KEYING THE GERMAN NAVY'S ENIGMA

By David Kahn

The German navy prepared keys for the Enigma cipher machine that was the Wehrmacht's standard cryptographic system in a manner different from the army and the air force. They permitted the encipherers to select "random" starting positions of the rotors. The navy, on the other hand, prescribed these positions in keys when, in 1926, it adopted the Enigma. The motive for this is not known, but it proved superior to the other method, which was often compromised by the encipherers' using as settings three-letter sequences from the typewriter keyboard (QWE and RFV, for example) or from girlfriends' names or from obscene words. The consequence was that while Luftwaffe cryptograms in particular were read by the enemy early on, the Kriegsmarine Enigma defended its messages far better. Only when the British captured important keying documents could they begin to crack German naval messages.

Readying the machine for use began with an officer. Only officers could prepare the so-called "inner settings" of the machine: selecting the three rotors to be inserted into the machine, inserting them in the proper left-to-right order, and setting to its proper position the alphabet ring that rode the rotor like a tire on a wheel. The inner setting remained in use for two days, so before every other midnight — later in the war, before every other noon — the radio officer set the new inner key. After he was finished, the enlisted radiomen arranged the outer settings: turning the rotors to their proper starting positions and inserting the jacks of the two-ended cables into their proper sockets on their plugboard. These settings changed every day. Then, to encipher each message, the radioman handling it had to establish the intricate message key. Only then could he do the easy part: press the letters on the Enigma keyboard to put the plaintext into cipher.

To ready the machine, the officer and the radioman would:

a) Select the three rotors out of the eight furnished that the machine-setting list specified for that day.

b) On each, turn the alphabet ring to the position prescribed in the machine-setting list and lock it in place with the pin.

c) Assemble the rotors on their shaft so that they would be in the order prescribed by the machine-setting list and insert them into the machine.

d) Rotate the rotors until the three letters specified in the machine-setting list appeared in the lid windows.

e) Insert plugs into the plugboard to connect the pairs of letters prescribed by the machine-setting list.

With the machine thus prepared, the radioman moved to the message key. He would:

1) Determine the key net on which the message would be sent.

2) In the indicators book, find the section for that key net and pick out at random a three-letter key-net indicator.

3) Write this key-net indicator in the last three cells of the first line of the

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 2-5, 1990.

encipherment form in the book-group column (perhaps so-called because for some years the German original was encoded in the *Allgemeines Funkspruchbuch* before being enciphered in Enigma).

4) Make up a letter at random (a null) and write it in the first cell.

5) Determine from the message whether it is to be sent as a general-, officer-, or staff-grade message.

6) In the indicators book, turn to the section for that grade and pick out at random a three-letter message-grade indicator.

7) Write it in the first three cells of the second line of the encipherment form's book-group column.

8) Make up a letter at random and write it in the last cell of that line.

9) Combine the letters of the first cells in the two lines into a vertical pair.

10) Look it up in the bigram table in force and replace it with its cipher pair.

11) Write the two letters of this cipher pair horizontally into the first two cells of the first line of the radio-group column.

12) Repeat this process with the three remaining vertical pairs in the book-group column, writing them horizontally into the first two lines of the radio-group column.

13) Press, on the Enigma keyboard, the three letters of the original, unenciphered message-grade indicator and write down at the top of the message form the letters that light up on the illuminable panel. This is the message key.

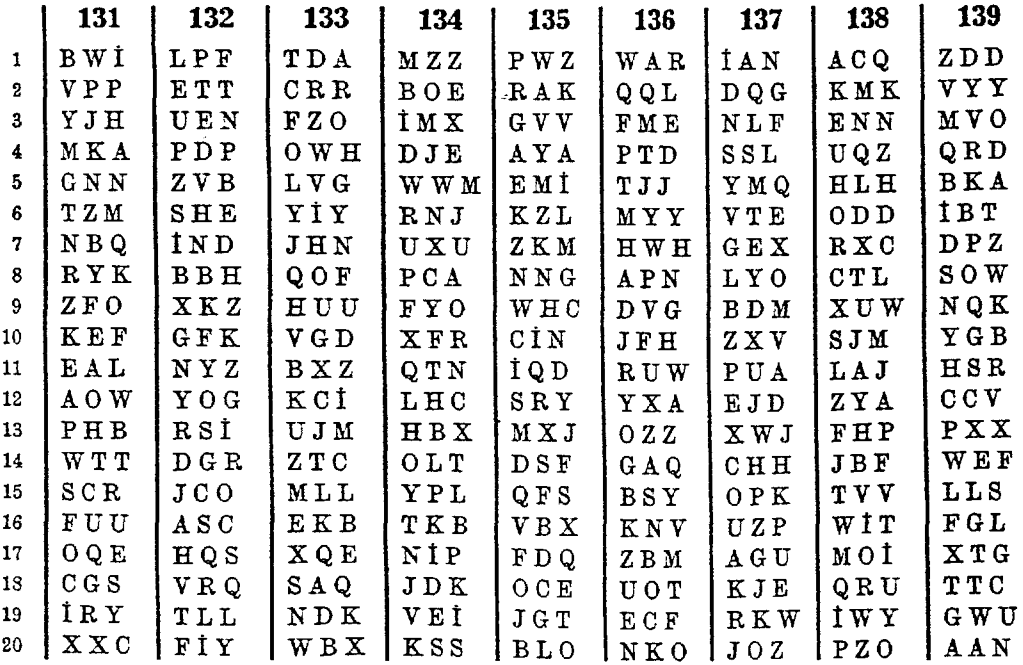
14) Turn the rotors until the letters of the message key show in the lid windows.

The cipher clerk then wrote the plaintext into the book-group columns of the cipher form without word breaks but with an *x* to separate sentences and with *q* replacing the invariant letter pair *ch*. Ready at last for the actual encipherment, he summoned a colleague. As he pressed on the typewriter keyboard the successive letters of the plaintext, his co-worker wrote down in the radio-group columns of the form the letters that lit up on the illumination panel — the letters of the cryptogram. The cipher clerk crossed out the book-group column to avoid its being transmitted by mistake.

In the U-boat arm, at least, ciphertext was not immediately sent. It was given to another radioman, who, using only the indicators that it carried, determined the message key and deciphered the cryptogram as would be done by a U-boat at sea. If he could not do so, the error was sought and corrected. Only when the cryptogram had been properly deciphered was it transmitted.

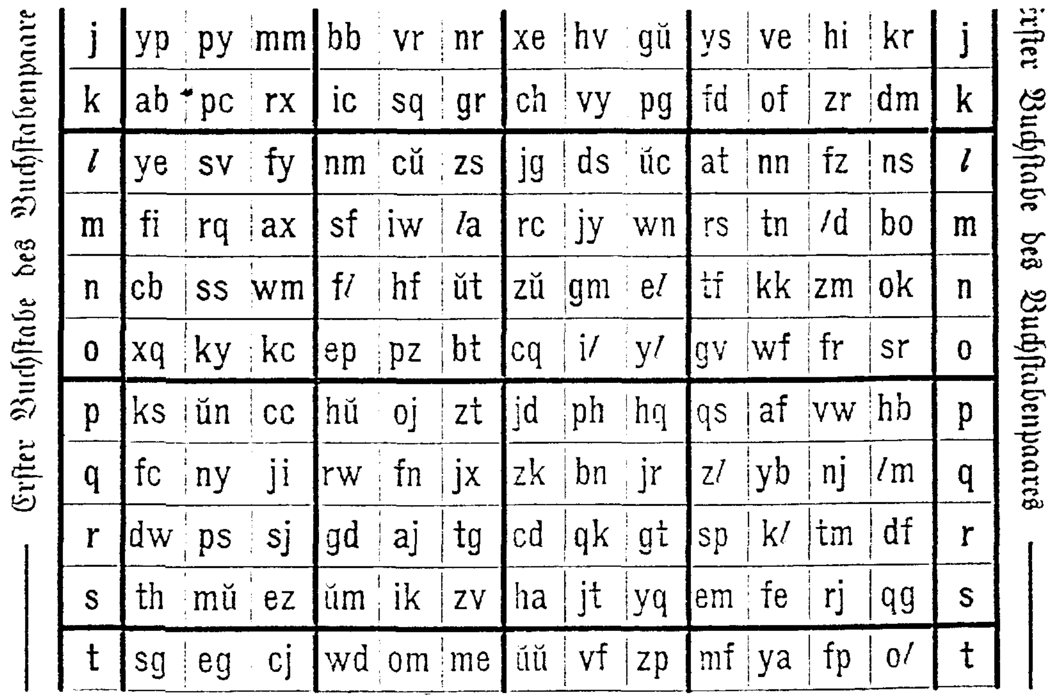
— 120 Wooleys Lane, Great Neck, New York 11023

[This is adapted from a book on the British World War II solution of the German naval Enigma, tentatively entitled The Atlantic Enigma, *to be published by Houghton Mifflin in 1991.]*



	131	132	133	134	135	136	137	138	139
1	BWİ	LPF	TDA	MZZ	PWZ	WAR	İAN	ACQ	ZDD
2	VPP	ETT	CRR	BOE	RAK	QQL	DQG	KMK	VYY
3	YJH	UEN	FZO	İMX	GVV	FME	NLF	ENN	MVO
4	MKA	PDP	OWH	DJE	AYA	PTD	SSL	UQZ	QRD
5	GNN	ZVB	LVG	WWM	EMİ	TJJ	YMQ	HLH	BKA
6	TZM	SHE	YİY	RNJ	KZL	MYY	VTE	ODD	İBT
7	NBQ	İND	JHN	UXU	ZKM	HWH	GEX	RXC	DPZ
8	RYK	BBH	QOF	PCA	NNG	APN	LYO	CTL	SOW
9	ZFO	XKZ	HUU	FYO	WHC	DVG	BDM	XUW	NQK
10	KEF	GFK	VGD	XFR	CİN	JFH	ZXV	SJM	YGB
11	EAL	NYZ	BXZ	QTN	İQD	RUW	PUA	LAJ	HSR
12	AOW	YOG	KCİ	LHC	SRY	YXA	EJD	ZYA	CCV
13	PHB	RSİ	UJM	HBX	MXJ	OZZ	XWJ	FHP	PXX
14	WTT	DGR	ZTC	OLT	DSF	GAQ	CHH	JBF	WEF
15	SCR	JCO	MLL	YPL	QFS	BSY	OPK	TVV	LLS
16	FUU	ASC	EKB	TKB	VBX	KNV	UZP	WİT	FGL
17	OQE	HQS	XQE	NİP	FDQ	ZBM	AGU	MOİ	XTG
18	CGS	VRQ	SAQ	JDK	OCE	UOT	KJE	QRU	TTC
19	İRY	TLL	NDK	VEİ	JGT	ECF	RKW	İWY	GWU
20	XXC	FİY	WBX	KSS	BLO	NKO	JOZ	PZO	AAN

Portion of indicators book

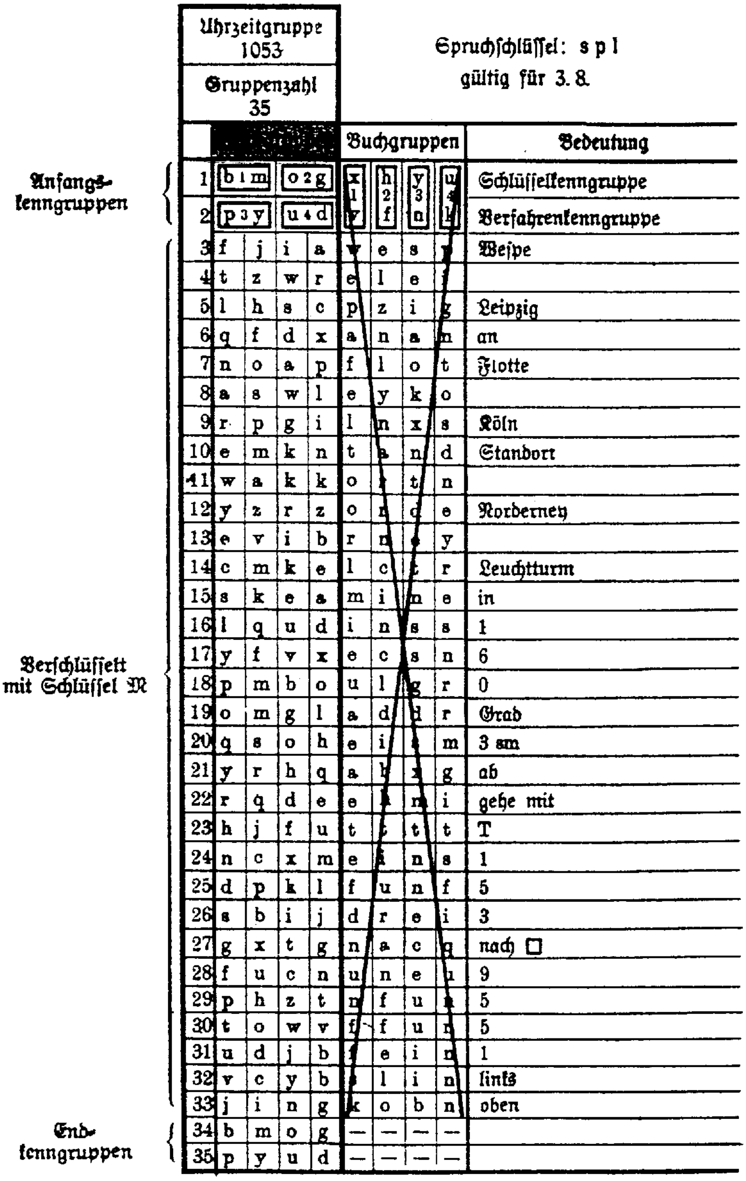


Erſter Buchſtabe des Buchſtabenpaares

j	yp	py	mm	bb	vr	nr	xe	hv	gŭ	ys	ve	hi	kr	j
k	ab	pc	rx	ic	sq	gr	ch	vy	pg	fd	of	zr	dm	k
l	ye	sv	fy	nm	cŭ	zs	jg	ds	ŭc	at	nn	fz	ns	l
m	fi	rq	ax	sf	iw	/a	rc	jy	wn	rs	tn	/d	bo	m
n	cb	ss	wm	f/	hf	ŭt	zŭ	gm	e/	tf	kk	zm	ok	n
o	xq	ky	kc	ep	pz	bt	cq	i/	y/	gv	wf	fr	sr	o
p	ks	ŭn	cc	hŭ	oj	zt	jd	ph	hq	qs	af	vw	hb	p
q	fc	ny	ji	rw	fn	jx	zk	bn	jr	z/	yb	nj	/m	q
r	dw	ps	sj	gd	aj	tg	cd	qk	gt	sp	k/	tm	df	r
s	th	mŭ	ez	ŭm	ik	zv	ha	jt	yq	em	fe	rj	qg	s
t	sg	eg	cj	wd	om	me	ŭŭ	vf	zp	mf	ya	fp	o/	t

ſter Buchſtabe des Buchſtabenpaares

Portion of a bigram table



Uhrzeitgruppe 1053	Spruchſchlüſſel: s p l gültig für 3. 8.
Gruppenzahl 35	

						Buchgruppen				Bedeutung
Anfangskenngruppen	1	b 1 m		o 2 g		x 1	h 2	y 3	u 4	Schlüſſelkenngruppe
	2	p 3 y		u 4 d		y	f	n	k	Verfahrenkenngruppe
Verſchlüſſelt mit Schlüſſel M	3	f	j	i	a	w	e	s	p	Weſpe
	4	t	z	w	r	e	l	e	i	
	5	l	h	s	c	p	z	i	g	Leipzig
	6	q	f	d	x	a	n	a	n	an
	7	n	o	a	p	f	l	o	t	Flotte
	8	a	s	w	l	e	y	k	o	
	9	r	p	g	i	l	n	x	s	Köln
	10	e	m	k	n	t	a	n	d	Standort
	11	w	a	k	k	o	r	t	n	
	12	y	z	r	z	o	n	d	e	Norderney
	13	e	v	i	b	r	n	e	y	
	14	c	m	k	e	l	c	t	r	Leuchtturm
	15	s	k	e	a	m	i	n	e	in
	16	l	q	u	d	i	n	s	s	1
	17	y	f	v	x	e	c	s	n	6
	18	p	m	b	o	u	l	g	r	0
	19	o	m	g	l	a	d	d	r	Grad
	20	q	s	o	h	e	i	a	m	3 sm
	21	y	r	h	q	a	b	x	g	ab
	22	r	q	d	e	e	k	n	i	gehe mit
	23	h	j	f	u	t	t	t	t	T
	24	n	c	x	m	e	a	n	s	1
	25	d	p	k	l	f	u	n	f	5
	26	s	b	i	j	d	r	e	i	3
	27	g	x	t	g	n	a	c	q	nach □
	28	f	u	c	n	u	n	e	u	9
	29	p	h	z	t	n	f	u	a	5
	30	t	o	w	v	f	f	u	n	5
	31	u	d	j	b	f	e	i	n	1
	32	v	c	y	b	a	l	i	n	links
	33	j	i	n	g	k	o	b	n	oben
Endkenngruppen	34	b	m	o	g	—	—	—	—	
	35	p	y	u	d	—	—	—	—	

A naval Enigma encipherment (from a manual)

Translations: *Uhrzeitgruppe* = time group. *Gruppenzahl* = number of groups. *Spruchschlüssel* = message key. *gültig fur 3.8.* = valid for 3rd August. (Invisible under oblong tint:) *Funkgruppen* = radio groups. *Buchgruppen* = book groups. *Bedeutung* = meaning. *Anfangskenngruppen* = beginning indicator groups. *Schlüsselkenngruppe* = key-net indicator. *Verfahrenkenngruppe* = message-grade indicator. *Verschlüsselt mit Schlüssel M* = enciphered by Enigma. *Endkenngruppen* = final indicator groups.