Coding

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

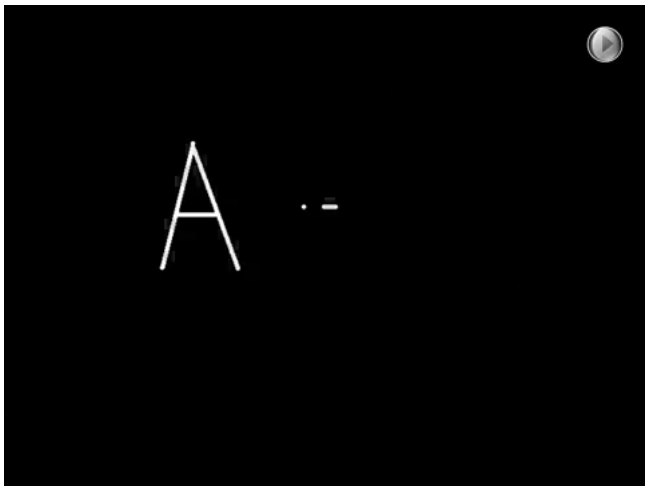
Coding

- Some coding can be used to provide secrecy... except to few. So, there is a intrinsec, 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 intrisec meanings. Much more freedom.
- You can encode a cipher text...
- ... but you can encrypt an encoded text as well.

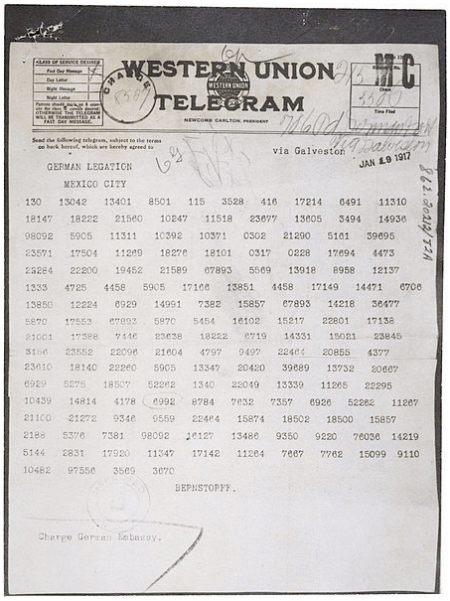
Morse alphabet encoding



Morse message typing

“Da-dit-da” classes in 1941

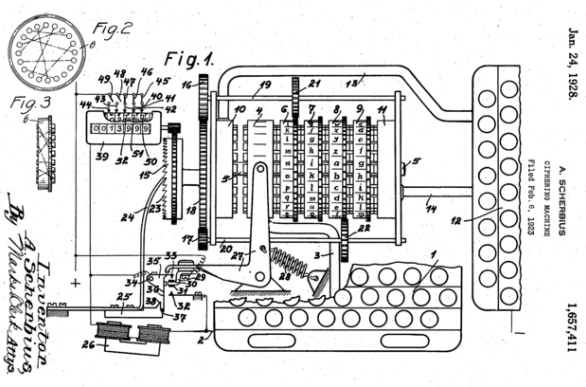
A typical cypher text



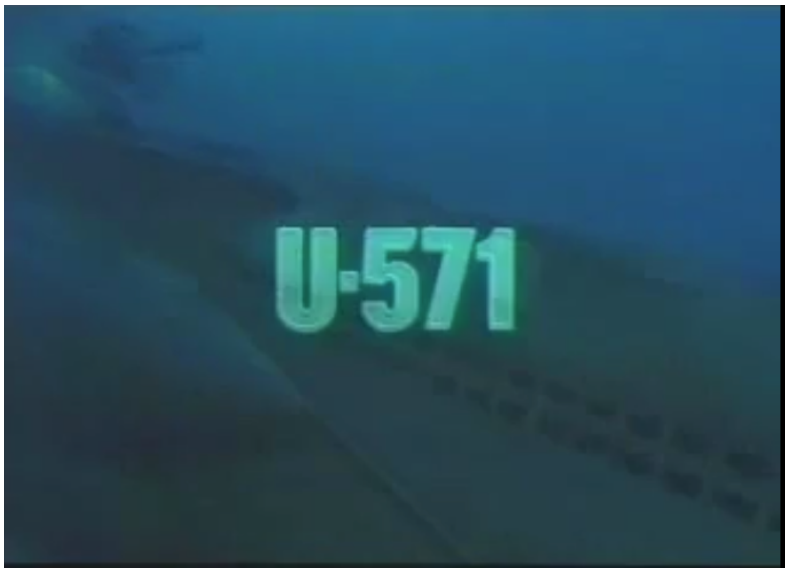
Cryptology

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

Scherbius and his patent



Did you watch this movie ?

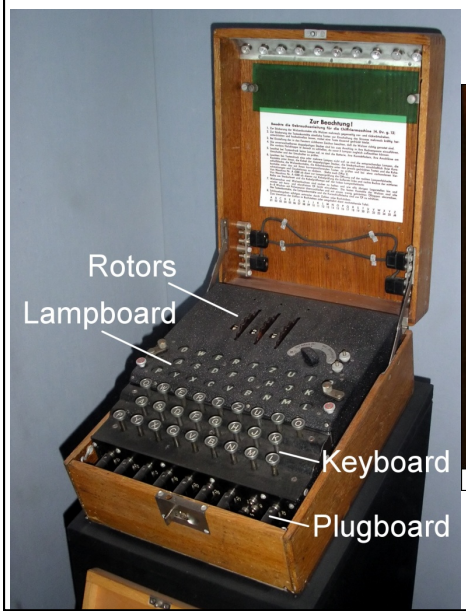


As usual... Hollywood is lying...

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

The actual hero: Lt. Alec Dennis

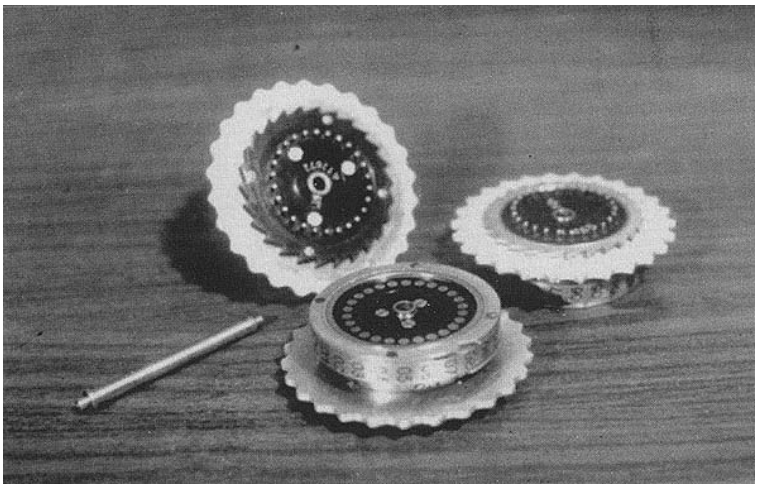
Enigma



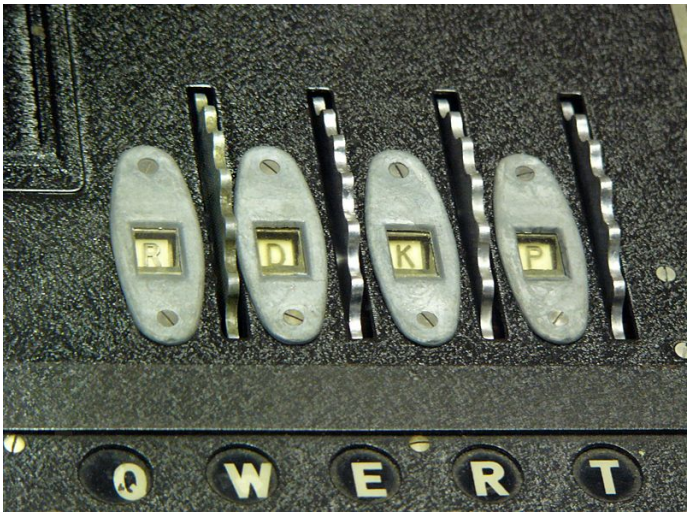
FOUR-ROTOR ENIGMA (GVG / PD)

Enigma models

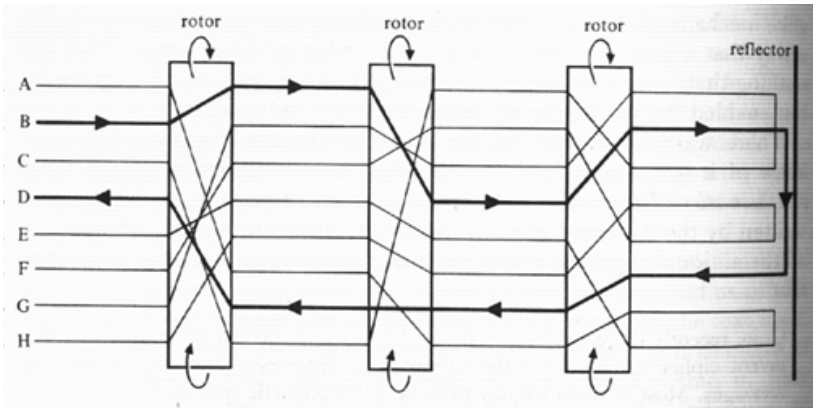
Enigma rotors



Enigma rotor position settings

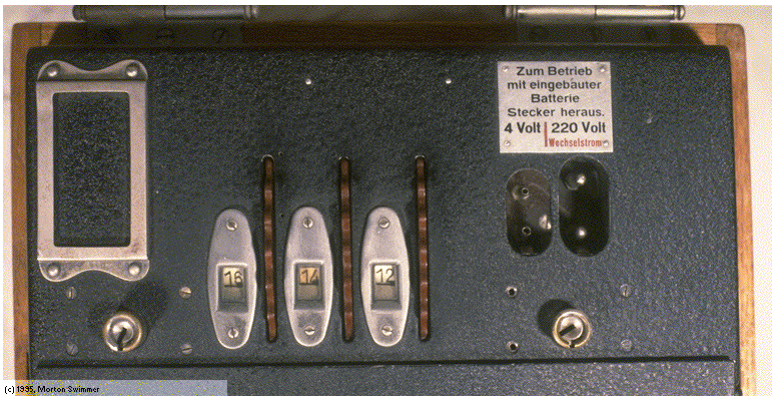


Enigma basic internals

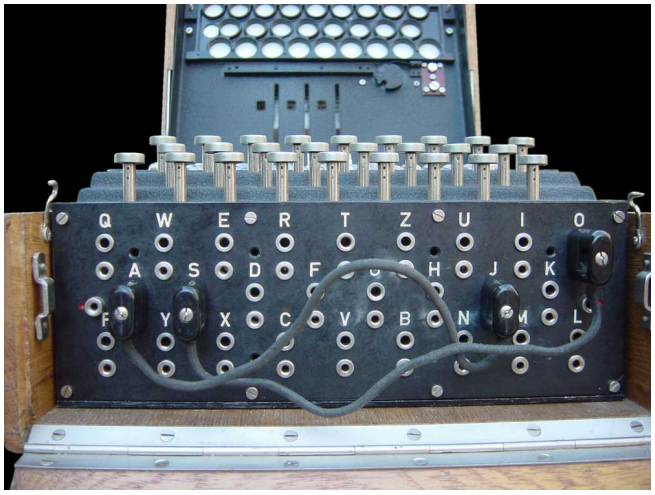


Enigma 8 rotors model

Power and battery inlets

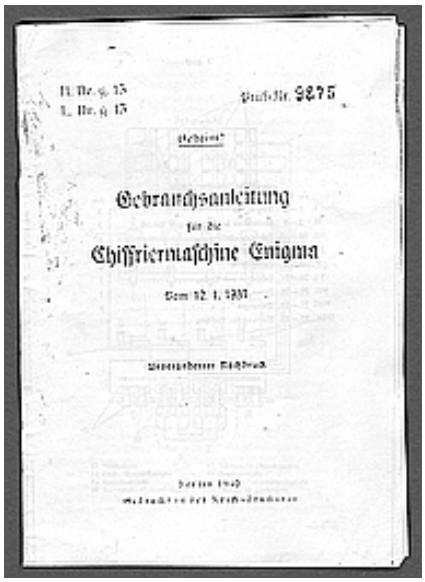


Enigma plugboard panel



Enigma hardware kit

Enigma users guide

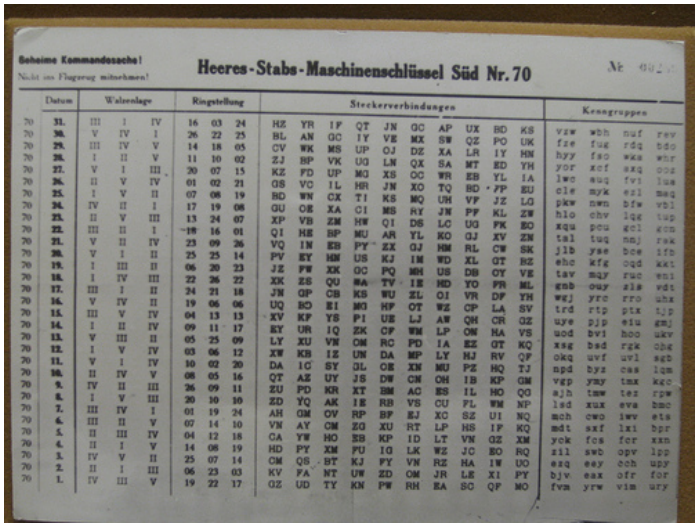


Gebrauchsanleitung

für die

Chiffriermaschine Enigma

Wehrmacht Enigma Codebook

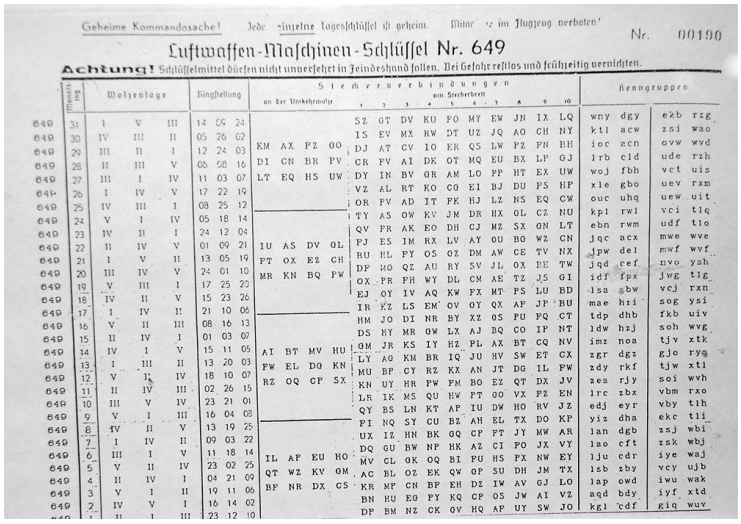


Geheime Kommandosache!

Heeres-Stabs-Maschinenschlüssel Süd Nr. 70

	Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
70	31.	III I IV	16 03 24	HZ YR IF QT JN GC AP UX BD KS	vzw wbh nuf rev
70	30.	V IV I	26 22 25	BL AN GC IY VE MX SW QZ PO UK	fze fug rdq bdo
70	29.	III IV V	14 18 05	CV WK MS UP OJ DZ XA LR IY HN	hyy fzo wks whr
70	28.	I II V	11 10 02	ZJ BP VK UG LN QX SA MT ED YH	yor xof xxq ooz
70	27.	V I III	20 07 15	KZ FD UP MQ XS OC WR EB YL IA	lwc auq fvi lue
70	26.	II V IV	01 02 21	GB VC IL HR JN XO TQ BD FP EU	cle myk esl meq
70	25.	I V II	07 08 19	BD WN CX TI KS MQ UH VF JZ LQ	pkw nwn bfw vbl
70	24.	IV II I	17 19 08	GU OE XA CI MS RY JN PP KL ZW	hlo ohv lqe tup
70	23.	II V III	13 24 07	XP VB ZM HW QI DS LC UQ FK EO	xqu pou xol xon
70	22.	III II I	18 16 01	QI HE BP MU AR YL KO GJ XV ZN	tal tuq nmj rox
70	21.	V II IV	23 09 26	VQ IN EB PY ZX GJ HM RL CW SK	jlb yse bce ifb
70	20.	V I II	25 25 14	PV EY HN US KJ IM WD XL GT BZ	ehc kfg oqd kkt
70	19.	I III II	06 20 23	JZ FW XK GC PQ NH US DB OY VE	tav mqy rwc wnl
70	18.	I IV III	22 26 22	XK ZS QU RA TV IE ND YO FR ML	gnb ouy zls wdt
70	17.	III I II	24 21 18	JN GP CB KS WU ZL QI VR DF YH	wej yro rro uha
70	16.	V IV II	19 06 06	UQ SO EI MJ HF OT WZ CP LA SV	trd rtp ptx tjp
70	15.	III V IV	04 13 13	XV KF YS PI UE LJ AW QH CR GZ	uye pjp eiu emj
70	14.	I II IV	09 11 17	EY UR IQ ZK CF WM LP ON HA VS	uod bvi hoo ukv
70	13.	V III II	05 25 09	LY XU VN OM RC PD IA EZ GT KQ	xsg bsd rgk obr
70	12.	I V IV	03 06 12	XW KB IZ UN DA MP LY NJ RV QF	okq uvf uvl sqb
70	11.	V I IV	10 02 20	DA IC SY JL OE XM WJ PZ HQ TJ	npd byz cas lqm
70	10.	II IV V	08 05 16	QT AZ UY JS DW CM OH IB KP GM	vgp ymy tmx kxc
70	9.	IV II III	26 09 11	ZU PD KR XT BM AC ES IL NO QO	ajh tmw tez rgw
70	8.	I V III	20 10 10	ZD YQ AK IE RB VS CU FL WM NF	lsd xux eva bmc
70	7.	III IV I	01 19 24	AH GM OV RP BF EJ XC SZ UI NQ	mch cwo iwv ets
70	6.	III II V	07 14 10	VN AY GM ZG XU RT LP HS IF KQ	mdt sxf lxi bpr
70	5.	II III IV	04 12 18	CA YW HO ES KP ID LT VN GZ XM	yok fos fer xxn
70	4.	II I V	14 08 19	HD PY XM FU IQ LK WZ JC EO RQ	xil swb opw lpp
70	3.	IV V II	25 07 14	CM QS BT KJ FY VN RZ HA IW UO	sqq eay zoh upy
70	2.	II I III	06 23 03	KV FA NT UW ZD OM JR LE XI PY	bjv eax ofr for
70	1.	IV III V	19 22 17	GZ UD TY KN PW RH EA SC QF MO	fvm yrw vim ury

Luftwaffe Enigma Codebook



Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. [illegible] im Flugzeug verboten!

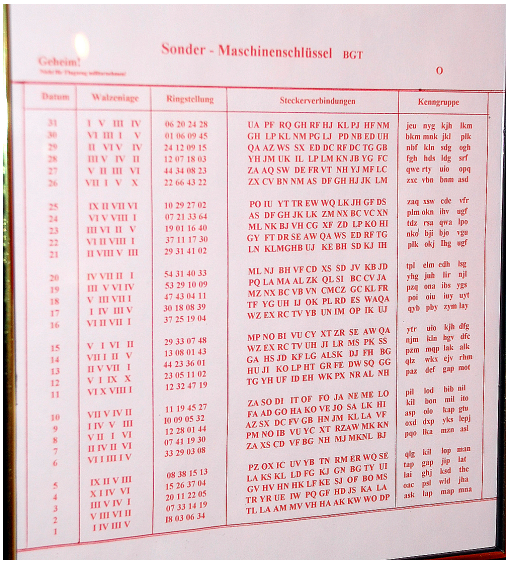
Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Tagesdatum	Walzenlage	Ringstellung	Steckerverbindungen an der Umkehrwalze	Kenngruppen
649 31	I V III	14 09 24	SZ GT DV KU FO MY EW JN IX LQ	wny dgy ezb rzg
649 30	IV III II	05 26 02	IS EV MX RW DT UZ JQ AO CH NY	ktl acw zsi wao
649 29	III II I	12 24 03	KM AX PZ GO DJ AT CV IO ER QS LW PZ FN BH	joc zcn ovw wvd
649 28	II III V	06 08 16	DI CN BR FV CR PV AI DK OT MQ EU BX LP GJ	lrb cld ude rzh
649 27	III I IV	11 03 07	LT EQ HS UW DY IN BV GR AM LO PP HT EX UW	woj fbh vct uis
649 26	I IV V	17 22 19	VZ AL RT KO CO EI BJ DU PS HP	xle gbo uev rxm
649 25	IV III I	08 25 12	OK PV AD IT PK HJ LZ NS EQ GW	ouc uhq uew uit
649 24	V I IV	05 18 14	TY AS OW KV JM DR HX GL CZ NU	kpl rwl vci tlq
649 23	IV II I	24 12 04	QV FR AK EO DH GJ MZ SX GN LT	ebn rwm udf tlo
649 22	II IV V	01 09 21	IU AS DV GL PJ ES IM RX LV AY OU BQ WZ GN	jqc acx mwe wve
649 21	I V II	13 05 19	PT OX EZ CH RU HL FY OS QZ DM AW CE TV NX	jpw del mwf wvf
649 20	III IV V	24 01 10	MR KN BQ FW DP MO QZ AU RY SV JL OX DE TW	jqd cef nyo ysh
649 19	V III I	17 25 23	OX FR FH WY DL CM AE TZ JS GI	idf fpx jwg tlg
649 18	IV II V	15 23 26	EJ OY IV AQ XW FX MT FS LU BD	isa sbw vcj rxn
649 17	I IV II	21 10 06	IR XZ LS EM GV OY QX AP JP BU	mae hzi sog ysi
649 16	V II III	08 16 13	HM JO DI NR BY XZ OS PU FQ GT	tdp dhb fkb uiv
649 15	II IV I	01 03 07	DS HY MR QW LX AJ BQ CO IP NT	ldw hzj soh wvg
649 14	IV I V	15 11 05	QM JR KS IY HZ PL AX BT CQ NV	imz noa tjv xtk
649 13	I III II	13 20 03	AI BT MV HU LY AQ KM BR IQ JU HV SW ET CX	zgr dgz gjo ryq
649 12	V II IV	18 10 07	FW EL DQ KN MU BP CY RZ KX AN JT DG IL PW	zdy rkf tjw xtl
649 11	II IV III	02 26 15	RZ OQ CP SX KN UY HR PW FM BO EZ QT DX JV	zea rjy soi wvh
649 10	III V IV	23 21 01	LR IK MS QU HW PT OO VX PZ EN	irc zbx vbm rxo
649 9	V I III	16 04 08	QY BS LN KT AP IU DW HO RV JZ	edj eyr vby tih
649 8	IV II V	13 19 25	FI NQ SY GU BZ AH EL TX DO KP	yiz dha ekc tli
649 7	I IV II	09 03 22	UX IZ HN BK QQ CP PT JY MW AR	lan dgb zsj wbi
649 6	III I V	11 18 14	DQ GU BW NP HK AZ CI FO JX VY	lao cft zsk wbj
649 5	V II IV	23 02 25	IL AP EU HO MV GL OK OQ BI FU HS PX NW EY	iju cdr iye waj
649 4	II IV I	04 21 09	QT WZ KV OM AC BL OZ EK QW QP SU DH JM TX	isb zby vcy ujb
649 3	V I II	19 11 06	BF NR DX CS KR MP CN BP EH DZ IW AV GJ LO	iap owd iwu wak
649 2	IV V I	16 14 02	BN HU EQ FY KQ CP OS JW AI VZ	aqd bdy iyf xtd
649 1	II I III	23 12 10	DP BM NZ CK QV HQ AP UY SW JO	kgl zdf giq wuv

Kriegsmarine Enigma Codebook



Geheim!

Sonder - Maschinenschlüssel BGT

O

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppe
31	I V III IV	06 20 24 28	UA PF RQ GH RF HJ KL PJ HF NM	jcu nyg kjh ikm
30	VI III I V	01 06 09 45	GH LP KL NM PG LJ PD NB ED UH	hkm mnk jkl plk
29	II VI V IV	24 12 09 15	QA AZ WS SX ED DC RF DC TG GB	nhf kln sdg egh
28	III V IV II	12 07 18 03	YH JM UK IL LP LM KN JB YG FC	fgh hds ldg srf
27	V II III VI	44 34 08 23	ZA AQ SW DE FR VT NH YJ MF LC	qwe rty uio opq
26	VII I V X	22 66 43 22	ZX CV BN NM AS DF GH HJ JK LM	zxc vbn bnm asd
25	IX II VII VI	10 29 27 02	PO IU YT TR EW WQ LK JH GF DS	zaq xsw cde vfr
24	VI V VIII I	07 21 33 64	AS DF GH JK LK ZM NX BC VC XN	plm okn ihv ugf
23	III VI II V	19 01 16 40	ML NK KJ VH CG XF ZD LP KO HI	tdz rsa qwa lpo
22	VI II VIII I	37 11 17 30	GY FT DR SE AW QA WS ED RF TG	nko bji hjo vgu
21	II VIII V III	29 31 41 02	LN KLMGHB UJ KE BH SD KJ IH	plk okj lhg ugf
20	IV VII II I	54 31 40 33	ML NJ BH VF CD XS SD JV KB JD	tpl elo edh lsg
19	III V VI IV	53 29 10 09	PQ LA MA AL ZK QL SI BC CV JA	yhg juh lir njl
18	V III VII I	47 43 04 11	MZ NX BC VB VN CMCZ GC KL FR	jzq ona ibs ygs
17	I IV III V	30 18 08 39	TF YG UH IJ OK PL RD ES WAQA	poi oiu iuy uyt
16	VI II VII I	37 25 19 04	WZ EX RC TV YB UN IM OP IK UJ	qyb pby zym lzy
15	V I VI II	29 33 07 48	MP NO BI VU CY XT ZR SE AW QA	ytr uio kjh dfg
14	VII I II V	13 08 01 43	WZ EX RC TV UH JI LR MS PK SS	njm klo bgv dfc
13	II V VII I	44 23 36 01	GA HS JD KF LG ALSK DJ FH BG	pom mgn lak afk
12	V I IV X	23 05 11 02	HU JI KO LP HT GR FE IW SQ GG	qlz wkx cjy rhm
11	VI X VIII I	12 32 47 19	TG YH UF ID EH WK PX NR AL NH	paz def gap moe
10	VII V IV II	11 19 45 27	ZA SO DI IT OF FO JA NE ME LO	pil lod hib nil
9	I IV V III	10 09 05 32	FA AD GO HA KO VE JO SA LK HI	kil hon mil ilo
8	V II I VI	12 28 01 44	AZ SX DC FY GB HN JM KL LA VF	asp olo kap gto
7	II IV II VI	07 41 19 30	PM NO IB VU YC XT RZAW MK KN	osd dup yks lopj
6	VI I III I V	33 29 03 08	ZA XS CD VF BG NH MJ MKNL BJ	pqo jka mzo asl
5	IX II V III	08 38 15 13	PZ OX JC UV YB TN RM ER WQ SE	qlg kil lop mnn
4	X I IV VI	15 26 37 04	LA KS KL LD FG KJ GN BG TY UI	zap gup jip lat
3	III V IV I	20 11 22 05	GV HV HN HK LF KE SJ OF BQ MS	lai ghj ked the
2	V III VI II	07 33 14 19	TR YR UE IW PQ GF HD JS KA LA	oac psl wld jka
1	I IV III V	18 03 06 34	TL LA AM MV VH HA AK KW WO DP	ask lap mnp mna

How strong was Enigma ?

- For 3 rotors interchange orientation:
  - 26 x 26 x 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 x 6 x 100.391.791.500 = ~10.000.000.000.000.000

Enigma in use

Enigma in battlefield

Wireless Enigma

Station listeners

Morse listening

Key assigment 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 codebook!

Enigma X Morse

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

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.

Marian Rejewski

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

Alan Turing

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

Bletchley Park (Station X)

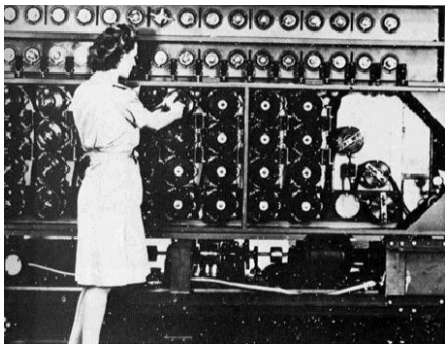
Bletchley Park at War

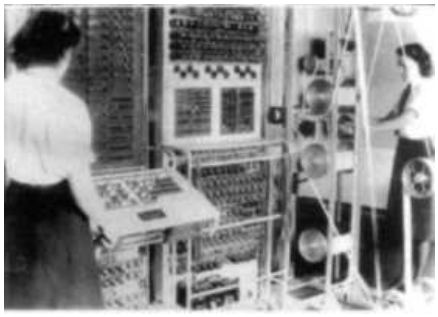
Bletchley Park at War

Royal visitors

The girls... and the boss

The girls, Turing bombs & Colossus





Bletchley Park, today

The girls, today ☺

Some *clues* used...

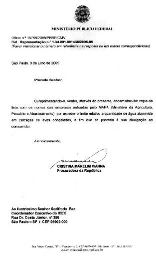
- Enigma project/design characteristics:
  - One letter never was encrypted as itself;

Some *clues* used...

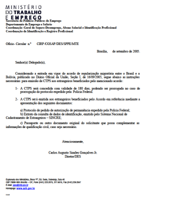
- Procedures:
  - Military document rigid shapes (wheater reports, comm reports, other known templates etc);

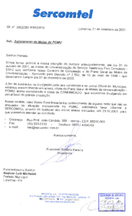
What about a guess ?

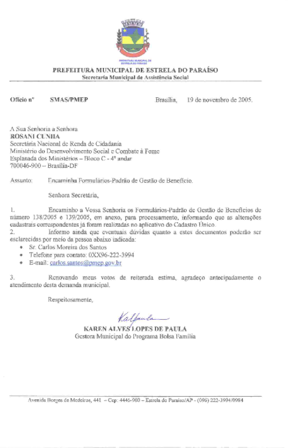
What is this ?

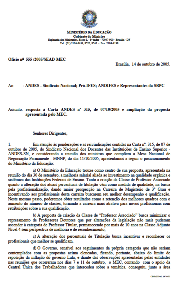

MINISTÉRIO PÚBLICO FEDERAL

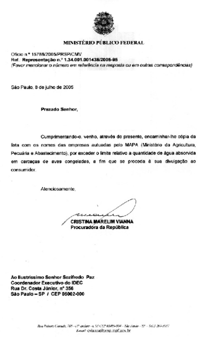
Official document shaping






PREFEITURA MUNICIPAL DE ESTRELA DO PARAÍSO




MINISTÉRIO PÚBLICO FEDERAL

Typical German wheather 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 Centi-grade
	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
Durcheinanderlaufende Dünung				z

Wetterspruchschlüssel (S_p)..... = 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 sm (F I, W II) ..... = k
Dünung (K) = aus SW hoch ..... = v
Unterschrift (UU) ..... = qm

Some *clues* used...

- Morse code radio-operator personal characteristics:
  - "Hand signatures";
- Military unit and it's localization.

Some *clues* used...

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

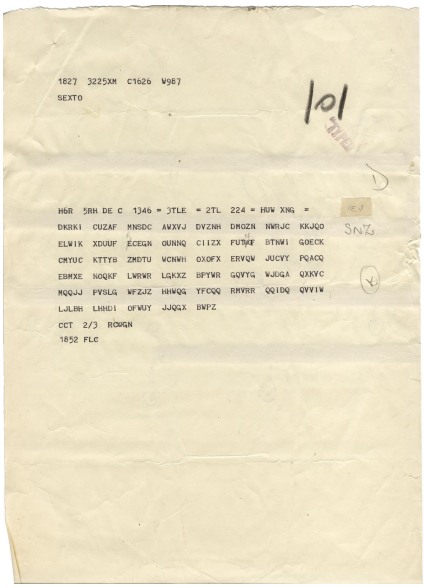
Some *clues* used...

- Other common mistakes:
  - Not random session key choice;
  - Key reuse;
  - Aforisms use;
  - Encrypt public well known messages;
  - Same message sent using other ciphers.

... so Turing & his crew realized the key universe decreases to (only):

105.456

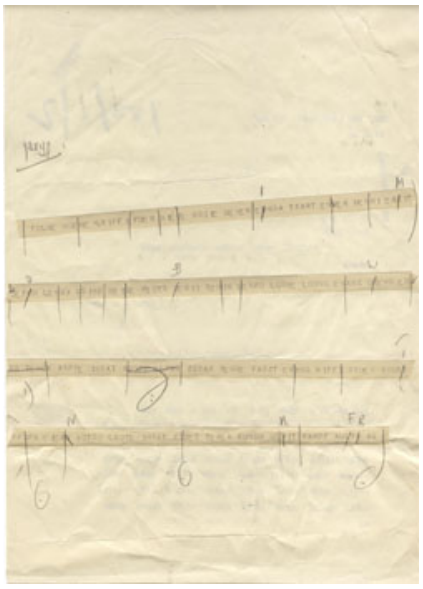
Typical encrypted message



1827 3225XM C1626 V987
SEXTO

101

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =
DKRKI CUZAF MNSDC AWXVJ DVZNH DMQZN NWRJC KKJQO
ELWIK XDUUF ECEQN OUNNQ C11ZX FUTKF BTNWI GOECK
CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCYY FQACQ
EBMXE NOQKF LWRWR LQKXZ BPYWR GQVYG WJDGA QXXYC
MQQJJ FVSLG WFZJZ HHWQG YFCQQ RMVRR QQ1DQ QVVIW
LJLBH LHHD1 OFWUY JJQGX BWPZ
CCT 2/3 ROWGN
1852 FLC



Typical decrypted U-Boat message

ADM
TO I D 8 G ZIP/ZTPG/18733
FROM N S

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

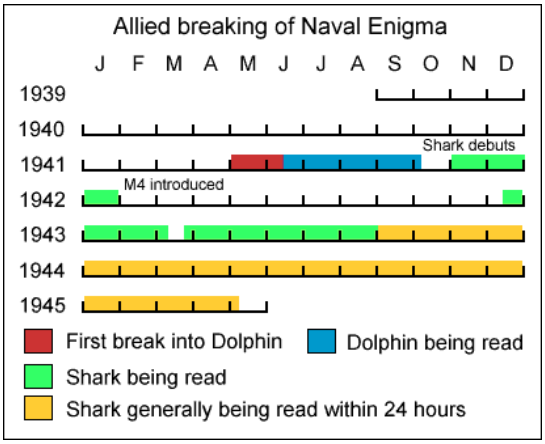
FROM: MOHR

''D'' CLASS BRITISH CRUISER SUNK IN SQUARE PE 7985. AM CONTINUING PASSAGE SOUTH.

(DEPT.NOTE: SQUARE PE = ?).

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

Naval Enigma cracking roadmap



Protecting sources: the Coventry case

Norway: May, 1945

QKRQW UQTZK FXZOM JFOYR HYZWV BXYSI WMMVW BLEBD MWUWB TVHMR
FLKSD CCEXI YPAHR MPZIO VBBRV LNHZU POSYE IPWJT UGYOS LAOXR
HKVCH QOSVD TRBPD JEUKS BBXHT TGVHG FICAC VGUVO QFAQW BKXZJ
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 QXKTL DVDCW KAEDH CPHJI WZMMT
UAMQE NNFCH UIAWC CHNCF YPWUA RBBNI EPHGD DKMDQ LMSNM TWOHM
AUHRH GCUMQ PKQRK DVSWV MTYVN FFDDS KIISX ONXQH HLIYQ SDFHE
NCMCO MREZQ DRPBM RVPQT VRSWZ PGLPI TRVIB PXXHP RFISZ TPUEP
LKOTT XNAZM HTJPC HAASF ZLEFC EZUTP YBAOS KPZCJ CYZOV APZZV
ELBLL ZEVDC HRMIO YEPFV UGNDL ENISX YCHKS JUWVX USBIT DEQTC
NKRLS NXMXY ZGCUP AWFUL TZZSF AHMPX GLLNZ RXYJN SKYNQ AMZBU
GFZJC URWGT QZCTL LOIEK AOISK HAAQF OPFUZ IRTLW EVYWM DN

May, 1945

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

May, 1945

Daily Mail

4 A.M. EDITION

NO. 15,285 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

ADOLF 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 Fuhrer 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. For that aim only, the war would go on. Germany would have to continue the fight against Britain and America as long as they "hindered this purpose".

The naming of Doenitz as the new Führer comes as a bombshell. It suggests that what remains of Germany has been split into two camps — those who wish to fight on, led by Doenitz, and those who want to surrender, led by Himmler.

It is significant no reference was made in the announcement to Himmler, who has already offered unconditional surrender to Britain and the United States, and was expected to comply with the Allied demand that capitulation must be made also to Russia.

None of the big names of Nazism were there to pledge support to the new Führer. Where was Goebbels? Where was Ribbentrop? No marshal or general was called to the microphone to give force to an Order of the Day by Doenitz calling on the Army to fight on.

'WE FIGHT SOVIETS'

Doenitz cannot hold Reich together

By WILSON BROADBENT

THE HATER OF BRITAIN TAKES OVER

Food ships into Holland, and—

Surrender begins on three fronts

'IMPORTANT NEWS TO-DAY' — GERMANS

'TRICKERY' — MOSCOW

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;
- Real cryptoanalysis is a mix of science, art and good luck.
- What did we learn ?

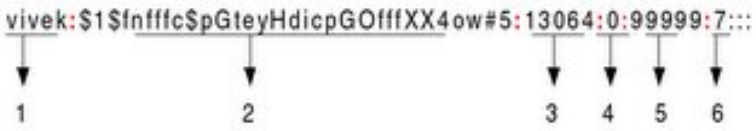
Hashes

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

Passwords

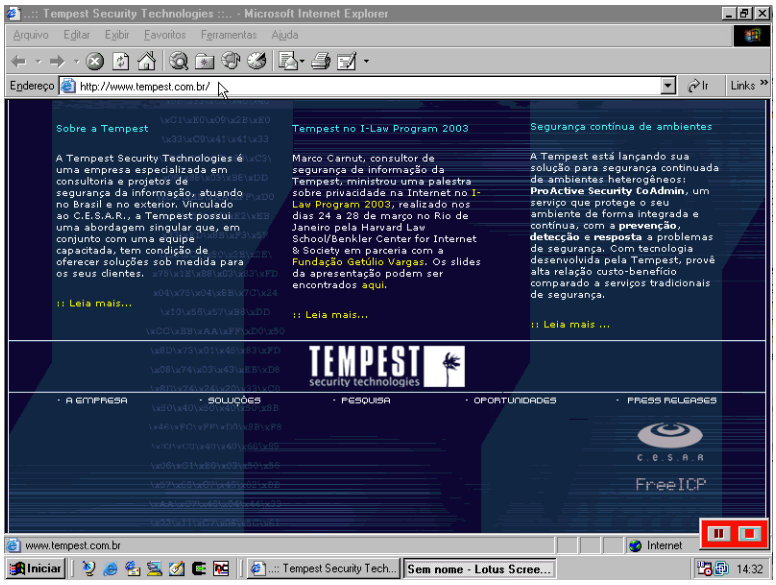
- Passwd file

- Shadow file



A real case

An actual case...



Lessons

- It seems software engineering procedures/ practices and security are not friends!
  - To get functionality and performance, you have to pay using security currency.
- Security is not a plugin.
- Good crypto is not enough. Be careful with all the stuff around it.

Lessons

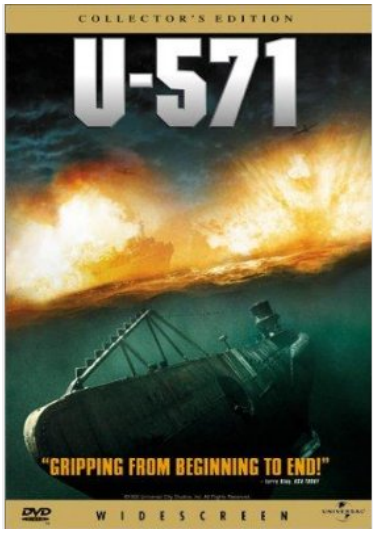
- Data is never born in encrypted form;
- Data is not useful while in encrypted form;
- Opportunities arises when data is being handled to be encrypted or decrypted;

Lessons

- Design and procedures are crucial.
- Users (and software engineers) hates procedures! In his minds, this means additional work.
- Good cryptography sometimes looks like a Gordian Knot! So be careful with the things around it!

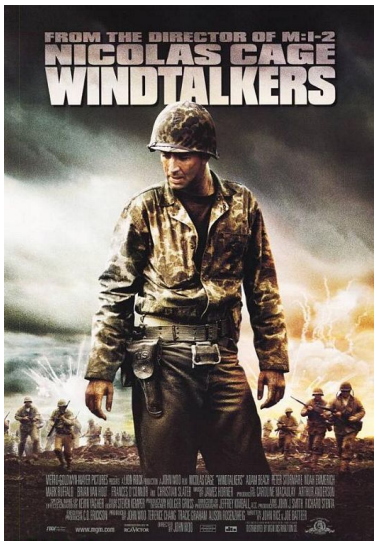
To have fun…

- U-571



To have fun…

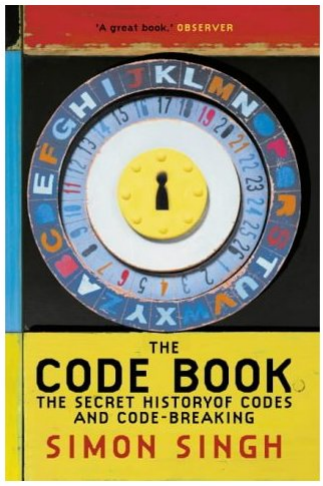
- Windtalkers



To have fun…

- The Codebook: The Secret History of Codes and Code-breaking
- Simon Singh
  2000

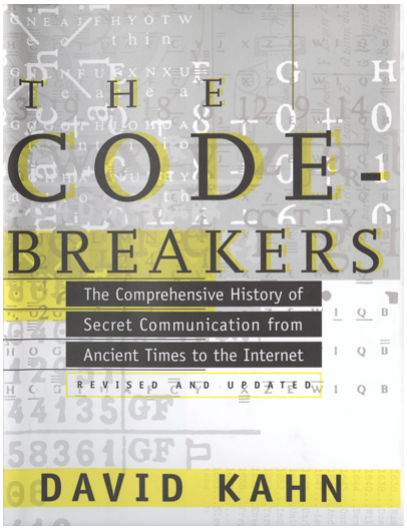
- **ISBN-10: 1857028899**
- **ISBN-13: 978-1857028898**



To have fun…

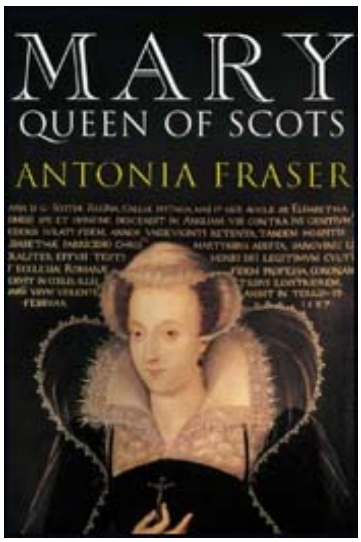
- The codebreakers

- David Kahn
  1996



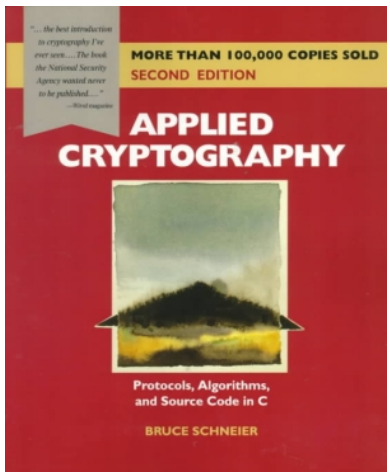
To have fun…

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



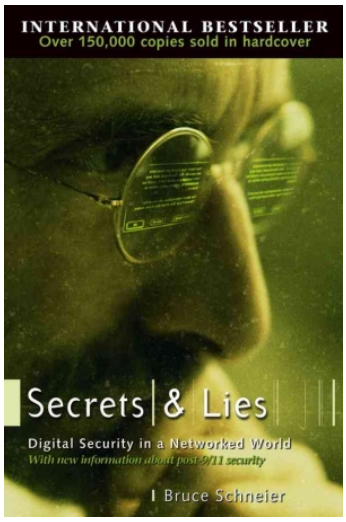
To have fun…

- Applied cryptography
- Bruce Schneier
- 1995.

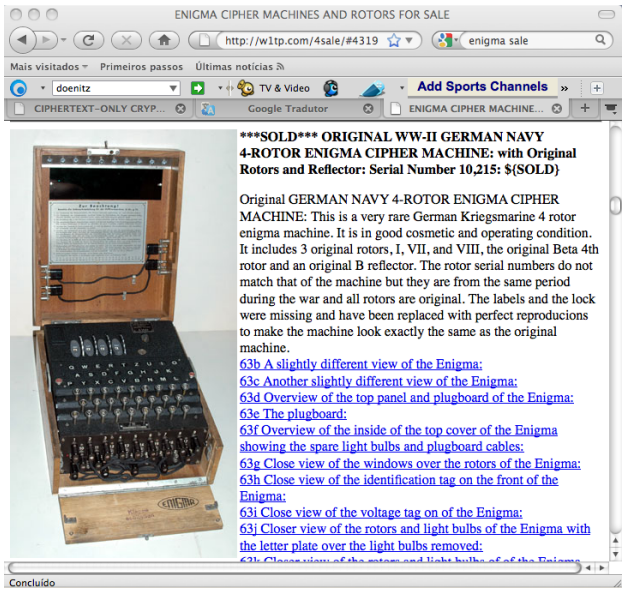


To have fun…

- Secrets and Lies
- Bruce Schneier
- 2004.



To have fun…



Thank you

Evandro Curvelo Hora
evandro@tempest.com.br