M.Dv. 32/1

Check No. 578

<u>Secret</u> !

THE ENIGMA GENERAL PROCEDURE

(<u>Der Schluessel M Verfahren M Allgemein </u>)

Entered in Secret Book List
of the 59th Patrol Flotilla
under serial No. 66

Supreme Command of the Navy

Berlin 1940

M.Dv. 32/1

_____

Note by Tony Sale:

An attempt has been made in this PDF version of the "General Procedure" to render it as near a "photo copy" as possible.

The rather idiosyncratic use of space before and after commas, for instance, is just as it was in the typing of the original document.

Since this has been re-constructed from scanning and Optical Character Reading of photo copies of the original there may still be some "garbles" left. I would appreciate reporting of any found.

I am indebted to Julian Sinton, Frode Weierud, Andrew Hodges and many others for help in removing garbles.

A.E.S March 2001

M.Dv. 32/1

I authorize the manual "The Enigma, General Procedure" ("Der Schluessel M. Verfahren M Allgemein") - M.Dv. 32/1.

It goes into effect as soon as it is issued.   At the same time, the following manual goes out of effect: "The Enigma Cipher Manual and General Procedure" ("Der Funkschlussel M Schlusselanleitung und Verfahren M Allgemein") M.Dv. 32/1 - Reprint 1939 (Umdruckausgabe 1939).

Changes in the manual, or in the distribution provided for it, are forbidden.

The Radio officer is responsible for the constant supervision of the

copies of this manual which are in the radio room.

When not in use, this manual is to be secured.

If there is danger that this manual fall into enemy hands, it is to be effectively destroyed by fire.   If this is not possible, then it must be destroyed in some other effective way or sunk in deep water.

At shore service stations, the principle of these regulations likewise applies.

Berlin, August 1940.

Supreme Command of the Navy

DISTRIBUTION

All service stations equipped with the Enigma.

M.Dv. 32/1

GENERAL

1.   Unless other cipher procedures are especially prescribed, all secret communications are to be enciphered on the Enigma. The abbreviated plain text is enciphered directly.

2.   If no working Enigma is available, then such radio messages as should be enciphered per Enigma, general Procedure, are to be en-cihered according to the Reserve Hand Procedure, General, (R.H.V. Allg.) - M.Dv. 929/1.

3.   General regulations about the Enigma and the Ciphers of the Day for the Enigma are given in the (Most Secret) publication, "Der Schluessel M Allgemeine Bestimmungen" ("General Regulations for the Enigma") - M.Dv. 32/3.

4.   For ciphering per Enigma, General Procedure, the following things are necessary besides the Enigma and all that goes with it:

    a) Cipher of the Day for the Enigma, General, (Tagesschluessel M Allgemein)

    b) K-Book - M Dv. 98 - with cipher procedure and cipher book for indicator groups.

PREPARATION OF THE PLAIN TEXT

Abbreviation

5.   The message must be as brief as possible, but nevertheless clearly understandable.

      The formation of the text is the originating station's affair.

6.   In order that the messages attain the brevity necessary for radio traffic, all abbreviations can be used which are customary in standard written German and in the Navy. Final syllables and single letters can in many cases be omitted without damage to intelligibility, and the umlauted letters, a, o, and u can in general be represented by a, o, and u. The letter C is to be used instead of CH. Periods after abbreviations can be omitted whenever such an omission does not impair intelligibility.

7.   All systematic and uniformly applied abbreviation of words is, however, to be avoided. For example, it would be wrong always to abbreviate "Funkspruch" by "Fkspr.", because such regularities are an aid to unauthorized deciphering. However, the most important principle is that the sense of the message must be clear and unmis-takable to the receiver. Before being enciphered, every message is to be checked in this regard.

      A varying treatment of abbreviation renders unauthorized de-ciphering basically more difficult.

M.Dv. 32/1

8.   In references to position, course, speed, and D/F bearings,
     the following abbreviations are used:
                 Quadrat   = QU   (Square)
                 Grossquadrat = GRQU   (Large Square)
                 Festpunkt   = FPKT   (Fixed Point)
                 Seemeile(n) = SM   (Nautical Mile(s))
                                        (Knots)

9.   All other expressions such as Grad, Kurs, Fahrt, Richtung,
     Uhr (degree, course, speed, direction, o'clock), etc., are to be
     written out as words.   If the report of the Large Square follows
     directly upon that of the Square, then the abbreviation for Large
     Square is omitted and only the letters for the Large Square are given.

          For example:

     a)   1281   AN = QU EINS ZWO ACHT EINS ANTON NANNI

     b) Festpunkt Fritz = FPKT FRITZ

     c) 24 sm = ZWO VIER SM

     d) Kurs 210 = KURS DREI EINS NUL GRAD

     e) 2035 Uhr = ZWO NUL DREI FUNF UHR

                         Stress Marks
sic.
11.   Instead of dashes or quotation marks or underlining, words to
     be set off by these things are preceded and followed by a J.   This
     is epecially desirable when proper names, unusual geographical
     terms, words from foreign languages, etc., are to be distinguished
     from the rest of the text.   If necessary, especially important words
     can be given twice in succession; and in such a case, each term in
     question is put between a pair of J's each time it occurs.

          e.g. Cap Gris Nez = J CAPGRISNEZ J J CAPGRISNEZ J

               Designation of Service Stations .

12.   Service station designations within the message text are written
     out. Extensive use is to be made of abbreviations; but care is to
     be taken that the names are not garbled in the process.   Periods
     after abbreviations are omitted.   Names with several meanings, such
     as "Ruegen" or "Emden", are to be provided with some clarifying tag
     if there is any chance of confusion:

               e.g. Insel Ruegen or Krz. Emden.
                   (Island)   (Cruiser)

l3.   To service station abbreviations which differ from others by
     only one or two letters, and in names of ships and boats where
     there is danger of confusion, the distinguishing letter is given
     three times.

          for example: B.d.U.   = BDUUU
                        F.d.T.   = FDTTT
                        U 18   = UUU EINS ACHT
                        2. T. Fl. = ZWOTE TTTFL

M.Dv. 32/1

14.   Paragraphs 12 and 13 also hold for addresses and signatures.

                     Addresses and signatures .

15.   In General Procedure, addresses and signatures are taken from
             the Radio Name List, prefixed with a 'beta' and inserted after the time
             group or after the last radio group. They thus fall outside of
             the ciphered part of the message.

16.   In the Fleet and Acknowledgment Procedures, addresses are to
             be put at the beginning of the message text and to be enciphered
             along with it. In these Procedures, the usual thing is to give
             the address first and to separate it by "VON" from the address
             following it. Extensive use is to be made of abbreviations (see
             paragraphs 12, 13, and 19).

17.   On frequencies on which messages with the same addresses and
             signatures frequently recur, the opening can be varied by alternating
             between putting the signature first and putting the address first.
             The address is to be separated from the signature by "AN" or "VON",
             depending on the order.

18.   The word "VON" or "AN" is to be given twice in succession.
             The letters "VVV" and "AAA", respectively, may be used in place of
             these words.

                  For example: a) BDUUU AN AN UUUZEHN

                                b)   UUUZEHN VVV BDUUU

19.   In frequent use of service stations' names, the form of abbre-
             viation is to be varied as much as possible without giving rise
             to misunderstanding.   This is in order to vary the length of the
             messages and their external appearance.

                  Examples:

                  a) Befehlshaber der Unterseeboote:

                          BDUUU
                          BEF. UNTERSEEBOOTE
                          BEFHBR. UUUBTE, and so on.

                  b) Befehlshaber der Kreuzer:

                          BDKKK
                          BEF. D. KRZR.
                          BEFEHLSHBR. DER KREUZ. , and so on.

                  c) F.d.M. Ost:

                          FDMMM. OST
                          FUEHR. MMM OST
                          MINENSUCHFUEHR. OST, and so on.

      d) Befehlsheber der Kuestenbefestigungen von Nordfriesland

          KUESTENBEFEHLH. NORDFRIESLAND
          NORDFRIESLANDBEFEHLHBR., and so on.

      e) Minensuchboot (Minesweeper)

          MINENSUCHBOOT
          MINBOOT
          MMMBOOT
          MMM. . . .(with boat-number following), and so on.

20.   If several addresses follow in succession then care is to
be taken that they do not get misunderstood.   If necessary, they
are to be separated by Y (comma) (see paragraph 25).

21.   If the text of the message is as understandable without address or
signature as with it, then one of the two, or in some
cases even both of them, can be dispensed with -- for example, in
situation reports, weather reports, and so on.

<u>Punctuation Marks</u> .

22.   A period is expressed by X, colon by XX, question mark by
UD, comma by Y, slant, dash and hyphen by YY, parenthesis by KK.

      In general, punctuation marks cannot be dispensed with --
except for a period at the end, which is not to be put in. Before
eliminatlng punctuation marks in the interests of brevity, check
the text carefully for intelligibility.

<u>Numbers</u>

23.   Numbers are written out in letters.   In numbers of several
digits, the words for separate digits follow right after one
another.

      For example: 223 = ZWO ZWO DREI

24.   The following numbers, hovever, can be written in one word:

      ZEHN, ELF, ZWOELF, ZWANZIG, DREISSIG, etc.

      HUNDERT, TAUSEND, etc.

25.   In a series of numbers, any two which would be separated by
a comma in correctly written German are to be separated by Y.
For example:

      a) Pruefnr. 18, 20 und 25 = PRUFNR EINS ACHT Y ZWO NUL UND
       (Check No.)   ZWO FUNF

      b) M 4, 7, 11 = MMM VIER Y SIEBEN Y ELF

M.Dv. 32/1

a) Kaliber 21,5 cm = KALIBER ZWO EINS Y FUNF CM
   (Caliber 21.5 centimeters)

(Note that German uses a comma where we use a decimal point.
   Furthermore, German uses a period -- in numbers -- where
   we use a comma: thus 8.000.000 = eight million; 20,5 =
   20.5. - Translator).

In any series of numbers, care is to be taken that commas are
also inserted when they have been omitted in the message text.

Example: An M 2, 23, 1 21 15.

      Commas must be put in here -- one after 1, and one
after 21. Otherwise there will be possible confusions of the
last three numbers with 12, 11, and 5, or 121 and 15, or 12
and 115.

26.   When there is an immediate succession of numbers (of any number
     of digits) between which no comma is permissible, they are separated
     by YY.   For example:

     281 2 fdl. Kreuzer = QU ZWO ACHT EINS YY ZWO FDL. KREUZER

27.   ordinal numbers are to be expressed either by X after the number
     or by appending the syllable "TE" or "STE" to the number. For example:

     1. April = EINS X APRIL or ERSTER APRIL
     (April 1st)

<div align="center">Summary of Text Aids .</div>

28.

J-----J = Stress Mark	QU = Square
X = Period	GRQU = Large Square
Y = Comma	FBKT = Fixed Point
UD = Question Mark	SM = Nautical Miles, Knots
XX = Colon	(Hyphen
KK------KK = Parenthesis	YY = (Dash
	(Slant

<div align="center">Urgency Signs</div>

29.   In Fleet and Acknowledgment Procedures urgency signs are to
     be put in before the address and signature and are to be enciphered
     along with them.

30.   In order to avoid having the text of "SSD-messages" always
     begin with these letters, one of the following three code words can
     be used instead of "SSD":

          BIENE, WESPE, MUECKE,

     After being deciphered, these words are to be supplanted by
     SSD again.

M.Dv. 32/1

Making Messages Longer

31.   The regullations about treatment of texts, either of regular
radio messages or of those which are enciphered according to various
cipher procedures or cipher memoranda, are expanded by the regula-
tlons here following.

32.   Messages are made to vary in length by adding letters and
           words at the end.

           Directly following upon the last word of the plain text to
be enciphered, three or four identical <u>bigrams</u> are to be added,
and then after them one or more generally-known random words of
neutral content, e.g Wassereimer, Fernsprecher, Eichbaum, Dachfirst,
Kleiderschrank, (water pail, telephone, oak tree, roof ridge,
wardrobe) and the like.   For example:

                    ...ABGESUCHT KB KB KB GARDEROBENSTANDER

           Words which are contrary to good breeding and good order,
personal communications, and the like, are forbidden.   In choosing
these words and the repeated bigrams care is to be taken thst they
cannot be connected in any way with the actual text of the message.

33.   The purpose of using well known words of the German language
for padding is to give the cipherer a guarantee that he has de-
ciphered correctly.

Padding and Separation of Groups

34.   The plain text prepared according to the foregoing regulations
is divided up by letters into four-letter groups and entered on
the cipher form into the column entitled "Book Groups", writing
from left to right.

35.   If the last group contains fewer than four letters, it is to
be padded to four letters with any consonants before being enciphered.
Care is to be taken here that no misunderstandings are possible;
it is especially important to avoid using customary final syllables.

           Padding with text aids and procedure signs of the radio service
or with any other usual abbreviations or with punctuation marks is
forbidden.

Subdivision of Messages .

36.   In order not to delay the process of enciphering and deciphering,
it is sometimes necessary to divide a message, if it is long, into
two or more separate messages.   In this case the word "FORT"
(standing for "Fortsetzung" = "continuation") is to be inserted
somewhere in the last third of every messsge division except the
last.   In the first third of the second message division, and of
every one thereafter, the word "FORT" is likewise to be inserted,
in this case followed by the time group of the preceding message
division belonging to it.   Care is to be taken that time groups,
after being enciphered, do not get altered.

37.   For enciphering and deciphering message divisions, several
cipher groups are to be used at the same time, whenever possible.
The chronological order of the time groups does not need to correspond

to the order of message divisions according to content. The
separate message divisions can also be sent in any succession.

38.   The whole message -- unless radio operational necessities
dictate otherwise -- is always to be designated only by the time
group of the message division which is first in order according to
content.

39.   On the final copy of such a message received, the time group
of the first message division is to be especially marked;   the
separate message divisions are to be put together in consecutive
orden to make up the whole message, and the points of division are
not to be emphasized. The contents of the message may of course
necessitate a subdivision into outline or paragraph form in its
final presentation.

INDICATOR GROUPS

41.   The indicator groups needed to indicate the Enigma as the
ciphering device end the General Procedure as the procedure to be
used the indicator group procedure, and the "Cipher Book for
Indicator Groups" ("Schluesselheft fuer Kenngruppen") are all con-
tained in the K-Book -- M.Dv. 98.

42.   Every message is given two different indicator groups from the
K-Book, of which

        The first serves as cipher indicator group to indicate the
use of the Enigma as the cipher device, and to indicate further the
use of the Cipher of the Day for Home Waters or for Non-home Waters
or for Special Ship Cipher,

        The second serves as procedure indicator group to indicate
the General Procedure and to form the Message Cipher (Spruchschluessel).

43.   It is of the utmost consequence for cipher security that
different indicator groups are used for every message .

Book Indicator Groups .
(Buchkenngruppen)

44.   The two three-letter indicator groups taken from the K-Book
are called Book Indicator Groups. The first thing that happens to
them is that they get wrttten in unchanged, in the column entitled
"Book Groups" (Buchgruppen), in the following manner:

                The Cipher Indicator Group as first Book Group, and
                The Procedure Indicator Group as second Book Group.

After that, the book Groups are filled out to four letters according
to indicator group procedure.

<div align="center">

Radio Indicator Groups .
(Funkkenngruppen)

</div>

45.   The Book Indicator Groups now filled out to four letters are
enciphered according to indicator group procedure. The enciphered
Book Indicator Groups are called Radio Indicator Groups; they are
entered in the column entitled "Radio Groups" (Funkgruppen), as
follows:

        as first and second Radio Groups (the Beginning Indicator Groups),
        and then repeated in identically the same order as the
        next-to-last and last Radio Groups (the End Indicator Groups).

<div align="center">

Message Cipher
(Spruchschluessel)

</div>

46.   For every radio message sent according to Enigma General Procedure,
a special Message Cipher (three-letter group) is used.

4?.   The Message Cipher is obtained as follows. The Cipher of the
Day for enciphering the message according to General Procedure is
set in, and the letters of the three-letter Procedure Indicator
Group (Book Indicator Group, entered as per paragraph 44) are punched
once in succession on the machine. The three letters which light up
one after the other when this is done are the Message Cipher.

48.   The Message Cipher is formed in the same way for deciphering
as for enciphering.

First set this in on the Enigma	Then punch the	The result is the
Cipher of the Day for Enigma General of which the Basic Setting (Grundstellung) is (for example) G R D	Procedure Indicator Group (Book Indicator Group) (for example) V F N	Message Cipher (for example) S P L

49.   The Message Cipher is to be noted down on the cipher form.

50.   With the Message Cipher thus obtained, which is set in in the
windows of the Enigma from left to right, the ciphering of the
actual message is begun.

M.Dv 32/1

51.   The enciphering whereby, through the use of the Enigma, the
          Procedure Indicator Group becomes the Message Cipher, is to be
          carefully distinguished from the enciphering whereby, through the
          indicator group procedure (paragraph 45) the Procedure Indicator
          Group becomes a Radio Indicator Group. These two processes are
          to be kept apart in operation.

                              CIPHERING

56.   Before beginning any job of ciphering, be sure that all the
          settings on the Enigma are valid and correct.

57.   By turning the setting wheels (Einstellraeder), the Message
          Cipher otained as per paragraph 47 is set in on the windows of
          the cover.

58.   In enciphering, the keys labelled with the letters of the
          "Book Groups" to be ciphered, are pushed all the way down, one
          after the other, and the letters which light up are written down
          under "Radio Groups".

59.   In deciphering, the "Radio Groups" are in similar fashion
          turned into "Book Groups".

60.   If a wrong key was pressed down by mistake, then the right
          cipher wheel (Schluesselwalze) is to be turned back several steps
          snd the ciphering of as many letters -- including the wrongly
          pressed one --- is to be repeated as the number of steps the wheel
          was turned back.

          In this process, care is to be taken to make sure -- by
          comparison with the last correctly ciphered letters, that the
          wheels again have their correct positions.

          If necessary, not only the right wheel, but also the middle
          one and in some cases even the left one are to be turned back as
          many steps as they had advanced during the preceding ciphering
          motions now to be repeated.

61.   If it is not possible, by comparison with the correctly
          ciphered group to restore the correct setting, then go back to
          the beginning setting (Message Cipher) and repeat the entire
          ciphering. The time of this operation can, however be shortened
          for the distance up to the last unmistakably correctly ciphered
          group by counting the number of letters up to this point and by
          then pressing any key that number of times.   After reaching this
          point, the ciphering is then continued.

                      Treatment of Cipher Mistakes .

62.   In correcting cipher mistakes, follow NV-2 and the Instructions
          for Use in the K-book.

M.Dv. 32/1

Practical Method of Enciphering .

63.   Select two of the Book Indicator Groups provided for Enigma
general Procedure in the K-book; and of these, enter the Cipher
Indicator Group as the first Book Group and the Procedure Indicator
as the second Book Group on the cipher form.

         Do not forget to leave the space for the dummy letter .

         In order to expedite cipher service, cipher forms with en-
ciphered indicator groups written on them are to be kept ready for
outgoing messages. The Message Cipher is to be written on too
and the date of validity to be noted.

64.   Read the plain text through and then, beginning in the third
line of the column entitled "Book Groups", enter the text onto the
cipher form in four-letter groups. If necessary, fill the last
group out to four places, with attention to the section above,
entitled "Preparation of the Plain Text" (see paragraphs 5 ff.)

65.   Set in the valid Cipher of the Day (including the basic setting)
for Enigma General Procedure and push down the keys for the Procedure
Indicator Group (Book Group) once. The result is the Message Cipher.

66.   Set in the Message Cipher and encipher the "Book Groups " con-
secutively from the third line on. Enter the resulting letters
as four-letter groups in to the "Radio Groups" column, one group
to a line, writing from left to right. The indicator groups do
not get enciphered along with the others.

67.   Check by ciphering the message back again .

68.   Fill out and encipher the Book Indicator Groups according to
the cipher procedure for Indicator Groups in the K-Book.   Enter
the resulting cipher letters in the "Radio Groups" column as first
and second groups and in the same order as next-to last and last
groups.   Check by ciphering the indicator groups back.

69.   Prepare the message for sending :

         a) Addresses and signatures -- only in general radio procedure.

         b) Time group -- date end serial number to complete it.

         c) Group count -- radio groups including radio indicator groups.

70. Example :

         The following SSD-message with time group l053 is to be sent
in Fleet Procedure on the 3rd August:

         SSD   To Fleet, Cruiser "Koeln".   Position bearing of 160 degrees
               to Norderney Lighthouse three miles distant. Going
               with T l53 to square 9551 left top.
                                        Cruiser "Leipzig."

M.Dv. 32/1

SSD   An

Flotte, Kreuzer "Koeln".

Standort Norderney Leuchtturm in 160deg 3 sm ab.   Gehe mit
T 153 nach (sqr) 9551 links oben.

Kreuzer "Leipzig"

SEE DIAGRAM NEXT PAGE

									Meaning
	Time Group 1053				Message Cipher: S P L valid for 3 August				
	Group Count 35								
					Book Groups				Meaning
Beginning Indicator Groups	1	b	i	m	o	j	g	r	h2f	y3n	u4k	Cipher Indicator Group
	2	p	j	y	u	d	d					Procedure Indicator Group
Enciphered with Enigma	3	f	j	i	a	w	e	s	b	Wespe
	4	t	z	w	r	e	l	e	i	
	5	l	h	s	e	o	z	i	g	Leipzig
	6	q	f	d	x	s	n	e	n	an
	7	n	o	a	o	f	l	o	t	Flotte
	8	a	e	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	t	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	l	n	e	in
	16	l	q	u	d	i	n	s	s	1
	17	y	f	v	x	e	c	e	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	s	m	3 am
	21	y	r	h	q	s	b	x	g	ab
	22	r	q	d	e	e	h	h	i	gehe mit
	23	h	j	f	u	t	t		t	T
	24	n	c	x	m	e	h	n	s	1
	25	d	o	k	l	f	u	n	f	5
	26	s	b	i	j	d	r	s	i	3
	27	g	x	t	g	n	s	c	q	nach □
	28	f	u	c	n	u	n	e	u	9
	29	o	h	z	t	n	f	u	n	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	s	l	i	n	links
	33	j	i	n	g	t	o	b	n	oben
End Indicator Groups	34	b	m	o	g	-	-	-	-	
	35	p	y	u	d	-	-	-	-	

M.Dv. 32/1

Practical Method of Deciphering

71.   Check the Radio Indicator Groups to see that the beginning ones and end ones are identical .

72.   Decipher the Radio Indicator Groups according to cipher procedure for indicator groups in the K-Book and   enter the Cipher Indicator Group as the first Book Group and the Procedure Indicator Group as the second.   Look up the meaning of the Indicator Groups in the K-Book and then cross out the beginning and end groups (Radio Groups).

73.   Set in the Cipher of the day (including basic settings) and push down the keys bearing the letters of the Procecure Indicator Group (Book Group) once.   The result ia the   Message Cipher .

74.   Set in the Messsage Cipher and decipher the Radio Groups consecutively from the third line on.   Enter the resulting letters in four-letter groups, one group to a line, in the "Book Group" column, writing from left to right.

75.   Reproduce the abbreviated plain text of tbe "Book Group" column in the column labelled "Meaning" (Bedeutung).

76.   Look up the address and signature in the Radio Name List (Funknamenliste). (Only in the case of General Radio Procedure).

(Translator's Note : Confusion of the two following terms is
         to be avoided:

         Schluesselverfahren M Allgemein : Enigma General Procedure,
         or General Enigma Procedure -- as opposed to Officer and
         Staff.

         Allgemeines Funkverfahren : General Radio Procedure, or
         General Procedure -- as opposed, for examule, to Fleet
         Procedure, Acknowledgment Procedure, and so on.   See NV-2.

                                                            - Tr.)

TREATMENT OF MESSAGE ACCORDING

TO ENIGMA OFFICER AND STAFF PROCEDURES

81.   For the cipher work to be done by the officer, see the manual entitled "Enigma Officer and Staff Procedures" ("Der Schluessei M Verfahren M Offizier und M Stab") -- M.Dv. 32/2.

M.Dv. 32/12

82.   The following work is to be done   by the radio personnel .

                         Ciphering .

83.   The message is handed in to the radio room after having been
            enciphered according to Officer Procedure or Staff Procedure and
            is then to be enciphered like a message according to   Enigma General
            Procedure .

84.   The time group is to be fixed in the same way as for a General
            message, unless the already enciphered message has a time group
            when it is handed in to the radio room.

85.   The following items are to be entered in the column " Book
            Groups " immediately following the beginning indicator groups:

                (i) Urgency signs   )
) as per Enigma General Procedure
                (2) Addresses and signatures)

                (3) The word "Offizier" or, as the case may be, "Stab".

                (4) The indicator letter immediately following, written out
                     as a word.

            The last of the groups formed by (1) to (4) is to be filled
        out to four letters.   The dummy letters in this case are the first
        letters of the written out indicator letter. Suppose, for example,
        that the indicator letter is "Anton".   Then

                    one dummy letter will be   a,
                    two dummy letters will be   an,
                    three dummy letters will be ant.

                (5)   The four-letter enciphered groups of the message as it
            has been handed into the radio room, unaltered.

                Experienced cipher workers may omit the step of entering these
            groups into the column of "Book Groups".

86.   The message, having been entered according to paragraph 85,
            is now to be enciphered according to Enigma General Procedure,
            including the groups referred to in paragraph 85 (5).

87.   Prepare the message for sending, according to paragraph 69.

88.   For reasons of cipher security, sending Officer and Staff
            messages without enciphering them according to Enigma General is
            absolutely forbidden.

99.   <u>Example</u>:   The following message, enciphered according to Enigma Officer, is handed to the radio room on 25 August at 1043 o'clock.

        AN FLOTTE, B. D. K. VON GRUPPE WEST. OFFIZIER. CESAR.
HPFG HKLM IGPV BWXK CEYA ZBOU GDBW ZUIE BTGZ IMEY BGNJ QOXK
HFXU NAFD SJFT RJQT MSPP CLRR VECO DAHY KPAH LLVI WNKM SQEO ZPGD

        This message, including the four-letter groups, gets entered into the "Book Groups" column as per paragraph 85 and then gets enciphered according to Enigma General Procedure.

SEE DIAGRAM NEXT PAGE

(next page missing from copy used, Tony Sale)

Deciphering

90.   If in deciphering a message, you discover that it is an
        Officer or Staff message, hand the cipher form to the officer handling
        such messages. First complete the deciphering of the enciphered
        groups according to Enigma General; in that process the addresses
        and signatures and the rest of the enciphered text will come to light.

Relay by Wire of Received Radio Messages   .

91.   If the received Officer or Staff radio message, for further
        deciphering, by the actual recipient, has to be relayed on the Naval
        teletype network, then it is to be delivered to the teletyping station
        in the following form.

        a) Urgency sign.

        b) Addresses, derived from the message.

        c) Service label, "Geheim verschluesselt FT" ("Secretly enciphered
           radio message") with time group.

        d) The word "Offizier", or, as the case may be "Stab".

        e) The indicator letter (omitting the dummy letters), e.g. Casar.

        f) The four-letter groups enciphered according to Officer or
           Staff Cipher.

        g) Signature, derived from the message.

        If any groups were either missed or doubtful in reception, this
        is to be noted in a special "supplement" ("Zusatz") to the signature
        in g).   To this supplement is to be added the signature of the re-
        laying radio station, or Naval Communications Officer, or Command.

        This message is to be sent as Secret Teletype (Geheimfernschreiben).

PRACTICAL CIPHER SERVICE .

96.   In order to speed up the cipher service, ciphering groups are
        formed of two men each (cipherer and copyist). Experienced personnel
        can dispense with writing down the plain text in the "Book Groups"
        column. Instead of this, the most practical procedure is as follows:

97.   Ciphering. The first man (the cipherer) reads the message
        through before enciphering it, in order to get acquainted with the
        contents and to get used to the handwriting. After that he sets in
        the Message Cipher. The cipherer and copyist are responsible for
        the correctness of the setting. The cipherer then keys the message
        in as regular a tempo as possible. The second man (the copyist)
        reads the cipher letters which light up and he enters them on the
        cipher form into the "Radio Groups" column (see paragraphs 58 and
        66).   Indicator Groups and Message Ciphers, with notation of valid
        dates, are to be kept ready on the cipher forms.

M.Dv. 32/1

98.   <u>Deciphering</u> .   The cipherer, reading the radio groups off the
         cipher form or off the preliminary cipher form, keys them; the copy-
         ist reads the deciphered letters which light up and writes them
         down as plain text on the cipher form or preliminary cipher form.

99.   <u>Dictating aloud</u> is to be avoided.

100.   <u>Cipher forms</u> . For <u>outgoing</u> messages, cipher forms are to be
         used with the consecutive page numbers A ....

           For <u>incoming</u> messages, cipher forms are to be used with con-
         secutive numbers B...., C...., D...., etc. With aid of the various
         designating letters B,C,D, etc, it is possible to arrange the
         incoming messages by frequencies.

101.   For incoming messages, the <u>preliminary cipher forms</u> are also
         to be used as soon as the deciphering is completed, they are to be
         pasted on to the cipher forms to which they belong.

l02.   <u>Aids</u> . The supplementary Lamp Apparatus L for the Enigma
         (Lampenzusatzgeraet L zum Schluessel M) is to be used in cipher service
         whenever it is available.

           <u>Instructions to Supplement the "Cipher Manual</u>

           <u>for the Army Enigma" When Using the Army Cipher</u>

                   <u>on the Naval Enigma</u> .

106.   The cipher wheels of the Army Enigma are connected (geschaltet)
         as are those wheels of the Naval Enigma which are designated with
         the same numbers.

107.   The following things are necessary for ciphering with the
       Army Enigma:

           a) Schluesselanleitung zur Schluesselmaschine Enigma (Cipher
       Manual for the Army Enigma -- M.Dv 168.

           b) Cipher of the Armed Forces and of the Authorities according
       to the regulations entitled "Die Wehrmachtschluessel (The Armed
       Forces' Cipher) -- M.Dv. 390.

           c) Allgemeine Schluesselregeln fuer die, Wehrmacht (General
       Cipher Rules for the Armed Forces) -- M.Dv. 534.

       (<u>Translator's Note</u> :   Throughout this document, and in general,
           the English word <u>Enigma</u> has been used to translate the
           German <u>Schluessel M</u> , more properly translated <u>Naval Enigma</u> .
           The German equivalents for what is here translated   <u>Army</u>
           <u>Enigma</u> are: <u>Schluesselmaschine Enigma</u> and <u>Wehrmacht - M -</u>
           <u>Schluessel</u> . When one of these is used the other usually
           follows it in the German text in parentheses. - Tr.)

M.Dv. 32/1

Servicing Regulations .

111.   The Enigma , without cipher wheels is "Secret Material" . The
        cipher wheels, and the Enigma with the   cipher wheels set in, are
        "Secret Command Material ."   (These expressions are, respectively,
        "Geheimsache" and "Geheime Kommandosache" -- corresponding,
        respectively, to the British Secret and Most Secret . - Tr.)

112.   Opening up the Enigma , setting in the Inner Setting, and
        changing the cipher wheels is to be done   by officer only .

            Only in the use of Enigma General Procedure, if there is no
        officer present or detailed, a reliable Non-Commissioned officer
        can be given the authority, in writing, to do these things as
        a "specially delegated person" according to the Regulations Re-
        garding Secret Material (Verschlusssachenvorschrift).

113.   For changing the cipher wheels (wheel order), the cover of the
        Enigma is to be opened all the way. The holding lever (Haltehebel)
        which is to the left of the wheels is to be moved forward. The
        "Umkehrwalze" is to be pushed to the left end the wheels are to be
        pressed together. The wheel axle is to be lifted out with the wheels.

114.   In putting the wheels in , take care to have them in the order
        called for. The axle collar is to the left, the contact points of
        the wheels point to the right.

115.   For setting the letter rings (Ringstellung), the spring catch
        (Haltefederknopf) on the cipher wheels is to be raised and the red
        mark on the spring peg to be put next to the letter called for by
        the Ringstellung.

            In the case of Enigmas with check-numbers from M 1822 on up,
        inclusive, the groove-lever (Rasthebel) next to the letter ring is
        to be pressed in and the body of the wheel turned. The two white
        dots on the surface of the contact side of the wheel are to be put
        next to the letter called for by the Ringstellung.

116.   The Enigma is to be locked after every time it is opened and
        the key to the Enigma and to the wheel-box is to be kept by an officer.

117.   Connect the Enigma with the source of current indicated on the
        plate fastened to tne cover.

118.   To check the lights, take out all plug (Stecker) connections.
        press the Q-key, then the W-key; let the Q-key go, press the E-key;
        let the W-key go, and so on.   Each time, a light should go on.

            If a light does not go on, put in a new bulb. Get the bulbs
        from D V (Druckschriftenverwaltung - Registered Publications Office).

M.Dv. 32/1

119.   Do not pull out the <u>double plug cords</u> (Doppelsteckerschnuere) by the cords, but by the plugs. Push plug points all the way in, otherwise there will be no contact. When the machine is working, the wooden flap must always be shut so that it presses against the plugs.

Reich Printing Office
5887 40 2B

(<u>Translator's note</u> : The original document ended here. The paragraphs below were added as of 19 September 1940. The final diagram may possibly be of a later date. - Tr.)

Use of the Enigma for the Army Cipher

(Der Schluessel M bei Anwendung des Wehrmacht-Maschinenschluessels) (Heeresverfahren)

Preparation of the Plain Text

121.   Principle: Be brief and unmistakable.   Regularity of structure is to be avoided.

Changing the message text at your own discretion is forbidden; so also is the mingling of cipher groups with plain text.

Abbreviations are permissible only with the authorization of the Command Station or of the originator of the message.

122.   Express <u>punctuation marks</u> and <u>periods</u> at the end of <u>abbreviations</u> by "X",

Exception: Question mark = "X FRAGE X" or "FRAGEZEIQEN" or "ANFRAGE X OB" etc.

<u>Stress mark</u> is "X .... X".

Stress and punctuation marks are to be inserted only when absolutely necessary.

Princinle: Insert the letter "X" as seldom as possible.

123.   <u>Umlaute</u> : a = AE, o = OE, u = UE.

For "ch" and "ck", use "Q". Exception: In name's of places and persons, use CH and CK.   For the single character sz, use SZ.

124.   Write <u>numbers</u> out by digits as words.

125.   Addresses. and signatures are to be inserted in the message texts at a different place each time and to be enciphered also. Take care that no misunderstandings are possible. Addresses and signatures are to be omitted when they correspond to the receiving and sending stations.

M.Dv. 32/1

126.   There is no <u>minimum length</u> of an enciphered message; <u>maximum</u>
           length is 250 letters (equal to 50 five-letter groups).

                          <u>Indicator Group</u> .

127.   <u>Indicator group consists of five letters</u> , of which the first
           two are dummies, the last three are indicator letters. The
           indicator group is put in as the <u>first</u> radio group. It does not
           get enciphered.

128.   Dummy letters are chosen arbitrarily, and they must constantly
           change.

129.   Indicator group letters are taken from the indicator group
           table printed on the Cipher Table (Cipher of the Day). Every day
           three different indicator groups are available. Always vary the
           order of the letters within the group. For example, the following
           indicator groups can be formed from ABH:

               ABH AHB BAH BHA HAB HBA

130.   In the case of messages divided up into several parts, each
           message division must be designated with different indictator groups
           and dummy letters.

                          <u>Cipher Memoranda</u>
                        (Schluesselunterlagen)

131.   The Cipher of the Day contains:

           a) Wheel order (in Roman numerals).

           b) Ringstellung (in Arabic numbers or letters).

           c) Plug connections (in letters).

               When the Ringstellung is given in numbers, then instead of the
           number a letter is to be used, according to the following scheme:

           01 = A   07 = G 12 = L   17 = Q   22 = V
           02 = B   08 = H 13 = M   18 = R   23 = W
           03 = C   09 = I 14 = N   19 = S   24 = X
           04 = D   10 = J 15 = O   20 = T   25 = Y
           05 = E   11 = K 16 = P   21 = U   26 = Z
           08 = F

132.   The Cipher of the Day changes at 0000 o'clock.

M.Dv. 32/1

Enciphering .

133.　　　　Set in the Cipher of the Day on the Enigma (Schluessel M)
according to Cipher Table.

134.　　　　Form the indicator group as per paragraph 127 ff and enter it
as the first five-letter Radio Group.　 Do not encipher it !

l35.　　　　Choose Grundstellung at will and set it in in the three
windows of the Enigma from left to right, e.g. W E P.　 The Grund-
stellung must be different for every message -- including every
message division.　 The Grundstellung is put into the message
heading as a three-letter group unenciphered.

136.　　　　Chose a Message Cipher (e.g. X F R).

　　　　For every message -- including every message division -- a
different Message Cipher is to be used.

　　　　Note　 Using any of the following for Grundstellung and Message
Cipher is forbidden:　 any letter three times, words, abbreviations,
traffic signs, call signs, letters in alphabetical order or in
order of the Enigma key-board.

137.　　　　With the Cipher of the Day and chosen Grundstellung set in,
key the Message Cipher once.

　　　　Insert the result (e.g. H F I) as a three-letter group directly
after the Grundstellung in the message heading.

138.　　　　Set in the chosen unenciphered Message Cipher (e.g. X F R)
in the windows of the Enigma reading from left to right, and key
the letters of the prepared plain text one after the other.　 The
letters lighting up are to be entered after the last letter of the
unenciphered indicator group as the 6th, 7th, 8th, etc. letters of the
Radio Groups as five-letter groups.

　　　　Note:　 The last group can consist of one, two, three, four,
or five letters.

139.　　　　Prepare the message heading.　 It contains:

　　　　　 Time Group

　　　　　 Letter Count (including indicator group)

　　　　　 Grundstellung (unenciphered, three-letter)

　　　　　 Enciphered Message-Cipher (three-letter).

140.　 Example:　　 Time of sending (Time group) 1775 o'clock.

　　　　　 Grundstellung: W E P

　　　　　 Message Cipher: X F R (enciphered: H F I)

Indicator Group Letters: N U Z. (transposed: Z N U)

Dummy Letters: U L

Text of Message -- including Indicator group -- consists
      of 129 letters.

The message then reads:

1755 - 129 - WEP HFI - ULZNU SGEXU etc. up to 129 letters in all

i.e. 25 five-letter groups and 4 letters.

Note: In sending the message, the heading is given twice. For
example:

1755 1755 - 129 129 - WEP HFI WEP HFI -

Deciphering .

141.   Determine from the letter count (the second number in the
      Heading) whether you have received correctly.

142.   Cross out the dummy (i.e. first two) letters of the indicator
      group (i.e. of the first radio group).   Arrange the last three
      letters of the indicator group in alphabetical order and determine
      from the Cipher Table (Cipher of the Day) which Cipher of the Day
      has been used.

      Note:

            Since the Supreme Command of the Army has not listed the
      meanings of all indicator groups in a list comparable to that of
      the K-Book's List of Groups, the receiver must look up the indi-
      cator group of all available Cipher Tables (Armed Forces' Cipher,
      Armed Forces Staff and Authorities Machine and Hand Ciphers)
      (Wehrmacht-, Wehrmacht-Stabs- und Behoerden-Maschinen- und -Hand-
      schluessel).   (This probably adds up to five ciphers, maybe six.
                                                            - Tr.)

143.   Set in the Cipher of the Day on the Enigma.

144.   Take the Grundstellung from the Message Heading (first
      letter group) and set it in in the windows of the Enigma reading
      from left to right.

145.   Key the letters of the enciphered Message Cipher (second
      letter group of the Heading) on the Enigma. The result is the
      Message Cipher.

146.   Set the Message Cipher in the windows of the Enigma reading
      from left to right and key the letters of the radio group(s) --
      from the second radio group on -- one after the other.   The result
      is the plain text of the message.

	Enigma General	Armed Forces' Machine Cipher
	(Navy)	(Army)
Change of Cipher of the Day	0000 o'clock	0000 o'clock
Ringstellung	Letters	Numbers or Letters
Plug Connections (Steckerverbindungen)	Numbers	Letters
Grundstellung	as per Cipher of the Day	Choose at will, set them in the Message Heading
Message Cipher	Result of Procedure Indicator Group and Cipher of the Day	Choose at will, encipher with Cipher of the Day and Grundstellung, insert in Message Heading
Indicator Groups	a) As per K-Book b) Both of them used as both beginning and end Indicator Groups c) Encipher as per K-Book	a) Indicator Group Letters printed on the Cipher Table (Cipher of the Day) b) One Indicator Group as first Radio Group c) Unenciphered, letters transposed.
Punctuation	X = Period XX = Colon UD = Question mark Y = Comma YY = Slant, dash, hyphen	X = All punctuation marks, and period after abbreviations. X FRAGE X etc. = Question mark FRAGEZEICHEN
Stress Mark	J ---- J	X ---- X