Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

Enigma Message Procedures Used by the Heer, Luftwaffe and Kriegsmarine

Dirk Rijmenants

Available online: 17 Sep 2010

To cite this article: Dirk Rijmenants (2010): Enigma Message Procedures Used by the Heer, Luftwaffe and Kriegsmarine, Cryptologia, 34:4, 329-339

To link to this article: http://dx.doi.org/10.1080/01611194.2010.486257

Cryptologia, 34:329–339, 2010

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2010.486257

Taylor & Francis
Taylor & Francis Group

Enigma Message Procedures Used by the Heer, Luftwaffe and Kriegsmarine

DIRK RIJMENANTS

Abstract This paper is an effort to merge existing information about the message procedures, the enciphering methods and the required documents used with the German Enigma cipher machine by the German Heer (Army), Luftwaffe (Air Force) and Kriegsmarine (Wartime Navy) during the Second World War.

Keywords Doppelbuchstabentauschtafel, Enigma, Heer, Kenngruppenbuch, Kriegsmarine, Luftwaffe, Machinenschlüssel, Wehrmacht

Introduction

The Enigma cipher machine was used extensively in all parts of the German forces during the Second World War. Many different key sheets, code books and procedures were applied in order to secure the communications with the Enigma. This paper does not intend to describe all existing ways this was done, but explains the procedures, methods and documents that were commonly used.

Different parts of the German Armed Forces often used slightly different procedures or documents to apply these procedures. This could be due to differences in army unit structures, other security regulations or other technical means. An example was the complex Kriegsmarine procedures with special key management and enciphering procedures, applied as a security measure. Another example, due to different technical means, was the Luftwaffe (Air Force) introducing the Enigma Uhr and the rewireable D reflector, which had an effect on the key setting procedures and required other key sheets.

In general, we can divide the message procedures into two main procedures: the Heer/Luftwaffe and Kriegsmarine procedures. The main difference between these procedures is the way they select the Spruchschlüssel or message key, the initial start position of the Enigma rotors. The Heer/Luftwaffe used random message keys and the Kriegsmarine relied on a complex system of encrypted message keys and various key sheets and code books. This paper describes these two most commonly used procedures.

Without a doubt, the Enigma machine provided strong encryption for those days. However, communications security requires more than a good cipher machine, message procedures and key management. The Polish Cipher Bureau was the first to develop a successful attack on the military Enigma. Unfortunately, in 1939 the Bureau was no longer able to break the codes due to increased sophistication in the design of the Enigma, new procedures and lack of funds for the code breakers. When Germany invaded Poland, the Polish knowledge and several replica Enigma machines were handed over to French and British intelligence.

Address correspondence to Dirk Rijmenants, Middenstratt 77, Beringen B-3982, Belgium. E-mail: dirk.rijmenants@telenet.be

The Polish achievements inspired the Allies, who initially considered the military Enigma too strong to tackle. The Allied codebreakers used a combination of Signal Intelligence, tactical information, military operations, innovative technology and mathematics to create a wedge in this relatively secure machine. Unsafe procedures, poor application of these procedures and tactical mistakes turned the Enigma machine into the Achilles heel of the German war machine. Germany kept on using Enigma in all parts of their forces, which resulted in catastrophic consequences for Nazi Germany.

The Heer/Luftwaffe Procedures

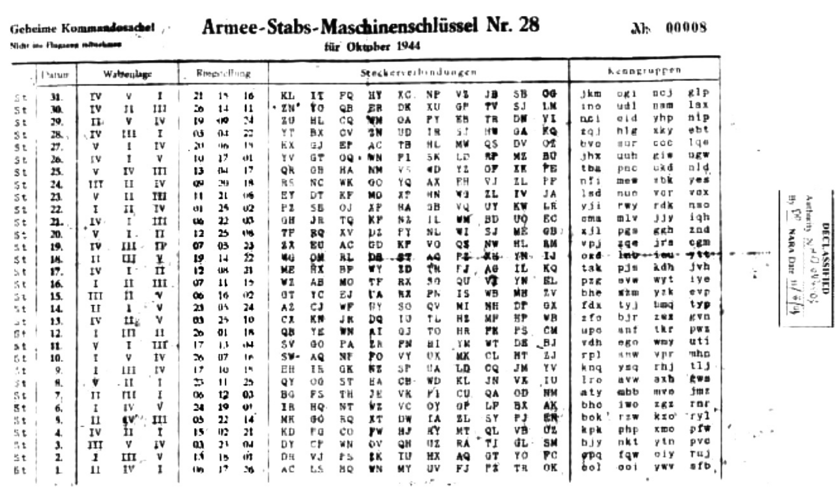
To obtain secure communications, the Heer (German Army) used several procedures to transmit and receive messages. For a message to be correctly encrypted and decrypted, both the sender and receiver needed to set up their Enigma in exactly the same way. These settings were distributed on key sheets. For reasons of security, different parts of the armed forces had their own network, with different key sheets and with a network having its own codename [4, 11].

Each key sheet contained the following information [2, ch. IV–V]:

- **Walzenlage:** Choice and order of wheels
- **Ringstellung:** The ring setting, the position of the rotor wiring, relative to the alphabet rings
- **Steckerverbindungen:** The plug connections on the plugboard
- **Kenngruppen:** Groups to identify the key to the receiver.

The key sheets were distributed beforehand and contained the basic settings for a whole month, one per day. In general, the key sheets were in the custody of an officer responsible for setting up the machine rotors and ring settings.

The order of the days is reversed (Figure 1) for practical reasons. The officer, responsible for handing out the key for that day, could snip off the current day at the bottom of the sheet and give it to the radio operator to set the machine. After being used, the strip of paper with the key for that day was destroyed.


Geheime Kommandosache! Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28 für Oktober 1944

Nr. 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SB	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DW	YI	nci	eid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	19	EX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	coc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	PI	SK	LD	RP	MZ	BU	jhx	uuh	gie	ugw
St	25.	V	IV	III	13	04	17	QR	OB	HA	NM	VS	WD	YZ	OF	IK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	FH	VJ	ZL	PF	nfi	mew	zbk	yes
St	23.	V	II	III	11	21	06	EY	DT	KF	MO	XP	HN	WJ	ZL	IV	JA	lsd	nuo	vor	vox
St	22.	I	II	IV	01	25	02	PZ	SB	OJ	XP	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nao
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KP	NZ	IL	WM	BD	UQ	EC	oma	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TP	BQ	XV	DZ	FY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	II	07	03	23	ZX	EU	AC	GD	KP	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	MG	OM	RL	DB	ST	AQ	PZ	XH	YN	IJ	oxd	lmb	ieu	ytt
St	17.	IV	I	II	12	08	31	ME	RX	BF	WY	ZD	TN	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SQ	QU	VZ	YN	EL	pzg	ovw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	UA	RX	PN	IS	WB	MH	ZV	bhe	xkm	yzk	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	BY	SO	QV	MI	NH	DP	GX	fdx	tyj	umq	typ
St	13.	IV	III	V	03	25	10	CX	KN	JK	DQ	IU	TL	HZ	MP	HP	WB	zfo	bjr	zex	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	OJ	TO	HR	FK	PS	CM	upo	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ER	FN	BI	YK	WT	DE	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NF	PO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	15	EH	IE	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lro	avw	axh	gwa
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	FI	CU	QA	OD	NM	aty	mbb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	OP	LP	BX	AK	bho	iwo	zgz	rnr
St	5.	II	IV	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	FG	CO	PW	HJ	KY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	21	04	DY	CP	WN	OV	QH	UZ	RA	TI	GL	SM	bjy	nkt	ytn	pvc
St	2.	I	III	V	13	15	01	DH	VJ	FS	EK	TU	HX	AQ	GT	YO	FC	gpq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	bol	ooi	ywv	sfb

DECLASSIFIED

Figure 1. An Army Staff machine key.

The Kenngruppen

To identify the key that was used for a particular message, the operator had to insert a five letter group called *Buchstabenkenngruppe* (letter identification group) as the first group of the message [2, ch. V]. The *Buchstabenkenngruppe* is composed of two randomly selected letters and one of the four possible three-letter *Kenngruppen* on the key sheet for that day. If we take day 31 from the Army Staff key 28 (Figure 1), we see the *Kenngruppen* JKM, OGI, NCJ and GLP. In this case, some examples of a correct *Buchstabenkenngruppen* are FDJKM, KVOGI or QNNCJ. The letters of this five-letter group could be permuted in any order. This five letter group at the start of the message should not be encrypted with the rest of the message! If a message was divided into several parts, the operator had to insert another *Buchstabenkenngruppe* for each part of the message. When counting the letters for the message header, the five letters of the *Buchstabenkenngruppe* must be included. The receiving operator immediately recognized which key was to be applied by looking at the last three letters of the first group.

The army dropped the use of Kenngrruppen on 1 Sept 1943, and the Luftwaffe followed on 1 Nov 1943 [5, p. 84] [10, pp. 72–73] [7, p. 106]. The same happened with other services like the SS, but some surviving key sheets from 1945 do carry the Kenngruppen as before.

The Message Key

The setting of the machine was typically valid for one day in the Army and Air Force (the inner settings of Navy machines were valid for two days, as described later on). Using the same settings for a large number of messages would increase the statistical amount of data available to break a particular key. Therefore, each message was sent with a different start position for the Enigma rotors, randomly selected by the operator. This was called the *Spruchschlüssel* or message key.

Until 1938, the German military used the daily key and base setting (Grundstellung) [6, pp. 48–49] [10, pp. 447, 518], according to the key sheet. The operator selected a random message key. This message key was encoded twice, to exclude errors. As example, the trigram **GHK** is encoded twice, resulting in **XMC FZQ**. Next, the operator moved the rotors to the message key **GHK** and encoded the message. The two trigrams, being the encoded message key, were transmitted, together with the message. The receiver sets his machine on the base setting, as described in the key sheet, and decodes the trigrams **XMC FZQ** back into the **GHK** message key. Next, he sets the message key **GHK** as the start position on his machine, to continue decoding the rest of the message. However, this procedure was actually a security flaw. The message key is encoded twice, resulting in a relation between first and fourth, second and fifth, and third and sixth characters. This security problem enabled the Polish Cipher Bureau to break the pre-war Enigma messages.

However, German cryptologists were aware of the security flaw, and from May 1940 on, the Heer/Luftwaffe changed the message key procedures to increase security. Heer/Luftwaffe radio operators now selected for each message a new randomly chosen base setting or *Grundstellung*, let's say **WZA**, and a random message key or *Spruchschlüssel*, let's say **SXT**. He moved the rotors to the random base setting **WZA**, and encoded the random message key **SXT**. Let us presume that the result was **UHL**. He sets up the message key **SXT** as the start position and encodes the

```
1230 = 3tle = 1tl = 250 = WZA UHL =
 FDJKM LDAHH YEOEF PTWYB LENDP
 MKOXL DFAMU DWIJD XRJZY DFRIO
 MFTEV KTGUY DDZED TPOQX FDRIU
 CCBFM MQWYE FIPUL WSXHG YHJZE
 AOFDU FUTEC VVBDP OLZLG DEJTI
 HGYER DCXCV BHSEE TTKJK XAAQU
 GTTUO FCXZH IDREF TGHSZ DERFG
```

Figure 2. Example of a typical Heer/Luftwaffe message.

message. Next, he transmits the random base setting **WZA**, the encoded message key **UHL** and the message. The receiver sets up the machine's base setting according the first trigram **WZA**, and decodes the second trigram **UHL** to obtain the message key **SXT**. Next, he uses the message key **SXT** as the start position to decode the actual message. If a message was divided into several parts, the operator had to use a new base setting and message key for each part of the message [2, ch. IX, A].

For example, the message in Figure 2 was created at 12h30, consists of three parts (3 *Teile*), of which this is the first, and contains 250 characters (*Buchstabenkenngruppe* included). WZA is the base setting (*Grundstellung*) to decipher the encrypted message key (*Spruchschlüssel*) UHL. The *Buchstabenkenngruppe* FDJKM shows that the key that was used is the one with *Kenngruppe* JKM.

The Kriegsmarine Procedures

The Kriegsmarine procedures on sending messages with the Enigma cipher machine were far more complex and elaborate then the Heer and Luftwaffe procedures. The Kriegsmarine Enigma key sheets consisted of two parts. The first sheet, called *Schlüsseltafel M Allgemein – Innere Einstellung* (Figure 3), contained the three rotors and their ring settings, the thin beta or gamma rotor and the reflector, and this only for the odd days of a month [1, part I, B, par. 15]. The second sheet, called *Schlüsseltafel M Allgemein – Aussere Einstellung* (Figure 4), contained the plugs and Grundstellung or basic position for each day of the month [1, part I, B, par. 14]. There was an additional key for the officers and a special Schlüssel M NIXE was used for private communication between the Captain and the U-boat Command, without other boats being able to read the message [9]. Also, different operational locations had their own keys. The three main areas or cipher nets were Home Waters (Heimische Gewässer), Outer Waters (Ausserheimische Gewässer) and South (Süd). From 1942 onward, each of these areas was even further divided into smaller cipher areas, each of them with their own keys and operational instructions. Some standard messages were encoded with the Kurzsignalheft code book, prior to encryption with the Enigma, to reduce transmission time.

Kriegsmarine Kenngruppen

The Kriegsmarine system of *Kenngruppen* was completely different from the Heer/Luftwaffe *Kenngruppen*. In addition to the key sheets, the Kriegsmarine used a *Kenngruppenbuch* on their main cipher nets to determine the message key, which was the start position of the rotors at the beginning of a message. Note that the

INNER SETTINGS FOR TRITON KEYS, JUNE 1945

P SECRET-ULTRA

FIGURE 12 a

Schlüssel M "T r i t o n"

Monat: J u n i 1945 Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein
(Schl.T. M Allg.)

Innere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monats-tag	Innere Einstellung				
29.	B	Beta A	VII G	IV N	V O
27.	B	Beta A	II T	I Y	VIII F
25.	B	Beta A	V M	VI Q	I T
23.	B	Beta A	VI B	II H	III D
21.	B	Beta A	I W	VIII L	II E
19.	B	Beta A	VIII K	I U	IV G
17.	B	Beta A	IV U	VI Q	I H
15.	B	Beta A	VII D	I J	II N
13.	B	Beta A	I O	IV U	VII L
11.	B	Beta A	VI I	I L	II I
9.	B	Beta A	III X	IV C	VII R
7.	B	Beta A	V Z	I U	VIII A
5.	B	Beta A	II E	VI Z	I L
3.	B	Beta A	VIII Y	V F	II C
1.	B	Beta A	IV R	VII A	III X

Achtung! Umkehrwalze und Zusatzwalze beachten!

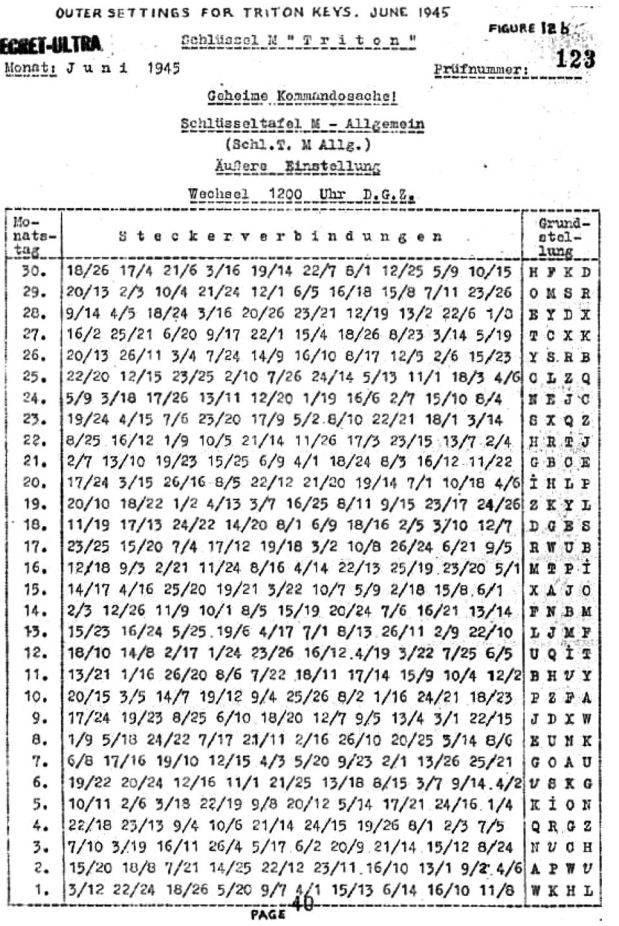
PAGE 39

Figure 3. Kriegsmarine TRITON key sheet – inner settings.

Kenngruppenbuch is not to be confused with the Kenngruppenheft for Kurzsignalen messages, which has a completely different procedure.

The *Kenngruppenbuch* comprised an allotment list called Zuteilungsliste (Figure 5), a column and substitution table selection by date called Tauschtafelplan (Figure 6) and a large number of Kenngruppen tables called Spalte (Figure 7). The Zuteilungsliste told the operator which table or Spalte he should use for his particular cipher net. This list consisted of two parts. The first part showed the Spalte number given the name of the cipher nets and the second part showed the names of the different cipher nets given the Spalte number. The Tauschtafelplan told the operator which column of that Spalte was used to select his trigram [1, part I, C, par. 24].

The operator had to select two kenngruppen or trigrams. The first trigram was called *Schlüsselkenngruppe* or key indicator. The second trigram, called



OUTER SETTINGS FOR TRITON KEYS. JUNE 1945

FIGURE 12b

TOP SECRET-ULTRA Schlüssel M "T r i t o n" 123

Monat: J u n i 1945 Prüfnummer:

Geheime Kommandosache!

Schlüsseltafel M - Allgemein

(Schl.T. M Allg.)

Äußere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monatstag	Steckerverbindungen	Grundstellung
30.	18/26 17/4 21/6 3/16 19/14 22/7 8/1 12/25 5/9 10/15	H F K D
29.	20/13 2/3 10/4 21/24 12/1 6/5 16/18 15/8 7/11 23/26	O M S R
28.	9/14 4/5 18/24 3/16 20/26 23/21 12/19 13/2 22/6 1/8	E Y D X
27.	16/2 25/21 6/20 9/17 22/1 15/4 18/26 8/23 3/14 5/19	T C X K
26.	20/13 26/11 3/4 7/24 14/9 16/10 8/17 12/5 2/6 15/23	Y S R B
25.	22/20 12/15 23/25 2/10 7/26 24/14 5/13 11/1 18/3 4/6	C L Z Q
24.	5/9 3/18 17/26 13/11 12/20 1/19 16/6 2/7 15/10 8/4	N E J C
23.	19/24 4/15 7/6 25/20 17/9 5/2 8/10 22/21 18/1 3/14	S X Q Z
22.	8/25 16/12 1/9 10/5 21/14 11/26 17/3 23/15 13/7 2/4	H R T J
21.	2/7 13/10 19/23 15/25 6/9 4/1 18/24 8/3 16/12 11/22	G B O E
20.	17/24 3/15 26/16 8/5 22/12 21/20 19/14 7/1 10/18 4/6	I H L P
19.	20/10 18/22 1/2 4/13 3/7 16/25 8/11 9/15 23/17 24/26	Z K Y L
18.	11/19 17/13 24/22 14/20 8/1 6/9 18/16 2/5 3/10 12/7	D O E S
17.	23/25 15/20 7/4 17/12 19/18 3/2 10/8 26/24 6/21 9/5	R W U B
16.	12/18 9/3 2/21 11/24 8/16 4/14 22/13 25/19 23/20 5/1	M T P I
15.	14/17 4/16 25/20 19/21 3/22 10/7 5/9 2/18 15/8 6/1	X A J O
14.	2/3 12/26 11/9 10/1 8/5 15/19 20/24 7/6 16/21 13/14	F N B M
13.	15/23 16/24 5/25 19/6 4/17 7/1 8/13 26/11 2/9 22/10	L J M F
12.	18/10 14/8 2/17 1/24 23/26 16/12 4/19 3/22 7/25 6/5	U Q I T
11.	13/21 1/16 26/20 8/6 7/22 18/11 17/14 15/9 10/4 12/2	B H V Y
10.	20/15 3/5 14/7 19/12 9/4 25/26 8/2 1/16 24/21 18/23	P Z P A
9.	17/24 19/23 8/25 6/10 18/20 12/7 9/5 13/4 3/1 22/15	J D X W
8.	1/9 5/18 24/22 7/17 21/11 2/16 26/10 20/25 3/14 8/6	E U N K
7.	6/8 17/16 19/10 12/15 4/3 5/20 9/23 2/1 13/26 25/21	G O A U
6.	19/22 20/24 12/16 11/1 21/25 13/18 8/15 3/7 9/14 4/2	V S K G
5.	10/11 2/6 3/18 22/19 9/8 20/12 5/14 17/21 24/16 1/4	K I O N
4.	22/18 23/13 9/4 10/6 21/14 24/15 19/26 8/1 2/3 7/5	Q R C Z
3.	7/10 3/19 16/11 26/4 5/17 6/2 20/9 21/14 15/12 8/24	N V C H
2.	15/20 18/8 7/21 14/25 22/12 23/11 16/10 13/1 9/2 4/6	A P W V
1.	3/12 22/24 18/26 5/20 9/7 4/1 15/13 6/14 16/10 11/8	W K H L

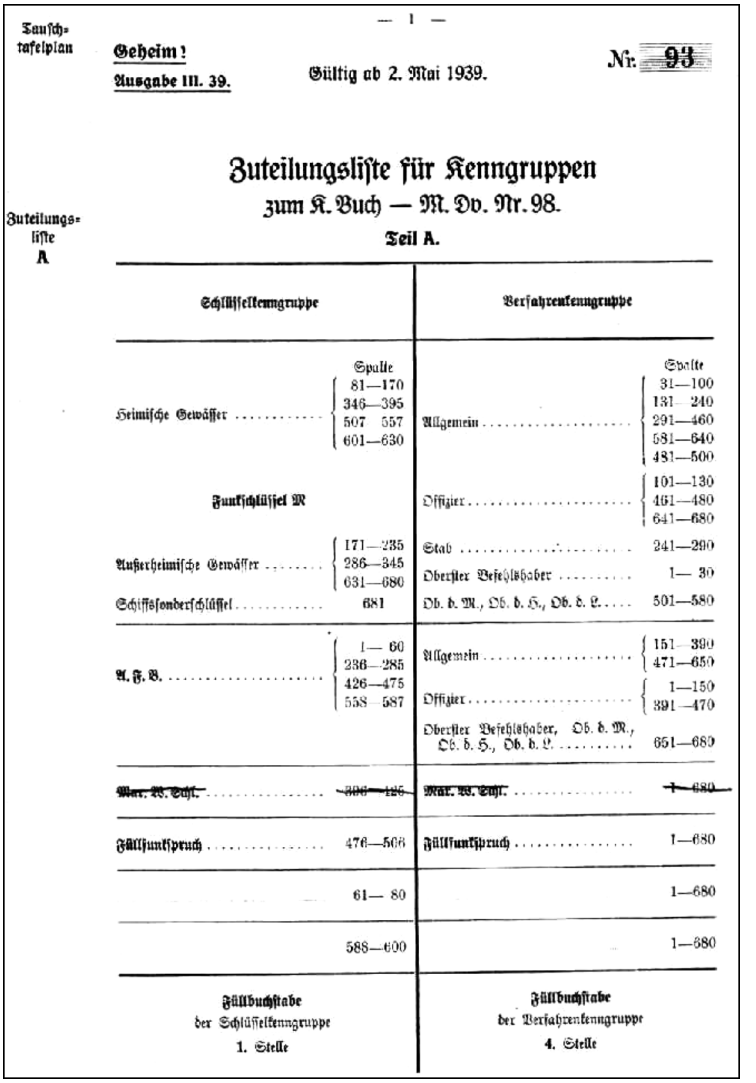
PAGE 40

Figure 4. Kriegsmarine TRITON key sheet – external settings.

Verfahrenkenngruppe or encryption indicator, was used to obtain the message key. The *Schlüsselkenngruppe* and *Verfahrenkenngruppe* had their own tables as determined in the Zuteilungsliste. With the Enigma machine in the *Grundstellung* – the base position of that day – the operator would key in the *Verfahrenkenngruppe* and the result would be the message key that was used as start position to encipher the message. The two trigrams together were called the message indicator and underwent an additional bigram substitution encryption with the bigram key booklet before they were sent along with the encrypted message [3].

The Bigram Table

The Kriegsmarine message indicator (the *Schlüsselkenngruppe* and *Verfahrenkenngruppe* together) were encoded with a bigram table called Doppelbuchstabentauschtafel or double-letter conversion table. A set of bigram tables consisted of nine different tables, labelled A to J. A calendar determined which of the substitution tables was used on a particular day. The bigram table was reciprocal, meaning that if a bigram AB was encoded in KW, the bigram KW would also decode to AB.



Tausch-
tafelplan

— 1 —

Geheim!

Ausgabe III. 39. Gültig ab 2. Mai 1939. Nr. 93

Zuteilungsliste für Kenngruppen
zum K. Buch — M. Dv. Nr. 98.
Teil A.

Zuteilungs-
liste
A

Schlüsselkenngruppe	Spalte	Verfahrenkenngruppe	Spalte
Heimische Gewässer	81—170, 346—395, 507—557, 601—630	Allgemein	31—100, 131—240, 291—460, 581—640, 481—500
Funkschlüssel M		Offizier	101—130, 461—480, 641—680
Außerheimische Gewässer	171—235, 286—345, 631—680	Stab	241—290
		Oberster Befehlshaber	1— 30
Schiffssonderschlüssel	681	Ob. d. M., Ob. d. H., Ob. d. L.	501—580
A. F. B.	1— 60, 236—285, 426—475, 558—587	Allgemein	151—390, 471—650
		Offizier	1—150, 391—470
		Oberster Befehlshaber, Ob. d. M., Ob. d. H., Ob. d. L.	651—680
~~Mar. W. Schl.~~	~~306—425~~	~~Mar. W. Schl.~~	~~1—680~~
Füllfunkspruch	476—506	Füllfunkspruch	1—680
	61— 80		1—680
	588—600		1—680
Füllbuchstabe der Schlüsselkenngruppe **1. Stelle**		**Füllbuchstabe** der Verfahrenkenngruppe **4. Stelle**	

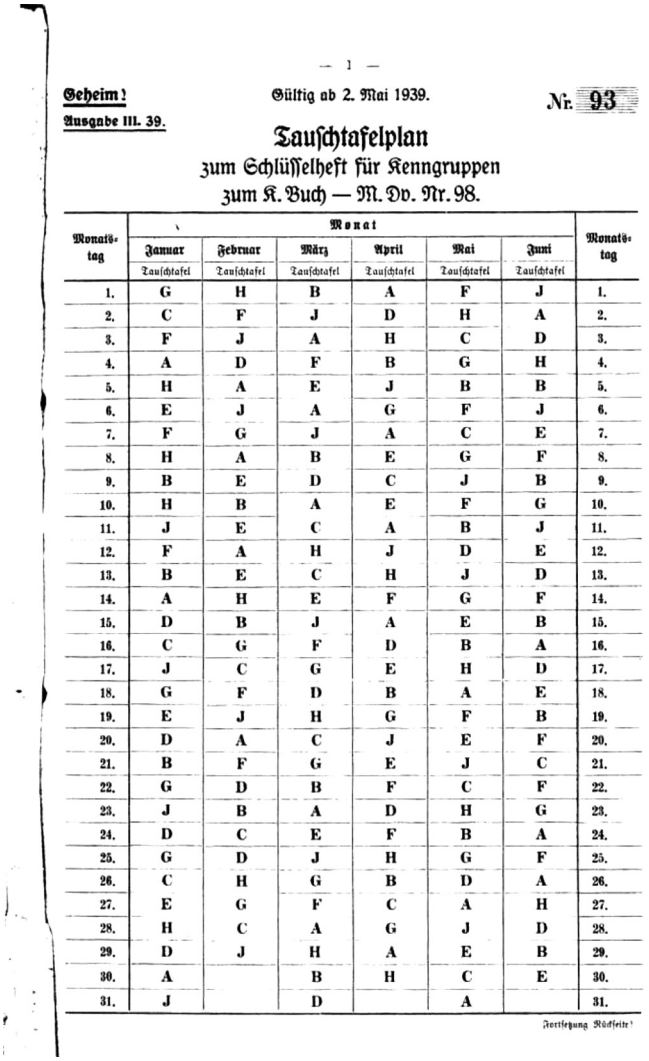
Figure 5. Kenngruppenbuch, table selection by Cipher Net.

The operator wrote the two trigrams from the message indicator underneath each other but added one random dummy letter at the beginning of the first trigram and one dummy letter at the end of the second trigram. To encode, bigrams were taken vertically from the message indicator and encoded according to the bigram table [1, part I, C, par. 26].

As an example, we will encode the message indicator HLG KQK with Bigram Table "Fluss."

The random dummy letters, in our example A and Z, are added to the trigram *Schlüsselkenngruppe* HLG and *Verfahrenkenngruppe* KQK.

AHLG
KQKZ



— 1 —

Geheim! Gültig ab 2. Mai 1939. Nr. 93

Ausgabe III. 39.

Tauschtafelplan

zum Schlüsselheft für Kenngruppen
zum K. Buch — M. Dv. Nr. 98.

Monats-tag	Monat						Monats-tag
	Januar	Februar	März	April	Mai	Juni	
	Tauschtafel	Tauschtafel	Tauschtafel	Tauschtafel	Tauschtafel	Tauschtafel	
1.	G	H	B	A	F	J	1.
2.	C	F	J	D	H	A	2.
3.	F	J	A	H	C	D	3.
4.	A	D	F	B	G	H	4.
5.	H	A	E	J	B	B	5.
6.	E	J	A	G	F	J	6.
7.	F	G	J	A	C	E	7.
8.	H	A	B	E	G	F	8.
9.	B	E	D	C	J	B	9.
10.	H	B	A	E	F	G	10.
11.	J	E	C	A	B	J	11.
12.	F	A	H	J	D	E	12.
13.	B	E	C	H	J	D	13.
14.	A	H	E	F	G	F	14.
15.	D	B	J	A	E	B	15.
16.	C	G	F	D	B	A	16.
17.	J	C	G	E	H	D	17.
18.	G	F	D	B	A	E	18.
19.	E	J	H	G	F	B	19.
20.	D	A	C	J	E	F	20.
21.	B	F	G	E	J	C	21.
22.	G	D	B	F	C	F	22.
23.	J	B	A	D	H	G	23.
24.	D	C	E	F	B	A	24.
25.	G	D	J	H	G	F	25.
26.	C	H	G	B	D	A	26.
27.	E	G	F	C	A	H	27.
28.	H	C	A	G	J	D	28.
29.	D	J	H	A	E	B	29.
30.	A		B	H	C	E	30.
31.	J		D		A		31.

Fortsetzung Rückseite!

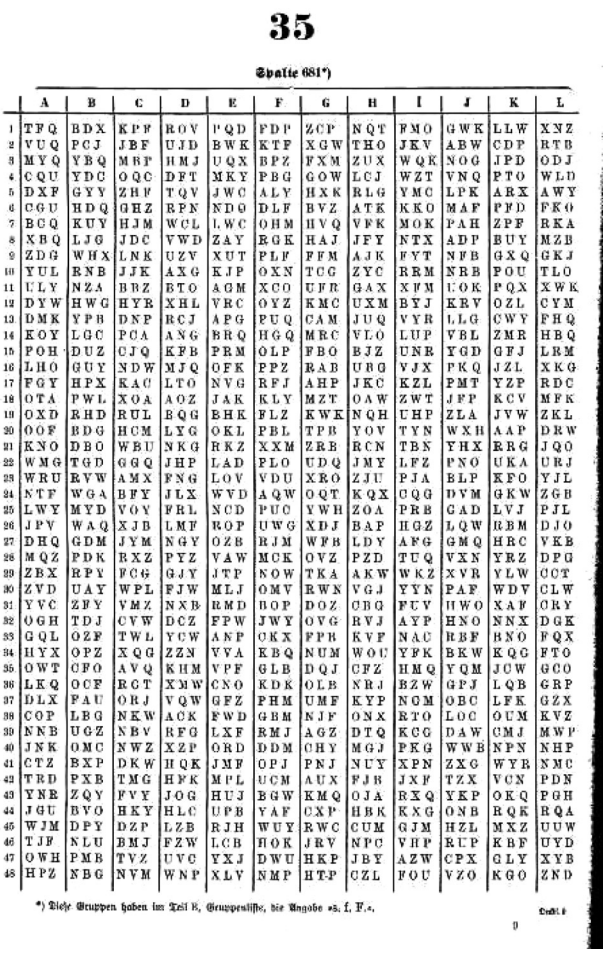
Figure 6. Kenngruppenbuch, column and substitution table selection by date.

Bigram coding with table B from below (Figure 8): AK = BD, HQ = BJ, LK = EM, GZ = EJ.

The resulting message indicator: BDBJ EMEJ.

The receiving operator decoded the eight letters of the message indicator with the help of his bigram table. The resulting first trigram would show him the used key. Next, he would key in the second trigram in his Enigma, with the rotors in the *Grundstellung*. The resulting trigram was the recovered message key. He would set this message key as rotor positions and finally decipher the rest of the message. The above example was used on the 3-rotor M3 Enigma. The procedure for the four-rotor M4 Enigma was identical, but used all four letters, instead of three, and one random letter.

The names of U-boats and addressees were encoded with the Marinefunknamenliste codebook. In our example (Figure 9), CLX stands for BDU (Befehlshaber der



35

Spalte 681*)

	A	B	C	D	E	F	G	H	I	J	K	L
1	TFQ	BDX	KPF	ROV	PQD	FDP	ZCP	NQT	FMO	GWK	LLW	XNZ
2	VUQ	PCJ	JBF	UJD	BWK	KTF	XGW	THO	JKV	ABW	CDP	RTB
3	MYQ	YBQ	MRP	HMJ	UQX	BPZ	FXM	ZUX	WQK	NOG	IPD	ODJ
4	CQU	YDC	OQC	DFT	MKY	PBG	GOW	LCJ	WZT	VNQ	PTO	WLD
5	DXF	GYY	ZHF	TQV	JWC	ALY	HXK	RLG	YMC	LPK	ARX	AWY
6	CGU	HDQ	GHZ	RFN	NDO	DLF	BVZ	ATK	KKO	MAF	PFD	FKO
7	BCQ	KUY	HJM	WCL	LWC	OHM	IVQ	VFK	MOK	PAH	ZPF	RKA
8	XBQ	LJG	JDC	VWD	ZAY	RGK	HAJ	JFY	NTX	ADP	BUY	MZB
9	ZDG	WHX	LNK	UZV	XUT	PLF	FFM	AJK	FYT	NFB	GXQ	GKJ
10	YUL	BNB	JJK	AXG	KJP	OXN	TCG	ZYC	RRM	NRB	POU	TLO
11	ULY	NZA	BBZ	ETO	AGM	XCO	UFR	GAX	XFM	UOK	PQX	XWK
12	DYW	HWG	HYR	XHL	VRC	OYZ	KMC	UXM	BYJ	KRV	OZL	CYM
13	DMK	YPH	DNP	RCJ	APG	PUQ	CAM	JUQ	VYR	LLG	CWY	FHQ
14	KOY	LGC	PCA	ANG	BRQ	HGQ	MRC	VLO	LUP	VBL	ZMR	HBQ
15	POH	DUZ	CJQ	KFB	PRM	OLP	FBO	BJZ	UNR	YGD	GFJ	LRM
16	LHO	GUY	NDW	MJQ	OFK	PPZ	RAB	UBG	VJX	FKQ	JZL	XKG
17	FGY	HPX	KAC	LTO	NVG	RFJ	AHP	JKC	KZL	PMT	YZP	RDC
18	OTA	PWL	XOA	AOZ	JAK	KLY	MZT	OAW	ZWT	JFP	KCV	MFK
19	OXD	RHD	RUL	BQG	BHK	FLZ	KWK	NQH	UHP	ZLA	JVW	ZKL
20	OOF	BDG	HCM	LYG	OKL	PBL	TPB	YOV	TYN	WXH	AAP	DRW
21	KNO	DBO	WBU	NKG	RKZ	XXM	ZRB	RCN	TBN	YHX	RRG	JQO
22	WMG	TGD	GGQ	JHP	LAD	PLO	UDQ	JMY	LFZ	PNO	UKA	URJ
23	WRU	RVW	AMX	FNG	LOV	VDU	XRO	ZJU	PJA	BLP	KFO	YJL
24	NTF	WGA	BFY	JLX	WVD	AQW	OQT	KQX	CQG	DVM	GKW	ZGB
25	LWY	MYD	VOY	FRL	NCD	PUC	YWH	ZOA	PRB	GAD	LVJ	PJL
26	JPV	WAQ	XJB	LMF	ROP	UWG	XDJ	BAP	HGZ	LQW	RBM	DJO
27	DHQ	GDM	JYM	NGY	OZB	RJM	WFB	LDY	AFG	GMQ	HRC	VKB
28	MQZ	PDK	RXZ	PYZ	VAW	MCK	OVZ	PZD	TUQ	VXN	YRZ	DPG
29	ZBX	RPY	FCG	GJY	JTP	NOW	TKA	AKW	WKZ	XVR	YLW	CCT
30	ZVD	UAY	WPL	FJW	MLJ	OMV	RWN	VGJ	YYN	PAF	WDV	CLW
31	YVC	ZFY	VMZ	NXB	RMD	BOP	DOZ	CBG	FUV	UWO	XAF	ORY
32	OGH	TDJ	CVW	DCZ	FPW	JWY	OVG	RVJ	AYP	HNO	NNX	DGK
33	GQL	OZF	TWL	YCW	ANP	OKX	FPR	KVF	NAC	RBF	HNO	FQX
34	HYX	OPZ	XQG	ZZN	VVA	KBQ	NUM	WOU	YFK	BKW	KQG	FTO
35	OWT	CFO	AVQ	KHM	VPF	GLB	DQJ	CFZ	HMQ	YQM	JCW	GCO
36	LKQ	OCF	RCT	XMW	CNO	KDK	OLB	NRJ	BZW	GPJ	LQB	GRP
37	DLX	FAU	ORJ	VQW	GFZ	PHM	UMF	KYP	NGM	OBC	LFK	GZX
38	COP	LBG	NKW	ACK	FWD	GBM	NJF	ONX	RTO	LOC	OUM	KVZ
39	NNB	UGZ	NBV	RFG	LXF	RMJ	AGZ	DTQ	KCG	DAW	CMJ	MWP
40	JNK	OMC	NWZ	XZP	ORD	DDM	CHY	MGJ	PKG	WWB	NPN	NHP
41	CTZ	BXP	DKW	HQK	JMF	OPJ	PNJ	NUY	XPN	ZXG	WYB	NMC
42	TRD	PXB	TMG	HFK	MPL	UCM	AUX	FJB	JXF	TZX	VCN	PDF
43	YNE	ZQY	FVY	JOG	HUJ	BGW	KMQ	OJA	RXQ	YKP	OKQ	PGH
44	JGU	BVO	HKY	HLC	UPB	VAF	CXP	HBK	KXG	ONB	RQK	RQA
45	WJM	DPY	DZP	LZB	RJH	WUY	RWC	CUM	GJM	HZL	MXZ	UUW
46	TJF	NLU	BMJ	FZW	LCB	HQK	JRV	NPC	VHP	RUP	KBF	UYD
47	QWH	PMB	TVZ	UVC	YXJ	DWU	HKP	JBY	AZW	CPX	GLY	XYB
48	HPZ	NBG	NVM	WNP	XLV	NMP	HTP	CZL	FOU	VZO	KGO	ZND

*) Diese Gruppen haben im Teil B, Gruppenliste, die Angabe »s. f. F.«.

Druck d

0

Figure 7. Kenngruppenbuch, Kenngruppen table 681.

Unterseeboote or Commander of the U-boat Fleet). The message is for BDU, is created at 15h40 on the 8th day, has serial number 107 and consists of 24 groups. At the beginning of the message we have the message indicator BDBJ EMEJ, which is repeated at the end of the message. The group length of four letters and the repetition of the message indicator at the end were characteristic for Enigma and R.H.V. (Reserve Hand Verfahren) naval messages.

The Navy procedure as describe above was used by the main naval cipher areas. Many cipher nets, used in less important areas such as in the Black Sea, Balkan and the Far East didn't use this complex procedure with the Kenngruppenbuch to select message keys. Instead, they applied the insecure "throw-on" system with double enciphered message key that was abolished by the Heer in 1940 [1, part I, C, par. 30].

Procedures and Abbreviations

The Army Enigma machine only used the 26 alphabetic characters. Numbers were spelled out. Signs were replaced by rare character combinations. A space was

Geheim! Prüfnr. 516

Kennwort: Fluß

Doppelbuchstabentauschtafel für Kenngruppen — Tafel B

AA = RN	BA = IK	CA = KJ	DA = PK	EA = TC	FA = XP	GA = NE	HA = JR	IA = NN	JA = WE	KA = EI	LA = EU	MA = RG
B = KW	B = RT	B = PO	B = EZ	B = JX	B = OI	B = JO	B = NO	B = VF	B = OY	B = GW	B = KH	B = IP
C = FM	C = EY	C = JV	C = AW	C = OM	C = IU	C = BK	C = GY	C = DN	C = NQ	C = IM	C = VO	C = WW
D = YE	D = AK	D = BM	D = JM	D = MJ	D = RB	D = FL	D = TB	D = FW	D = KK	D = SE	D = YA	D = TA
E = NR	E = OW	E = MZ	E = WB	E = HY	E = PA	E = ZT	E = ZI	E = RP	E = TN	E = AG	E = CV	E = BQ
F = UC	F = WQ	F = EK	F = XY	F = AS	F = DZ	F = SA	F = QY	F = EO	F = VS	F = JH	F = SC	F = KV
G = KE	G = QA	G = KT	G = ZA	G = PU	G = NV	G = LR	G = OA	G = WS	G = FR	G = PN	G = JU	G = NS
H = XU	H = ZZ	H = AZ	H = BS	H = WO	H = ZK	H = TP	H = CU	H = NU	H = KF	H = DT	H = ZQ	H = VK
I = PC	I = OG	I = ND	I = MT	I = FA	I = QR	I = MW	I = QS	I = TM	I = PM	I = LV	I = RX	I = XC
J = JP	J = HQ	J = TQ	J = OE	J = GZ	J = LN	J = AU	J = IS	J = XO	J = SV	J = CA	J = WZ	J = ED
K = BD	K = GC	K = GX	K = FP	K = CF	K = EL	K = QN	K = PG	K = BA	K = IT	K = JD	K = EM	K = ZF
L = QI	L = PR	L = RE	L = RI	L = FK	L = GD	L = WH	L = KR	L = MS	L = UP	L = TO	L = OK	L = DR
M = HT	M = CD	M = WA	M = VV	M = LK	M = AC	M = PB	M = SF	M = KC	M = DD	M = BW	M = TR	M = SU
N = MR	N = NL	N = OS	N = IC	N = TY	N = CP	N = OX	N = SZ	N = QZ	N = PX	N = UX	N = FJ	N = LO
O = BZ	O = US	O = DY	O = YJ	O = IF	O = VE	O = JT	O = FY	O = YV	O = GB	O = QC	O = MN	O = NX
P = XI	P = SX	P = FH	P = NF	P = NC	P = DK	P = RY	P = MX	P = MB	P = AJ	P = VJ	P = BT	P = FZ
Q = OZ	Q = ME	Q = QF	Q = GU	Q = WV	Q = PY	Q = IZ	Q = BJ	Q = OV	Q = XH	Q = RS	Q = IV	Q = OJ
R = UK	R = YN	R = XJ	R = ML	R = KS	R = JG	R = CY	R = OP	R = SH	R = HA	R = HL	R = GG	R = AN
S = EF	S = DH	S = ZB	S = QG	S = QW	S = UE	S = RF	S = RJ.	S = HJ	S = YZ	S = ER	S = NW	S = IL
T = IY	T = LP	T = SW	T = KH	T = XD	T = SR	T = XV	T = AM	T = JK	T = GO	T = CG	T = UF	T = DI
U = GJ	U = XK	U = HH	U = WH	U = LA	U = WX	U = DQ	U = UQ	U = FC	U = LG	U = XZ	U = XW	U = BY
V = QU	V = TI	V = LE	V = HW	V = PL	V = TL	V = UM	V = LZ	V = LQ	V = CC	V = MF	V = KI	V = UT
W = DC	W = KM	W = VP	W = SO	W = SK	W = ID	W = KB	W = DV	W = PH	W = QL	W = AB	W = PW	W = GI
X = UV	X = VY	X = UG	X = NT	X = HZ	X = YS	X = CK	X = WJ	X = UD	X = EB	X = ZY	X = PP	X = HP
Y = SG	Y = MU	Y = GR	Y = CO	Y = BC	Y = HO	Y = HC	Y = VN	Y = AT	Y = TU	Y = NZ	Y = QD	Y = VB
Z = CH	Z = AO	Z = YI	Z = FF	Z = DS	Z = MP	Z = EJ	Z = YD	Z = GQ	Z = UW	Z = WP	Z = HV	Z = CE

Fortsetzung s. Rückseite

Figure 8. Bigram substitution table for Kenngruppen – Table B (part A through M).

omitted, or replaced by an X. The X was generally used as point or full stop. Some signs were different in other parts of the armed forces. The Heer replaced a comma by ZZ and the question sign by FRAGE or FRAQ. The Kriegsmarine however, replaced the comma by Y and the question sign by UD. The combinations CH, as in Acht (eight) or Richtung (direction) were replaced by Q (AQT, RIQTUNG). Two, three or four zero's were replaced by CENTA, MILLE and MYRIA. The Heer and Luftwaffe transmitted the messages in groups of five characters. The Kriegsmarine transmitted the Enigma messages in four-letter groups. To make cryptanalysis harder, more than 250 characters in the message were forbidden. Longer messages were divided into several parts, each using its own message key [8].

To make cryptanalysis even harder, some complications were introduced in the Heer and Luftwaffe message procedures during the war. Since the third, leftmost rotor, only advanced every 676 keystrokes, this rotor didn't have much effect during enciphering. Such long messages were forbidden for security reasons. However, the operator could encipher a certain four letter code into the message, for instance CYOP, and change the left rotor position. When the receiving operator encountered these letters during deciphering, he also turned the leftmost rotor to another position, in this case to position O. Another complication, added at the end of the

```
CLX 1540/8/107 24

BDBJ EMEJ DERH RFRS OQRV DTYH QWBV HILS CXHR OPOD
GTQL DDHI KFTG EDZS WXQS EDFR HGYG EDZZ UYQV DTYY
EDGH KIRM BDBJ EMEJ
```

Figure 9. Typical format of a Kriegmarine message [3].

war, was the permuting of the rotors during the key period. Every 8 hours, a given rotor order was permuted. If the rotors for that day were 241, this changed during the day to 124 and 412. The ring setting of an individual rotor did not change, and moved along with its rotor.

Recourses

I would like to express my gratitude to Ralph Erskine, Frode Weierud, Tony Sale, David Kahn, the National Cryptologic Museum, NARA and many other people and sources, for their valuable information, assistance and for providing me with the many documents that enabled me to compose this paper.

About the Author

Dirk Rijmenants' main interests are the historical and technical aspects of cryptology, and WW2 and Cold War cipher machines. He is the author of the Cipher Machines and Cryptology website and maintains a weblog, related to cryptology and intelligence. His current research interests include Signals Intelligence and espionage during the Cold War.

References

1. Alexander, C. H. O'D. *Cryptographic History of Work on the German Naval Enigma*. National Archives, Kew: HW 25/1.
2. Chef des Oberkommandos der Wehrmacht. January 1940. "Schlüsselanleitung zur Schlüsselmaschine Enigma vom 13.1.40," Berlin: Gedruckt in der Reichsdruckerei.
3. Erskine, Ralph. "The Kenngruppenbuch Indicator System Used with the Main Wartime Naval Enigma Ciphers," http://frode.home.cern.ch/frode/crypto/bgac/KM-IndicatingSystem.pdf
4. Hamer, David H., Geoff Sullivan, and Frode Weierud. July 1998. "Enigma Variations: An Extended Family of Machines," *Cryptologia*, 22(3):211–229.
5. *The History of Hut 6*, Vol. II. National Archives, Kew: HW 43/71.
6. Kozaczuk, Wladyslaw. 1984. *ENIGMA: How the German Machine Cipher Was Broken*, edited/translated by Christopher Kasparek. Frederick, MD: University Publications of America.
7. Marks, Philip. April 2001. "Umkehrwalze D: Enigma's Rewirable Reflector – Part I," *Cryptologia*, 25(2):101–141
8. Sale, Tony. 2001. "The Bletchley Park translated Enigma Instruction Manual," http://www.codesandciphers.org.uk/documents/egenproc/egenproc.pdf
9. Sale, Tony. 2001. "Translated Enigma Offizier and Staff Procedures 1940," http://www.codesandciphers.org.uk/documents/officer/officer1.pdf
10. Smith, Michael and Ralph Erskine. 2001. *Action This Day*, London: Bantam Press.
11. Sullivan, Geoff and Frode Weierud. July 2005. "Breaking German Army Ciphers," *Cryptologia*, 29(3):193–232.