


Did you watch this movie ?

THE FOLLOWING **PREVIEW** HAS BEEN APPROVED FOR  
**ALL AUDIENCES**

BY THE MOTION PICTURE ASSOCIATION OF AMERICA

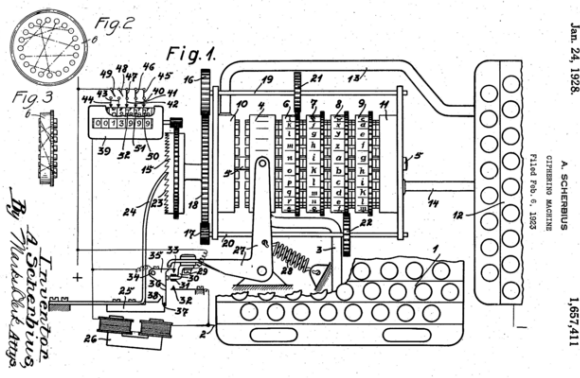
THE FILM ADVERTISED HAS BEEN RATED

**PG-13** PARENTS STRONGLY CAUTIONED   
Some Material May Be Inappropriate for Children Under 13

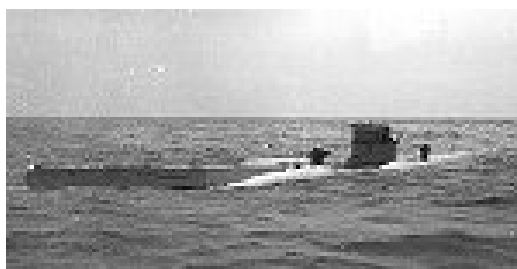


**Tempest**  
Security Intelligence

## Scherbius and his patent



As usual... Hollywood is lying...  
(U-110 captured by Royal Navy)



## Alec Dennis



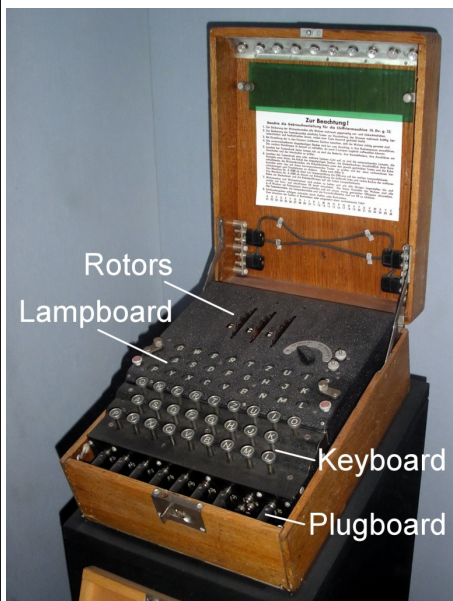
British. Australian. Code 23  
Standing. 185920. Capt. 23  
with 23. 185920. 185920.

ADM
Admiralty

Re. Code 23 185920  
① Captain of U Boat 110 is to be referred  
to as special Prisoner of War. Operation  
Prisoner is to be treated with greatest  
tenderness and for people allowed to know  
as possible  
— 0830B/10



## Enigma



FOUR-ROTOR ENIGMA (GVG / PD)

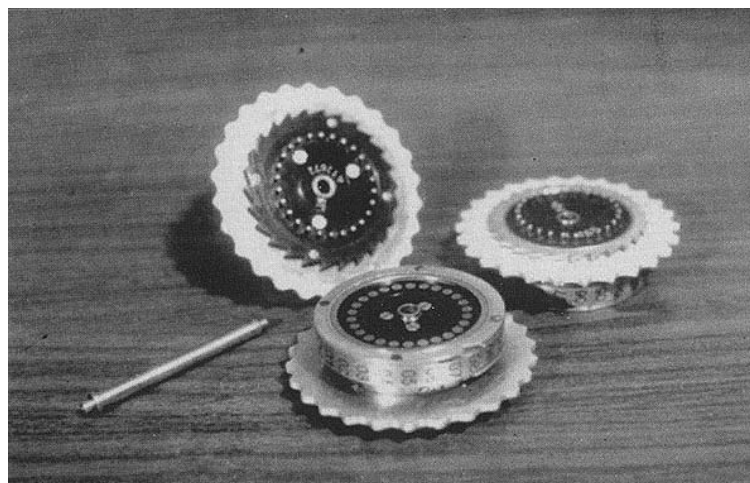


## Enigma models



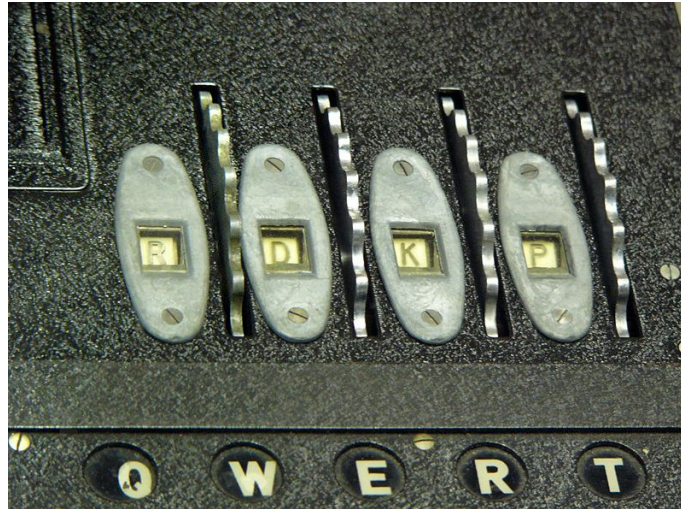
Tempest  
Security Intelligence

## Enigma rotors



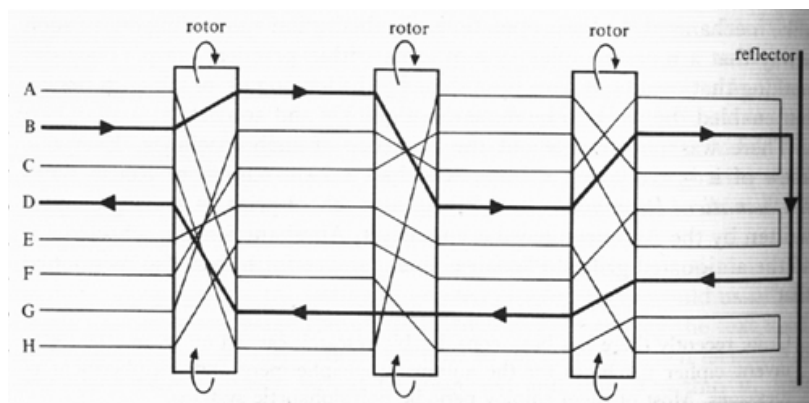
Tempest  
Security Intelligence

## Enigma rotor position settings



Tempest  
Security Intelligence

## Enigma basic internals



Tempest  
Security Intelligence

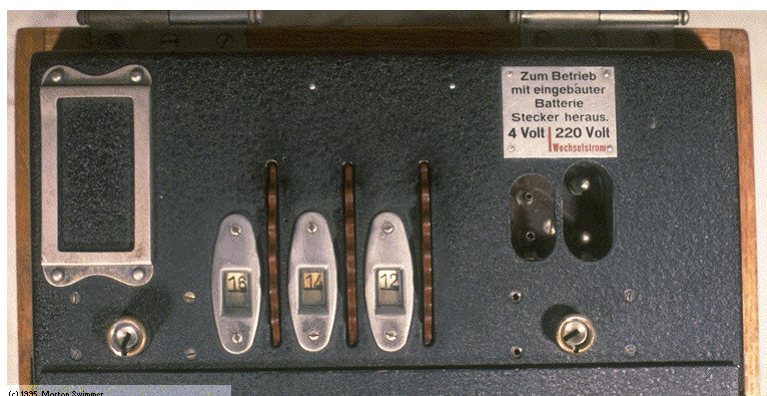


## Enigma 8 rotors engine



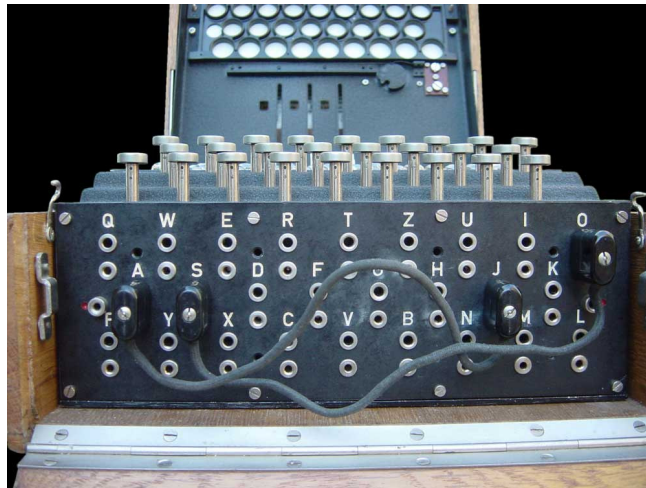
Tempest  
Security Intelligence

## Power and battery inlets



Tempest  
Security Intelligence

## Enigma plugboard panel



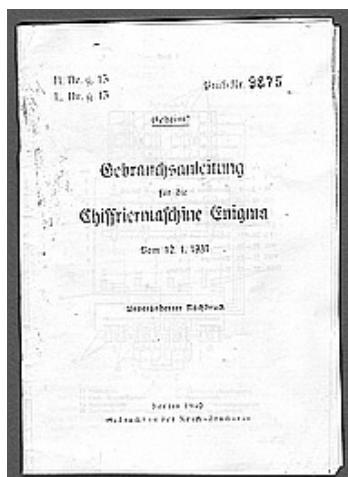
Tempest  
Security Intelligence

## Enigma hardware kit



Tempest  
Security Intelligence

# Enigma users guide



Tempest  
Security Intelligence

# Wehrmacht Enigma Codebook

Geheime Kommandosache!  
Nicht im Flugzeug mitzuführen!

**Heeres-Stabs-Maschinenschlüssel Süd Nr. 70**

Nr. 6021

Datum	Wahrsage	Ringstellung	Steckerverbindungen	Keimguppen
70 31. III I IV	16 03 24	HZ YR IF QT JN GC AP UX BO KB	vsw wbb nuf rsv	
70 30. V IV I	26 22 25	HL AN OC IY VE SK SW QZ PO UK	fse fuk rdq bdo	
70 29. III IV V	14 18 05	CV WK MS UP OJ DZ XA LR IY MN	hyy fso waa whr	
70 28. I II V	11 10 02	ZJ BP VK UG LN QX SA MT ED YH	por xcf seq ood	
70 27. V I III	20 07 15	KZ FD UP MQ XS OC WR EB YL IA	lwo aug fet lue	
70 26. II V IV	01 02 21	GS WC IL HR JW XO TQ SD PP EU	cle nyk eel mag	
70 25. I V II	07 08 19	BO WN CX TI KS MQ UH VP JZ LO	pkw dno bfw vbl	
70 24. IV II I	17 19 08	GU OE XA CI MS RY JW PP KL ZW	hio chv lge lgg	
70 23. II V III	13 24 07	XP VB ZM HW QI DS LC UG FK BO	aku pou eel eon	
70 22. III II I	-18 16 01	MS BP MU AN TL KO OJ ZV ZN	tal tuq nuj rak	
70 21. V II IV	23 09 26	VQ IN EB PY ZX GJ HM RL CW SK	hio yse dse lfo	
70 20. V I II	25 25 14	PV EY HN US KJ IM WD XL OT SE	ehc kfg ood eel	
70 19. I III II	08 20 23	JE FW XK GC PQ MN US DB OY VE	tav mqr rac woi	
70 18. I IV III	22 26 22	KK SS QU WA TY IE HD YO FR ML	emb oay sja vdi	
70 17. III I II	24 21 18	JN GP CB KS WU ZL OI VS DF TR	wej jrc rro uka	
70 16. V IV II	19 06 06	LQ BO EI MG HP OT WZ CP LA SV	trd rtp ptx tip	
70 15. III V IV	04 13 13	RV KP YS PI UB LJ AW QR CR GZ	uye djp eiu emj	
70 14. I II IV	09 11 17	EV UR IQ ZK OF WM LP ON RA VS	wod bvi hoo xkv	
70 13. V III II	05 25 09	LY XU VN OM RC PD IA EE OT NQ	sgg bad rga oga	
70 12. I V IV	03 06 12	XW KB IE UN DA MP LY MJ RV QP	okq uvf url sct	
70 11. V I IV	10 02 20	DA IC SY DL OE XN MU PE RQ TJ	npd byz oas lqm	
70 10. I V III	06 05 16	OT AS UY JS DW ON OH IE KP OM	vpp jny tnx kko	
70 9. IV II III	26 09 11	ZU PD KR XT SM AC ES IL NO OO	ejs tme tes rpe	
70 8. I V	20 10 10	ZD YQ AK IE RB VS CU FL WN NP	lso xux eva bno	
70 7. III IV I	01 19 24	AN OM OV RP BF EJ XC SZ UI NQ	sch cwo lww eta	
70 6. III II V	07 14 10	VW AY ON ZG XU RT LP NS IP KQ	edl xsl lxl bpr	
70 5. II III IV	04 12 18	CA YW HO ES KP ID LT VN OZ XM	yck fca for xan	
70 4. II I V	14 08 19	HD PY XW PU IO LK WE JC BO RQ	sll swb opr lpp	
70 3. IV V II	25 07 14	OM OS BT KJ FY VN RE HA IW UO	sqg eay cob opp	
70 2. II I III	06 25 03	KV FA NT UW ZD OM JR LE XI PY	tjv eae ofr for	
70 1. IV III V	19 22 17	OZ UD TY KN PW RH RA SC QP MO	fva yrw via ury	

Tempest  
Security Intelligence



# Luftwaffe Enigma Codebook

Geheime Kommandoache! Jede einzelne Tagesstiftel ist geheim. Mitten im Flugzeug verboten! Nr. 00190

### Luftwaffen-Maschinen - Schlüssel Nr. 649

**Achtung!** Schlüsselmittel dürfen nicht unangelehrt in Feindeshand fallen. Bei Gefahrefreilos und frühzeitig vernichten.

Datum	Waldenlage	Ringstellung	Steckerverbindungen										Kongruppe			
			an der Umkehrtafel					am Spindelrad								
040 31	I V III	14 06 24	SZ	GT	DV	KU	FO	MY	EW	JM	IX	LQ	wny	dgy	exb	rig
040 30	IV III II	05 26 02	IS	EV	MX	RW	DT	UZ	JQ	AG	CH	NY	kli	acw	zoi	wao
040 29	III II I	12 24 03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	PH	BH
040 28	II III V	06 58 16	DI	CN	BR	PV	CR	PV	A1	DK	OT	MQ	EU	DX	LP	GJ
040 27	III I IV	11 03 07	LT	EQ	HS	UW	DY	IM	BV	OR	AM	LO	PP	HT	EX	UW
040 26	I IV V	17 22 19	VZ	AL	RT	KO	CO	EI	BJ	DU	P5	HP	xie	gbo	uev	rxm
040 25	IV III I	08 25 12	OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	ait
040 24	V I IV	09 18 14	TY	AS	OW	KV	DR	HX	GL	CZ	NU		kpl	rwl	vci	tiq
040 23	IV II I	24 12 04	QV	FR	AK	EO	DH	CJ	WZ	SX	ON	LT	ebn	rwm	udf	tlo
040 22	II IV V	01 09 21	IU	AS	DV	OL	PJ	ES	IM	RX	LW	AY	OU	BO	WZ	CN
040 21	I V II	13 05 19	PT	OX	EZ	CH	HU	HL	PY	O5	QZ	DR	AW	CE	PV	IX
040 20	III IV V	26 01 10	MR	KN	BQ	PW	DF	HO	QZ	AU	RY	SV	JL	OX	DE	TW
040 19	V III I	17 25 22	OX	FR	PH	WY	DL	CM	AE	TZ	J5	G1	idf	fpk	JWG	tig
040 18	IV II V	15 23 26	EJ	OY	IV	AQ	KW	FX	MT	P5	LU	BD	isa	gbw	vcj	rxn
040 17	I IV II	21 10 06	IR	KZ	LS	EM	OV	OY	QX	AP	JP	BU	mae	hzi	sog	ysi
040 16	V II III	08 16 13	HM	JO	DI	NR	BT	XZ	US	PU	PQ	CT	tdp	dhb	fkv	uiv
040 15	II IV I	01 03 07	DS	YV	MR	OW	LX	AJ	BQ	CO	IP	MT	idw	hzi	soh	wkg
040 14	IV I V	15 11 05	OM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz	noa	tjv	xtk
040 13	I III II	13 20 03	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr	dgi	gjo	ryg
040 12	V I IV	18 10 07	MU	BP	CY	RZ	XX	AN	JT	DO	IL	PW	tdy	rki	tjw	xli
040 11	II IV III	02 26 15	KN	UY	HR	PW	FM	BO	EA	QF	DX	JV	rea	rjy	sof	wh
040 10	III V IV	23 21 01	LR	IK	MS	GU	HW	FT	DO	VY	PZ	EN	irc	lax	vbm	rxo
040 9	V I III	16 04 08	QY	BS	LN	KT	AP	IU	DW	HO	HV	JZ	edj	eyr	vby	tih
040 8	IV II V	13 19 25	PI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	viz	dha	ekc	tli
040 7	I IV II	09 03 22	UX	IZ	HN	KB	GQ	CP	FT	JY	MW	AR	lan	dgb	rsj	wbi
040 6	III I V	11 18 14	DQ	GU	BW	HP	HK	AZ	CI	PO	JX	VY	tao	ctf	zsk	wbj
040 5	V II IV	23 02 25	WZ	CL	OZ	OQ	ET	HU	RS	FX	NW	EY	lju	cdr	iye	waj
040 4	II IV I	04 21 09	QT	WZ	KV	OM	AC	BL	OZ	EK	QW	OP	SU	DH	JM	TX
040 3	V I II	19 11 06	BP	NR	DX	CS	KR	MP	CN	BP	EH	DZ	LV	AV	GJ	LO
040 2	IV V I	16 14 02	BN	HU	EG	FY	KO	CP	OS	JW	AI	VZ	agd	bdy	iyf	xtd
040 1	II I III	23 12 10	DP	BM	NZ	CK	OV	HQ	AP	UY	SW	JO	hgi	cdf	gic	wuv

# Kriegsmarine Enigma Codebook

Geheim! Sonder - Maschinenschlüssel BGT 0

Datum	Waldenlage	Ringstellung	Steckerverbindungen	Kongruppe
31	I V III IV	06 20 24 28	UA PF HQ GH RF BJ KL PI HF NM	juw nyz kjh ihm
30	VI III I V	01 06 09 45	GU LP KL NM PGLI PD VR ED IH	ikm msk jkl jkl
29	II XIV I V	24 12 09 15	QA AZ WS SX ED DC RF DC TG GB	nbf kln sdg ogh
28	III V IV II	12 07 18 03	YH JM UK IL LP LM KN JB YG FC	ghb hds lhg erf
27	V II III VI	44 24 08 23	ZAAQSW DE FVYI NH YME LC	qwe rty nio wop
26	VII I V X	22 06 43 22	ZX CV BN NM AS DF GH IJ JK LM	zxc vbn hnm and
25	IX VIII VI	10 29 27 02	PO LU YT TR EW WO LK IH GF DS	raq twc cdc vfr
24	XIV VIII I	07 21 31 64	AS DF GH IJ KL ZM NX BC VC XX	plm oln abv wgf
23	III VI II V	19 01 16 40	ML NK RJ VH CG XF ZP LK OH	tdr rsa qrs tpo
22	VIII VIII I	37 11 17 30	GV PT DR SE AW QA WS ED RF TG	edf hij klm nop
21	IV VIII III	29 31 41 02	LN KLMGHI JK BEH SD KJ IH	pkl ojk lhg wgf
20	IV VIII I	54 31 40 33	ML NJ BH VF CB NS SD JV KR JD	tpi elm cdb hgt
19	III V VI IV	53 29 10 09	PO LA MA ALZ QLSI BC CV JA	ygh jnh lr njl
18	V III VII I	47 43 14 11	NZ NX BC VB VN CMCZ GC KL FR	prq ota the ygs
17	IV III V	30 18 08 39	TF YG UH IJ OK PL RD ES WAGA	pal oia try wpt
16	VIII VII I	37 25 19 04	WZ EX RC TV VB UM OP IK UJ	qyb phv rym lay
15	V I VI II	29 33 07 48	MP NO RI VU CY XZ ER SE AW QA	ytr uls kjh dfg
14	VIII II V	13 08 01 43	WZ EX RC TV UB JI LR MS PK SS	njm kln hgr otc
13	II V VI I	44 23 36 01	GA HS JD KFLG ALSK DJ FH BG	perm mngp lnh zlm
12	V I IX X	23 05 11 02	HU JI KO LP HT GR FE DW SQ GG	qhs vlx cty rhm
11	XIX VIII I	12 32 47 19	TG VH UF ID EH WK PX NR AL NH	paz def gap moe
10	VII V VI II	11 19 45 27	ZASO DI IT OF PO JA VE ME LO	pil lod hbi nll
9	II V VI III	10 09 05 32	FAAO GO HA KO VE JO SA LK HI	kli bon nll mo
8	V II I VI	12 28 03 44	AGSX DC FV GB HN JM KL LA VF	amg oia lmp gm
7	II IV VI VI	07 41 19 20	PM NO IB VU YC XT RZ AW BK KN	oid drp yks tpy
6	VIII III V	33 29 03 08	ZAXS CD VFRG NH MKNL BJ	popo hka mro zil
5	IX III V III	08 38 15 13	FZOX IC UV YB TN RM ER WOSE	qhc kll lmp man
4	X III V II	15 26 37 04	LAKS KL LDFG KI GN BG TY UI	trp gpp jjo lat
3	III IV I I	20 11 22 05	GV IV HN HK LF KE SJ OF BO MS	lnd shj kld the
2	V III VI II	07 33 14 19	TR YR EF DW PQ GF HD IS KA LA	oac pal wid jha
1	I IV III V	18 03 06 34	TL LA AM MV VE RA AK KW WO DP	ask lqj mtp ota

## How strong was Enigma ?

- For 3 rotors interchange orientation:
  - $26 \times 26 \times 26 = 17.576$  orientations.
- For 3 rotors positioning:
  - (123, 132, 213, 231, 312, 321) = 6 positions.
- Plugboard (typical 6 plug wires):
  - 6 letter pairs (26 letters) = 100.391.791.500
- Possible keys =
  - $17.576 \times 6 \times 100.391.791.500 = \sim 10.000.000.000.000.000$

## Session key use example

- Rotors orientation initial position = QCW
- Random session key choice = PGH
- Session key typing = PGHPGH (2 times)
- Session key encrypted = KIVBJE
- Session key decrypted = PGHPGH
- New session key used = PGH
  - Interesting note: PGH is not in the codebook!

## Enigma in use



Tempest  
Security Intelligence

## Enigma in battlefield



Tempest  
Security Intelligence

## Wireless Enigma



Tempest  
Security Intelligence

## Station listeners



Tempest  
Security Intelligence



## Using Enigma



## The Gordian Knot legend

- In 333 B.C. Alexander the Great had invaded Asia Minor and arrived in the central mountains at the town of Gordium; he was 23.
- The staves of the cart were tied together in a complex knot with the ends tucked away inside. Legend said that whoever was able to release the knot would be successful in conquering the East.
- Having arrived at Gordium it was inconceivable that the impetuous young King would not tackle the legendary “Gordian Knot”.

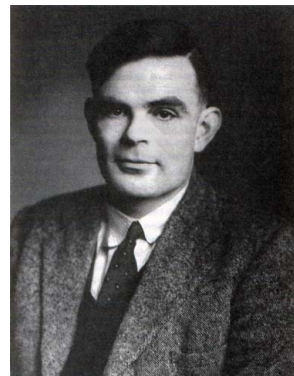
## The Gordian Knot legend

- His generals gathered round as he struggled with the Knot for a few minutes. Then he asked Aristander, his seer, “does it matter how I do it?”. Aristander couldn’t provide a definitive answer, so Alexander pulled out his sword and cut through the knot.
- The legend of the Gordian Knot appealed to us for Alexander’s decisive action and as a metaphor for radical solutions to complex problems.



Tempest  
Security Intelligence

## Marian Rejewski & Alan Turing



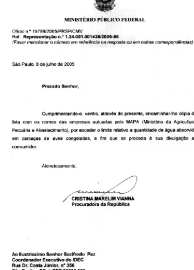
Tempest  
Security Intelligence

## Some tips used...

- In Enigma one letter never was encrypted as itself;
- Procedures: Wheater reports boilerplates/templates;
- Operators:
  - Morse code typing hand signatures;
  - Not random session key choice;
- ... and so on...
  - These procedures can decrease the key possibilities universe to (only) **105.456**



## Boilerplates & templates



# Weather reports

Ausgabe 2. Letter Table

1	1	Latitude in degrees.
2	2	Longitude in degrees.
3	3	General area and direction of pressure change.

(Tables 1 and 2 give ambiguous answers which are distinguished by the general area given in 3).

4	4	Air pressure to nearest 2 millibars.
5	5	Air temperature in degrees Centigrade
6	8	wind direction and strength.
7	6	Present weather and clouds.
8	7	Visibility.
9	9	Direction and type of swell.
10,11		Signature.

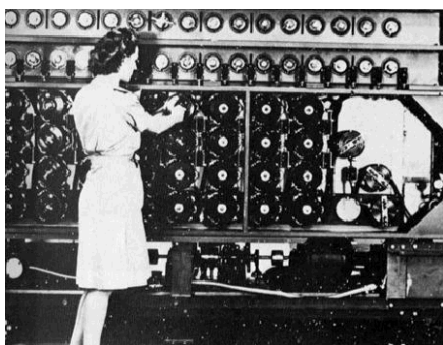
Tafel 9.  
K = Richtung und Art der Dünung.

Richtung, aus der die Dünung kommt	Art der Dünung			
	niedrig	mittelhoch	hoch	
N	a	i	q	
NO	b	j	r	
O	c	k	s	
SO	d	l	t	
S	e	m	u	
SW	f	n	v	
W	g	o	w	
NW	h	p	x	
Keine Dünung				y
Durchsichtstiefe Dünung				z

Weterschiffstafel (S<sub>p</sub>) ..... = m  
 Breite (φ) = 49° 35' Nord ..... = z  
 Länge (λ) = 18° 22' West ..... = y  
 Druckänderung (A) = Druck fallend .. = r  
 Luftdruck (P) = 1018,9 mb ..... = q  
 Lufttemperatur (T) = + 7,4° ..... = s  
 Windrichtung und -stärke (D) = West 5-6 (F I) ..... = o  
 Wettererscheinungen und Wolken (W) = bedeckt, aber noch Regen während der letzten Stunde (W II) .. = v  
 Horizontale Sichtweite (U) = bis 10 sm (F I, W II) ..... = k  
 Dünung (K) = aus SW hoch ..... = v  
 Unterschrift (UU) ..... = qm

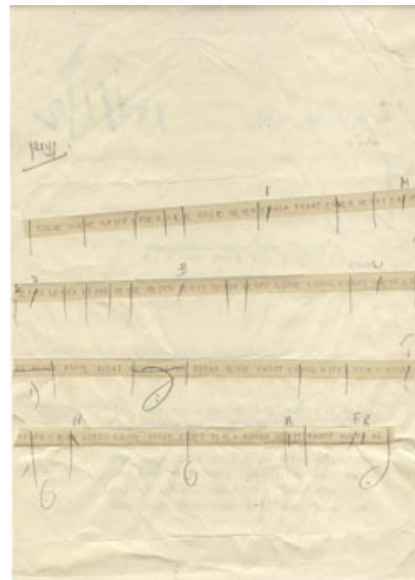
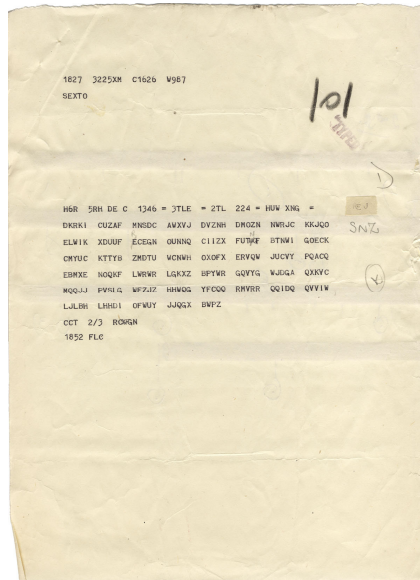


# Turing bombs & Colossus





## Typical encrypted message



## Typical decrypted U-Boat message

ADM  
 TO I D E G ZIP/ZTPG/18733  
 FROM N S

13768 KC/S T O I 1537/24/11/41  
 T O O 1551

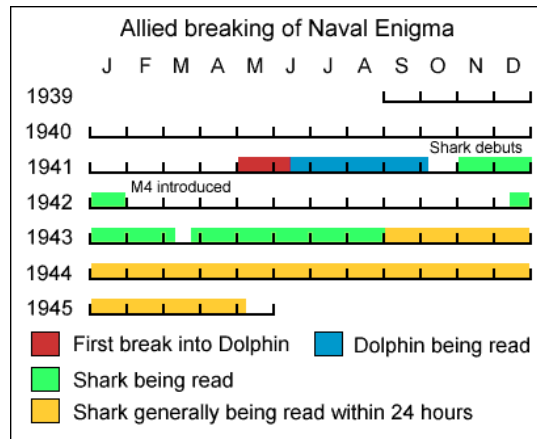
FROM: MOHR

'D' CLASS BRITISH CRUISER SUNK IN SQUARE PE 7965. AM CONTINUING  
 PASSAGE SOUTH.

(DEPT.NOTE: SQUARE PE = ?).

1423/25/11/41++CEL/LW

## Naval Enigma cracking roadmap



Tempest  
Security Intelligence

## Coventry: protecting sources



Tempest  
Security Intelligence

## Checkpoint

- Good cryptography not always means good privacy;
- Good procedure is your friend. Maybe the only one;
- Good procedures costs something, usually is not cheap;
- Functionality and performance are your enemies;
- Cryptoanalysis is a mix of science and art.

Tempest  
Security Intelligence

## Navajo Codetalkers



Tempest  
Security Intelligence

## Nowadays...



sql-injection-acc.exe

 Tempest  
Security Intelligence

## Lessons

- Software engineering and security are not friends!
  - To get functionality and performance, you have to pay using security currency.
- Procedure is fundamental.
- Users hates procedures!
- Good cryptography, sometimes, looks like a Gordian knot! Be careful with the things around it!

 Tempest  
Security Intelligence



To have fun...

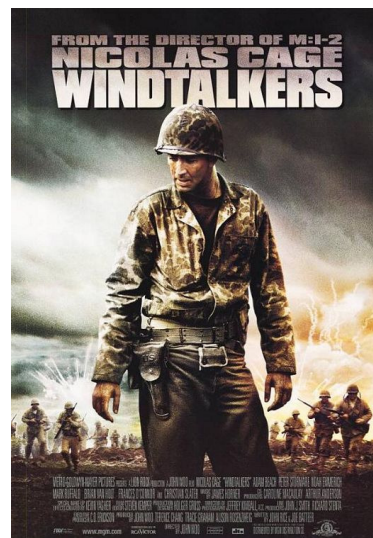
- U-571



Tempest  
Security Intelligence

To have fun...

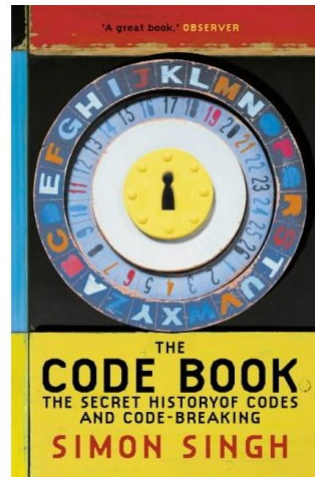
- Windtalkers



Tempest  
Security Intelligence

To have fun...

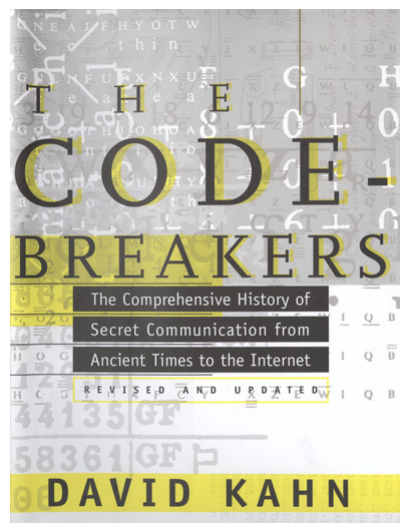
- The Codebook: The Secret History of Codes and Code-breaking
- Simon Singh  
2000
- ISBN-10: 1857028899
- ISBN-13: 978-1857028898



Tempest  
Security Intelligence

To have fun...

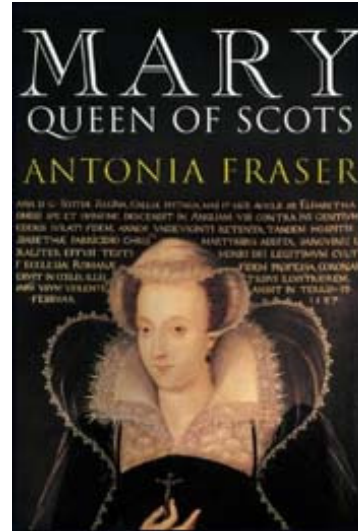
- The codebreakers
- David Kahn  
1996



Tempest  
Security Intelligence

To have fun...

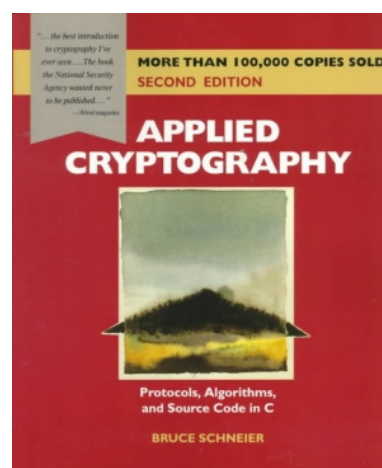
- Mary Queen of Scots
- Lady Antonia Fraser
- 1989.



Tempest  
Security Intelligence

To have fun...

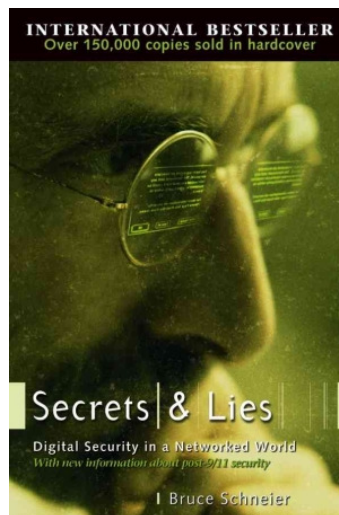
- Applied cryptography
- Bruce Schneier
- 1995.



Tempest  
Security Intelligence

To have fun...

- Secrets and Lies
- Bruce Schneier
- 2004.



 Tempest  
Security Intelligence

Thank you

Evandro Curvelo Hora  
evandro@tempest.com.br

 Tempest  
Security Intelligence