

Cursus Cryptografie

Enigma



Onderwerpen

- ontwikkeling
- cryptografische rotor
- Enigma
- Poolse periode
- Cryptoanalyse in Bletchley Park
- convooislag op de Atlantische Oceaan
- Turing bombe

Geschiedenis

- 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

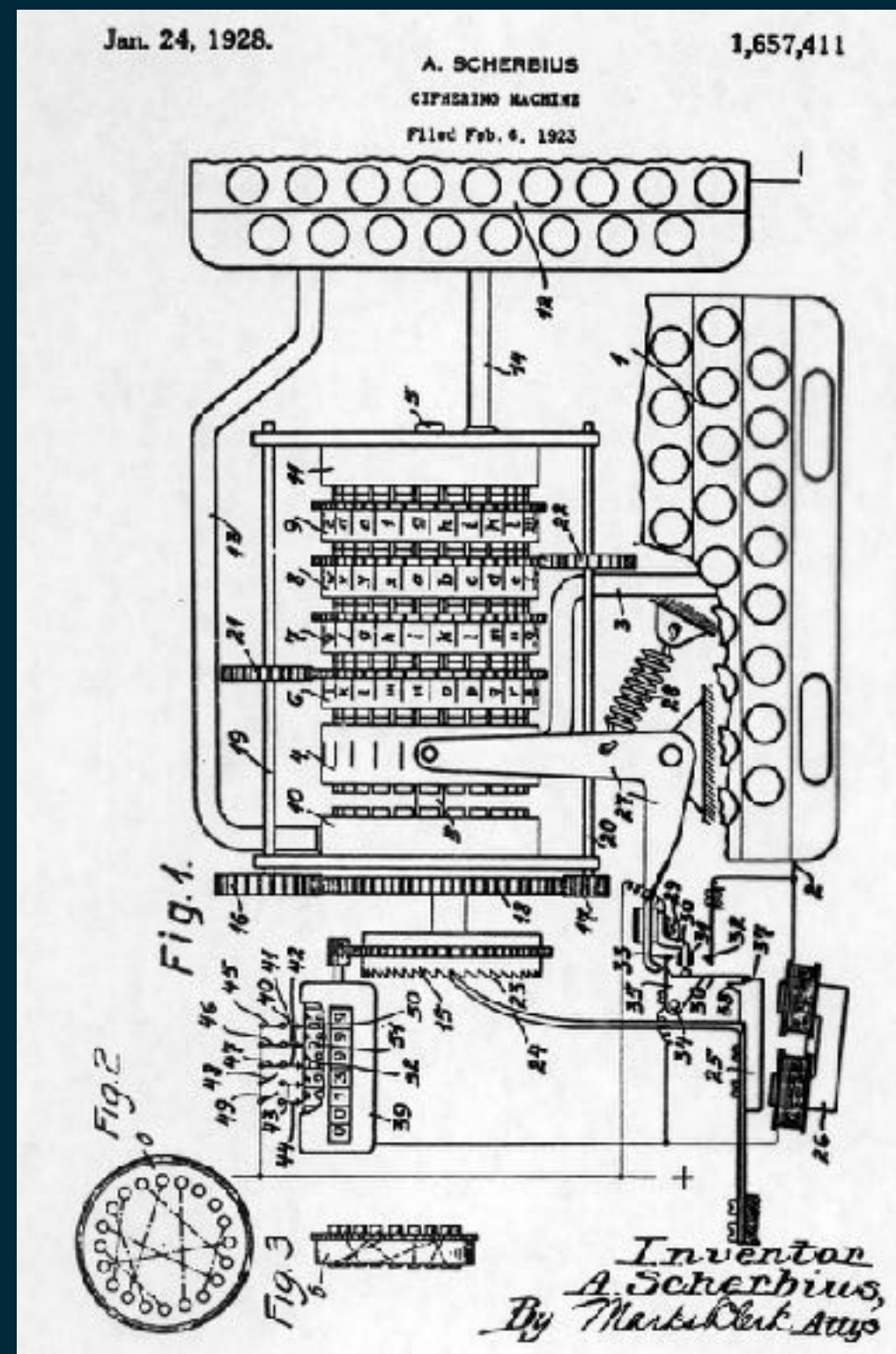


Van Hengel

Patent Scherbius



Arthur Scherbius



Modellen



Enigma-G
Abwehr



Enigma
Wehrmacht



4-rotor Enigma
Kriegsmarine

Andere rotor machines



USA: SIGABA



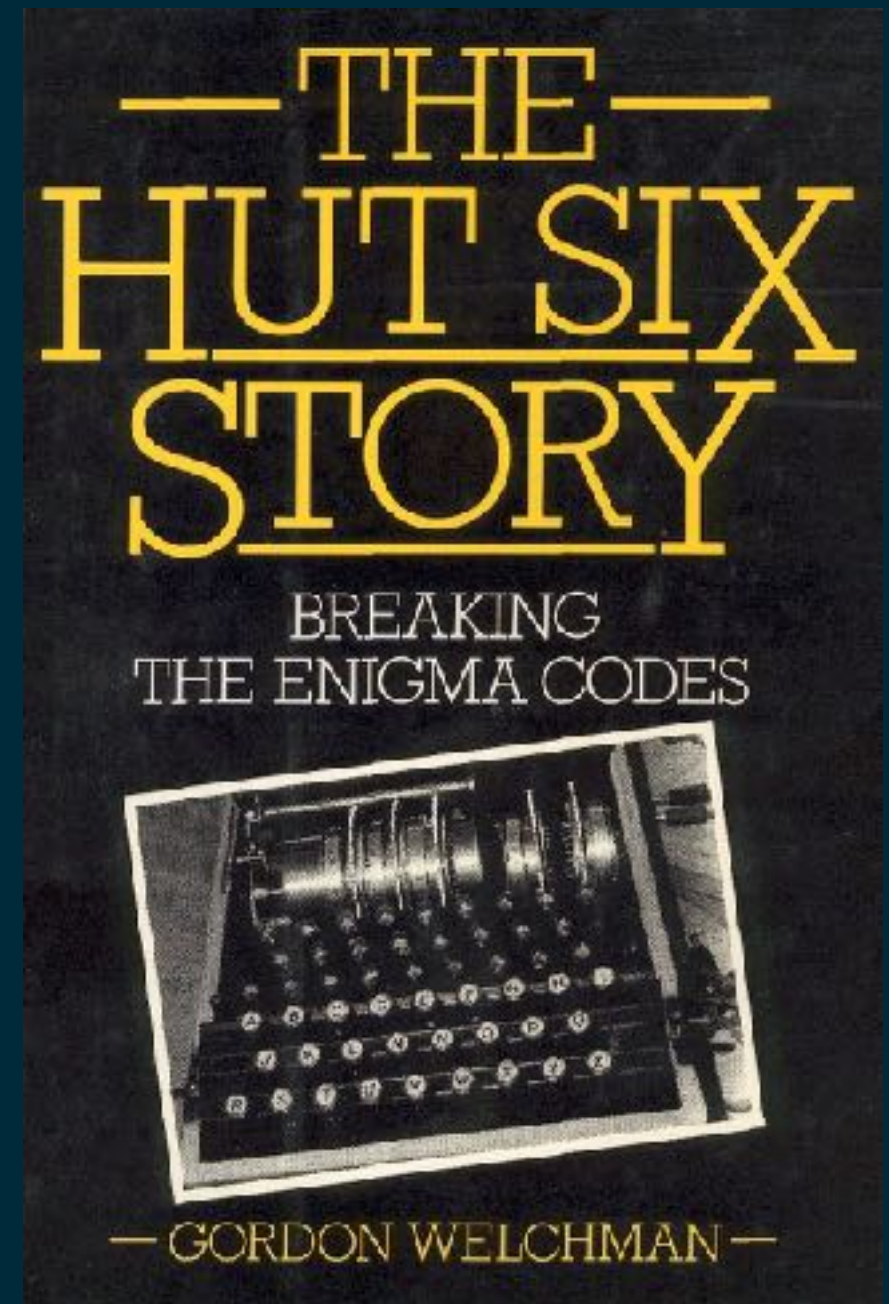
USSR: FIALKA

Enigma in aktie

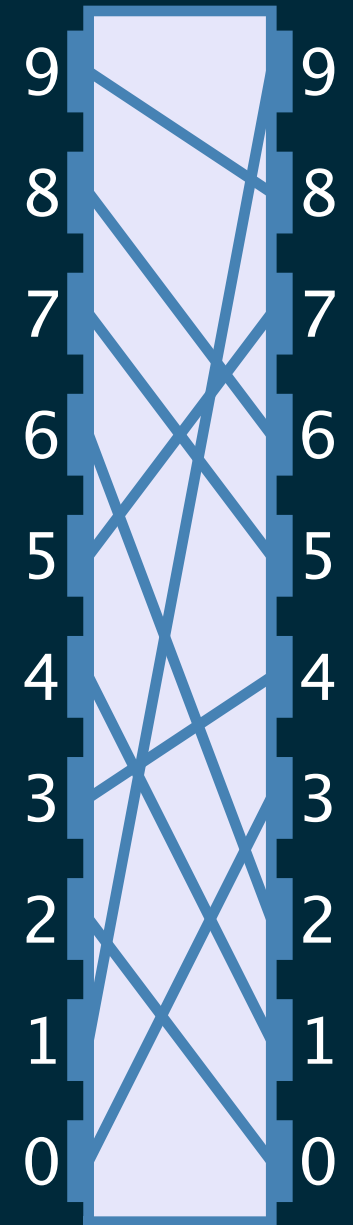
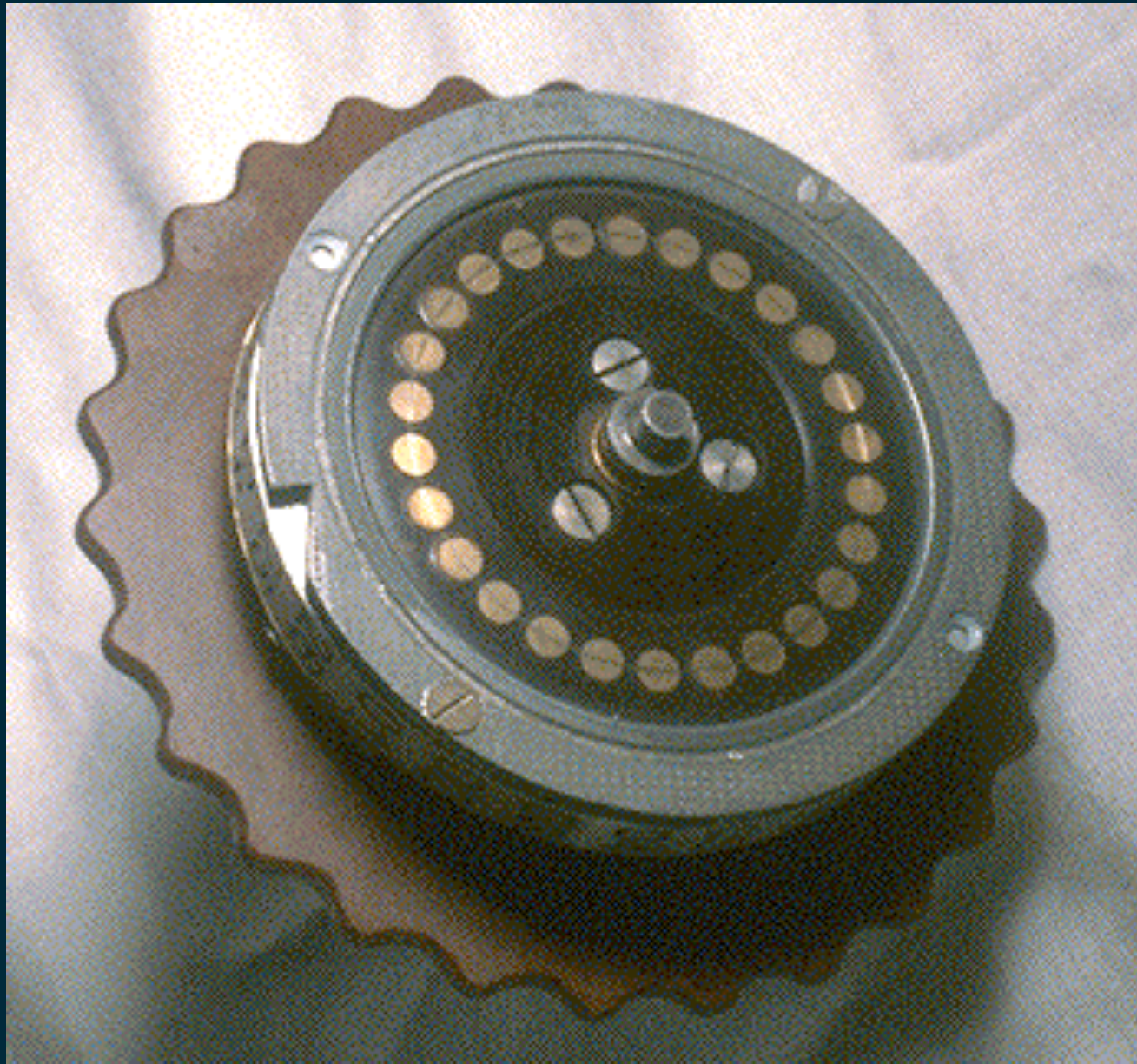


Cryptoanalyse

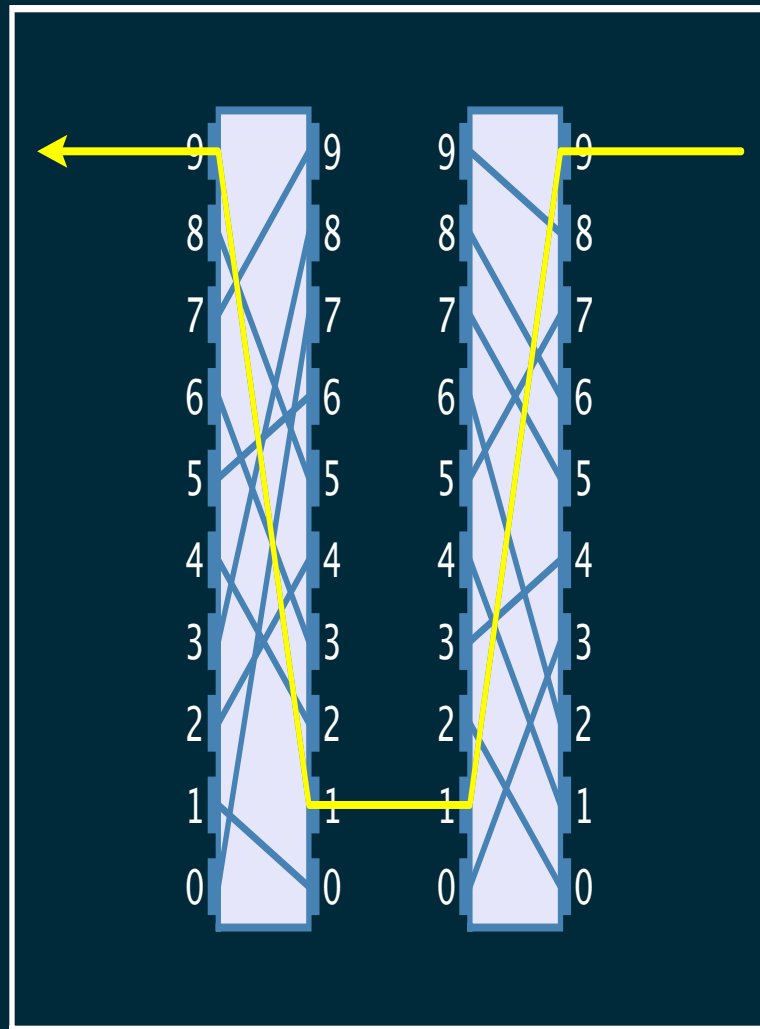
- 1932 Enigma in Polen gebroken
- 1939 Polen delen hun kennis
- 1939–1945 Bletchley Park
- 1940 eerste Turing bombe
- 1941 Schlüssel-M veilig verklaard
- 1942 blackout U-Boot traffic
- 1974 Winterbotham *The Ultra Secret*
- 1982 Welchman *The Hut Six Story*



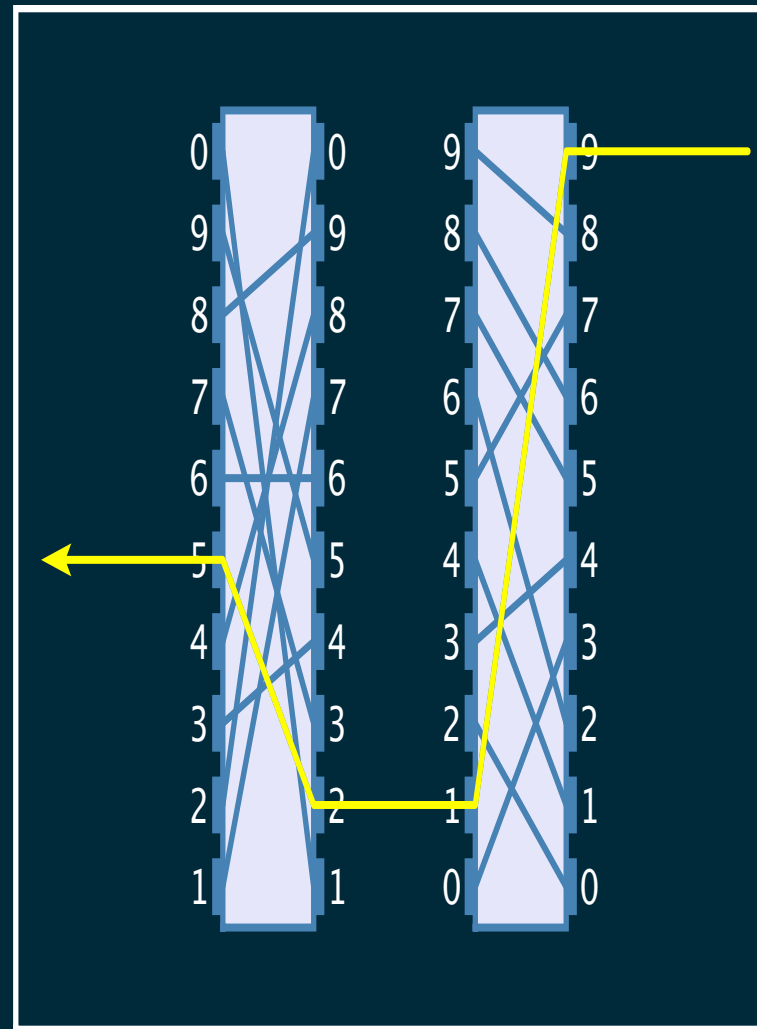
Enigma rotor



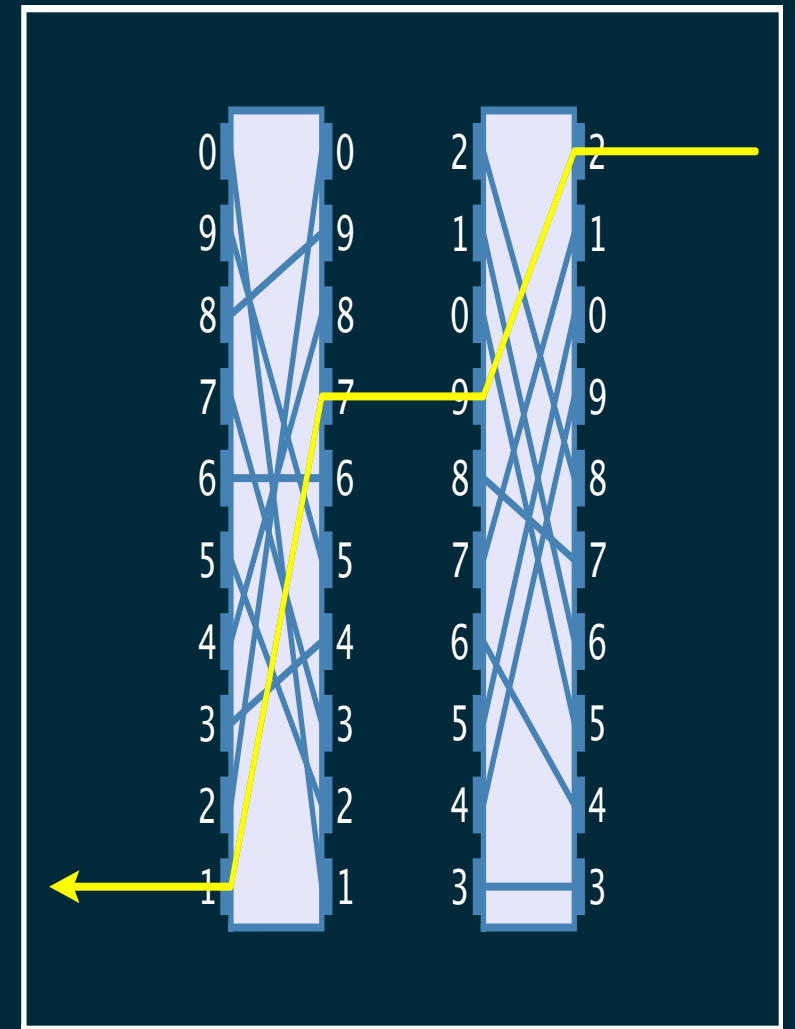
Rotor koppeling



stroomloop

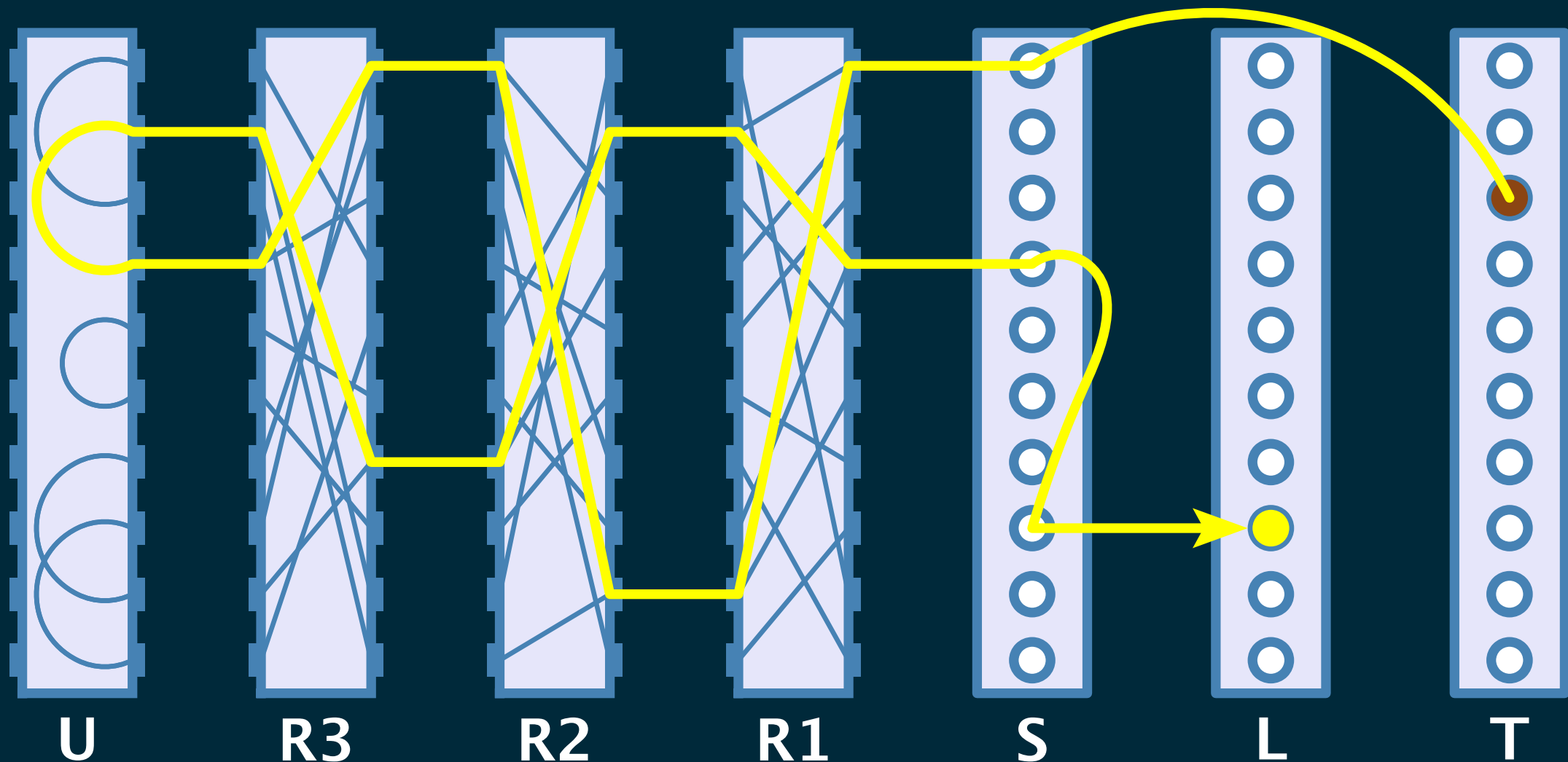


links 1 stap



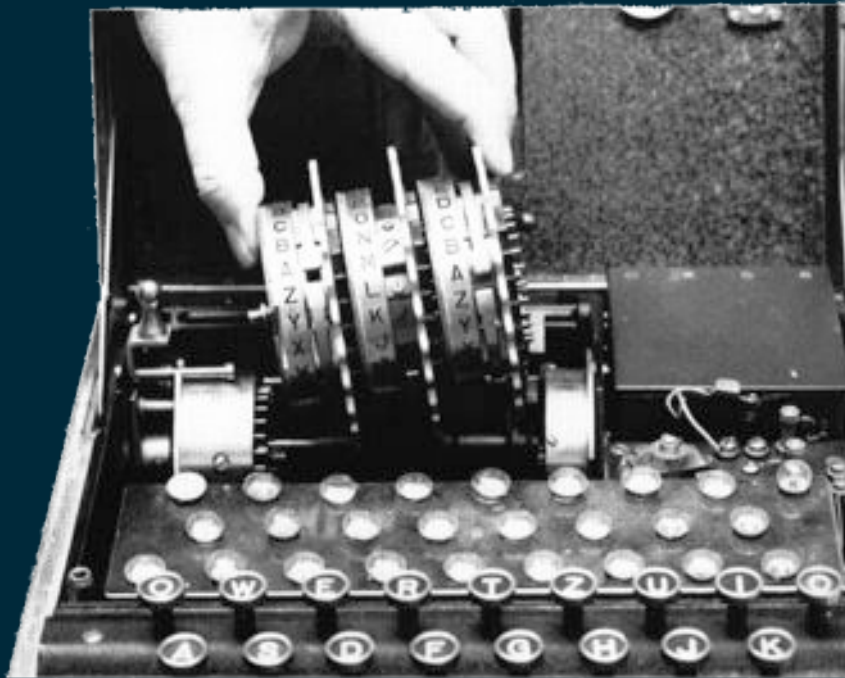
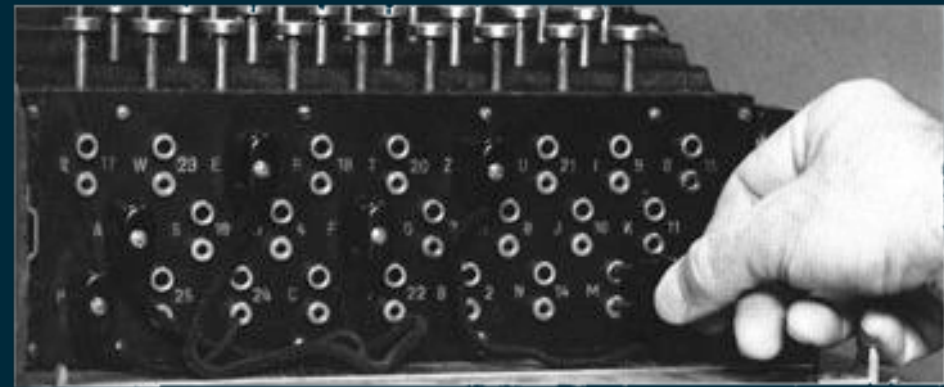
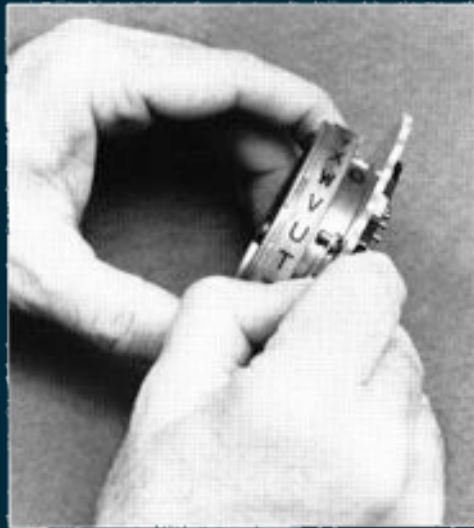
rechts 3 stappen

Enigma schema



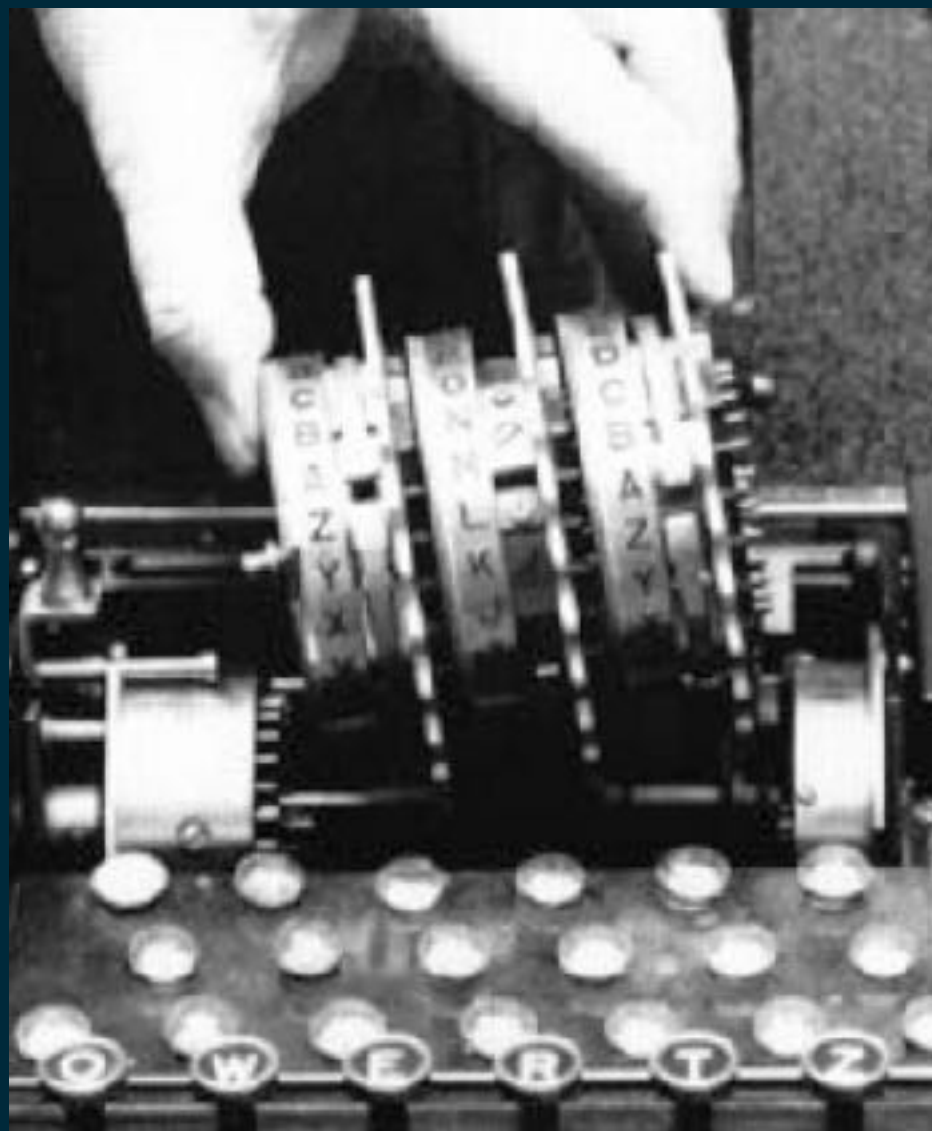
Enigma vercijfering is involutie
als $A \rightarrow B$ dan ook $B \rightarrow A$ maar nooit $A \rightarrow A$

Enigma instelling



let op enigma tot hier tentamenstof !

Herivel tip



	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
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																										

HDR TKZ JFW AQR GRI BOD
 DKT TFO RLI HTQ WNE ABX
 HSK ZRH KYS GEW AUY SAH
 JOO GKX GTK GLQ XWA FRJ
 XEI CAM DTR PWI SUM UZR

Figure 5.1 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. Ov. Nr. 32/1

Marineoberkommando Nordsee

Druckchriftenverwaltung

Mhrzeitgruppe 1053		Spruchschlüssel: s p l					
Gruppenszahl 35		gültig für 3. B.					
Anfangs- fenngruppen			Buchgruppen				Bedeutung
	1	b m	e g	v l	h 2 f	y 3 n	Schlüsselgruppe
	2	p y	u d	v l	h 2 f	y 3 n	Verfahrenleengruppe
	3	f j	i a	v e	a	y	Beife
	4	t z	w r	e l	c	i	
	5	l h	s e	p z	i	g	Leipzig
	6	q f	d x	a n	a	n	an
	7	n o	u p	f l	o	t	Stotte
	8	a s	w l	e y	k	o	
	9	r p	g i	l n	x	a	Rdm
	10	c m	k n	t u	n	d	Staubot
	11	w a	k k	e o	t	n	
	12	y z	r z	o e	e		Northern
	13	e v	i b	r n	e	y	
	14	c m	k e	l o	r		Seuchtturm
	15	s k	e a	m i	m	e	in
	16	l q	u d	i n	s		1
	17	y f	v x	e o	s	n	5
	18	p m	b o	u l	g	r	0
	19	o m	g l	a d	d	r	Grab
	20	q s	o h	a i	s	m	8 sm
	21	y r	h q	a t	g		ab
	22	r g	d e	e n	i		gehe mit
	23	h j	f u	t t	t		T
	24	n e	a m	e s	n	s	1
	25	d p	k l	f u	n	f	5
	26	a b	i j	d r	c	i	3
	27	g x	t g	u e	c	g	nach □
	28	f u	c n	u n	c	n	9
	29	p h	z t	n f	u	t	5
	30	t o	w v	f f	u	n	5
	31	u d	j h	e i	n		1
	32	v o	y h	a l	i	n	lins
	33	j i	n g	k o	b	n	oben
	34	b m	o g	—	—	—	
35	p y	u d	—	—	—		
End- fenngruppen							

Verchlüsselung
mit Schlüssel M

Ende-
fenngruppen

Poolse periode



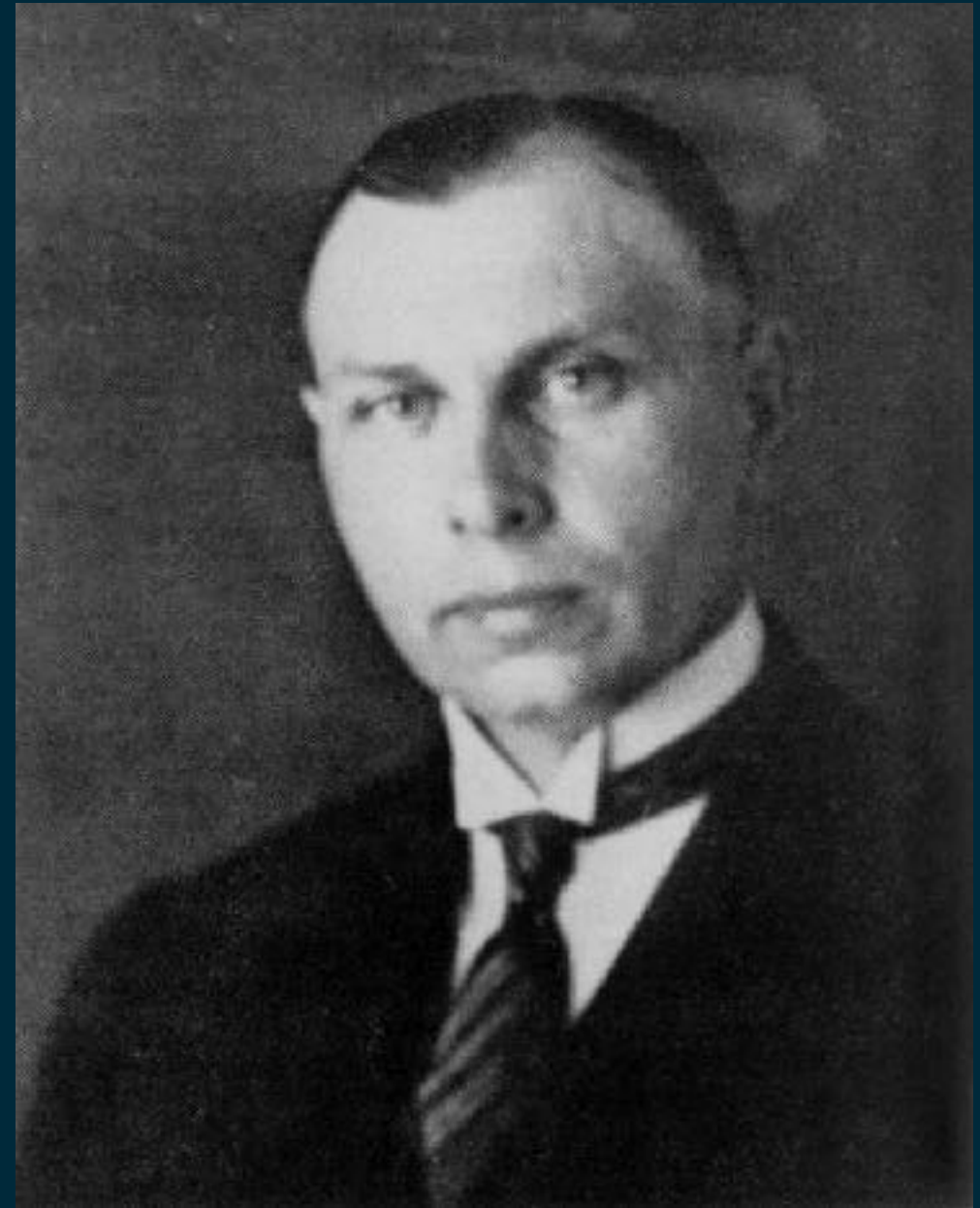
Ciężki

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

Asche documenten



Gustave Bertrand



Hans Thilo Schmidt

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 stopt*
- 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
- $A \rightarrow P \rightarrow R \rightarrow F \rightarrow A$ heet cykel (APRF)
- compleet alfabet in cykels (APRF)(GQZBJV)..()
- $A \rightarrow P$ en $P \rightarrow A$ heet involutie cykel (AP)
- Enigma (AP)(ZI)(GE)..() is product van involuties
- 2x achtereen Enigma substitutie uitvoeren geeft gepaarde cykels (AJUT)(KVZF)(Q)(M)..
- dubbele vercijfering Spruchschlüssel doet juist dit!

Dubbele vercijfering

tweemaal Spruchschlüssel $ABC \rightarrow PQR \rightarrow XYZ$

$E1: A \rightarrow P \text{ en } P \rightarrow A$

$E2: B \rightarrow Q \text{ en } Q \rightarrow B$

$E3: C \rightarrow R \text{ en } R \rightarrow C$

$E4: A \rightarrow X \text{ en } X \rightarrow A$

$E5: B \rightarrow Y \text{ en } Y \rightarrow B$

$E6: C \rightarrow Z \text{ en } Z \rightarrow C$

$P \rightarrow X$ is $E4(A) = E4(E1(P))$ dus $E4E1(P) \rightarrow X$

$Q \rightarrow Y$ is $E5(B) = E5(E2(Q))$ dus $E5E2(Q) \rightarrow Y$

$R \rightarrow Z$ is $E6(C) = E6(E3(R))$ dus $E6E3(R) \rightarrow Z$

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

Bletchley Park



Hut codebreakers



Alan Turing's bureau



zijn beertje

Bletchley Park

mach 15. WITTING WB 6773

Berlin to H Gr Kurland.

Date	B	Freq	M.H	From P23	To Serial	Serial No
14/2/45	0857	7691	14/2	To End	P1 To P23	KN/WB 6773

"TYPED"

N/A

FEB 21 14 16

B)

ALS RGTS M FUEHR M IM KAMPFEINSATZ VV OKH X PA AG

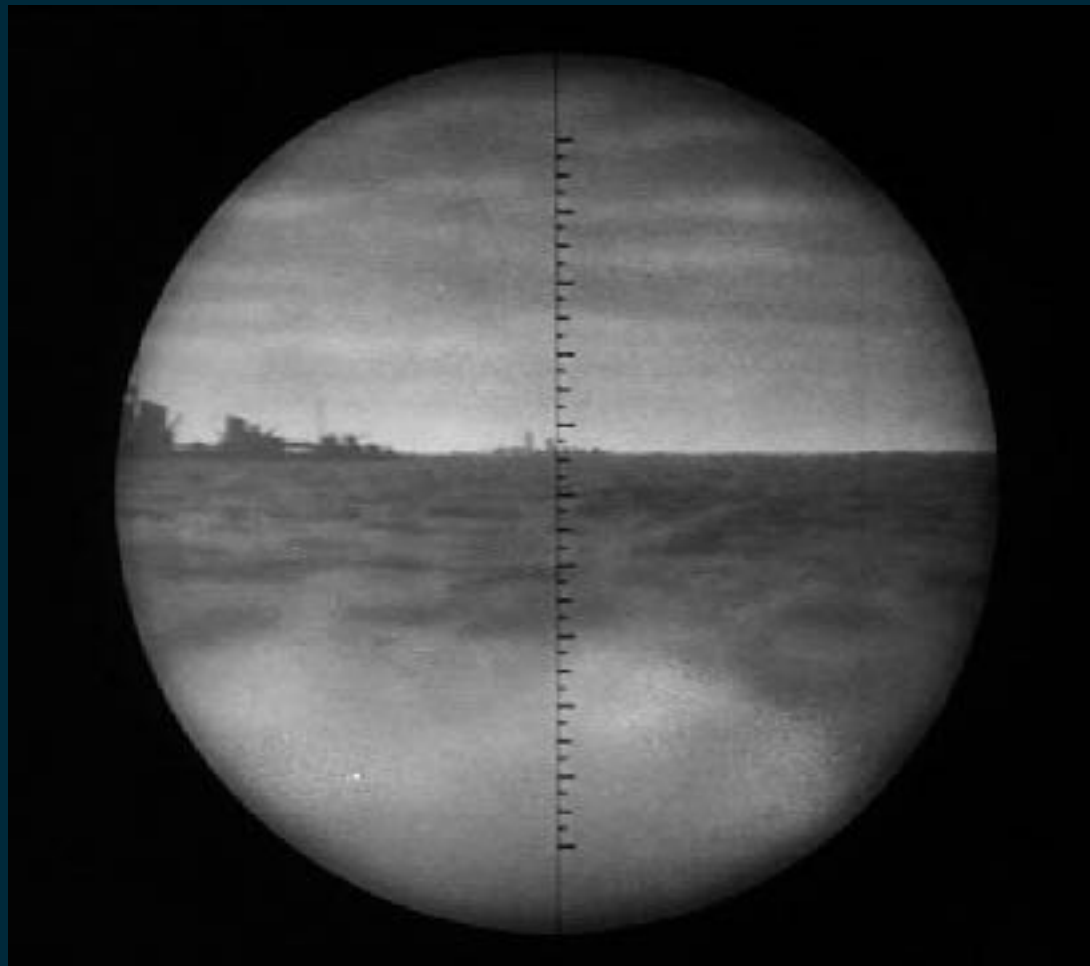
D. HUT 3
14/2
T.E. 0954
F. 7691
M.K. 14/2

intercept sheet

decrypt

VIDEO

Atlantic U-Boot theater



Tegenstanders



BdU Admiraal Dönitz



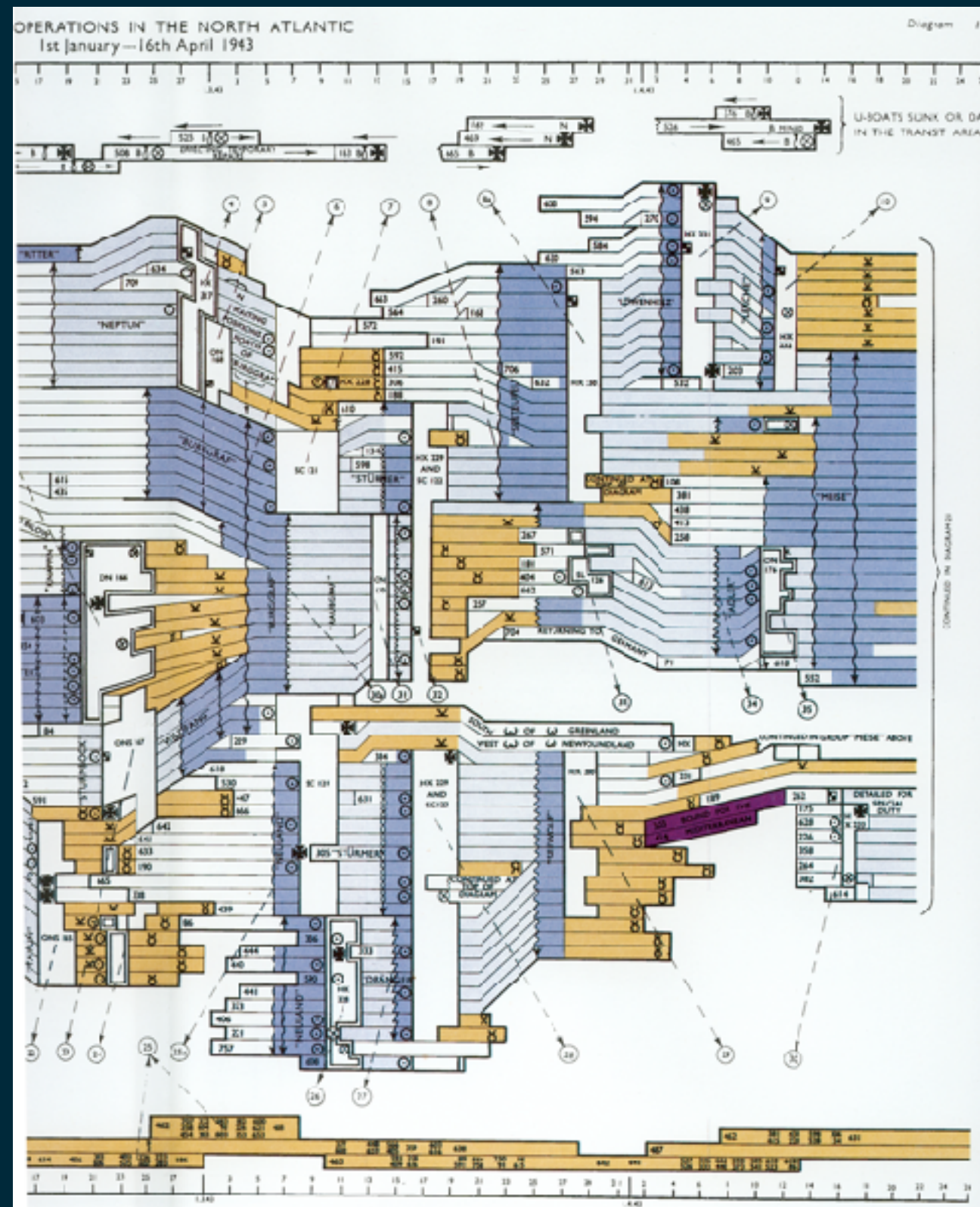
U-Boot tracking room

“Das Boot” U96 Type VIIC



- type VIIC is een Atlantische boot
1940-1944 567 stuks gebouwd
- lengte 67,5 meter bemanning 44 man
- bovenwater 17,7 knopen 9700-3450 mijl
onderwater 7,6 knopen 180-30 mijl
1 knoop = 1,850 km/uur
- duiken tot 100 meter in praktijk meer
- boeg 4 torpedo lanceerbuizen achter 1
max 14 torpedo's en 2 stuks dekgeschut

U-Boot operations



Duitse acties

- 1939 okt: U47 Günther Prien torpedeert *Royal Oak* in Scapa Flow
- 1940 juli: Dönitz verhuist BdU naar Lorient in Frankrijk
- 1941 juni: inzet van de Wulfpack-tactiek
- 1941 aug: boten geadresseerd naar commandant i.p.v. nummer
- 1941 sep: B-dienst ontcijfert British Naval Cypher #2
- 1941 dec: kapt. Rogge vermoedt ontcijfering na zinken raider *Atlantis*
- 1942 jan: happy time aan Amerikaanse oostkust
- 1942 feb: Triton netwerk krijgt M4 en nieuw Kurzsignalheft: blackout!
- 1942 mrt: B-dienst ontcijfert British Naval Cypher #3
- 1942 aug: U-Boten terug naar midden Atlantische Oceaan
- 1943 mrt: Wetterkurzschlüssel gewijzigd, laatste grote konvooislag
- 1943 mei: U-Boten teruggetrokken uit Atlantische Oceaan

Engelse acties

1941 mrt: Enigma en sleutels *Krebs* buitgemaakt in Lofoten-raid

1941 mei: codeboeken U110 buitgemaakt

1941 mei: weerschip *München* met sleutels mei-juni gekaapt

1941 juni: weerschip *Lauenburg* met sleutels juli gekaapt

1941 juli: *Heimisches Gewasser* gebroken



Lemp van U110

Lauenburg



Engelse acties

1941 nov: HMS Devonshire zinkt raider *Atlantis*

1942 feb: M4 brengt *submarine blackout* teweeg

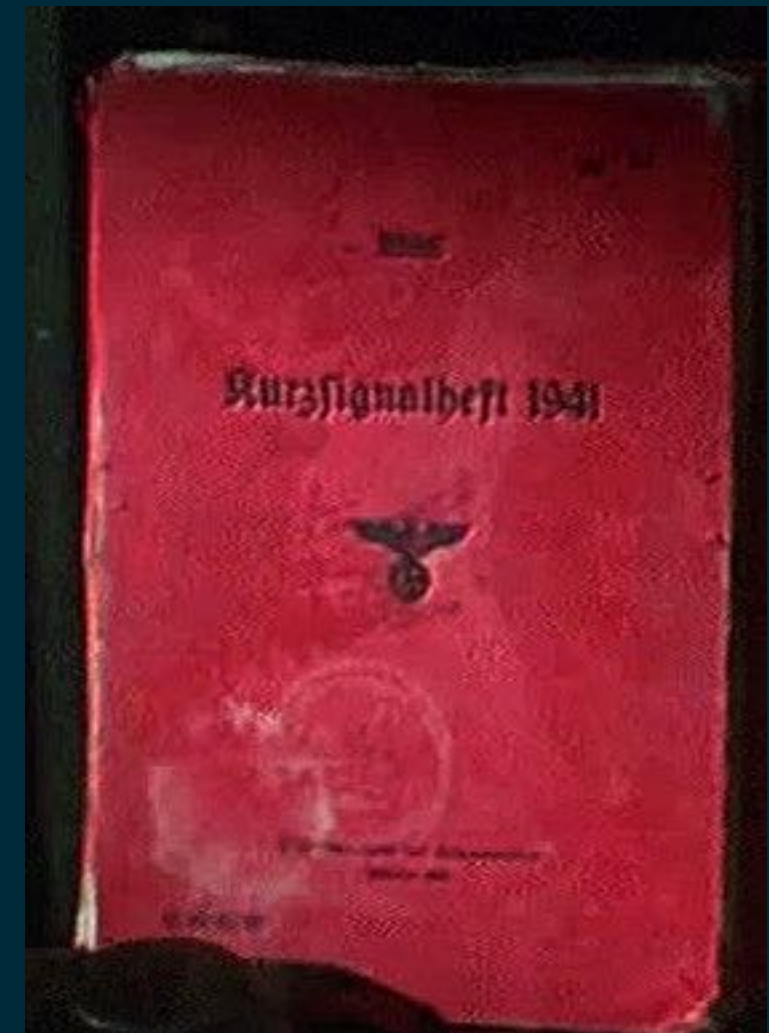
1942 nov: Kurzsignalheft van U559 arriveert

1942 dec: Triton weer gebroken

1943 mar: nieuwe Wetterkurzschlüssel blackout

1943 mar: konvooslag breekt Wetterkurzschlüssel

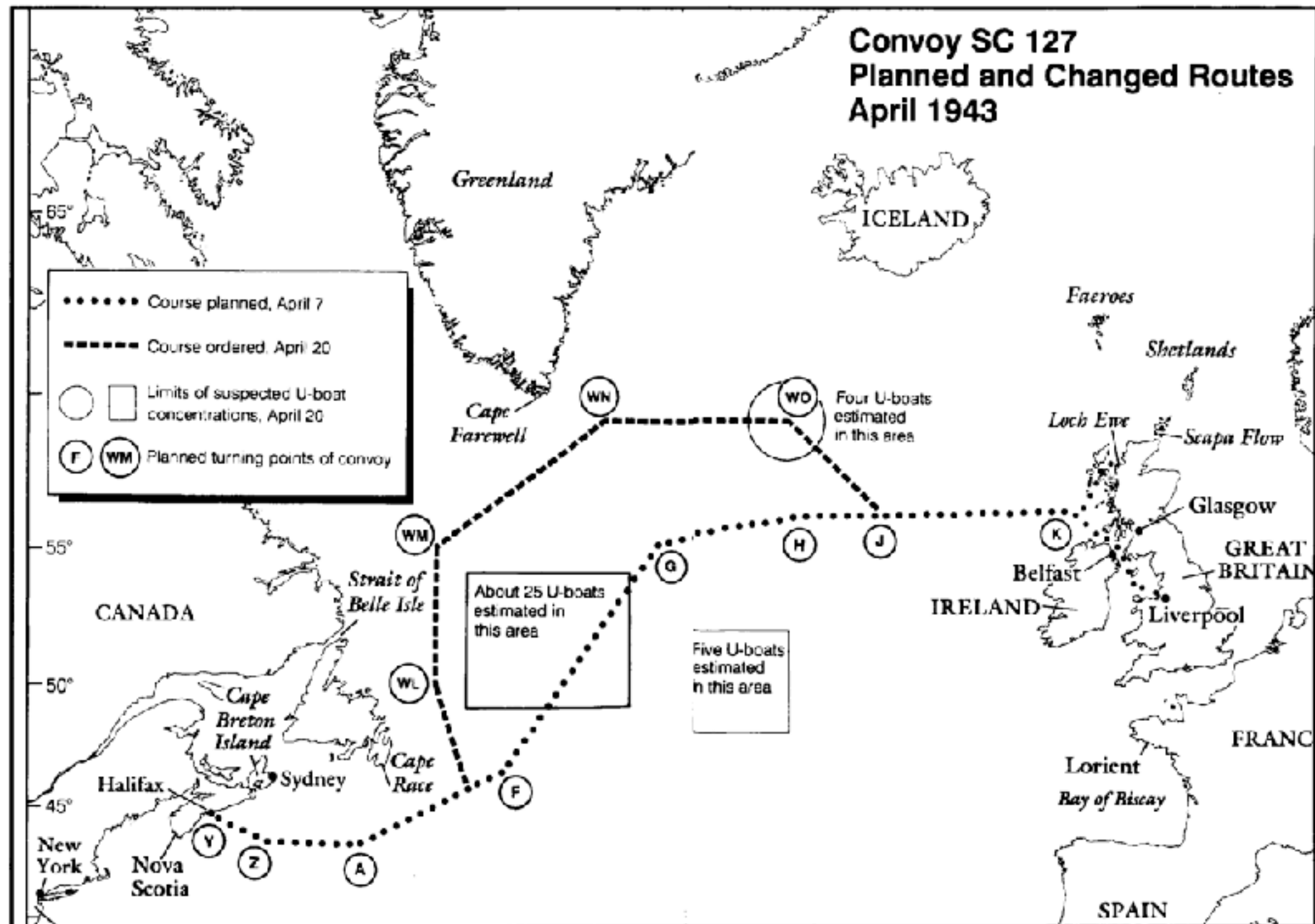
1943 dec: US Navy neemt breken Triton over



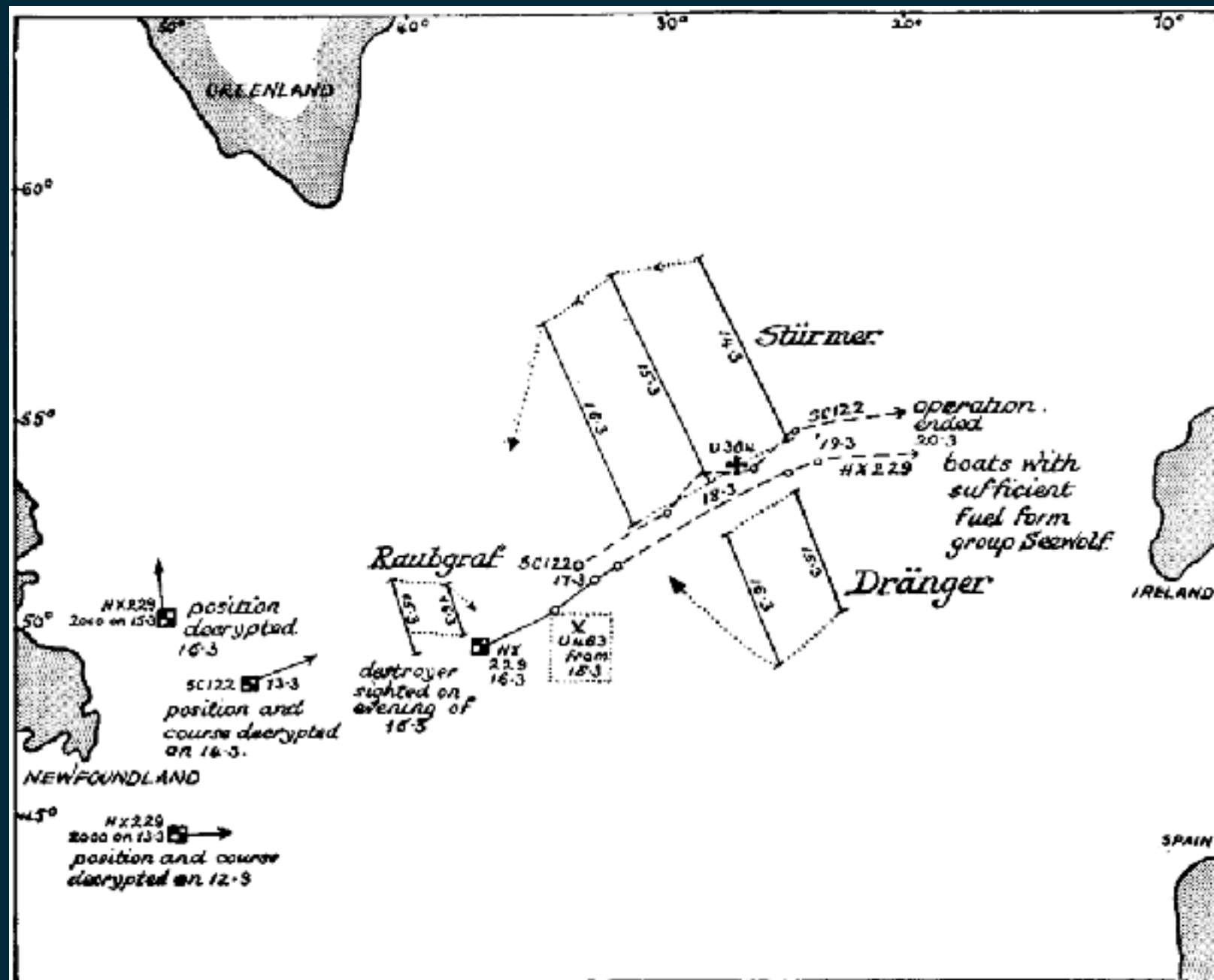
Breken Enigma sleutels

- 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 wijzigd 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

Konvooi operaties

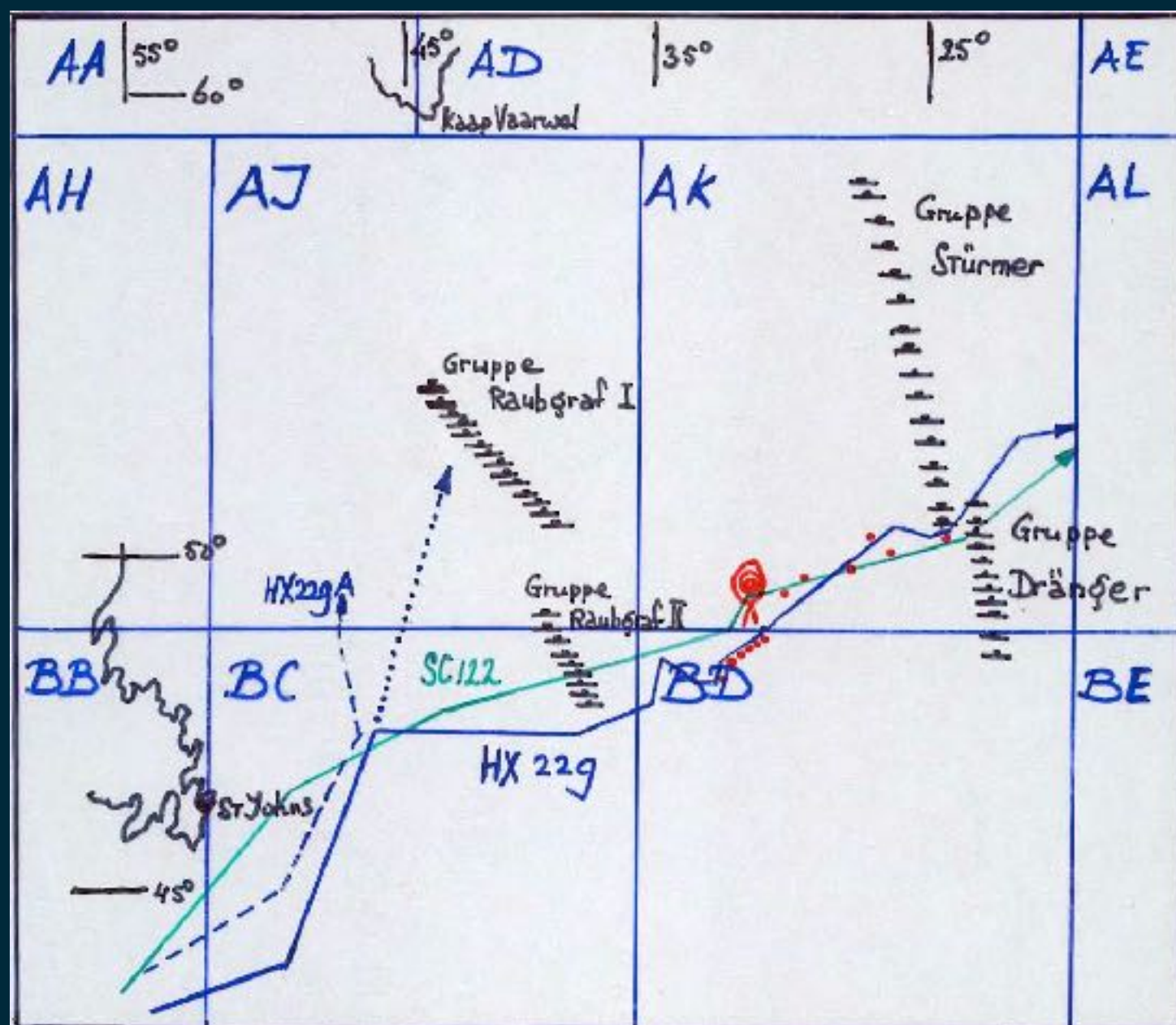


Wulfpack tactiek



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

Konvooislag maart 1943

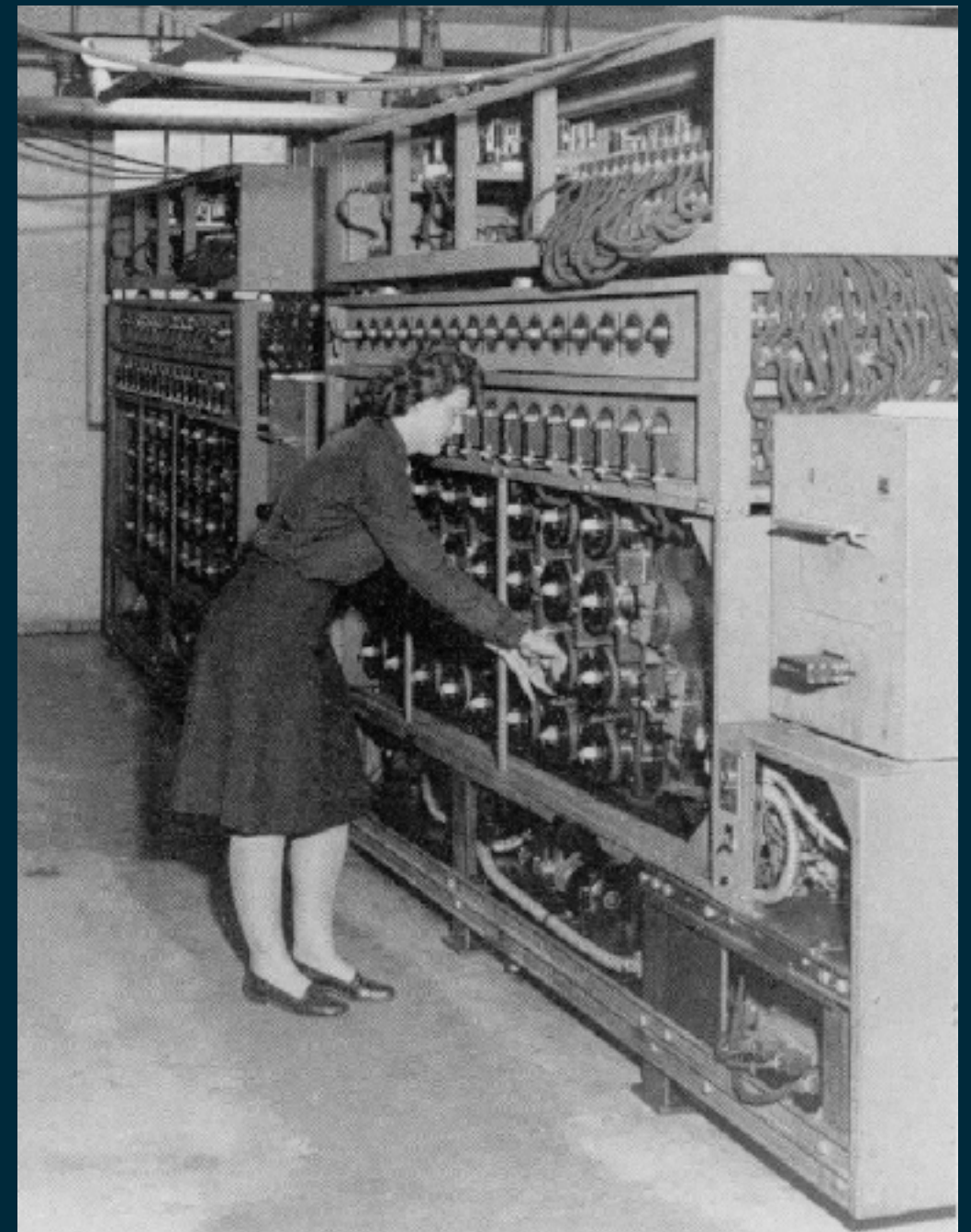
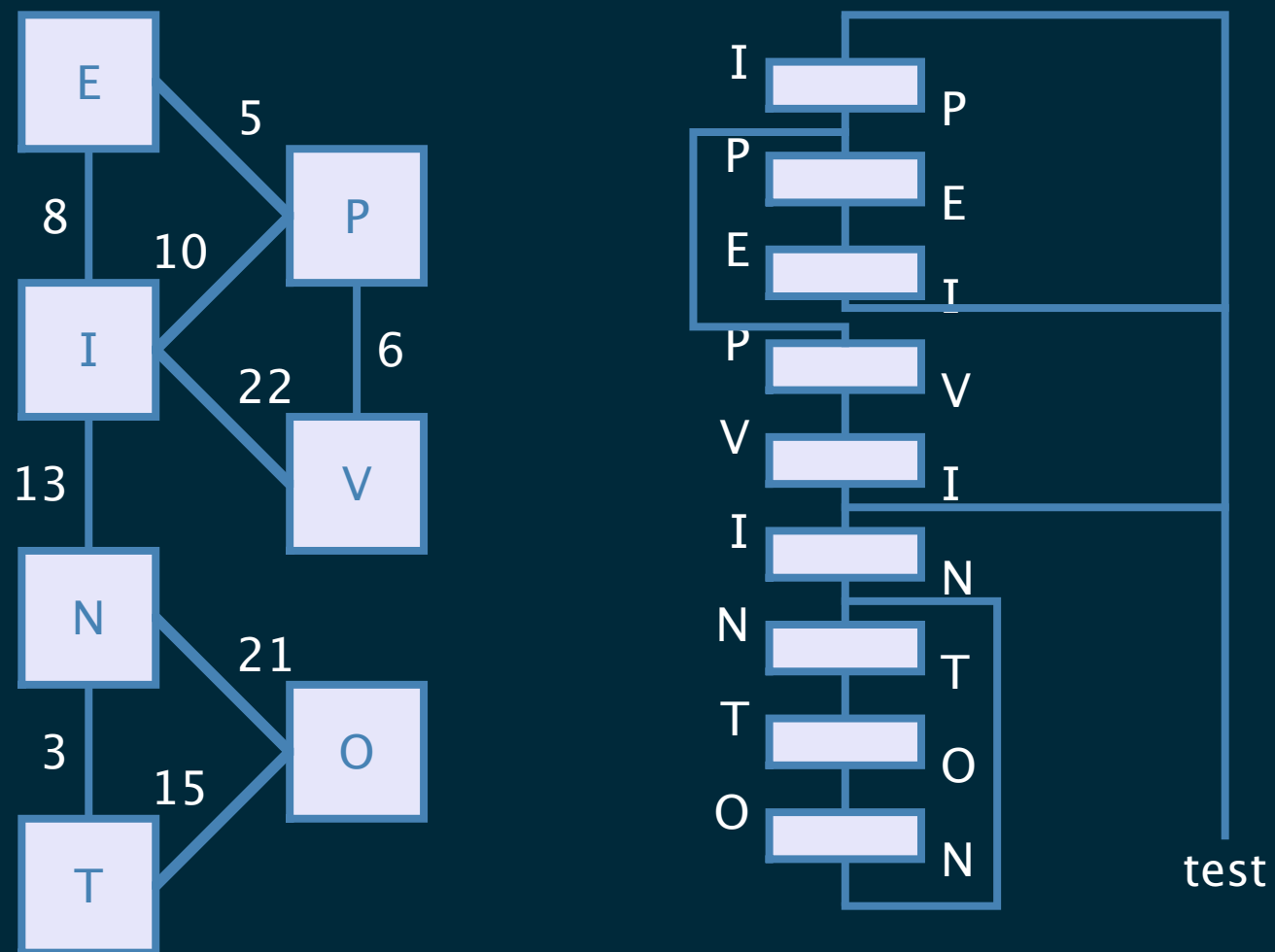


contactsignaal U338

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

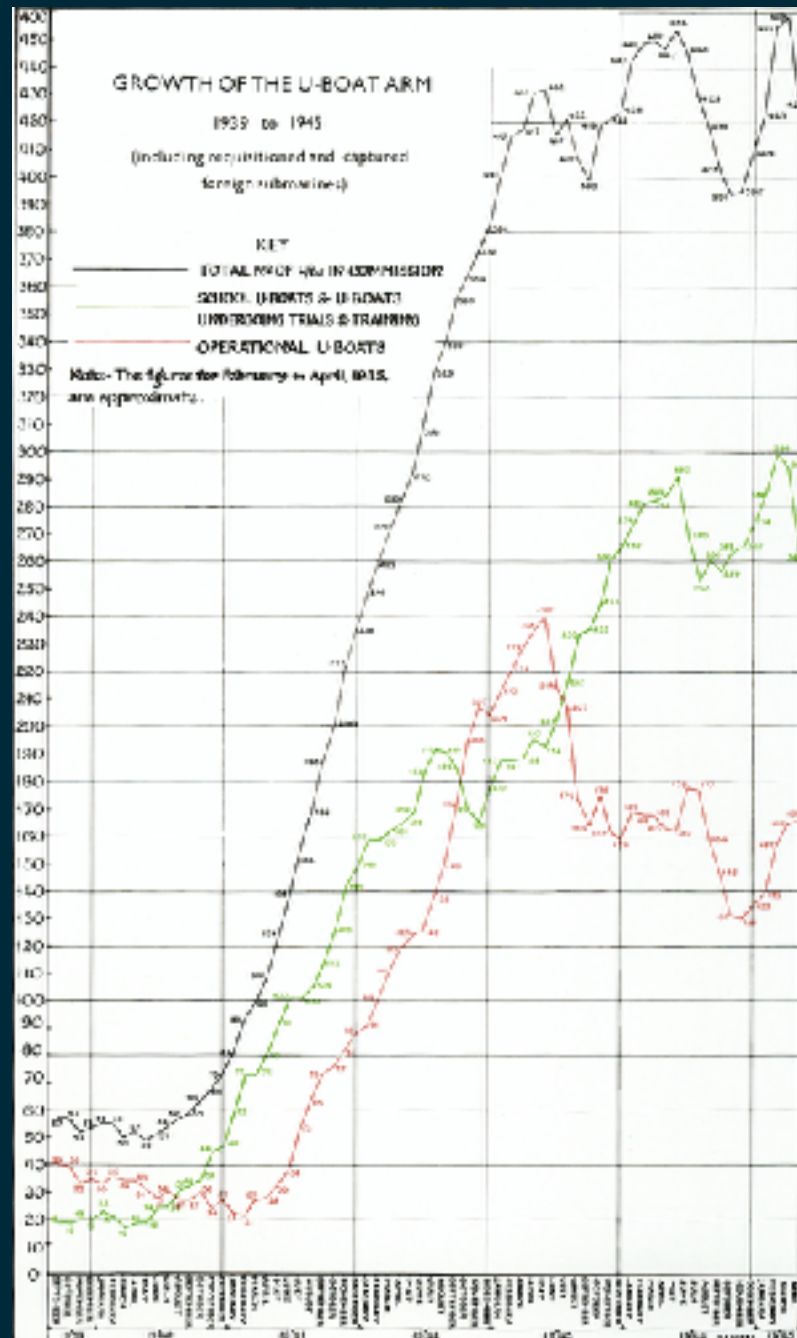


..N.PV.I.P..I.T.....OV.
 ..T.EP.E.I..N.O.....NI.
 lus NTO

Nagebouwde bombe



Effect van maart 1943



VIDEO

Breken van SHARK

