



Coding

- Popular codes:
 - Braille
 - ASCII
 - Traffic lights (yellow, green, red)
 - Morse
- Usually coding is used to provide known meanings to everyone, not secrecy.

Coding

- Some coding can be used to provide secrecy... except to few. So, there is a intrinsic, and secret, meaning.
 - “Climb Mount Niitaka”
- Coding is a good way to improve communications, mostly using:
 - Signs;
 - Colors;
 - Sounds.

Cipher

- Cipher is used when privacy is required to information in current language. There is no intrinsic meanings. Much more freedom.
- You can encode a cipher text...
- ... but you can encrypt an encoded text as well.

Morse coding



Tempest
Security Intelligence

Training radio operators

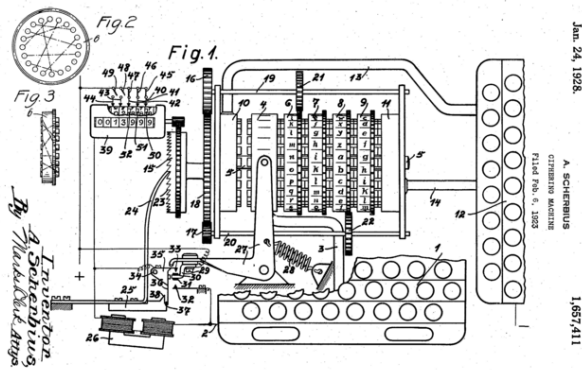


Tempest
Security Intelligence

Cryptology

- Cryptography
- Cryptoanalysis
- Axiom:
 - There is no safe communication channel or storage.

Scherbius and his patent



Did you watch this movie ?



Tempest
Security Intelligence

As usual... Hollywood is lying...

(U-110 and first Naval Enigma was captured by Royal Navy)



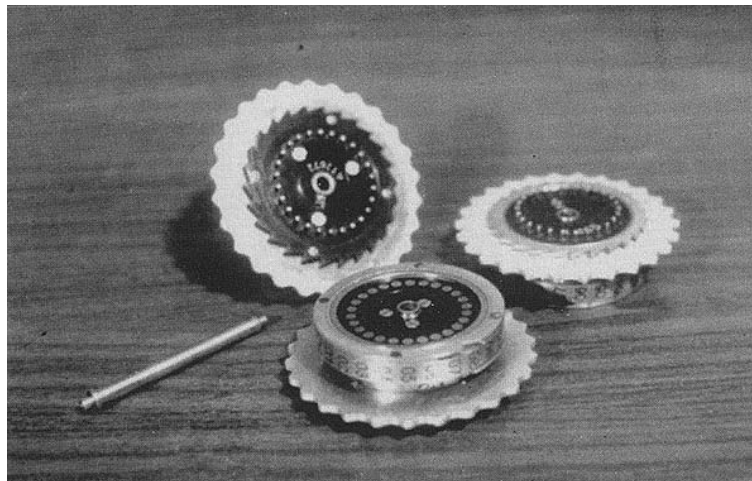
Tempest
Security Intelligence

Enigma models



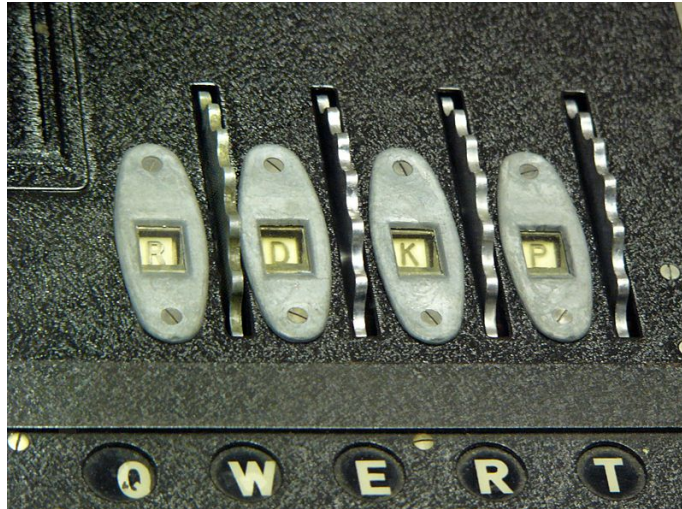
Tempest
Security Intelligence

Enigma rotors



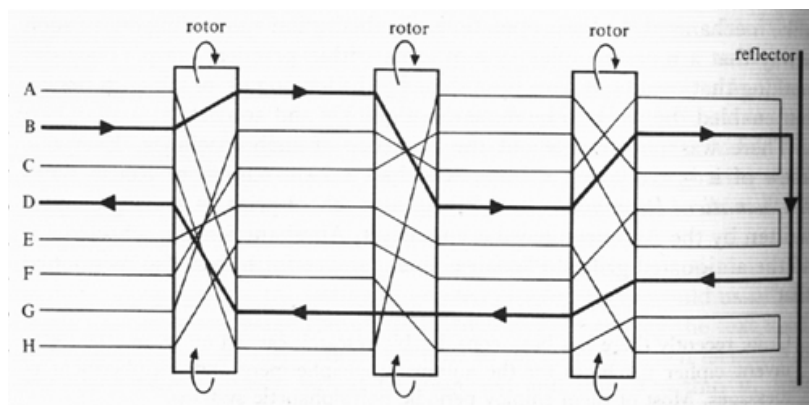
Tempest
Security Intelligence

Enigma rotor position settings



Tempest
Security Intelligence

Enigma basic internals



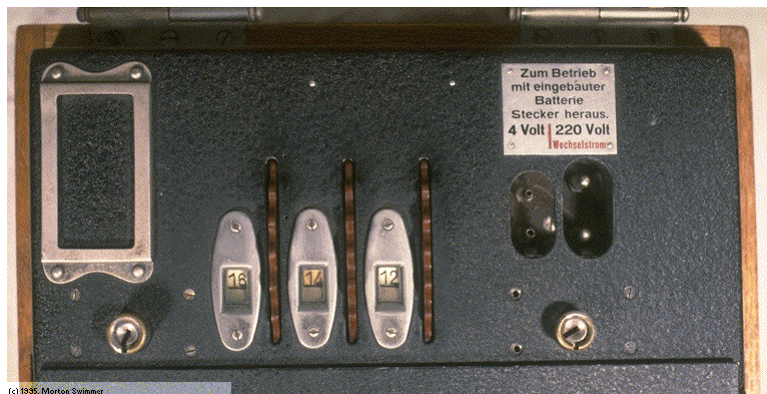
Tempest
Security Intelligence

Enigma 8 rotors model



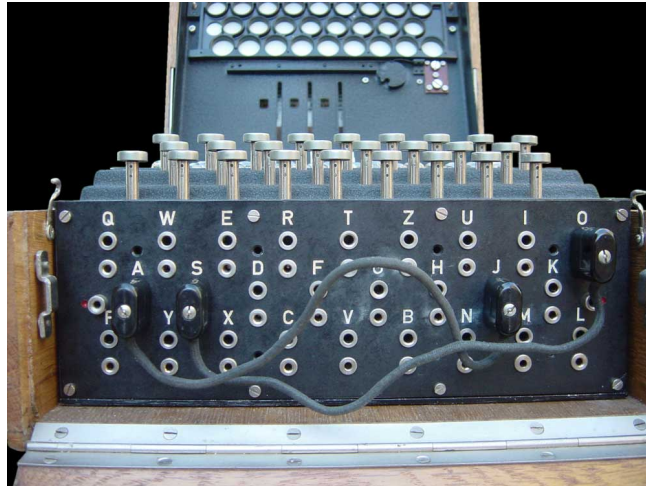
Tempest
Security Intelligence

Power and battery inlets



Tempest
Security Intelligence

Enigma plugboard panel



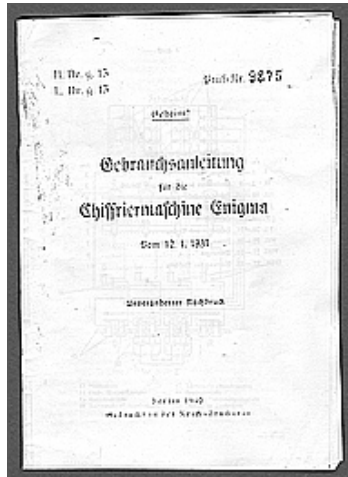
Tempest
Security Intelligence

Enigma field kit



Tempest
Security Intelligence

Enigma users guide



Tempest Security Intelligence

Wehrmacht Enigma settings sheet

Geheime Kommandosache! Heeres-Stabs-Maschinenschlüssel Süd Nr. 70 Nr. 0020

Nicht im Flugzeug mitzuführen!

Datum	Wahrsache	Ringstellung	Steckerverbindungen	Keimguppen
70 31.	III I IV	16 03 24	HZ YR IF QT JN GC AP UX BD KS	vzw wbb nuf rrv
70 30.	V IV I	26 22 23	HL AN OD IY VE MK SW QZ PO UK	fze fue rdq bdo
70 29.	III IV V	14 18 05	CV WK MS UP OJ DZ XA LR IY MN	hyy fso wka whr
70 28.	I II V	11 10 02	ZJ BP VK UG LM QX SA MT ED YH	por scf seq ooa
70 27.	V I III	20 07 15	KZ FD UP MQ XE OC WR EB YL IA	cle rpk eel maq
70 26.	II V II	01 02 21	OS YC IL HR JN KO TQ BO PP EU	pkw dno bfw vbl
70 25.	I V II	07 08 19	BD WN CX TI KS MQ UN VP JZ LO	slb chr lga lpp
70 24.	IV II I	17 19 08	GU OE XA CI MS RY JN PP KL ZW	equ pou eel kco
70 23.	II V III	13 24 07	ZP VB ZM HW QI DS LC UG PK BO	tal lug nuj rsk
70 22.	III II I	18 16 01	QI HS BP MU AR TL KO OJ XV ZN	gls yse boe lfb
70 21.	V II IV	23 09 26	VQ IN EB PY XX OJ HM RL CW SK	ehc kfe qgd xat
70 20.	I II	25 25 14	PV EY HM US KJ IM WD XL OT NZ	tav mgy ruc woi
70 19.	I III II	06 20 23	ZE FW XK OC PQ MN US DB OY VE	gmb ouy aia vdt
70 18.	I IV III	22 26 22	XK SS QU RA TY IE HD YO PR ML	wej yrc rro uaa
70 17.	III I II	24 21 18	JN GP CB KS BU ZL OI VR OF TH	trd rtp ptx ltp
70 16.	V IV II	19 06 06	UQ NO EI M3 HP OT WZ CP LA SV	uye pjp eiu emj
70 15.	III V IV	04 13 13	XV KP YS PI UB LJ AW QH CR GZ	wod bvi bno ukv
70 14.	I II IV	09 11 17	EY UR IQ ZK CP WM LP OW HA VS	seg bad rga oaa
70 13.	V III II	05 25 09	LY XU VW OM RC PD IA EE OT KQ	okq uvf vrl scb
70 12.	I V IV	03 06 12	XW KB IE UN DA MP LY MJ RV QP	spd byz oas lqm
70 11.	V I IV	10 02 20	DA IC SY JL OE XN MU PE HQ TJ	vpp yny tnx kxc
70 10.	III IV I	01 19 10	OT AS UT JE DW OM OH IB KP OM	ejb iaw taz rpe
70 9.	IV II III	26 09 11	ZU PD KR XT SM AC ES IL HO QO	lrd xux eva bno
70 8.	I V III	20 10 10	ZD YQ AK IE RB VS CU PL WN NP	mch cwo iaw eta
70 7.	III IV I	01 19 24	AN OM OV RP BF EJ XC SZ UI NQ	mdt xef lxi bpr
70 6.	III II V	07 14 10	VK AY OM ZG XU RT LP HS IF KQ	yok fca fca xaa
70 5.	II III IV	04 12 18	CA YV HO SB KP ID LT VN GZ XM	slt swb opv lpp
70 4.	II V II	14 08 19	HD PY XM PU IO LK WZ JC BO RQ	seq esp ocb opp
70 3.	IV V II	25 07 14	OM OS BT KJ FY VN RE HA IV UO	bjv eaa ofe for
70 2.	II I III	06 23 03	KY FA WT UW ZD OM JR LE XI PT	fva yvw vlm vry
70 1.	IV III V	19 22 17	OZ UD TY KN PW RH EA SC QP MO	

Tempest Security Intelligence

Luftwaffe Enigma settings sheet

Geheime Kommandosache! Jede einzelne Tagesstellung ist geheim. Mitternachts im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmaterial dürfen nicht unangelehrt in Feindeshand fallen. Bei Gefahr reflexlos und frühzeitig vernichten.

Datum	Waldenlage	Ringstellung	Steckerverbindungen		Kengruppe
			an der Umkehrtafel	am Spindelkasten	
040 31	I V III	14 06 24	SZ	GT DV KU FO MY EW JH IX LQ	wny dgy ebx rzg
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	joc acn oww wvd
040 28	II III V	06 58 16	DI CN BR FV	CR FV AI DK OT MQ EU DX LP GJ	lrb cid ude rth
040 27	III I IV	11 03 07	LT EQ HS UW	DY IM BV OR AM LO PF HT EX UW	woj fth vct uis
040 26	I IV V	17 22 19		VZ AL RT KO GO EI DJ DU PS HP	xie gbo uev rxn
040 25	IV III I	08 25 12		OR FV AD IT PK HJ LZ NS EQ CW	ouc uhq uew ait
040 24	V I IV	09 18 14		TY AS OW KV JM 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	FJ ES IM RX LV AY OU BO WZ CN	jgc acx mwe wee
040 21	I V II	13 05 19	PT OX EZ CH	HU HL FY OS QZ DM AW CE TV NX	jpw del mwf wvf
040 20	III IV V	24 01 10	MR KN BQ PW	DF NO QZ AU RV SV JL OX DE TW	jqd cef nvo ysh
040 19	V III I	17 25 22		OX FR FH WY DL CM AE Tz JS G1	idf fpk jvg tlg
040 18	IV II V	15 23 26		EJ OY IV AQ KW FX MT PS LU BD	lsa 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 GS PU FQ CT	tdp dhh fkb uiv
040 15	II IV I	01 03 07		DS BY MR QW LK AJ BQ CO IP NT	ldw hzj soh wwk
040 14	IV I V	15 11 05	AI BT MV HU	OM JR KS LY HZ PL AX BT CQ NV	imz noa tlv xtk
040 13	I III II	13 20 03	FW EL DG KN	LY AG KM BR IQ JU HV SW ET CX	zgr dgt gjo rfg
040 12	V I IV	18 10 07	RZ OQ CP SX	MU BP CY RZ XX AN JT DG IL PW	tdy rki tlv xtl
040 11	II IV III	02 26 15		KN UT HR PW FM BO EA QP DX JZ	zea rjy sog wwh
040 10	III V IV	23 21 01		LR IK MS GU FW FT DD VY PZ EN	lrc lxx vbm rxo
040 9	V I III	16 04 08		QY BS LN KT AP IU DW HO RV 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 ekk tli
040 7	I IV II	09 03 22		UX LZ HN BK GQ CP FT JY MW AR	lan dgb rsl wbl
040 6	III I V	11 18 14	IL AF EU HO	DQ GU BW NP HK AZ CI PO JX VY	lao cft zsk wbj
040 5	V II IV	23 02 25	QT WZ KV OM	MZ CL OX OQ EI PU HS FX NW EY	lju cdr iye waj
040 4	II IV I	04 21 09	BP NR DX CS	AC BL OZ EK QP OS SU DH JM TX	lsb zby vcy ujb
040 3	V I II	19 11 06		KR MP CN BP EH DZ LW AV GJ LO	lap owd iwu wak
040 2	IV V I	16 14 02		BN HU EG FY KO GP OS JW AI VZ	agd bdy iyt xtd
040 1	II I III	23 12 10		DP BM NZ CK OY HQ AP UY SW JO	hgi vdr giq wuv



Kriegsmarine Enigma settings sheet

Geheim! Sonder - Maschinenschlüssel BGT O

Datum	Waldenlage	Ringstellung	Steckerverbindungen	Kengruppe
31	I V III IV	06 20 24 28	UA FF RO GH RE HI KL PJ HF NM	juv nyz kph lhm
30	VI III I V	01 06 09 45	GH LP KL NM PG LI PD NR ED UH	lhm nmk hji ptk
29	II IVV IV	24 12 09 15	QA AZ WS SX ED DC RC DG GB	nbf kln ndg egh
28	III V IV II	12 07 18 03	YH JM UR HL LP LM KN JB YG FC	ghb hds idg arf
27	V II III VI	44 24 08 23	ZA AQ SW BE FR VT NH YM FL C	qnc ey uho nqg
26	VII I V X	22 06 43 22	ZX CV BN NM AS DF GH HJ JK LM	zxc vho hnn and
25	IX II VVI	10 29 27 02	PO HI YT TR EW WO LK JH GF DS	zsq twc colc vfr
24	VI V III I	07 21 33 64	AS DF GH JK LK ZM NX BC VXCXN	plm okn hrv efg
23	III VI II V	19 01 16 40	ML NK BJ VH CG XF ZD LP RO HI	tda rva qra lpo
22	V III V III I	37 11 17 30	GY FT DR SE AW QA WS ED RF TG	uad hji hjo vgr
21	IV V III V III	29 31 41 02	LN KL MG HJ KE BH SD KJ IH	ptk ohj lhg wfg
20	IV VIII I	54 31 40 33	ML NJ BH VF CB XS SD JV KR DJ	tpi elm eahs hqg
19	III V VI IV	53 29 10 69	POLA MA AL ZK OLSI BC CV JA	yhg jnh lir nji
18	V III VII I	47 43 04 11	MZ NX BC VB VN CMCZ GC KL FR	paq ota lno ygs
17	I IV III V	30 18 08 39	TF YG UR HJ OK PL RD ES WAGA	pat oia lry vst
16	V III VII I	37 25 19 04	WZ EX RC TV YE UM IM OP IK UJ	qyb phv zym lay
15	V I VI II	29 33 07 48	MP NO BE VU CY NZ ZA SE AW QA	ytr alo kjh dfg
14	V III II V	13 08 01 43	WZ EX RC TV UE JI LR MS PK SS	njm kln hgv otc
13	II V VII I	44 23 36 01	GA HS JD KFLG ALSK DJ FH BG	ptm nqg lnh jlk
12	V I IX X	23 05 11 02	HU JI KO LP HT GR FE DW SQ GG	qts stx cy rhm
11	V IX VIII	12 32 47 19	TG VHU F ID EH WK PX NR AL NH	paq def gap moe
10	VII V IV II	11 19 45 27	ZASO DI IT OF PO JA NE ME LO	pat lod hih oih
9	IV V III	10 09 05 32	FA AD GO HA KO VE JO SA LK HI	kli boon mli oho
8	V II I VI	12 28 01 44	AZ SX DC FV GB HN JM KL LA VF	wp oia trap gsa
7	IV IV VI	07 41 19 30	PM NO IB VL VU XE KZ AW HK KN	oid dtp yka lrpj
6	V III III V	33 29 03 08	ZX NS CD VFRG NH MJ MN LJ RJ	popo hxx mzo zst
5	IX II V III	08 38 15 13	FZ OX JC UV VW TW RM ER WOSE	qts kll hcp mian
4	X II V VI	15 26 27 04	LA KS KL LD FG KJ GN BG TY UI	trap ppp jjo lat
3	III IV I	20 11 22 05	GV HV HN HK LF KE SJ OF BO NS	lat shi ktd the
2	V III VI II	07 33 14 19	TR YR UE DW PQ GF HD IS KA LA	ooc pat wld jia
1	IV III V	16 03 06 34	TL LA AM MV VE RA KW WO DP	ask lqi trap 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 =
 - $17.576 \times 6 \times 100.391.791.500 = \sim 10.000.000.000.000.000$

 Tempest
Security Intelligence

Enigma in use



 Tempest
Security Intelligence

Enigma in battlefield



Tempest
Security Intelligence

Wireless Enigma



Tempest
Security Intelligence

Station listeners



 Tempest
Security Intelligence

Morse listening



 Tempest
Security Intelligence

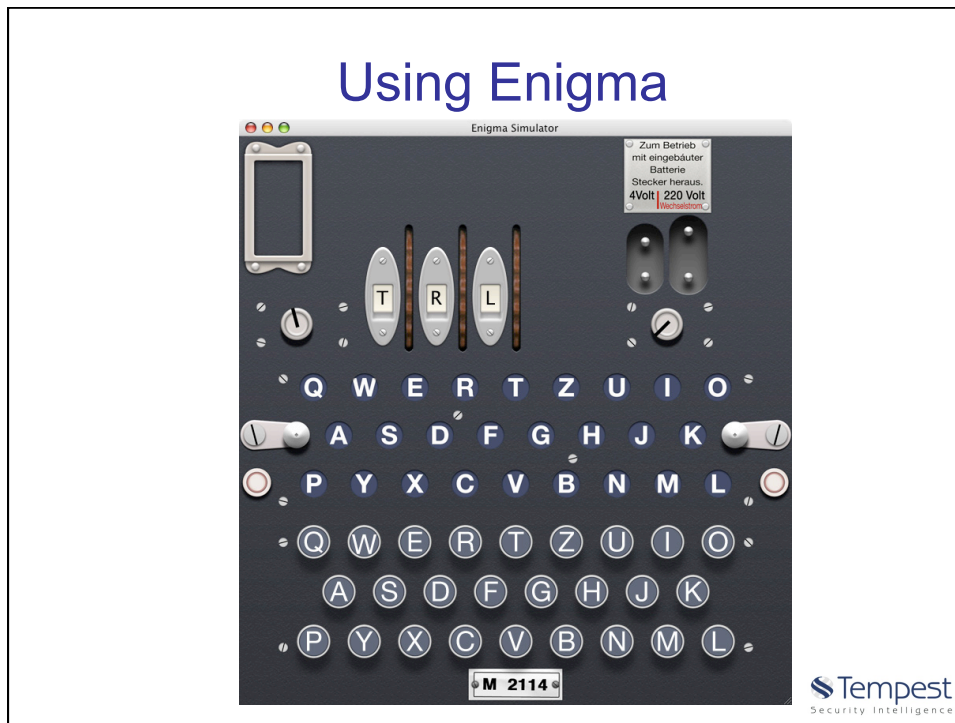
Key assignment session example

- Rotors orientation initial position = QCW
- Random session key op 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 settings sheet!

Enigma X Morse

- Enigma inputs and outputs were well suitable for use with:
 - Typeletter machines;
 - Morse coding.
- Morse coding were suitable for wired or wireless communications.



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 famous 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

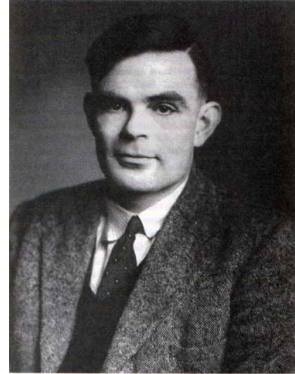
- Polish mathematician:
 - Enigma first break (before the WWII);



Tempest
Security Intelligence

Alan Turing

- British mathematician:
 - Station X codebreaking leader (at WWII).



 Tempest
Security Intelligence

Bletchley Park (Station X)



 Tempest
Security Intelligence

Bletchley Park at War



Tempest
Security Intelligence

Bletchley Park at War



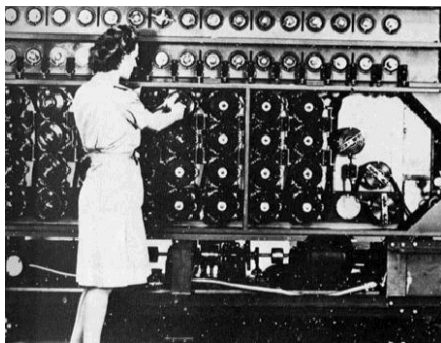
Tempest
Security Intelligence

Royal visitors



Tempest
Security Intelligence

Turing bomb & Colossus



Tempest
Security Intelligence

The girls...



Tempest
Security Intelligence

Bletchley Park, today



Tempest
Security Intelligence

The girls, today 😊



 Tempest
Security Intelligence

Some *clues* used...

- Enigma project/design characteristics:
 - One letter never was encrypted as itself;

 Tempest
Security Intelligence

Some clues used...

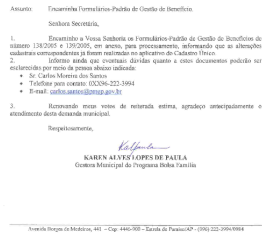
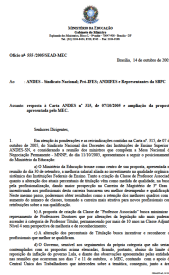
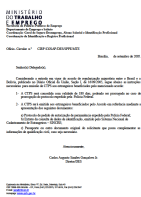
- Procedures:
 - Military document formal/rigid shapes (wheater reports, comm reports, other known templates etc);

What about a guess ?

What is this ?



Formal document shaping



Typical German 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
Durchwandelnde Dünung			z

Wetterdruckstiftsel (S_w) = 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 (V)
 = bis 10 km (F I, W II) = k
 Dünung (K) = aus SW hoch = v
 Unterschrift (U) = qm



Some clues used...

- Known operator's *hand signature*



Some *clues* used...

- Communications practical needs or characteristics:
 - Repetitions, used as “error detection code”.
- Signals intelligence
 - Radio direction finding;
 - Signal strength;
 - Known military unit localization;
 - Expected keywords;
 - Transmission IDs, trailers, headers...
 - Time scheduling for regular military reports (wheather, heartbeats...).



Some *clues* used...

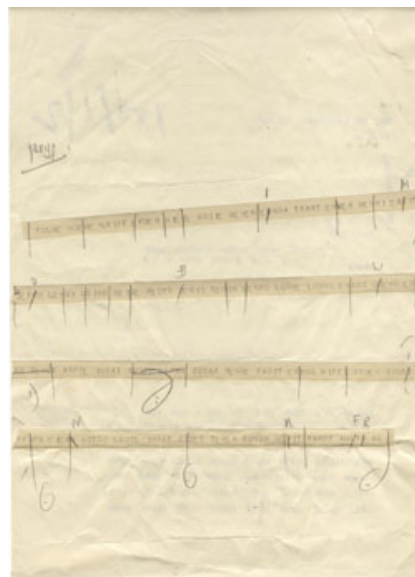
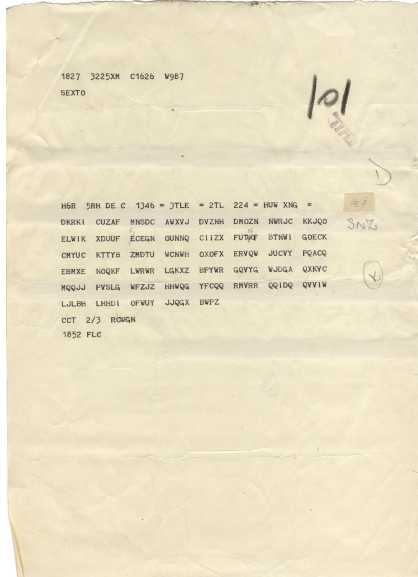
- Other common mistakes:
 - Not random session key choice;
 - Key reuse;
 - Aforisms use;
 - Same plain message sent using other ciphers;
 - Encrypt known plain messages;
 - Plain text disclosure from a known cryptogram.

... so Turing & his crew realized the key universe may decreases to:

105.456



Typical encrypted message



Typical decrypted U-Boat message

ADM
 TO I D E G ZIP/2TPG/18733
 FROM N S

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

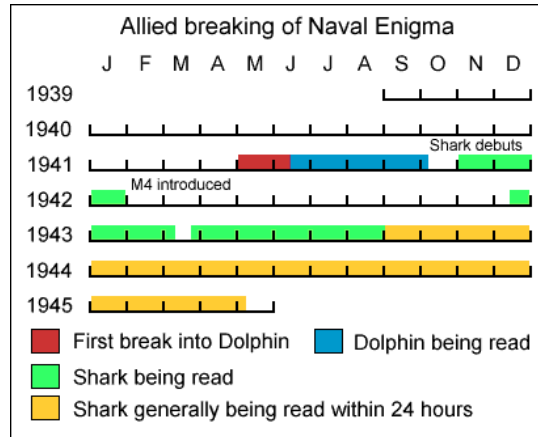
FROM: MOHR

'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

Protecting sources: the Coventry case



Tempest
Security Intelligence

Norway: May, 1945

QKRQW UQTZK FXZOM JFOYR HYZVW BXYSI WMMVW BLEBD MWUWB TVHMR
 FLKSD CCEXI YPAHR MPZIO VBBRV LNHZU POSYE IPWJT UGYOS LAOXR
 HKVCH QOSVD TRBPD JEUKS BBXHT TGVHG FICAC VGUVO QFAQW BKKZJ
 SQJFZ PEVJR OJTOE SLBQH QTRAA HXVYA UHTNB GIBVC LBLXC YBDMQ
 RTVPY KFFZX NDDPC CJBHQ FDKXE EYWPB YQWDX DRDHN IGDXE UJJPV
 MHUKP CFHLL FERAZ HZOHX DGBKO QKKTU DVDCW KAEDH CPHJI WZMMT
 UAMQE NNFCH UIAWC CHNCF YPWUA RBBNI EPHGD DKMDQ LMSNM TWOHM
 AUHRH GCUMQ PKQRK DVSWV MTYVN FFDSD KIISK ONXQH HLIYQ SDFHE
 NCMCO MREZQ DRPBM RVPQT VRSWZ PGLPI TRVIB PXXHP RFISZ TPUEP
 LKOTT XNAZM HTJPC HAASF ZLEFC EZUTP YBAOS KPZCJ CYZOV APZEV
 ELBLL ZEVDC HRMIO YEPFV UGNDL ENISX YCHKX JUWVX USBIT DEQTC
 NKRLS NXMXY ZGCUP AWFUL TZSSF AHMPX GLLNZ RXYJN SKYNQ AMZBU
 GPEJC URWGT QZCTL LOIEK AOISK HAAQF OPFUZ IRTLW EVYWM DN

 Tempest
Security Intelligence

Norway: May, 1945

- Der Führer ist tot.
- Der Führer ist tot.
Der Kampf geht weiter.
Dönitz.



 Tempest
Security Intelligence

May, 1945 - Headlines

Daily Mail 4 L.M. EDITION **BEAR BRAND**
 NO. 12,285 ONE PENNY FOR KING AND EMPIRE WEDNESDAY, MAY 2, 1945

The most dramatic news of the war

'HITLER DEAD—DOENITZ APPOINTED FÜHRER'

Admiral tells Germans: 'The fight goes on.' Himmler ignored

DOOLF HITLER, is dead, Grand Admiral Doenitz, Commander-in-Chief of the German Navy, has been appointed the new Führer. The German radio gave the news to the world at 10.25 last night in the following words: "It is reported from the Führer's headquarters that our Führer Adolf Hitler, has fallen this afternoon in his command post in the Reich Chancellery fighting to his last breath against Bolshevism."

"On April 30 the Führer appointed Grand Admiral Doenitz as his successor. The Grand Admiral will now speak to the German people."

Admiral Doenitz, who immediately came on the air, said his task was to save the German people from annihilation at the hands of Bolshevism, but that since only the war would go on, Germans would have to continue the fight against Britain and America as long as they "hated their oppressor."

The coming of Doenitz as the new Führer comes as a tremendous surprise that would astonish Germany and the world. The German people who wish to fight on, led by Doenitz, and those who wish to surrender, led by Himmler.

It is significant no reference was made in the announcement to Germany, who has already offered unconditional surrender to Britain and the United States, and was expected to comply with the allied demands that might be made on such terms. Doenitz said that the German people were to be guided by the Führer. "There was no question of the Führer's death," he said. "The Führer has fallen in the execution of his duty as a result of the struggle he has had to lead."

WE FIGHT SOVIETS

Doenitz said: "German men and women, soldiers of the German Army, our Führer, Adolf Hitler has fallen. The German people are bowed in respect and reverence."

He said: "I have no hesitation in saying that the German people have been deceived by the propaganda of Bolshevism and coordinated the life of the German people."

"At the end of this struggle he has not a hero's death in the eyes of the German people."

THE HATER OF BRITAIN TAKES OVER

Admiral Doenitz, the new Führer, once again holds the reins of power.

Food ships into Holland, and—Surrender begins on three fronts

REPORTS received in London late last night indicated that large German forces in north-western France have begun to surrender to the Allies with or without authority from Doenitz or Himmler.

GERMANY.—German occupation forces were reported from Holland to be evacuating the country with all speed. King Christian and the Duchess Royal Family were all back in Amsterdam, Cape Den Hague.

NORWAY.—Insurrections were said to be afoot in the German garrisons to lay down their arms at the Swedish frontier to escape German oppression.

CZECHOSLOVAKIA.—A delegation of German and Czech representatives was reported by Tuzovska radio to have left Prague to meet Allied representatives and to hand over the members of the German garrison.

SOUTHERN GERMANY.—Conflicting reports indicated that an important announcement would be made by the Commander of the Upper Danube garrisons this morning.

ITALY.—General Pirelli and Tasso, General Pirelli, Commander-in-Chief of the Italian Fifth Army, and General Pirelli, Commander-in-Chief of the Italian Fifth Army, had announced the surrender of that army.

HOLLAND.—Food ships for the Allies were said to enter Rotterdam, stopped at night. Food ships to enter the German occupied area of Holland were reported to have been made available to day.

'IMPORTANT NEWS TO-DAY'—GERMANS

GOETTER (South Germany) Radio announced that the news of the death of Hitler will be broadcast between 10.25 and noon to-day.—A.P.

'TRICKERY'—MOSCOW

Moscow radio said that the news of the death of Hitler's death repeats the usual trickery and lies of the propaganda.—A.P.

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;

Checkpoint

- Functionality and performance are your enemies, but users begs for it;
- Real cryptoanalysis is a mix of science, art and good luck;
- What did we learn ?



Hashes

- Usually you encrypt something to decrypt later.
 - Conventional cryptography must be used if you need to restore original data.
- But sometimes you don't want to...
 - Hashing can be used when you don't want, or you don't need, to restore original data.



Passwords

- Passwd file

```
oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash
```

↓ ↓ ↓ ↓ ↓ ↓ ↓

1 2 3 4 5 6 7

- Shadow file

```
vivek:$1$fnfffc$pgteyHdicpGOfffXX4ow#5:13064:0:99999:7:::
```

↓ ↓ ↓ ↓ ↓ ↓ ↓

1 2 3 4 5 6

 Tempest
Security Intelligence

Some actual cases...

 Tempest
Security Intelligence



Pro IT – Intranet

Ataque de SQL Injection no sistema de autenticação



TEMPEST
security technologies

06/01/2004



Pro IT – Intranet

Execução remota de comandos via SQL Injection



TEMPEST
security technologies

06/01/2004





Pro IT – Intranet

Manipulação do banco de dados via de SQL Injection




TEMPEST
security technologies


06/01/2004



Another actual case...



sql-injection-acc.exe



Lessons

- It seems software engineering procedures/ practices and security **are not friends!**
 - To get functionality and performance, you have to pay using **security** currency. **No other currency accepted.**
- **Security is not a plugin.** Software engineering uses **as a plugin**, and pretends other issues and impacts **are not his business**;
- **Good crypto is not enough.** Be careful with all the stuff **around it**. There is **no** silver bullet.



Lessons

- **Data is never born in encrypted form**;
- **Data is not useful while in encrypted form**, except for transportation;
- **Data doesn't exist alone!** It's necessary a **system** to handle it. **Data inherits any system vulnerabilities.**
- **Opportunities arise** when data **is being handled** to be encrypted, decrypted or even processed;



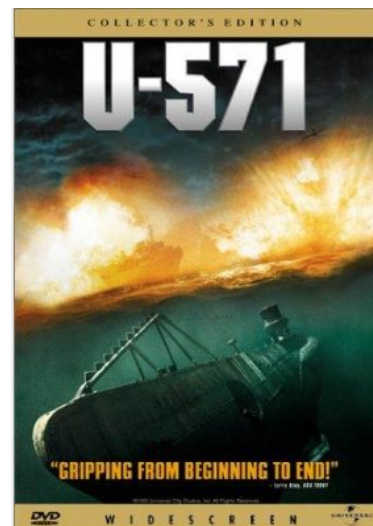
Lessons

- Software **design/architecture/coding** and **strong procedures** are crucial;
- Users (and software engineers) **hates procedures!** In his minds this means only additional work;
- Good cryptography sometimes looks like a Gordian Knot! So be careful with the things around it!

 Tempest
Security Intelligence

To have fun...

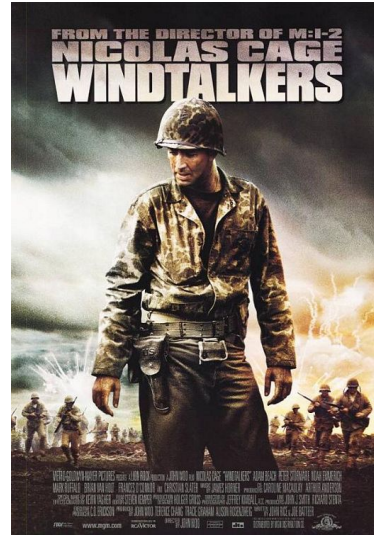
- U-571



 Tempest
Security Intelligence

To have fun...

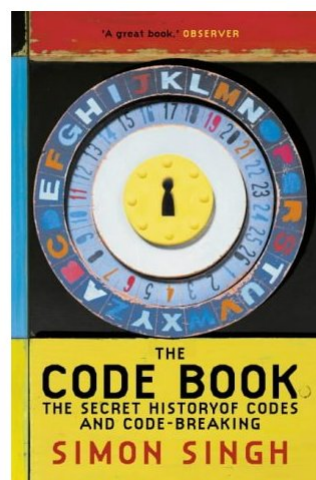
- Windtalkers



Tempest
Security Intelligence

To have fun...

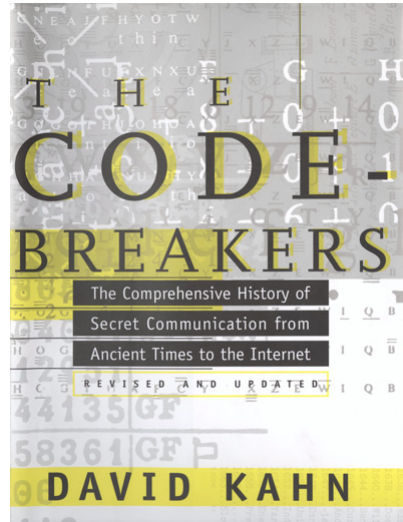
- The Codebook: The Secret History of Codes and Code-breaking
- Simon Singh
2000
- ISBN-10: 1857028899
- ISBN-13: 978-1857028898



Tempest
Security Intelligence

To have fun...

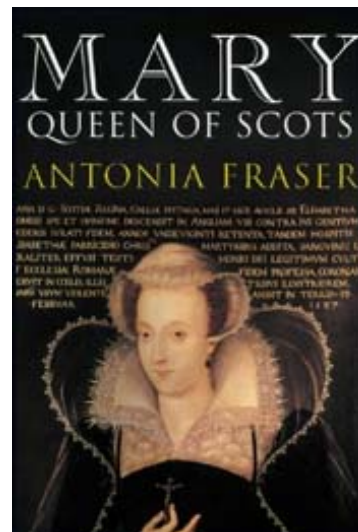
- The codebreakers
- David Kahn
1996



Tempest
Security Intelligence

To have fun...

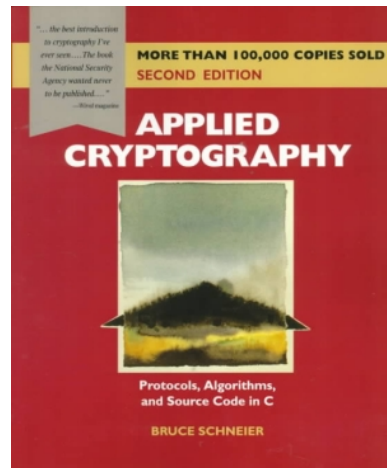
- Mary Queen of Scots
- Lady Antonia Fraser
- 1989.



Tempest
Security Intelligence

To have fun...

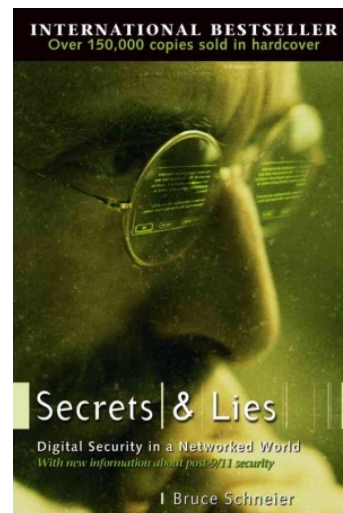
- Applied cryptography
- Bruce Schneier
- 1995.



Tempest
Security Intelligence

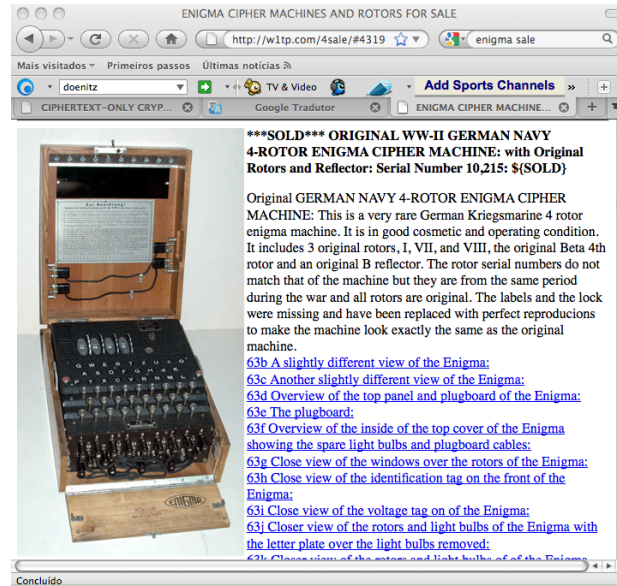
To have fun...

- Secrets and Lies
- Bruce Schneier
- 2004.



Tempest
Security Intelligence

To have fun...



******SOLD**** ORIGINAL WW-II GERMAN NAVY 4-ROTOR ENIGMA CIPHER MACHINE: with Original Rotors and Reflector: Serial Number 10,215: \$(SOLD)**

Original GERMAN NAVY 4-ROTOR ENIGMA CIPHER MACHINE: This is a very rare German Kriegsmarine 4 rotor enigma machine. It is in good cosmetic and operating condition. It includes 3 original rotors, I, VII, and VIII, the original Beta 4th rotor and an original B reflector. The rotor serial numbers do not match that of the machine but they are from the same period during the war and all rotors are original. The labels and the lock were missing and have been replaced with perfect reproductions to make the machine look exactly the same as the original machine.

[63b A slightly different view of the Enigma:](#)
[63c Another slightly different view of the Enigma:](#)
[63d Overview of the top panel and plugboard of the Enigma:](#)
[63e The plugboard:](#)
[63f Overview of the inside of the top cover of the Enigma showing the spare light bulbs and plugboard cables:](#)
[63g Close view of the windows over the rotors of the Enigma:](#)
[63h Close view of the identification tag on the front of the Enigma:](#)
[63i Close view of the voltage tag on of the Enigma:](#)
[63j Closer view of the rotors and light bulbs of the Enigma with the letter plate over the light bulbs removed:](#)
[63k Close view of the rotors and light bulbs of the Enigma:](#)

Tempest
Security Intelligence

Thank you

Evandro Curvelo Hora
evandro@tempest.com.br

Tempest
Security Intelligence