The Enigma Machine

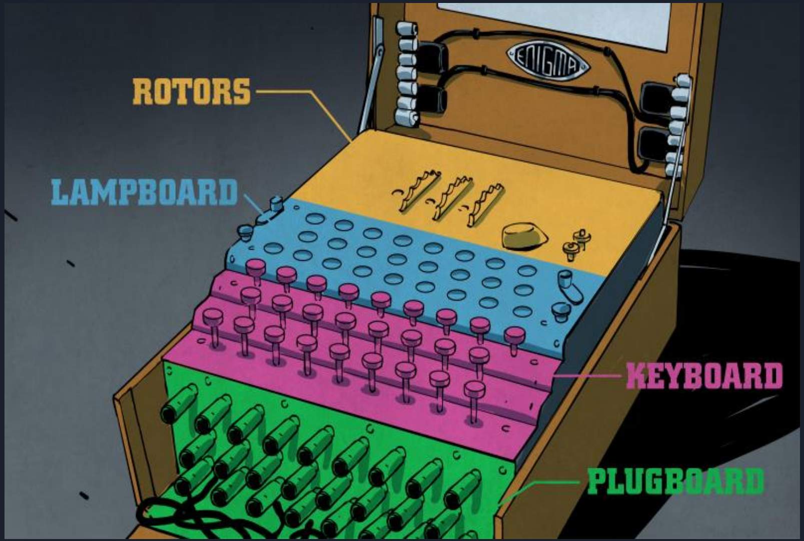
Leonard Fernando

What is it?

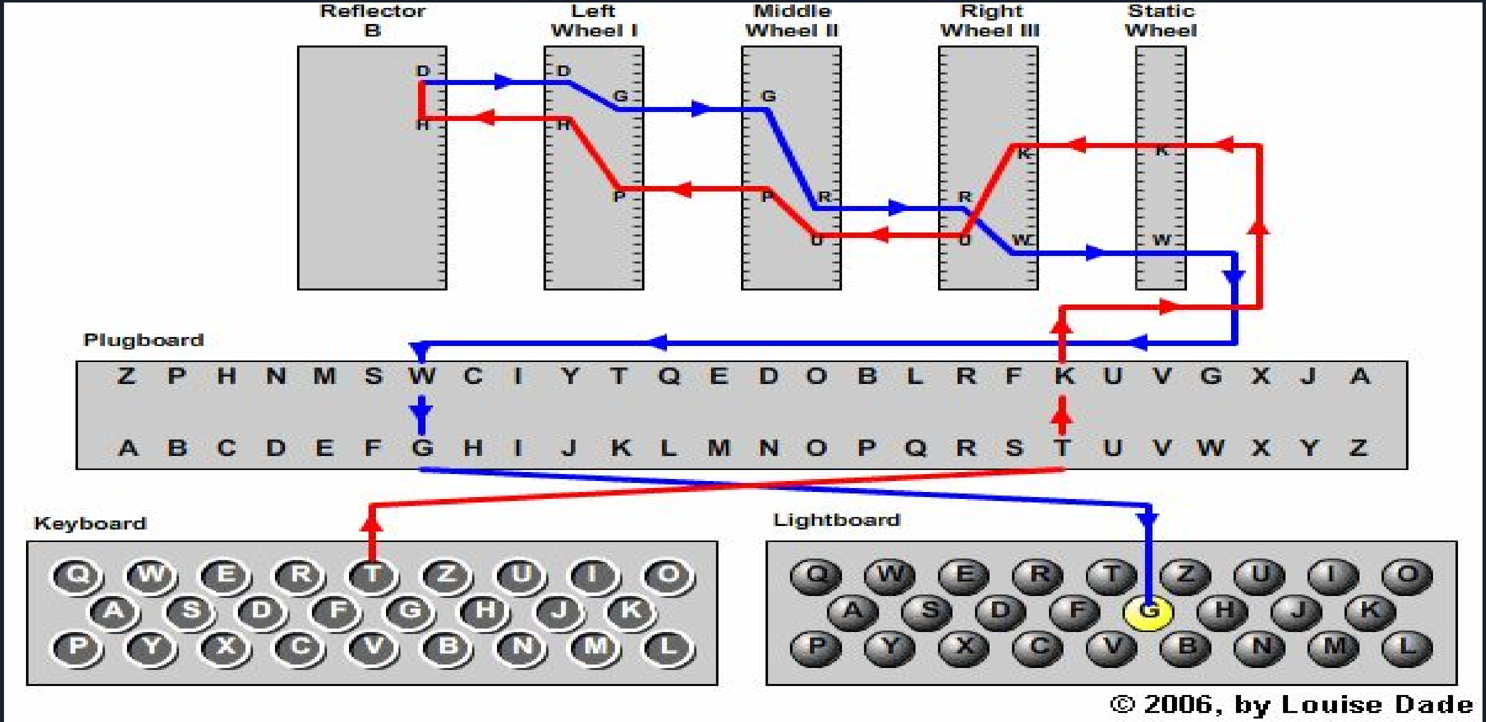
- The enigma machines were electro-mechanical rotor cipher machines developed by Arthur Scherbius in 1918.
- They were most notably used by Germany to encrypt military messages during WWII.
- The encryptions were thought to be uncrackable until July 9, 1941.

Design

- The enigma machine is a mechanically operated device with an electrical signal passing through its wires and mechanical parts.
- Its components consisted of a keyboard, a plugboard, a static rotor, scramblers, a reflector, and a lampboard.
- The static rotor, scramblers, and reflector are all contained in the ‘rotors’ component.



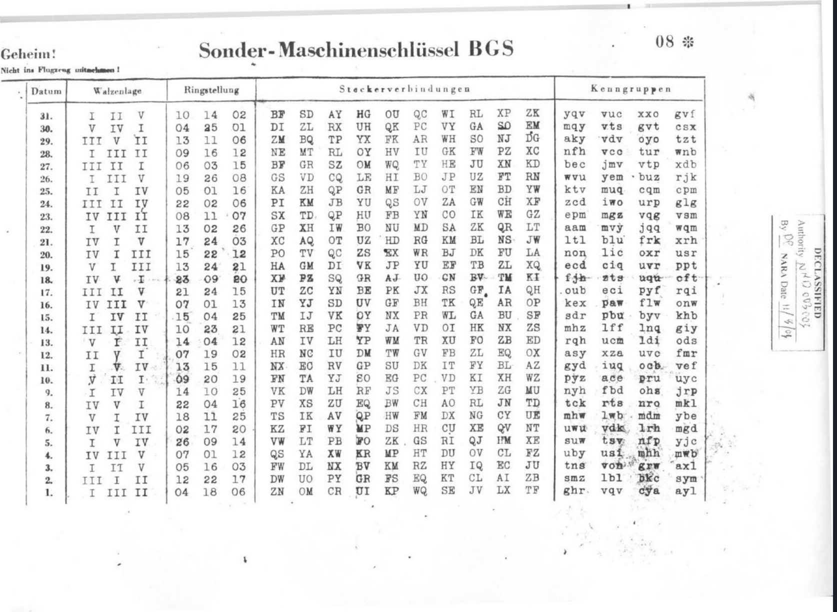
The Path to Encryption



© 2006, by Louise Dade

Cryptanalysis

- Code breakers were required to keep up with a code book that changed every month, which listed enigma settings for each day of the month.
- Enigma machines produced a polyalphabetic substitution cipher with a random key sequence. In theory, this would have been unbreakable.
- The keyspace of the Enigma cipher consists of several things: the rotors and their order, the 3 letter indicator settings, the 3 letter ring settings, and the plugboard settings.
- The total number of ways you can set the enigma machine was 158,962,555,217,826,360,000.



Geheim!

Nicht ins Flugzeug mitnehmen!

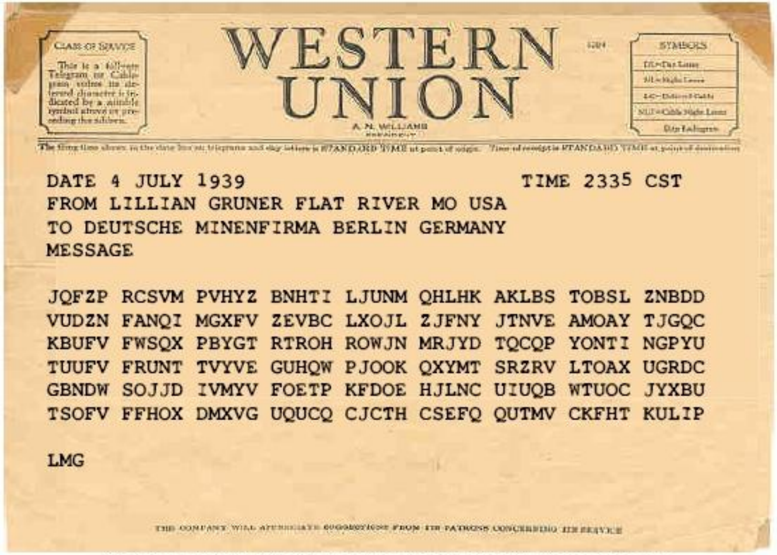
Sonder-Maschinenschlüssel BGS

08 ❊

Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
31.	I	II	V	10	14	02	BF	SD	AY	HG	OU	QC	WI	RL	XP	ZK	yqv	vuc	xxo	gvf
30.	V	IV	I	04	25	01	DI	ZL	RX	UH	QK	PC	VY	GA	SO	EM	mqy	vts	gvt	csx
29.	III	V	II	13	11	06	ZM	BQ	TP	YX	FK	AR	WH	SO	NJ	DG	aky	vdv	oyo	tzt
28.	I	III	II	09	16	12	NE	MT	RL	OY	HV	IU	GK	FW	PZ	XC	nfh	vco	tur	wnb
27.	III	II	I	06	03	15	BF	GR	SZ	OM	WQ	TY	HE	JU	XN	KD	bec	jmv	vtp	xdb
26.	I	III	V	19	26	08	GS	VD	CQ	LE	HI	BO	JP	UZ	FT	RN	wvu	yem	buz	rjk
25.	II	I	IV	05	01	16	KA	ZH	QP	GR	MF	LJ	OT	EN	BD	YW	ktv	muq	cqm	cpm
24.	III	II	IV	22	02	06	PI	KM	JB	YU	QS	OV	ZA	GW	CH	XF	zcd	iwo	urp	glg
23.	IV	III	II	08	11	07	SX	TD	QP	HU	FB	YN	CO	IK	WE	GZ	epm	mgz	vqg	vsm
22.	I	V	II	13	02	26	GP	XH	IW	BO	NU	MD	SA	ZK	QR	LT	aam	mvy	jqq	wqm
21.	IV	I	V	17	24	03	XC	AQ	OT	UZ	HD	RG	KM	BL	NS	JW	ltl	blu	frk	xrh
20.	IV	I	III	15	22	12	PO	TV	QC	ZS	EX	WR	BJ	DK	FU	LA	non	lic	oxr	usr
19.	V	I	III	13	24	21	HA	GM	DI	VK	JP	YU	EF	TB	ZL	XQ	ecd	ciq	uvr	ppt
18.	IV	V	I	23	09	20	XF	PZ	SQ	GR	AJ	UO	GN	BV	TM	KI	fjh	zts	uqu	cft
17.	III	II	V	21	24	15	UT	ZC	YN	BE	PK	JX	RS	GF	IA	QH	oub	eci	pyf	rqi
16.	IV	III	V	07	01	13	IN	YJ	SD	UV	GF	BH	TK	QE	AR	OP	kex	paw	flw	onw
15.	I	IV	II	15	04	25	TM	IJ	VK	OY	NX	PR	WL	GA	BU	SF	sdr	pbu	byv	khb
14.	III	II	IV	10	23	21	WT	RE	PC	FY	JA	VD	OI	HK	NX	ZS	mhz	lff	lnq	giy
13.	V	I	II	14	04	12	AN	IV	LH	YP	WM	TR	XU	FO	ZB	ED	rqh	ucm	ldi	ods
12.	II	V	I	07	19	02	HR	NC	IU	DM	TW	GV	FB	ZL	EQ	OX	asy	xza	uvc	fmr
11.	I	V	IV	13	15	11	NX	EC	RV	GP	SU	DK	IT	FY	BL	AZ	gyd	iuq	ocb	vef
10.	V	II	I	09	20	19	FN	TA	YJ	SO	EG	PC	VD	KI	XH	WZ	pyz	ace	pru	uyc
9.	I	IV	V	14	10	25	VK	DW	LH	RF	JS	CX	PT	YB	ZG	MU	nyh	fbd	ohs	jrp
8.	IV	V	I	22	04	16	PV	XS	ZU	EQ	BW	CH	AO	RL	JN	TD	tck	rts	nro	mkl
7.	V	I	IV	18	11	25	TS	IK	AV	QP	HW	FM	DX	NG	CY	UE	mhw	lwb	mdm	ybe
6.	IV	I	III	02	17	20	KZ	FI	WY	MP	DS	HR	CU	XE	QV	NT	uwu	vdk	lrh	mgd
5.	I	V	IV	26	09	14	VW	LT	PB	FO	ZK	GS	RI	QJ	HM	XE	suw	tsv	nfp	yjc
4.	IV	III	V	07	01	12	QS	YA	XW	KR	MP	HT	DU	OV	CL	FZ	uby	usi	mhh	mwb
3.	I	II	V	05	16	03	FW	DL	NX	BV	KM	RZ	HY	IQ	EC	JU	tns	von	grw	axl
2.	III	I	II	12	22	17	DW	UO	PY	GR	FS	EQ	KT	CL	AI	ZB	smz	lbl	bkc	sym
1.	I	III	II	04	18	06	ZN	OM	CR	UI	KP	WQ	SE	JV	LX	TF	ghr	vqv	cya	ayl

Enigma’s Flaw

- One of the flaws associated with enigma was the inability to encrypt a letter as itself.
- Furthermore, German troops would send messages with repeating words like “wetterbericht” or weather report.
- Taking advantage of these flaws, the British forces invented a machine to determine the right settings for the decryption of German messages.



CLASS OF SERVICE

This is a full-rate Telegram or Cablegram unless its deferred character is indicated by a suitable symbol above or preceding the address.

WESTERN UNION

A. N. WILLIAMS
PRESIDENT

SYMBOLS
DL=Day Letter
NL=Night Letter
LC=Deferred Cable
NLT=Cable Night Letter
Ship Radiogram

The filing time shown in the date line on telegrams and day letters is STANDARD TIME at point of origin. Time of receipt is STANDARD TIME at point of destination

```
DATE 4 JULY 1939                          TIME 2335 CST
FROM LILLIAN GRUNER FLAT RIVER MO USA
TO DEUTSCHE MINENFIRMA BERLIN GERMANY
MESSAGE

JQFZP RCSVM PVHYZ BNHTI LJUNM QHLHK AKLBS TOBSL ZNBDD
VUDZN FANQI MGXFV ZEVBC LXOJL ZJFNY JTNVE AMOAY TJGQC
KBUFV FWSQX PBYGT RTROH ROWJN MRJYD TQCQP YONTI NGPYU
TUUFV FRUNT TVYVE GUHQW PJOOK QXYMT SRZRV LTOAX UGRDC
GBNDW SOJJD IVMYV FOETP KFDOE HJLNC UIUQB WTUOC JYXBU
TSOFV FFHOX DMXVG UQUCQ CJCTH CSEFQ QUTMV CKFHT KULIP

LMG
```

THE COMPANY WILL APPRECIATE SUGGESTIONS FROM ITS PATRONS CONCERNING ITS SERVICE

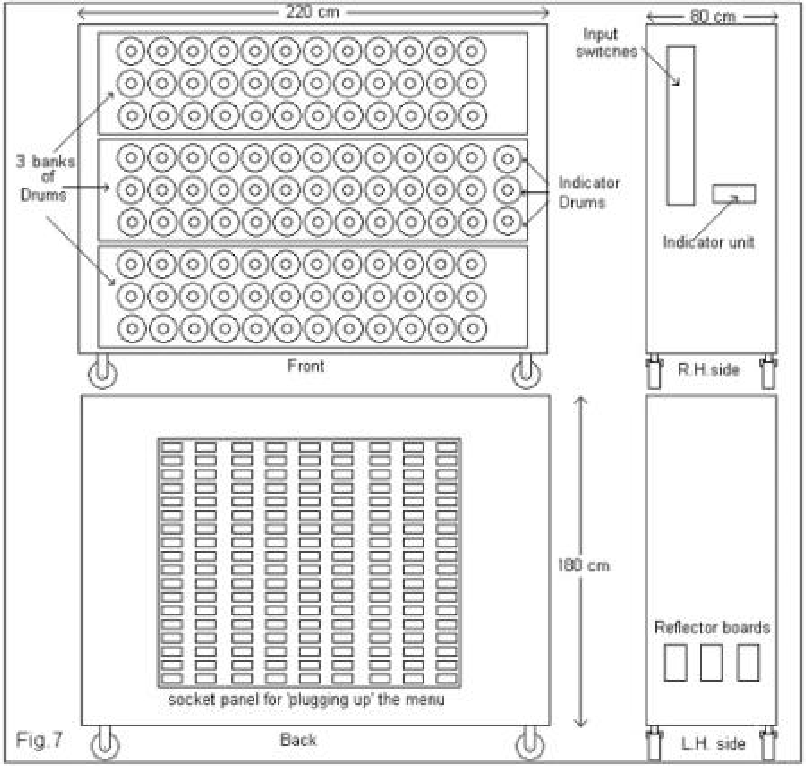
Figure 11: Gruner’s final and most important Enigma message

The Bombe Machine

- The Bombe machine was a electro-mechanical device used by British cryptologists to decipher German messages.
- The initial design of the bombe was produced in 1939 at the UK Government Code and Cypher School by Alan Turing.
- The machine had the ability to emulate several hundred enigma rotors which automated the deductions needed to rule out flawed possible attempts.

Design

- Each machine was about 7 feet wide, 6 feet 6 inches tall, 2 feet deep, and weighed about a ton.
- They had 12 miles of wiring and 97,000 different parts. Turing's prototype was built on a budget of £100,000, which is around £4m today or $4,722,220.
- The standard British bombe contained 36 Enigma equivalents, each with three drums wired to produce the same scrambling effect as the Enigma rotors.
- Once the machine was switched on, each of the three rotors moves at a rate mimicking the Enigma itself, checking on approximately 17,500 possible positions until it finds a match.



The Path to Decryption

- Each set of 3 rotors was a correlator that stepped through messages using a particular crypto setting (codeword) looking for a pattern match between the ciphertext & a suspected typical plaintext word eg "weather". If they found a match, they knew the setting they'd use could read the rest of the message.
- So the cogs went AAA, AAB, AAC...AAZ, ABA, ABB... and so on looking for a match(brute force attack).

Impact on the War

- Once the Enigma machine was cracked, 211 Bombe machines were built and ran around the clock.
- At its peak, the Bombe was able to help crack 3,000 German messages per day. By the end of the war that amounted to 2.5 million messages, many of which gave the Allies vital information about German positions and strategy.
- Some historians estimate that Bletchley Park's massive codebreaking operation, especially the breaking of U-boat Enigma, shortened the war in Europe by as many as two to four years.

Project Expansion

- For the future, I want to discuss the advancements made on enigma in the form of the British Typex machine.
- This cipher machine improved upon a number of flaws enigma had, which included encrypting a letter as itself.
- A coded implementation of this machine, Enigma, and the Bombe with cryptanalysis and comparison.