
S	S	S	Z	S	G
T	P	T	N	T	A
U	A	U	P	U	K
V	I	V	Y	V	M
W	B	W	F	W	U
X	R	X	V	X	S
Y	C	Y	O	Y	Q
Z	J	Z	E	Z	O
A	E	A	A	A	B
B	K	B	J	B	D
C	M	C	D	C	F
D	F	D	K	D	H
E	L	E	S	E	J
F	G	F	I	F	L
G	D	G	R	G	C
H	Q	H	U	H	P
I	V	I	X	I	R
J	Z	J	B	J	T
K	N	K	L	K	X
L	T	L	H	L	V
M	O	M	W	M	Z
N	W	N	T	N	N
O	Y	O	M	O	Y
P	H	P	C	P	E
Q	X	Q	Q	Q	I
R	U	R	G	R	W
S	S	S	Z	S	G
T	P	T	N	T	A
U	A	U	P	U	K
V	I	V	Y	V	M
W	B	W	F	W	U
X	R	X	V	X	S
Y	C	Y	O	Y	Q
Z	J	Z	E	Z	O

✂ Cut here

Rev: 2003-03-11-1047


REFLECTOR B
J
I
H
G
F
E
D
C
B
A
ROTOR
II
L
K
J
I
H
G
F
E
D
C
P
O
N
M
L
K
J
I
H
ROTOR
III
E
D
C
B
A
Z
Y
X
W
INPUT


Rotor I
Rotor II
Rotor III
Input / Output
Reflector B
Android
app on
Google Play

Instructions:

- Make sure that the grey bars on the Reflector and the Input/Output cylinders line up
- Turn the rotors so that the three letters of your message key are in line with the grey bars; use M C K.
- Turn just the right-hand rotor one step towards you You must do this before you read off the letter (even the first one!)
- When the right-hand rotor turns one step, at some positions other rotors turn over as well,
- If the letter on the middle rotor is shaded grey, turn all three rotors one step towards you,
- otherwise, if the letter on the right-hand rotor is shaded grey, turn the middle and right-hand rotors one step towards you,
- otherwise, turn just the right-hand rotor one step towards you.

Use the paper Enigma

```
apzps yrffr szhuc hqlin
 txtzj behia

Startposition:  MCK
Rotors:         I – II – III
Rotor settings: 1 -  1 -   1
Plugboard:      Empty
```

Only 26 characters

X = Period

Y = Comma

UD = Question Mark

XX = Colon

YY = Dash/Hyphen/Slant

KK*****KK = Parenthesis

J*****J = Stress Mark

Numbers are written out as words

The Wehrmacht used other abbreviations:

KLAM = Parenthesis

ZZ = Comma

X = Full stop (end of sentence)

YY = Point or dot

X****X = Inverted commas

Question mark (Fragezeichen in German) is usually abbreviated to one of the three following forms:

FRAGE, FRAGEZ or FRAQ

Foreign names, places etc. twice delimited by "X", e.g. XPARISXPARISX

The letters CH is written as Q, e.g. ACHT was written as AQT, RICHTUNG as RIQTUNG

It was prohibited to encipher the word "null" several times in succession. For several nulls these abbreviations are used:

00 = CENTA

000 = MILLE

0000 = MYRIA

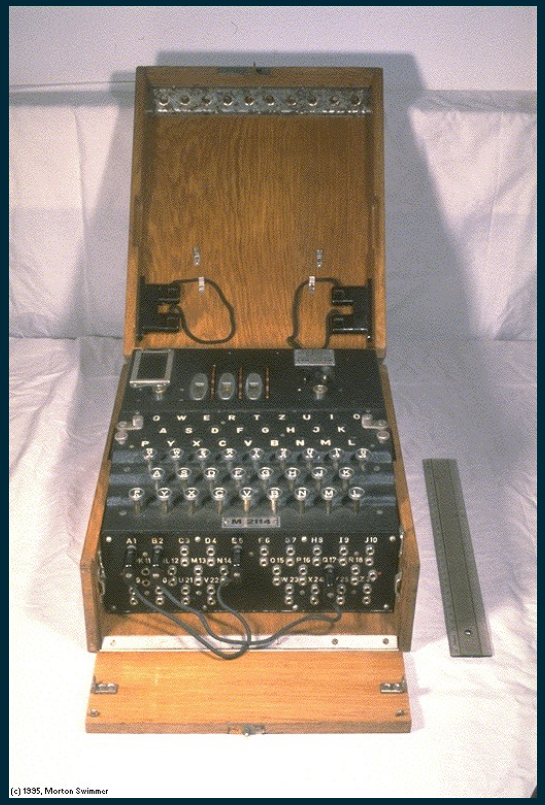
Examples: 200 = ZWO CENTA, 00780 = CENTA SIEBEN AQT NULL

Enigma Software Emulator 7.0

http://users.telenet.be/d.rijmenants/en/enigmasim.htm

Modellen

Enigma-G
Abwehr

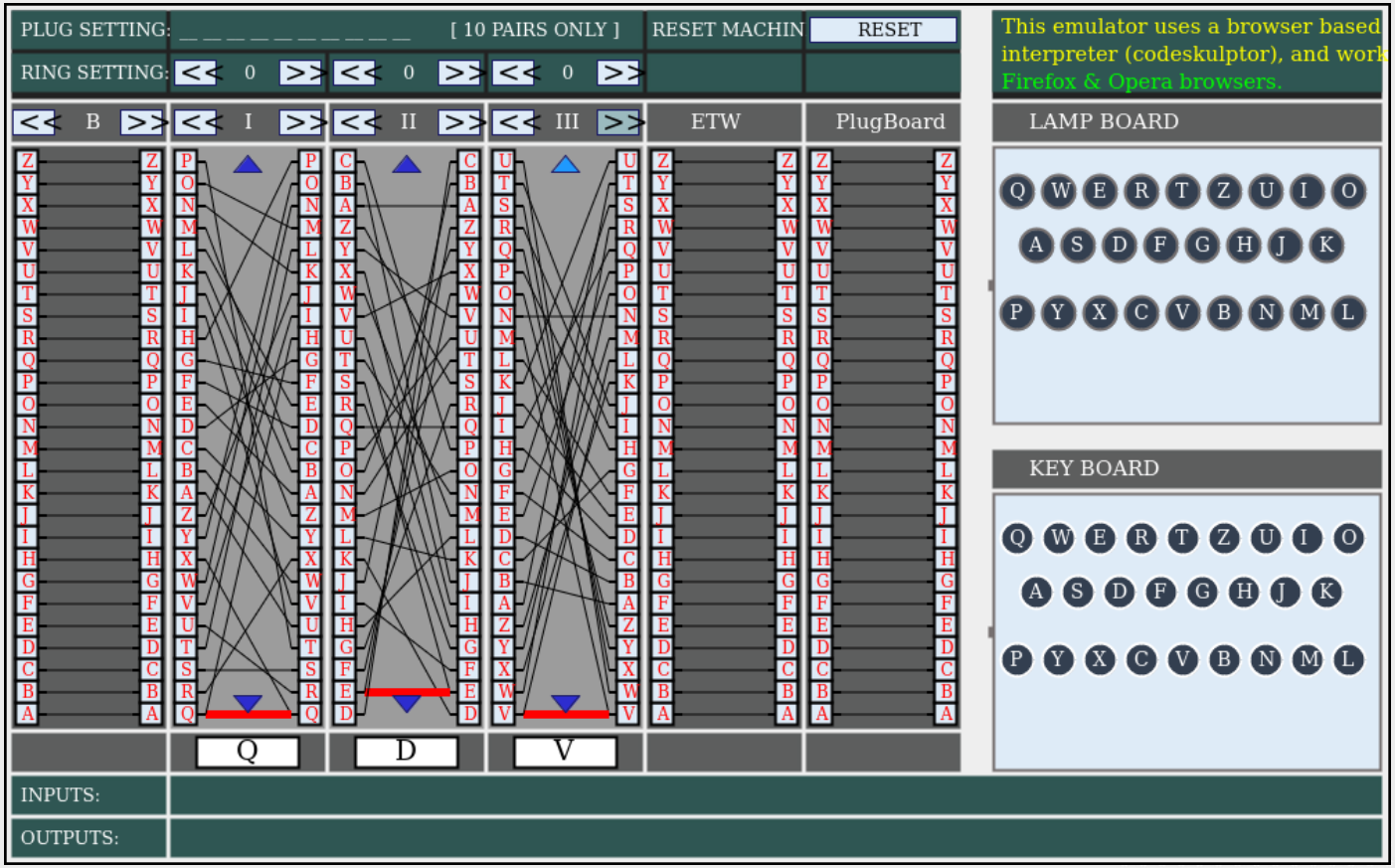


Enigma
Wehrmacht

4-rotor Enigma
Kriegsmarine

Double stepping

- Example QDV start setting



https://piotte13.github.io/enigma-cipher/

UNIVERSITY OF AMSTERDAM

Codebook UvA Cryptografie

GEHEIM! UVA CRYPTOGRAFIE FEBRUAR 2018

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
29	IV VI VIII	03 09 11	AN CK DT EY GQ HZ LV MO PR UX	TJT CQO YJQ LTO
28	II V I	13 26 20	AM BW CQ DR GY HP NZ OX ST UV	RET QJP KIR VPI
27	II VI V	09 03 01	BN DY EM FS HJ IV KX LP QR UW	KRH HFM JRM SAG
26	III V VI	20 15 25	AX BG CO EQ HV IS JT KP LZ MW	LLP IHC CRB XSW
25	IV V III	24 08 26	AL CJ DM EZ FP GH IY KS OU VX	HUF EXH GYD DCM
24	VI II VIII	07 05 14	AU BF CM DT EW GJ HL OR PS VZ	TKT RFA ZAG CLQ
23	VII V VIII	04 02 14	AP BN CX EH FI GO JR LV QU TZ	SQG CKG TTH LBO
22	VII VI III	14 17 20	AD BZ CN GH IU JQ KO MR SV WX	CQE MPY DJY KSA
21	VIII III II	01 05 22	AE BS DO FM HP IK LN TV WY XZ	FDG AGC FNU OVZ
20	VI VIII II	26 11 17	AK BX CJ EH IW MN PZ QV RT UY	PBT WSK VQS YBT
19	III VII II	19 12 06	AY CH DS EM FI GZ JK PT QV RU	DZR QMA QWR ZGO
18	III II I	24 03 23	AS CH EV FQ GU JN LX MP OW TZ	OAM FER HJB ITA
17	IV VI VII	23 17 23	AN BV DW ET HJ LS MZ OQ PU RY	FAR QQS CGH KIV
16	I VI IV	09 24 10	AW BP DI EN GY JU KQ LV MX OR	YZP TOE FME JWD
15	III VI II	21 14 09	AJ BT CV DF ES IZ LM NP QR UY	IJY LVA RLP MBC
14	V IV III	13 21 17	BO CR DI FW GN HL PX QV SU YZ	ZBX DLU TAV ZJP
13	I VI III	14 09 02	BF EP GH JV KN MU OY QT RX WZ	ECS RRI ABX XAA
12	III VIII II	11 12 02	AO BU CY FZ GM IR JN KL PQ TV	QWC QOQ QRU IOJ
11	VI I II	03 10 19	AU BE DK FI GS HO LR PT QX VZ	TVU JKJ XVU HKY
10	VI VII II	16 17 14	AW BL DG EF HZ JQ KR MT NO UX	NWB VUU DJB NOI
09	I II III	15 23 14	AV CF EK GJ HZ LO MN QX TU WY	HTR LFR CTR FTE
08	II III VIII	26 19 09	AN BU DJ EZ FR GX IP KV LQ OW	NGO AKE KVF HSD
07	VII I VIII	05 23 15	CJ DG EV FM IW LZ NQ OY PU SX	TMY JUA MOB YSZ
06	VI VII I	13 13 06	AV BQ CM ET FU HP IN KO RX WZ	VCG YKX KWU NMZ
05	VI I II	21 02 24	AG DV EJ FK IN LZ OP RS UY WX	TXA RUN KFI MCP
04	II IV I	18 08 09	AY BV CI EP FX GL HZ KR MT OS	LPH ZKT CJG IDD
03	V I VII	25 05 06	CY DV EF GL HX IQ KM NT OP WZ	ALD YAK SCE LJY
02	III II I	03 26 22	BV DL EU FG HQ MY NR OP SX TW	MZX QZL WXV IMO
01	VI V I	10 19 22	AL CU DF GP HN IR JM OV QT SY	BWY OAT GXH GCV

Please decode

Tag (Day)	Walzenlage (Rotors)	Ringstellung (Ringsetting)	Steckerverbindungen (Plug Connections)	
03	C V IV II	05 11 15	AW BM CJ DR EV GZ HO KU PQ TX	HID ZEC NXH HXO
02	B IV I III	11 26 03	AN BI CE DY FZ GR HT LQ SU WX	VVO GTC QPF OXT
01	B IV II I	03 26 04	AF BJ CQ DR EG IV KY LN MW UZ	JZC WLM VHM MPV

On day 02 the following message is intercepted:

U6Z DE C 1510 = 44 = SIH QUJ =

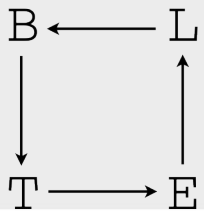
DXFEY IGHUE QYWVH OGSJQ BTYCE NUWGP LHSGP WT=

(Simplified for instructional purposes this cant be a real message)

Cracking Enigma

- Biuro Szyfrów
  - Marian Rejewski
  - Jerzy Różycki
  - Henryk Zygalski
- Cracked from 1932

BJGTDN LIFBAB
ETULZR TFREII



Zygalski sheets

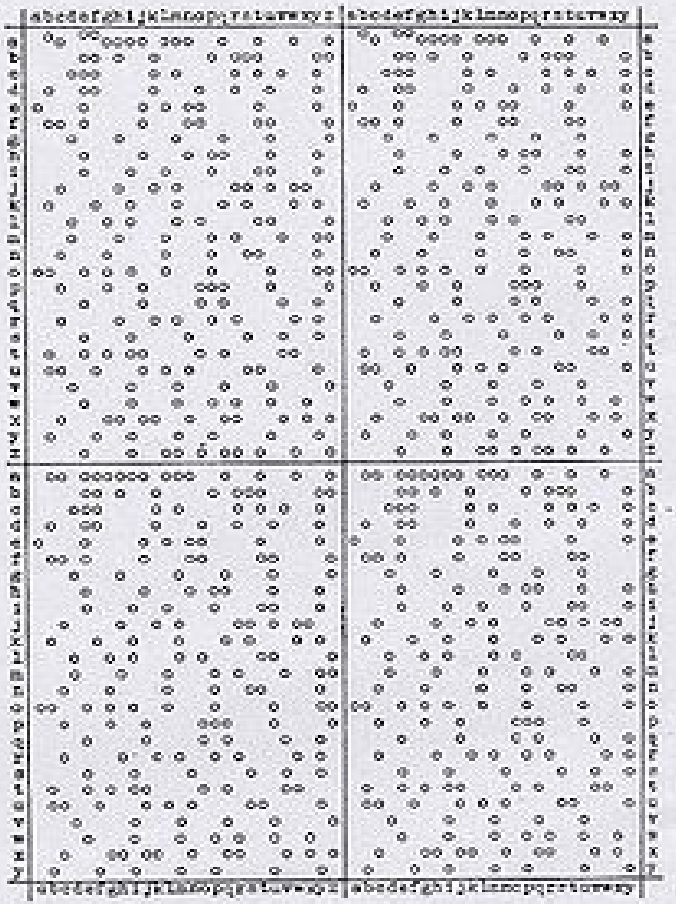


Fig. 5. Diagram of the perforated sheet

Noting to report.....

Exclusion of possible positions for the possible plaintext *Keine besonderen Ereignisse*

Ciphertext	O	H	J	Y	P	D	O	M	Q	N	J	C	O	S	G	A	W	H	L	E	I	H	Y	S	O	P	J	S	M	N	U
Position 1			K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E				
Position 2				K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E				
Position 3					K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E			

Cracking Enigma Weaknesses

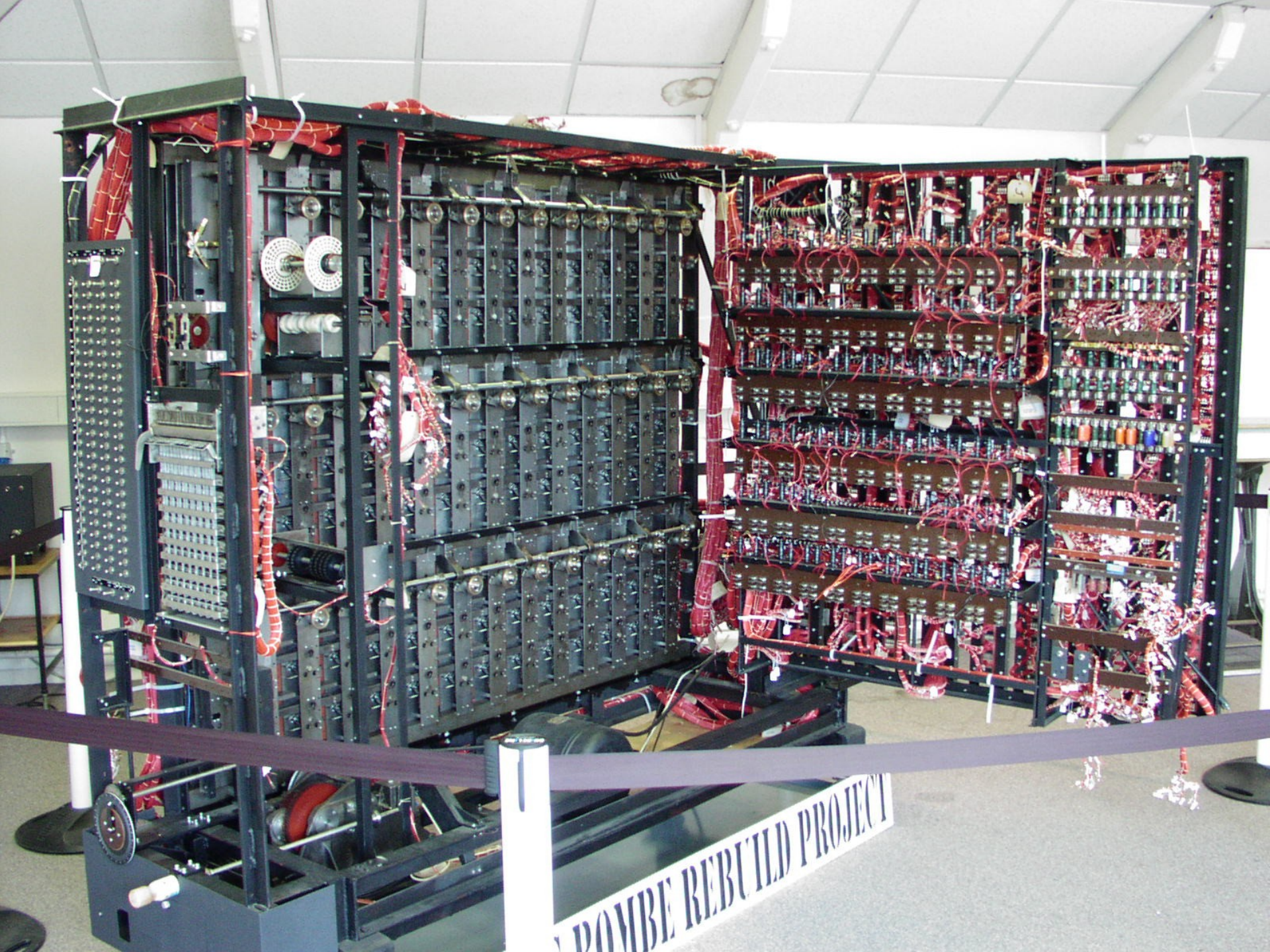
- Letter never translates to itself
- Double sending of encoding settings
- Chosen plaintext
  - Standard message formats
- CRIBS
- Exhaustive search impossible
- 10^{114} (approximately 380 bits)
- with known wiring and other operational constraints, this is reduced to around 10^{23} (76 bits).[3]

Improvements

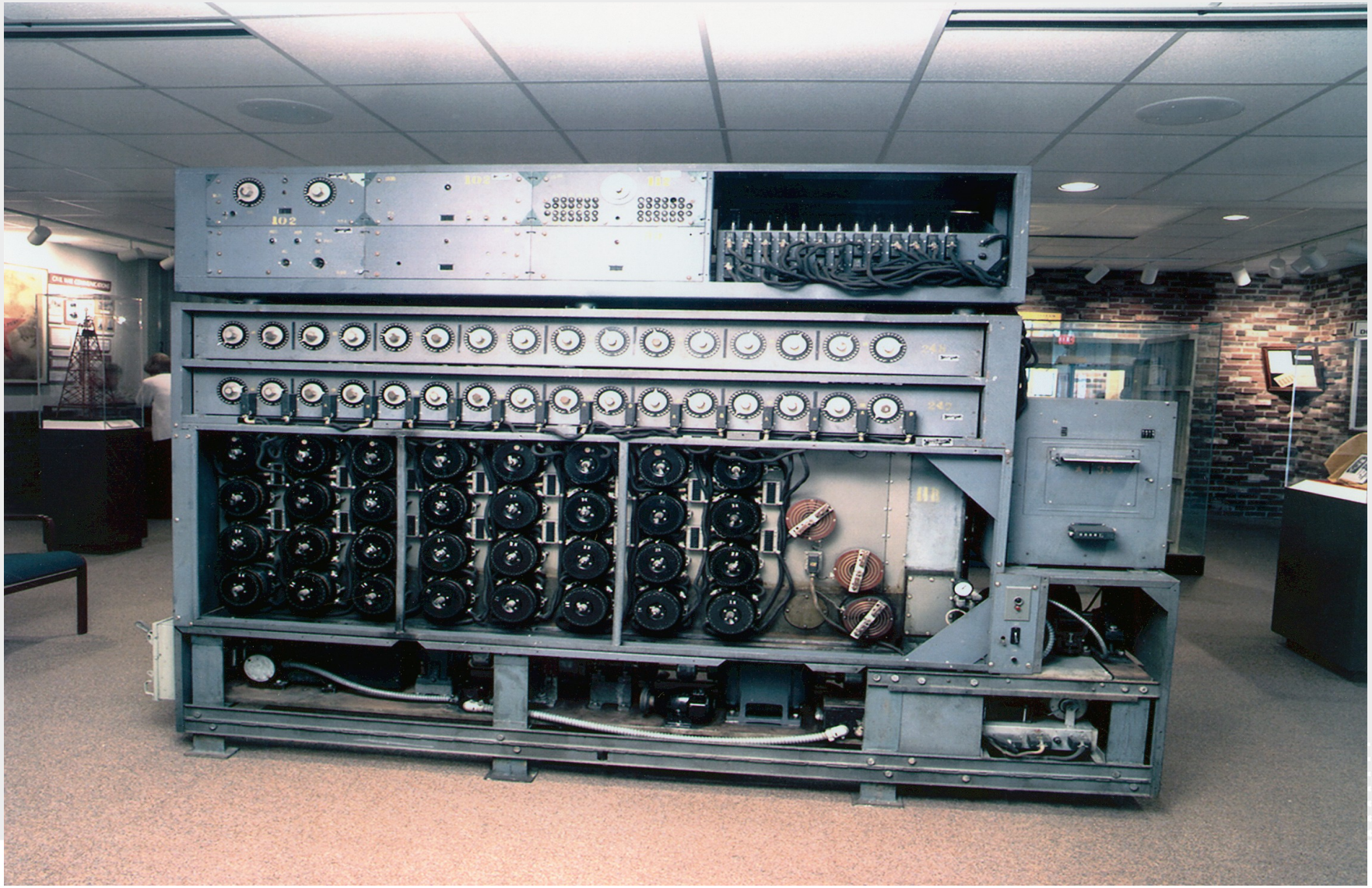
- From 3 wheels to choice 3 out of 5
- Custom versions (different wiring)
- Fourth wheel position
- Steckerbrett
- Procedural changes

Bombe

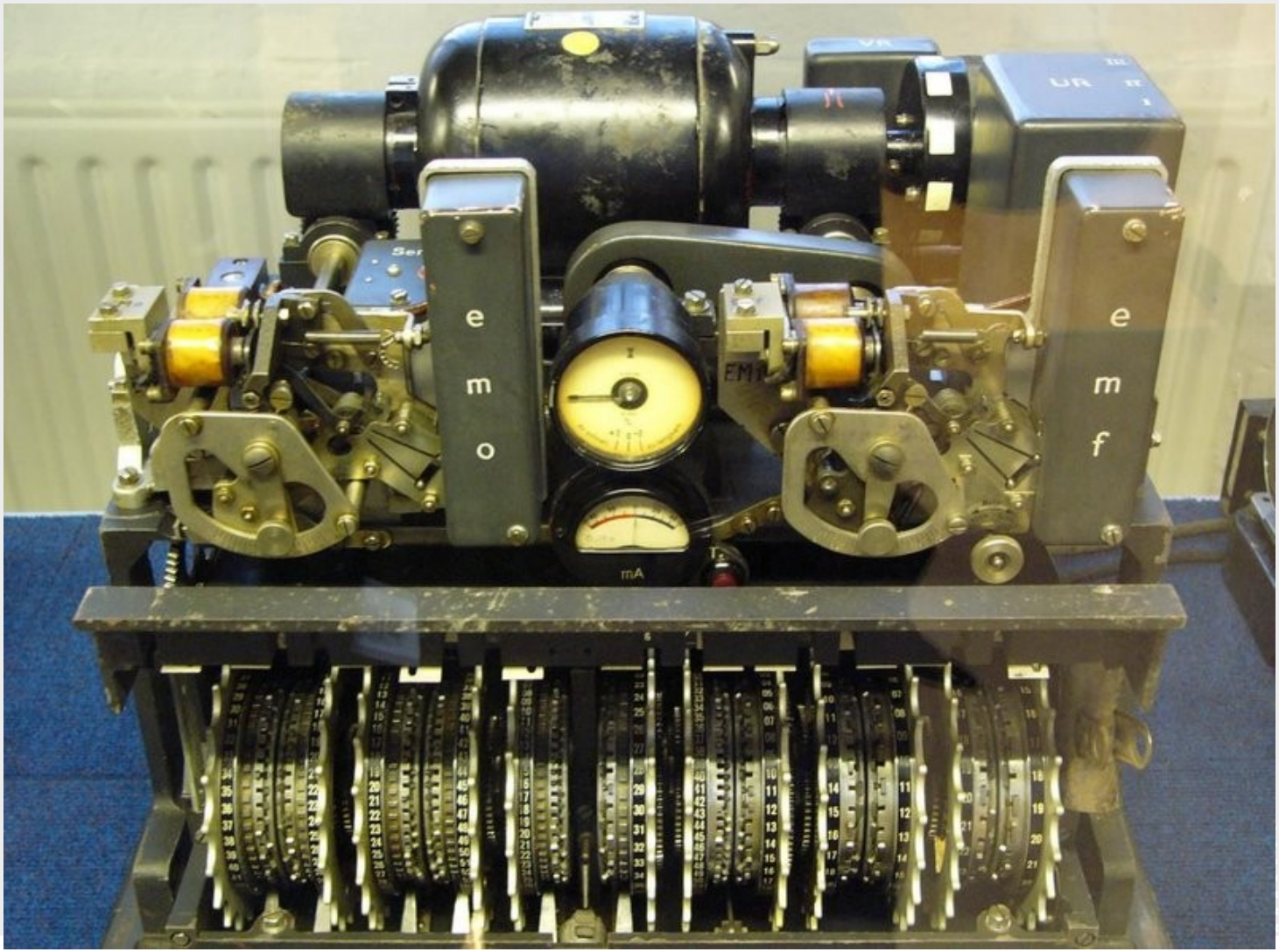
- Polish: bomba kryptologiczna
- Alan Turing
- Read/ chapter from Codebook CD


ROMBE REBUILD PROJECT

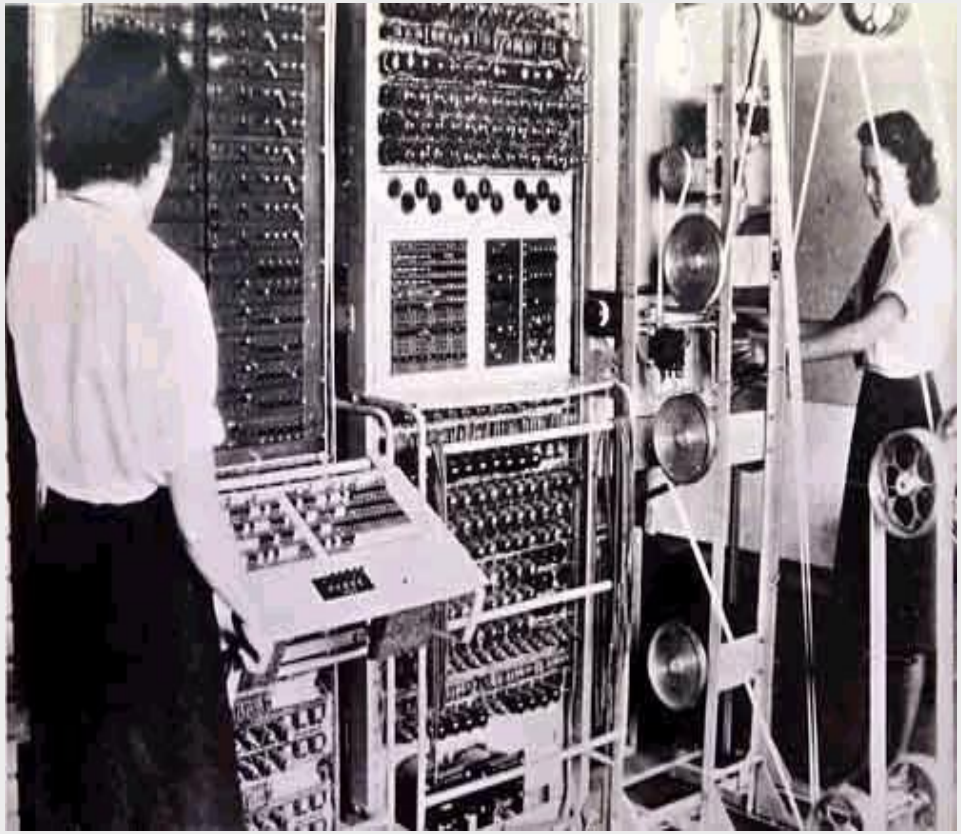
American Bombe

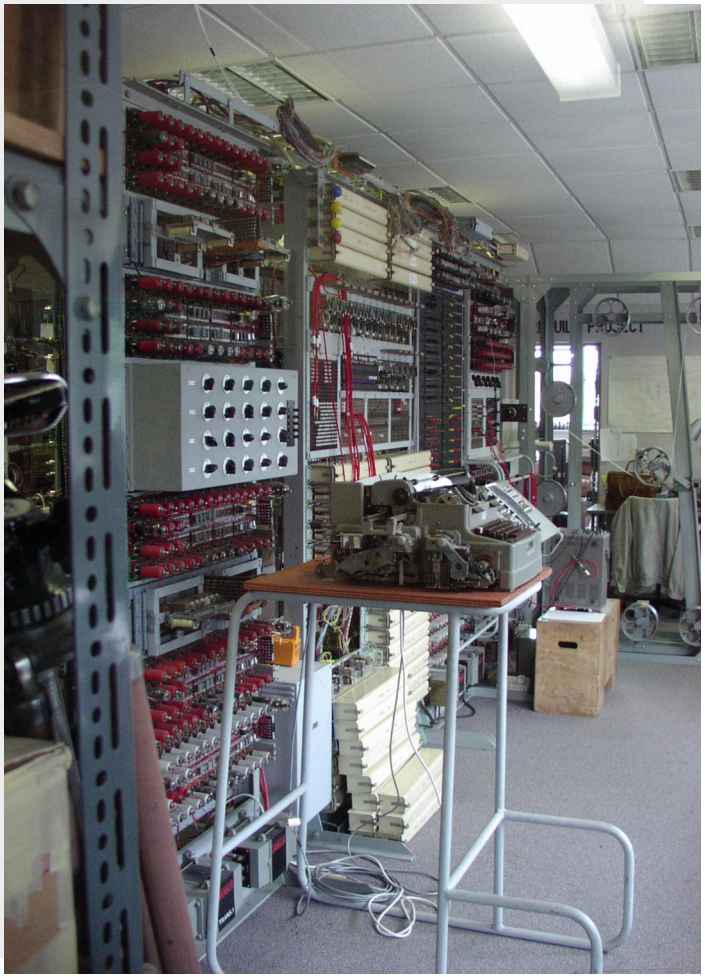


Lorenz SZ 40 / SZ 42



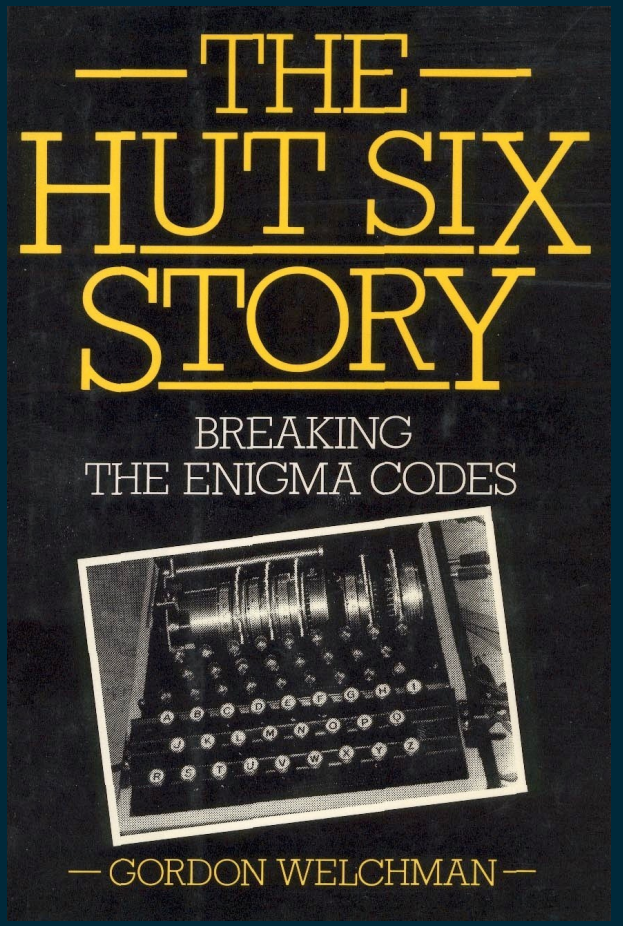
Colossus



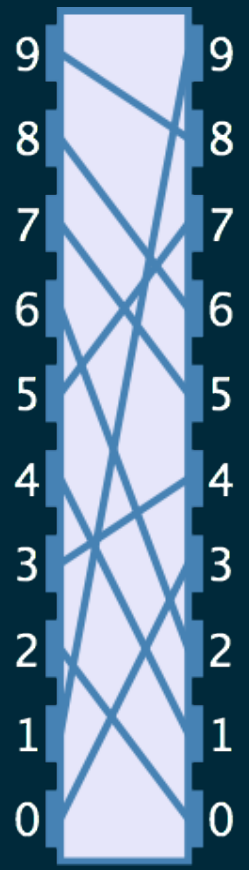


Cryptoanalyse

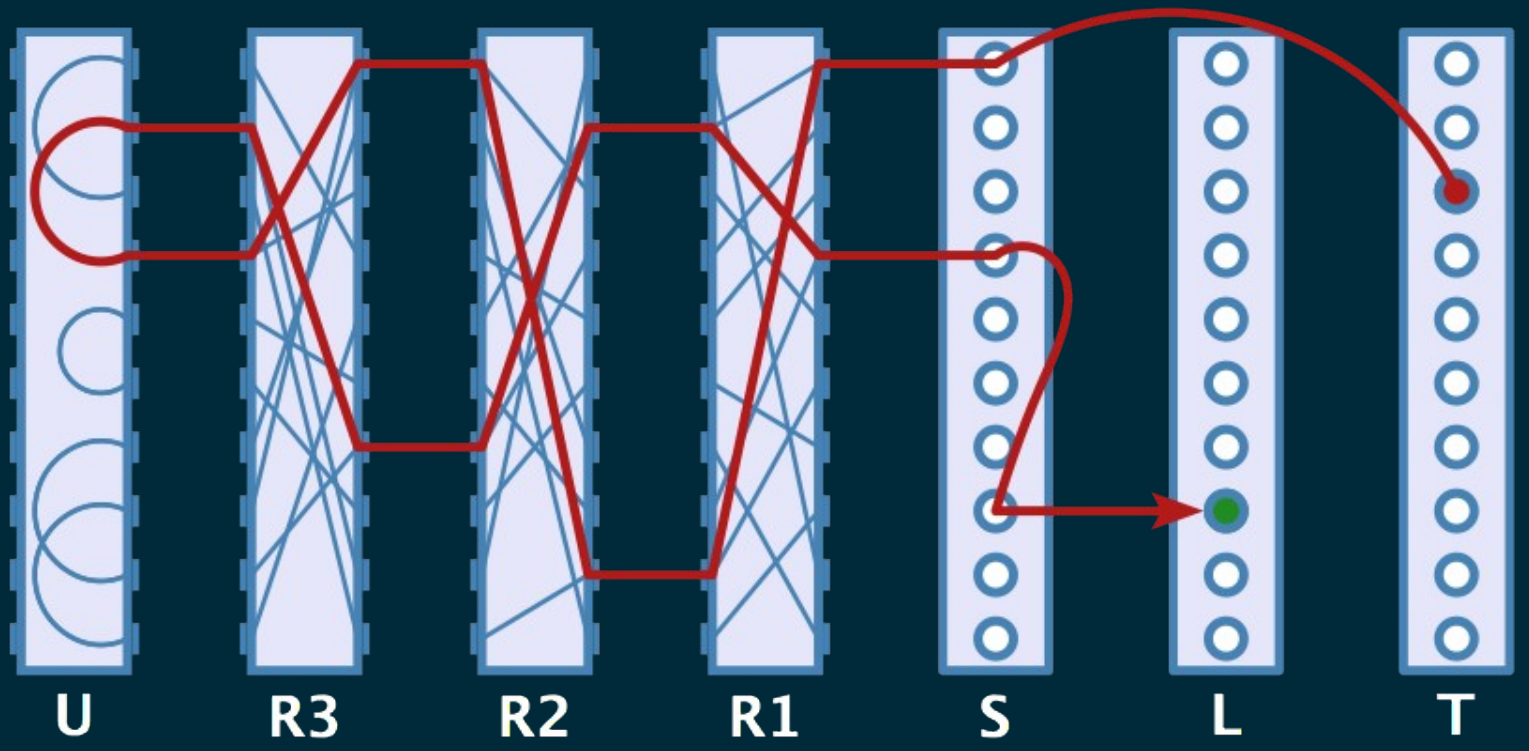
- 1932 Enigma in Polen gebroken
- 1939 Polen delen hun kennis
- 1939–1945 Bletchley Park
- 1940 eerste Turing bombe
- 1941 Schlüssel-M veilig verklaard
- 1942 blackout U-Boot traffic
- 1974 Winterbotham *The Ultra Secret*
- 1982 Welchman *The Hut Six Story*



Enigma rotor

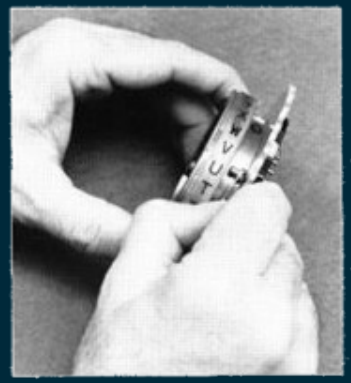


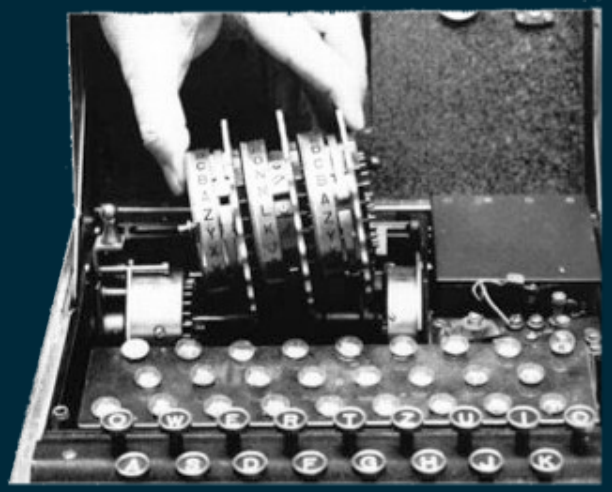
Enigma schema

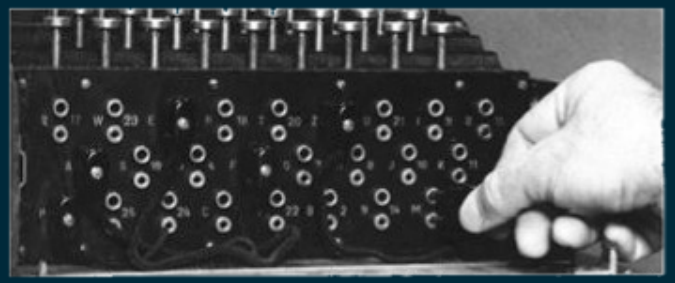


Enigma vercijfering is involutie: als A → B dan ook B → A

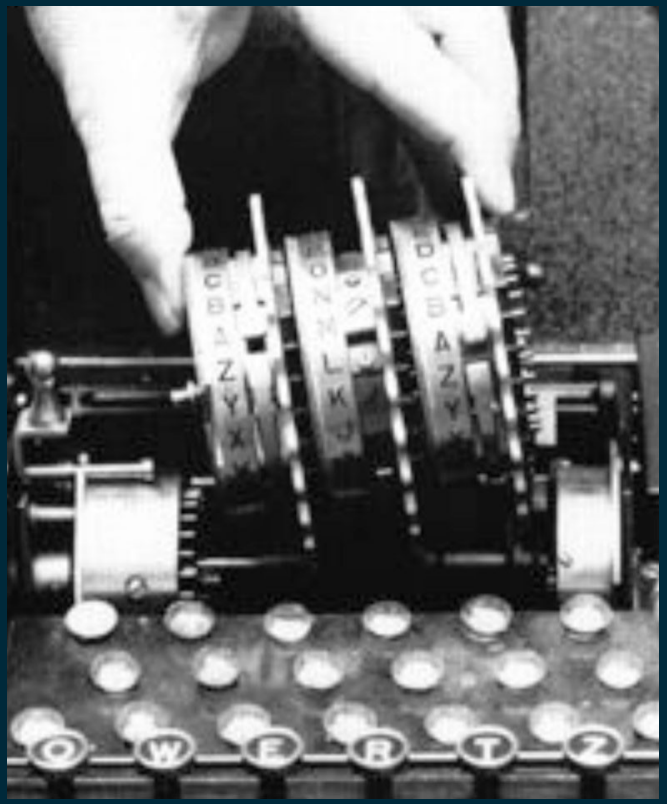
Enigma instelling

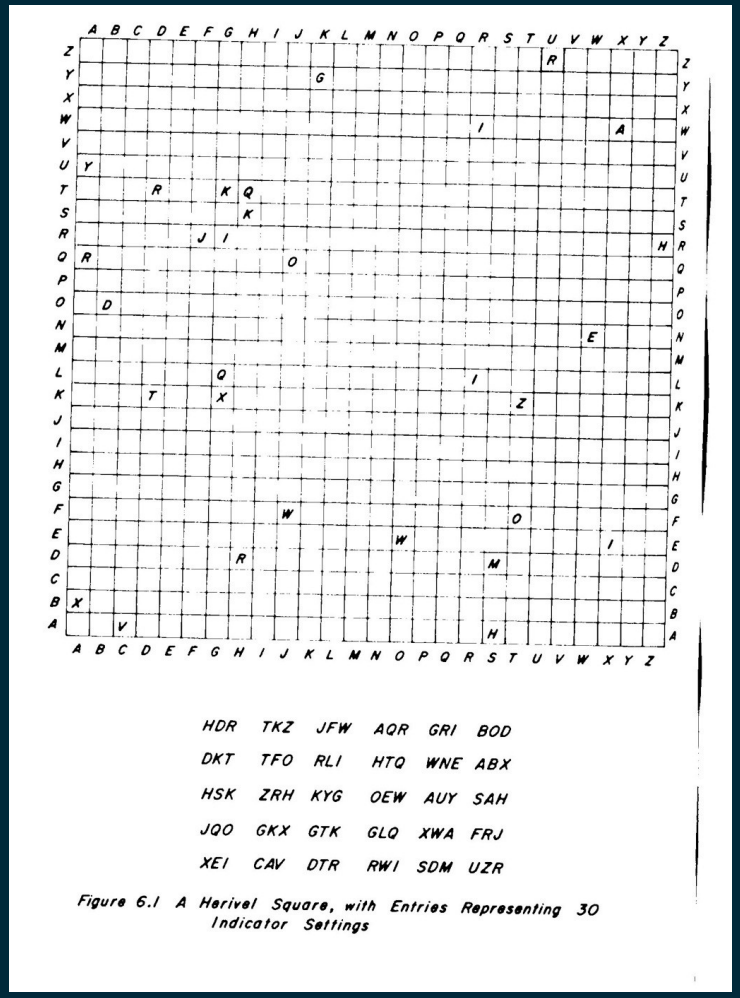






Herivel tip





HDR	TKZ	JFW	AQR	GRI	BOD
DKT	TFO	RLI	HTQ	WNE	ABX
HSK	ZRH	KYG	OEW	AUY	SAH
JQO	GKX	GTK	GLQ	XWA	FRJ
XEI	CAV	DTR	RWI	SDM	UZR

Figure 6.1 A Herivel Square, with Entries Representing 30 Indicator Settings

Vercijfering

Prüf-Nr. 4533

Geheim!

Der Schlüssel M

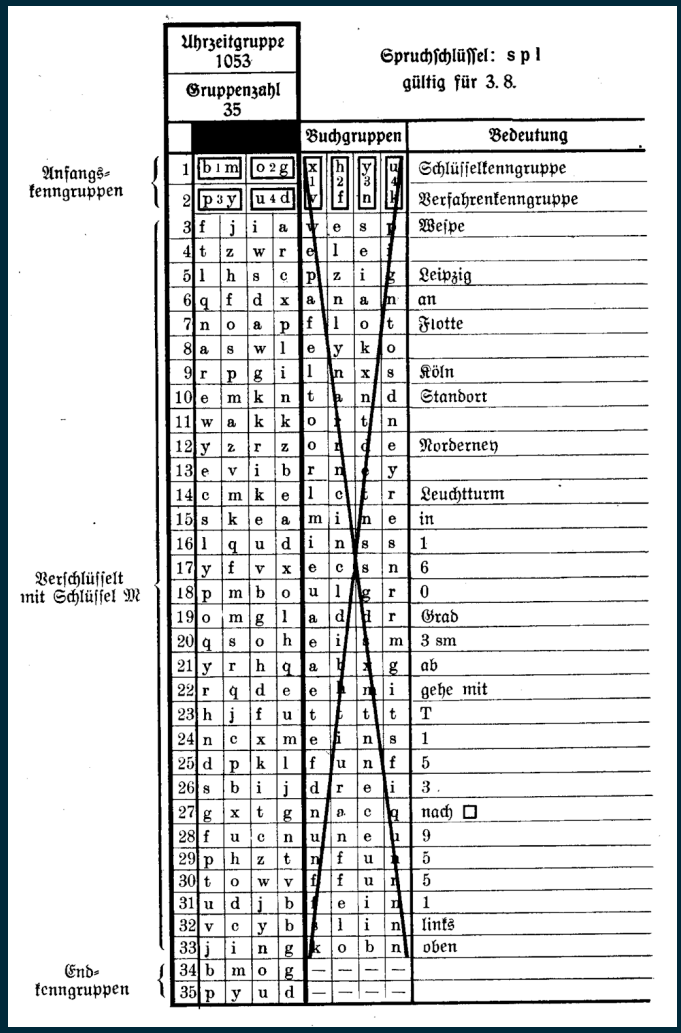
Verfahren M Allgemein

Oberkommando der Kriegsmarine
Berlin 1940

M. Dv. Nr. 32/1

Marineoberkommando Nordsee

Druckschriftenverwaltung

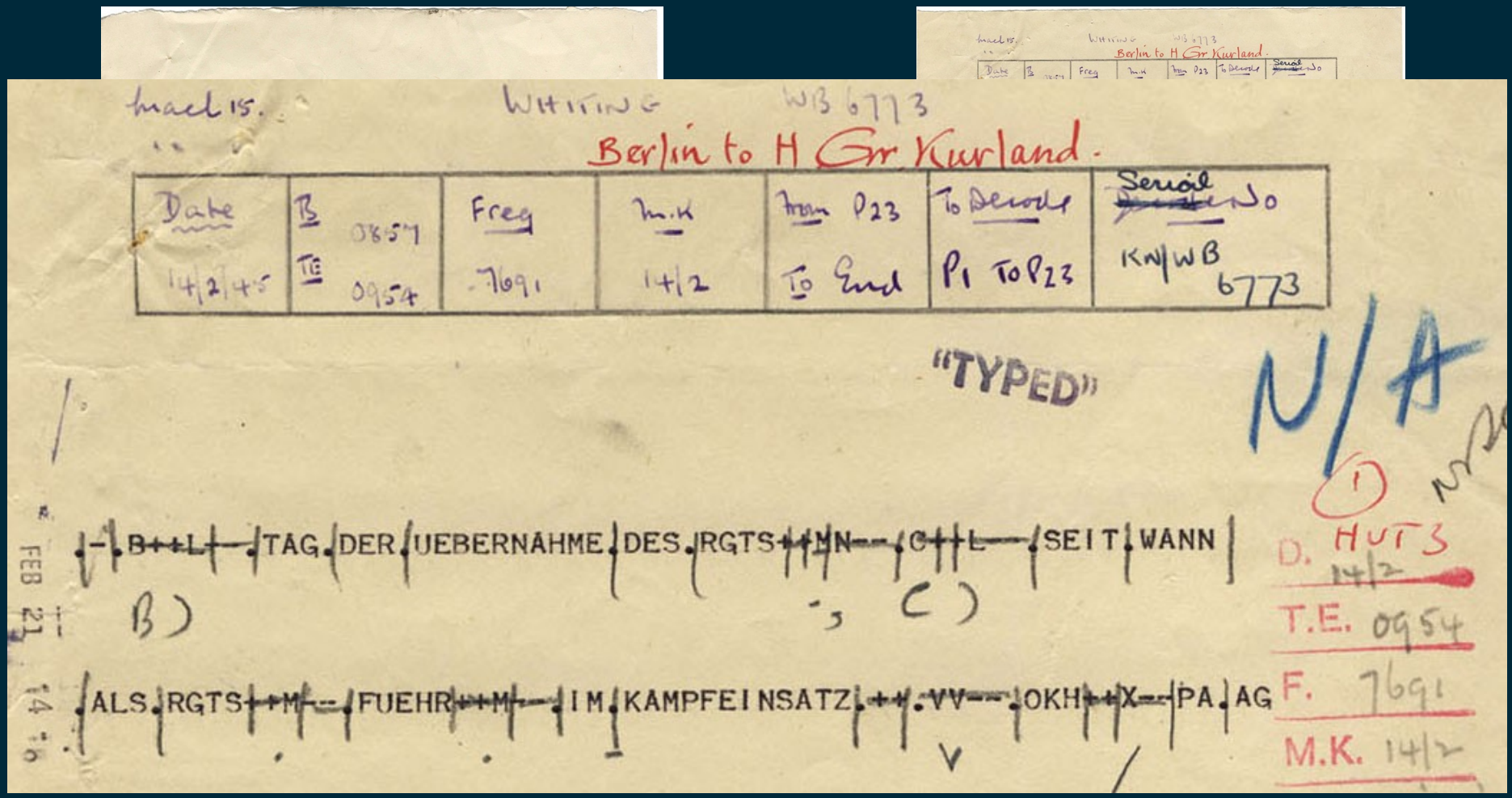


Uhrzeitgruppe 1053
Gruppenzahl 35

Spruchschlüssel: s p l
gültig für 3. 8.

						Buchgruppen				Bedeutung
Anfangskenngruppen	1	b 1 m		o 2 g		x 1 v	h 2 f	y 3 n	u 4 d	Schlüsselkenngruppe
	2	p 3 y		u 4 d		v	f	n	d	Verfahrenkenngruppe
Verschlüsselt mit Schlüssel M	3	f	j	i	a	w	e	s	p	Wespe
	4	t	z	w	r	e	l	e	f	
	5	l	h	s	c	p	z	i	g	Leipzig
	6	q	f	d	x	a	n	a	n	an
	7	n	o	a	p	f	l	o	t	Flotte
	8	a	s	w	l	e	y	k	o	
	9	r	p	g	i	l	n	x	s	Köln
	10	e	m	k	n	t	a	n	d	Standort
	11	w	a	k	k	o	x	t	n	
	12	y	z	r	z	o	r	g	e	Norderney
	13	e	v	i	b	r	n	e	y	
	14	c	m	k	e	l	c	t	r	Leuchtturm
	15	s	k	e	a	m	i	n	e	in
	16	l	q	u	d	i	n	s	s	1
	17	y	f	v	x	e	c	s	n	6
	18	p	m	b	o	u	l	g	r	0
	19	o	m	g	l	a	d	d	r	Grad
	20	q	s	o	h	e	i	s	m	3 sm
	21	y	r	h	q	a	b	x	g	ab
	22	r	q	d	e	e	h	n	i	gehe mit
	23	h	j	f	u	t	c	t	t	T
	24	n	c	x	m	e	i	n	s	1
	25	d	p	k	l	f	u	n	f	5
	26	s	b	i	j	d	r	e	i	3
	27	g	x	t	g	n	a	c	q	nach □
	28	f	u	c	n	u	n	e	u	9
	29	p	h	z	t	n	f	u	h	5
	30	t	o	w	v	f	f	u	r	5
	31	u	d	j	b	f	e	i	n	1
	32	v	c	y	b	s	l	i	n	links
	33	j	i	n	g	k	o	b	n	oben
Endkenngruppen	34	b	m	o	g	—	—	—	—	
	35	p	y	u	d	—	—	—	—	

Bletchley



intercept sheet

decrypt

Poolse periode

Ciężki

- jaarwisseling 1927/1928 eerste contact
- juli 1928 cryptoanalyse faalt
- Ciężki teamleider Biuro Szyfrów
- 1929 Rejewski, Rózycki en Zygalski binnengehaald
- 1 sep 1932 enigma werk begint
- 17 sep 1939 evacuatie uit Polen
- 1939-1942 werk in Vichy Frankrijk

Marian Rejewski

- 9 dec 1932 Rejewski breekt enigma m.b.v. Asche sleutels
- ontwikkeling van de *bomby*
- 1 feb 1936 maandelijks rotorwissel
  1 nov 1936 dagelijks rotorwissel
  1936-1938 groei aantal netwerken
  1939 extra rotors *analyse stokt*
- 25-26 juli 1939 Pyry conferentie
  Engelsen en Fransen worden ingelicht

Achilleshiel van enigma

Structuur enigma bericht tot 1940

```
1755-135 WEP ULZNU HFIKLB SGEXU ...
1755     = Zeitgruppe
135      = aantal letters vanaf Kenngruppe
WEP      = Grundstellung
ULZNU    = Kenngruppe
HFIKLB = 2x vercijferde Spruchschlüssel
```

Sedert 1 mei 1940 Spruchschlüssel eenmaal vercijferd te laat!

enigma substitutie

- rotor effectueert monoalfabetische substitutie
- A → P → R → F → A heet cykel (APRF)
- complete monalfabeet (APRF)(GQZBJV)..()
- A → P en P → A heet involutie (AP)
- enigma (AP)(ZI)(GE)..() product van involuties
- 2x achtereen enigma substitutie uitvoeren geeft gepaarde cykels (AJUT)(KVZF)(Q)(M)..
- dubbele vercijfering Spruchschlüssel doet dit!

Dubbele vercijfering

tweemaal Spruchschlüssel ABC ABC → PQR XYZ

```
E1: A → P  en  P → A
E2: B → Q  en  Q → B
E3: C → R  en  R → C
E4: A → X  en  X → A
E5: B → Y  en  Y → B
E6: C → Z  en  Z → C
```

```
P→X is E4(A) = E4(E1(P)) dus E4E1(P)→X
Q→Y is E5(B) = E5(E2(Q)) dus E5E2(Q)→Y
R→Z is E6(C) = E6(E3(R)) dus E6E3(R)→Z
```

drie dubbele vercijferingen E4E1, E5E2 en E6E3 !!!

Completeer cykelparen

- `??????` → `PQRXYZ` resulteert in
  `E4E1 = (P,X,...)`
  `E5E2 = (Q,Y,...)`
  `E6E3 = (R,Z,...)`

- `??????` → `TYMGNZ` verlengt tot
  `E5E2 = (Q,Y,N,...)` enz.

- veel berichtkoppen →
  complete cykels dubbele vercijfering

Test Spruchschlüssel

```
E4E1 = (DVPFKXGZYO)(EIJMUNQLHT)(BC)(RW)(A)(S)
E5E2 = (BLFQVEOUM)(HJPSWIZRN)(AXT)(CGY)(D)(K)
E6E3 = (ABVIKTJGFQNY)(DUZREHLXWPSMO)
```

vraag: kan een Spruchschlüssel AAA zijn?
antwoord: controleer op letters in juiste cykel

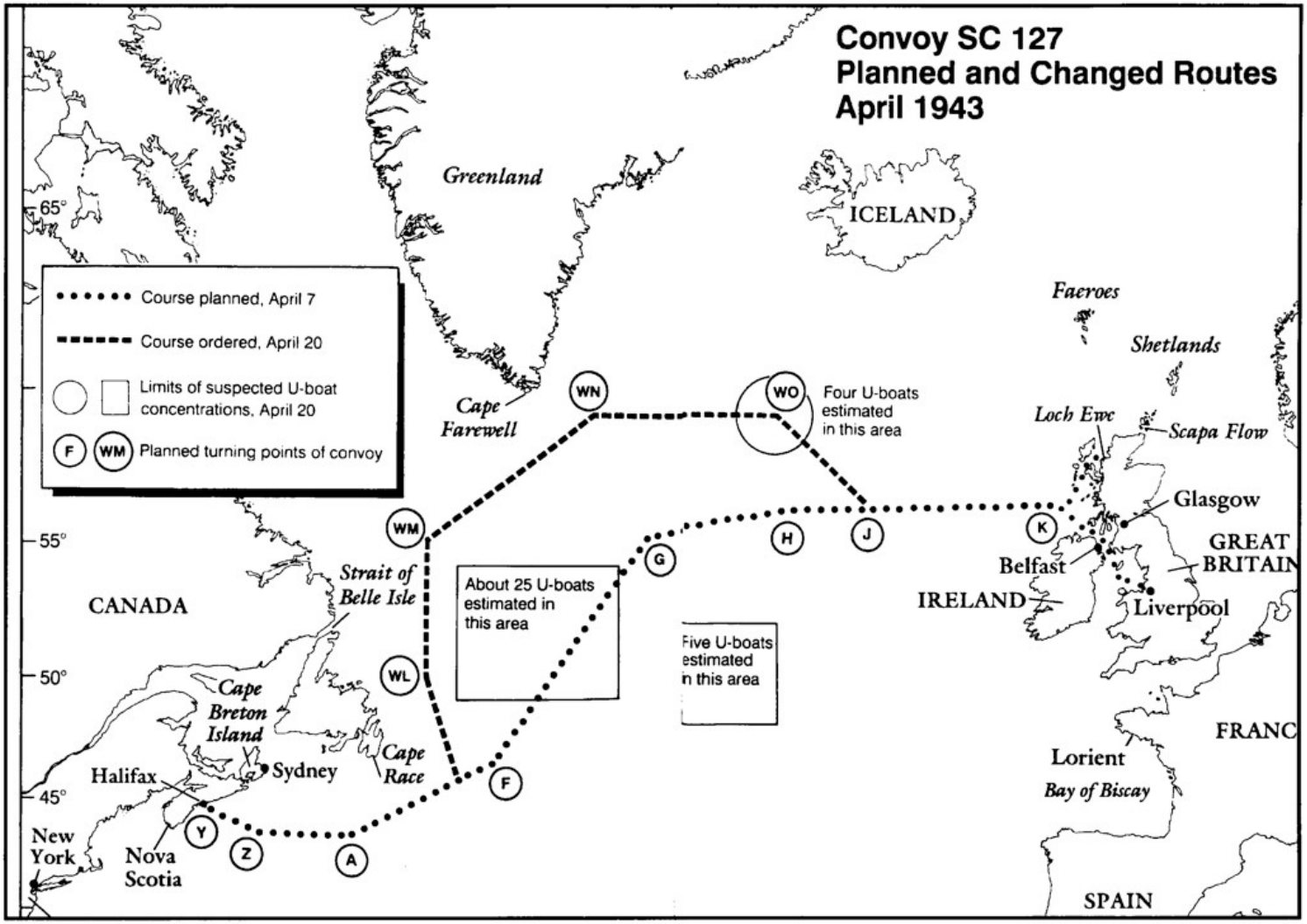
```
SUGSMF = AAAAAA? E5E2=UM niet in (AXT)(CGY) NEE

SYXSCW = AAAAAA? E4E1=SS in (A)(S)
                 E5E2=YC in (AXT)(CGY)
                 E6E3=XW in (ABV..)(DUZ..XW..)
antwoord JA
```

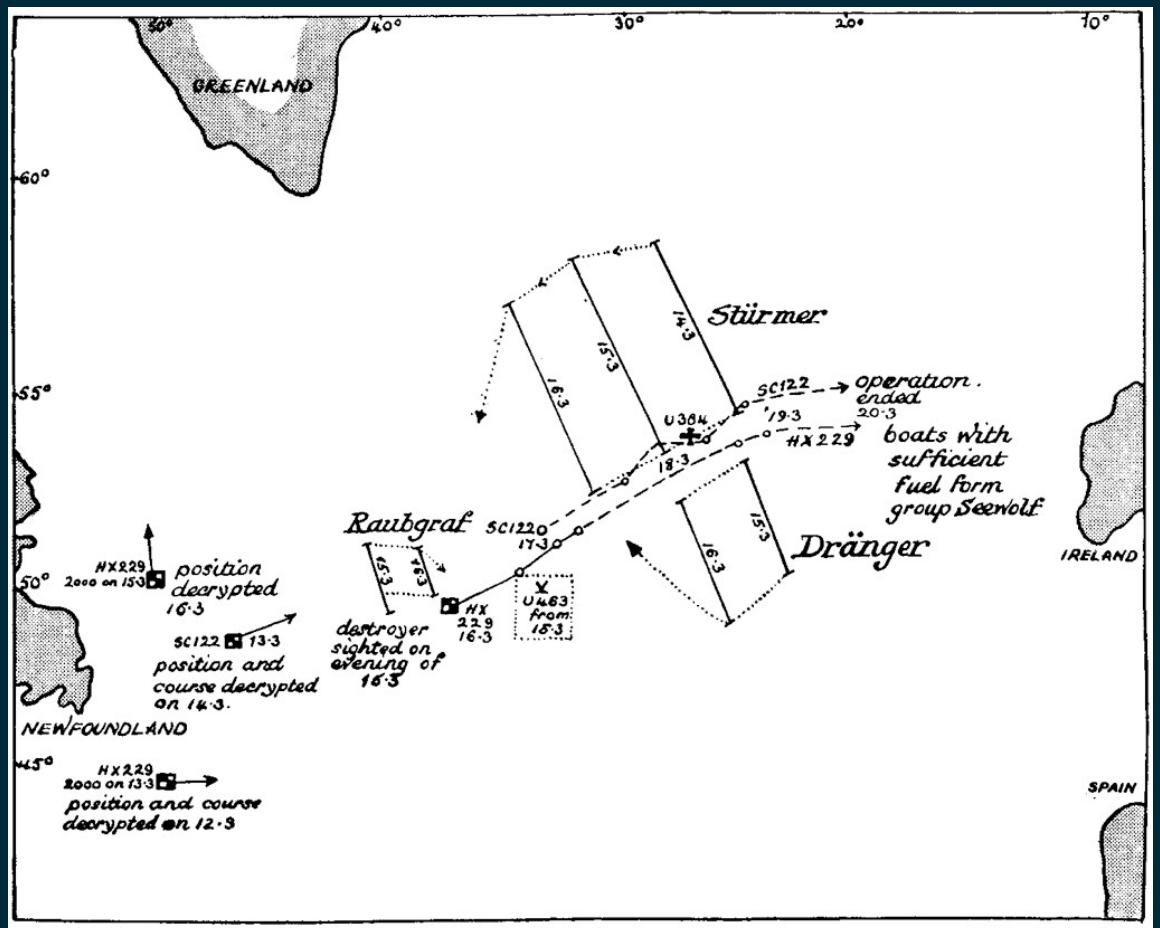
Breken enigma sleutels

- berichten gecodeerd en daarna Enigma vercijfering
- U-Boot zendt weerbericht in Wetterkurzschlüssel
- positie U-Boot wordt uitgepeild
- positie en weersituatie ter plaatse geeft crib
- instelling Enigma bepaald uit crib
- operationele berichten nu te ontcijferen met Kurzsignalheft
- blackout: BdU wijzigt Wetterkurzschlüssel
- gevolg: geen cribs, geen sleutel, operationele berichten niet ontcijferd
- fatale fout: BdU had tegelijkertijd Kurzsignalheft moeten wijzigen
- maart 1943: in grote konvooislag operationele berichten gebroken
- gevolg: reconstructie Wetterkurzschlüssel mogelijk gemaakt

Konvooien

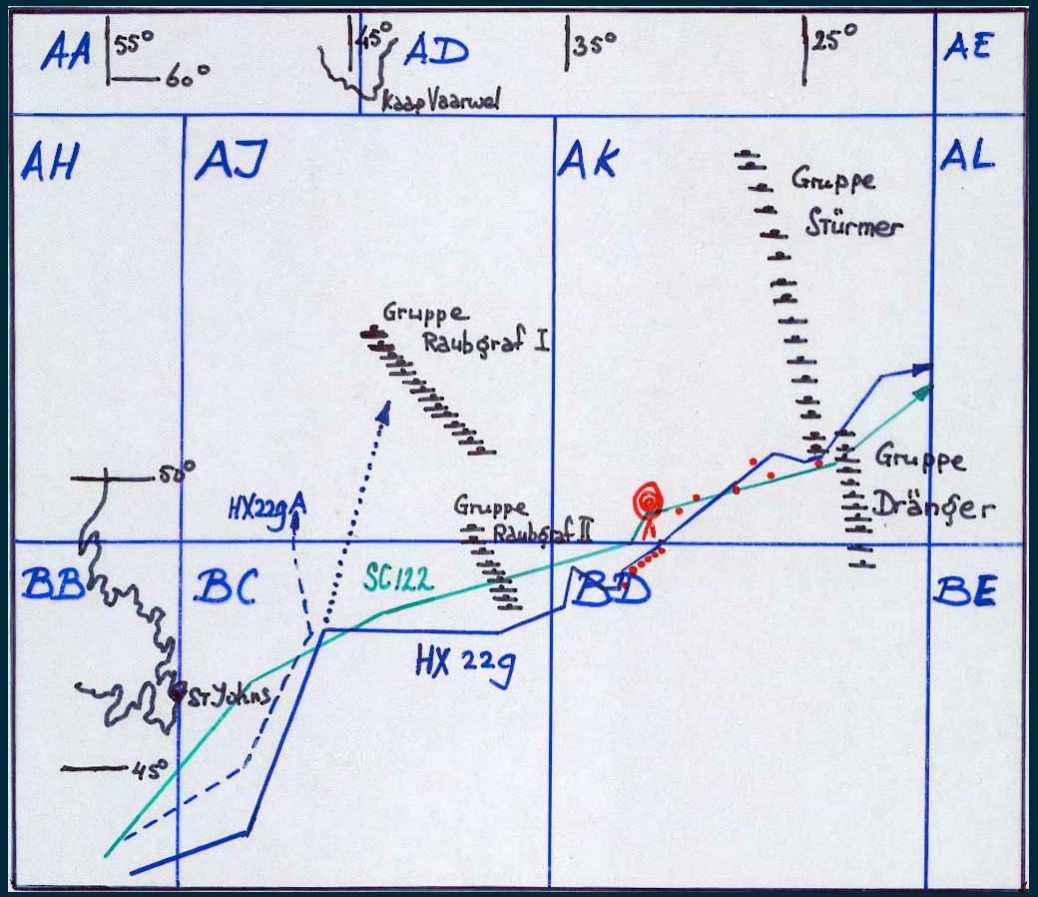

Convoy SC 127
Planned and Changed Routes
April 1943
Course planned, April 7
Course ordered, April 20
Limits of suspected U-boat concentrations, April 20
F WM Planned turning points of convoy
Greenland
ICELAND
Faeroes
Shetlands
Cape Farewell
WN
WO
Four U-boats estimated in this area
Loch Ewe
Scapa Flow
Glasgow
GREAT BRITAIN
Belfast
IRELAND
Liverpool
WM
H
J
K
G
About 25 U-boats estimated in this area
Five U-boats estimated in this area
Strait of Belle Isle
CANADA
WL
Cape Breton Island
Halifax
Sydney
Cape Race
F
Lorient
Bay of Biscay
FRANC
SPAIN
New York
Nova Scotia
Y
Z
A
65°
55°
50°
45°

Wulfpack tactiek



Groups *Raubgraf*, *Stürmer* and *Dränger*, 15th–20th March, 1943.
Operations against SC 122 and HX 229

Marine Quadratkarte

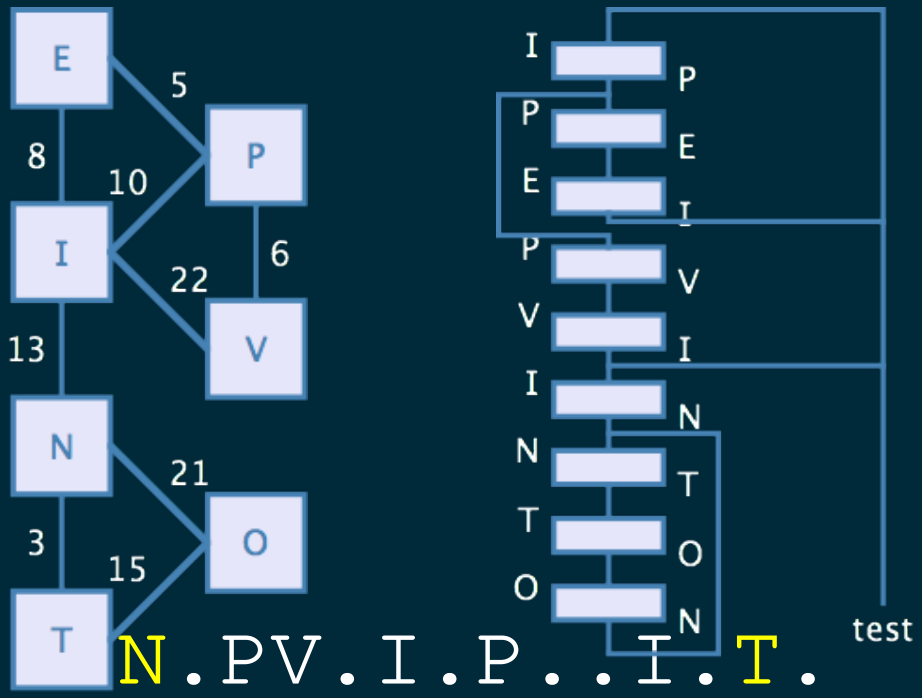


contactsignaal U338

17 maart 1943 03:02

bericht	*code*	*enigma*
Feind im Sicht	*CCHH*	*XGBT*
AK80	*JNOS*	*GZZV*
598	*NBYU*	*QAGN*
50 Grad	*QJRK*	*TBAB*
Fahrt 7 sm	*QRTU*	*ZVKL*

Turing bombe



N.PV.I.P..I.T.
....OV.
..T.EP.E.I..N.O.
....NI.
lus NTO

Effect van maart 1943