Ag WNV/Fu I Nr.3000/44 geh. Secret!

Secret!

Cipher Instructions for the Cipher System 44 (RS 44)

from 27 March 1944.

Berlin, 27 March 1944.

Ag WNV/Fu I Nr.3000/44 geh.

Secret!

Cipher Instructions for the Cipher System 44 (RS 44)

from 27 March 1944.

Berlin, 27 March 1944.

Armed Forces High Command
Chief Armed Forces Communication
Ag WNV/Fu I Nr.3000/44 geh.

S e c r e t !

I approve the Cipher Instructions for the Cipher System 44 (RS 44), edition from 27 March 1944.

Berlin, 27 March 1944.

Pro procurationem:

Fellgiebel

Table of Contents

Page

I. Explanation of Terms and Designations 5

II. General Regulations 5

III. Cipher Rules for the Cipher System 6

IV. Cipher Documents 11

V. Preparation of the Cipher Tools 12

VI. Ciphering 13

VII. Cipher Example 19

VIII. Deciphering 20

IX. Labeling of the Cipher Keys 23

X. Penal Provisions 24

Images 1 – 4 .....

Changes of minimum length, take-out column, message head

see attached decree:

(only partially readable)

I. Explanation of Terms and Designations

1. **Plain text** (open wording) in a text written in open language.
   Ciphered text (secret text) is a plain text ciphered with a certain key.
   Ciphering is the conversion of a plain text into a ciphered text.
   Deciphering is the conversion of a ciphered text into a plain text.
   Text conversion can refer to both, ciphering and deciphering.
   Cipher method is the rule applied to ciphering.
   Cipher key (cipher documents) are the changing documents used to convert plain text into ciphered text, e. g., raster blocks, and raster patterns.
   Cipher tools are the auxiliary means needed for text conversion, e. g., cipher blocks, cipher pages, etc.
   Indicator group serves for labeling of the cipher key in a message.
   Message key is the specification of the initial position for ciphering that is arbitrarily chosen by the cipher clerk or according to special rules; with respect to the raster key the specification of the position of the starting cell in a message chosen by the cipher clerk.
   Optional words are words that have to be chosen by the cipher clerk. These words are necessary for the change or filling of certain messages. They must not be related to the message content.

II. General Regulations

2. The **security of the ciphered messages** depends

a) on the unconditional confidentiality of the cipher keys and of the cipher instructions,
b) on the correct application of the cipher rules,
c) on the execution of the compulsory daily changes of the cipher documents.

3. The cipher documents and the cipher instructions for the raster key are secret. Each **breach of confidentiality rules** will be prosecuted as treason of military secrets (H.Dv.99, M.Dv. Nr. 9, L.Dv. 99, Ziffer 24 und § 88 RStGB).
4. Cipher keys which ceased to be in force allow the enemy very valuable conclusions. It is especially important to take care of the **safe keeping of the cipher keys** according to regulations and the in-time **destruction** or return of invalid cipher keys.
5. Raster patterns are to be handed out to the ciphering staff always for the current day and for a **maximum** of two days in advance. **Exposure** or **loss** of cipher documents has to be **reported immediately** so that a replacement cipher key can be issued.
6. Each **non-observance of the cipher rules** can enable the enemy to break into the cipher method and cause detriments in warfare.
7. **Arbitrary changing** of the cipher rules or the **application** of a **non-commanded method** will be prosecuted as non-observance of an order in service according to § 92 M St GB, if no punishment is required according to § 88 R St GB.

III. Cipher Rules for the Cipher System

8. The raster method is an offset method. It causes a scrambling of the plain text characters by the application of a **daily changing raster pattern**. The raster pattern that contains black and white cells (empty resp. writing cells) in an uneven distribution is placed like a line page under one of the transparent pages of the cipher block. According to specific rules (Number 19 to 27), beginning in an arbitrary but for every message changing position the message is

   during enciphering line by line entered into the white cells and then taken out column by column,

during deciphering column by column entered into the white cells and then taken out line by line.

9. As long as in the following nothing else is requested, the "General Cipher Rules for the Armed Forces" (H.Dv. G 7, M.Dv.Nr.534,L.Dv.g 7 or L.Dv.g 60) are to be applied to the enciphering and deciphering.

10. **The minimum length of messages has to be 60 characters. The maximum length is 200 characters.** Messages which don't reach the minimum length have to be filled up to at least 60 characters by adding of optional words.

11. Messages with more than 200 characters are to be **split** into parts with different lengths. Each message part has to be enciphered into a completely independent message.

12. Before they are entered into the cipher page **all place names and area designations in foreign language** (how they are written in maps) are to be enciphered with the commanded **place name alphabet** by searching their characters one by one in the upper, alphabetically ordered "plain" line of the place name alphabet and by replacing them by the character right below in the "secret" line. The deciphering is carried out accordingly by using the lower line pairs of the place name alphabet. Beginning and end of this cipher position are marked by the character pairs **aa** in the beginning and **ee** in the end.

    Place names and foreign language area designations are only then to be enciphered twice in a row if errors or confusion may occur without them. In case of repetition, no characters are to be inserted in between the place names – no single **"x"** as well.

13. **Map information according to the report network method** are surrounded by **aa** and **ee** as well. By doing that, characters are enciphered according to the phonetic alphabet (a = anton, b = berta, and so on with the exception of y = ipsilon - not ypsilon -) and numbers like all numbers according to H.Dv.g 7, M.Dv.Nr.534, L.Dv.g 7. Example: map information "xy 9a 35" has

to be enciphered like that: “a a x a n t i p p e i p s i l o n n e u n a n t o n d r e i f u e n f e e”. The enciphering of push lines has to be done in the same way.

14. **Non-confusing word abbreviations** have to be used in messages to the extent possible, even if as a result the character number 60 will not be reached and optional words need to be used.

15. From “General Cipher Rules for the Armed Forces” (H. Dv. G 7, M. Dv. Nr. 534, L. Dv .g 7 or L. Dv. g 60) the following basic rules for the raster key are especially emphasized:
    a) **Punctuation marks.** The basic rule has to be to use punctuation marks as little as possible. In general they are replaced by **“x”**. In case their distinction is necessary for the clarity of the message then they have to be expressed in the following way
       Period by “stop”,
       Comma by “coma”,
       Question mark by “fraq”,
       Parentheses by “klam”
       while all other punctuation marks have to be spelled out. In the end of a message a period has always, the question mark then to be avoided if the question is clearly understandable as a result of the word positioning. After abbreviations the character **“x”** is only then to be written if the meaning would be screwed up otherwise.
    b) **Umlauts** are to be written as single vocals (e. g., **ä = ae**, **ö = oe**, **ü = ue**).
       The character combination **“ch”** and **“ck”** are to be replaced by **“q”**, except in place names and proper names, where they are to be resolved to the single characters **“c”** and **“h”** and **“c”** and **“k”**. The character **“ß”** is to be resolved to the single characters **“s”** and **“z”**.
    c) **Numbers** are to be expressed by their single digits in words (e. g., **148 = eins vier aqt**). The digit **“2”** has to be enciphered as **“zwo”**.
       Only the following numbers are to be expressed with one word:

10 = zehn	60 = seqzig
11 = elf	70 = siebzig

20 = zwanzig	80 = aqtzig
30 = dreiszig	90 = neunzig
40 = vierzig	100 = hundert
50 = fuenfzig	1000 = tausend

Connections with the numbers mentioned above are illegal.

To be enciphered are 12 = eins zwo, 211 = zwo eins eins, 350 = drei fuenf null, 0430 = null vier drei null.

It is prohibited to encipher the word null more than once in a row *(consecutive)***.**

For multiple nulls the following short terms are to be used: 00 = zenta, 000 = mille, 0000 = miria, (e. g., 200 = zwo zenta, 3000 = drei mille, 40000 = vier miria, 500000 = fuenf zenta mille or fuenf miria null or fuenf null miria or fuenf mille zenta, 00780 = zenta sieben aqt null, 500043 fuenf mille vier drei).
Roman numbers receive the prefix “roem”.

Periphrases are possible: e. g., III Pz. Gren. Rgt. 10 = drittes btl pnz grn rgt zehn.

d) **Clock times** are enciphered uniformly – independent on whether they are written in plain text. Enciphering of multiple nulls in a row is prohibited here as well.
An “x” is written between hours and minutes.

Examples:
0000 Uhr as null uhr
0100 Uhr as eins uhr
1000 Uhr as zehn uhr
0011 Uhr as null x elf uhr
0906 Uhr as neun x null seqs uhr
1010 Uhr as zehn x zehn uhr
1326 Uhr as eins drei x zwo seqs uhr
1200 Uhr as eins zwo uhr
2000 Uhr as zwanzig uhr
2400 Uhr as zwo vier uhr

To avoid errors, the word “Uhr” has to be written after every clock time.

e) If the minimum length of a message is not reached then the message has to be filled with arbitrary **optional words** without changing the wording of the plain text. This is done by either prepending or appending the optional words. It is prohibited to extend the message by spelling out punctuation marks and abbreviations or by non-changing amendments like: Schluss, Ende etc. It is prohibited as well to partially or completely repeat the wording of the message. Optional words are to be changed constantly. Their length and initial letters have always to differ. They must not be related to any military terms (assumed names, disguising designations, words of the phonetic alphabet etc.) and to the content of the message.
When after deciphering the plain text is entered into the message blank then the optional words have to be omitted.
For the **labeling and delimitation of the optional words** from the message text are the two letters adjacent to the message content to be doubled. For example:
milqstrasze sprungtissqq angriff
abgesqlagen eeiisenbahn fensterbrett.

f) A message has to be written again on the radio station commander’s responsibility:
1. if the same message is enciphered with different keys,
2. if the transmitted message has to be enciphered anew because it was incorrectly enciphered,
3. if the receiver does not have the original cipher key for a transfer message

The new formulation has to happen on the radio station commander’s responsibility. **It must not distort the meaning of the message** and is properly achieved by **rearranging** the text. If possible the sender of the message is to be enlisted. **The after this newly formulated message has to be encrypted like an entirely new message.**

g) Daily at the same times, in the same form, with the same structure or with the same words transmitted messages endanger the key security especially. For that reason they have to be composed in an **ever-changing** form. Broadly,

frequently repeating identical phrases and clauses are to be avoided in messages.

IV. Cipher Documents

16. As **cipher key of the day** a daily changing **raster pattern** is issued. The raster pattern contains 24 rows and 25 columns. In each row are 10 white cells, the so-called writing cells. For the labeling of the columns, rows, and cells a **column watchword** is located at the upper border of the raster pattern and a **row watchword** at the right border of the raster pattern, which change daily as well.

Pattern of a column watchword:

cb	ac	ba	cd	eb	ee	db	aa	be	cc	da	ec	ae	bb	ca	dc	de	ab
3	20	**8**	13	**5**	19	**1**	14	**9**	21	18	15	24	**2**	12	**7**	10	22

ce	ed	dd	bc	ad	ea	bd
4	16	25	11	23	17	**6**

Pattern of a row watchword:

bd ac ca ea ae ee bc be dc aa ec ce dd cb ab eb bb cd
ed ad cc da ba db

On the front side of the raster pattern are located:

a) information about the cipher key type (division's hand cipher key, army hand cipher key etc.) and the day of the month,
b) a daily changing **character exchange table** for the enciphering of the characters in the message key

Example:

a	**b**	**c**	**d**	**e**
g	t	a	c	d
e	q	f	i	y
b	x	o	h	n

z	u	k	s	v
l	r	w	m	p

c) **Two place name alphabets** (1 and 2) for the encoding of place names and area designations in foreign language. The place name alphabets change on every first day of the month. By special decree will be commanded which of the two place name alphabets on the raster pattern is to be used in the specific theater of war.

Example for a place name alphabet:
Enciphering:

Plain:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Secret:	n	m	l	y	a	x	w	f	u	q	t	d	z	r	i	v	k	g	e	o	p	j	s	h	b	c

Deciphering:

Plain:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Secret:	e	y	z	l	s	h	r	x	o	v	q	c	b	a	t	u	j	n	w	k	i	p	g	f	d	m

V. Preparation of the Cipher Tools

17. The **key block** contains transparent cipher pages, which have a with the raster pattern matching ruling. The cipher clerk properly writes the place name alphabet for enciphering and deciphering which is valid for the current month on the inner side of the cover sheet of the key block. Special attention has to be paid to the change of the place name alphabet on the first of the month.

18. For enciphering, the raster pattern will be placed under the upper cipher page so that the ruling of the cipher page aligns exactly with the ruling of the raster pattern and that the column watchword and row watchword transfer straightly the upper and the right border of the cipher page.

VI. Ciphering

19. Entering of the Plain Text into the Cipher Page

The plain text is entered on the cipher page into the brightly shining through writing cells. The black cells are empty cells and are skipped. **The entering happens row-wise and begins in an arbitrary writing cell of the raster pattern.** Once the entry of the plain text reaches the last writing cell of the undermost row, the entry continues in the first writing cell of the top row. At this special attention has to be paid to that the minimum length of 60 characters will be reached and that the maximum length of 200 characters will not be exceeded.

20. Message Key

The writing cell in that the first character of the message is entered or one of the immediately preceding empty cells is chosen for the designation of the beginning of the message on the raster pattern and it is called **"starting cell of the message"**.
The position of the starting cell is transmitted as message key in the message head. The "plain" message key is expressed by two character pairs. The first pair indicates the column and the second indicates the row in whose crossing point the starting cell is located. The first, column-indicating character pair is taken out from the column watchword at the head of the raster pattern, the second, row-indicating character pair is taken out from the row watchword on the right of the raster pattern.

21. Selection of the Starting Cell

For the selection of the starting cell in the raster pattern there must not be any preference for certain rows or columns (e. g., the first row in the raster pattern or the first writing cell in the rows). Also, the adherence to a certain sequence for the selection of the starting cell is strictly prohibited; e. g., the first message should not start in the first row, the second in the second row etc.

Fundamental Rule: The starting cell is to be selected in the lower raster rows and in the upper raster rows with equal frequency.

22. **Cross-Out Rule**
    The two character pairs that form the plain message key are to be crossed out **immediately** in the column watchword and row watchword by a tilted line from the lower left to the upper right (e. g., bc crossed out with slash) or in case they had already been crossed out this way by another line from the upper left to the lower right (e. g., bc crossed out with an X) to cross out crosswise. In doing so, the character pairs have to remain readable.

    It is prohibited to select starting cells which are in one column or row with already crosswise crossed-out character pair as long as not yet all character pairs are crossed-out crosswise.

23. **Enciphering of the Message Key**
    The "plain" message key, in which only the letters from a to e exist, has to be enciphered with the help of the with the cipher key of the day provided character exchange table (compare with number 16b), by replacing the characters from a to e of the plain message keys with one of each of the in the character exchange table below them located five characters of choice. When applying the exchange table strict attention needs to be paid so that

    a) no preference of certain letters occurs,
    b) the enciphered message key always consists of four different letters

24. **The cipher pages can be prepared for a number of messages already before the enciphering of a message by choosing the starting cells**, by crossing out the rows and columns in the watchwords of the raster pattern, and by marking the starting cells (compare image 1). On the lower borders of the cipher pages the "plain" and "secret" message keys have to be written down. This saves the taking out of the raster pattern for the use of the character exchange table and time is gained for the enciphering of the messages themselves.

When calculating the cross sum to determine the take-out column (number 25 of the Schl. Anl.) a number can yield a number that is greater than 25. (Example: 1459 – 99 – cross sum: 5 + 9 + 9 + 9 = 32.)

In these cases, during counting, the column of the starting cell will be reached once again during step 25 to the right and it is to be included then. Only in the beginning of the counting the column of the starting cell must not be included.
(Vfg.OKH/Chef HNW IV 89bNr.11560/44g.v.31.7.44.)

26. Taking-out of the Ciphered Text

The letters in the individual columns are **taken out** from top **to bottom**, always starting with the top row of the raster pattern, and represent, written side by side, the ciphered text (secret text). The sequence in that the columns are taken out is indicated by the numbers of the column watchword.

27. Writing down of the Ciphered Text

The ciphered text (secret text) is written on the message blank in groups of 5 characters.

N o t e :

Page 11 exists twice. Once with the original text and once with one sticker with the additional note according to decree OKH from 7/31/44

the character exchange table below them located five characters of choice. When applying the exchange table strict attention needs to be paid so that

c) no preference of certain letters occurs,
d) the enciphered message key always consists of four different letters

24. The cipher pages can be prepared for a number of messages already before the enciphering of a message by choosing the starting cells, by crossing out the rows and columns in the watchwords of the raster pattern, and by marking the starting cells (compare image 1). On the lower borders of the cipher pages the "plain" and "secret" message keys have to be written down. This saves the taking out of the raster pattern for the use of the character exchange table and time is gained for the enciphering of the messages themselves.

25. Determination of the Take-out Column

The column in which the taking-out of the ciphered text begins, the take-out column, is determined in the following way: After entering the message into the cipher page, **tactical** time, number of characters, and message key are entered as message head into the message blank. The cross sum is derived from the minute count and the character count, i. e., the single digits of the minute count and the character count are added up. The resulting number is counted in the column watchword from the crossed-out column of the starting cell to the right, regardless of the number watchword and without counting the column of the starting cell. At the in this way resulting column begins the taking-out of the ciphered text.

26. Taking-out of the Ciphered Text

The letters in the individual columns are **taken out** from top **to bottom**, always starting with the top row of the raster pattern, and represent, written side by side, the ciphered text (secret text). The sequence in that the columns are taken out is indicated by the numbers of the column watchword.

27. Writing down of the Ciphered Text

The ciphered text (secret text) is written on the message blank in groups of 5 characters.

VII. Cipher Example

(Compare image 2)

28. **Plain Text:**
1203 –
Feind greift set 11.45 Uhr bei Orjechow mit 8 Panzern nach Südwesten an.

The text that has to be entered into the cipher page reads:

Feind greift seit elf x vier fuenf uhr bei aaigqalfisigqalfisee mit aqt panz naq suedwest an.

Herein the place name **Orjechow** is enciphered according to the place name register (compare number 16c) twice in a row and surrounded by aa and ee.

29. Column bb and row ae are chosen as starting cell in the raster pattern and as plain message key **bbae** written on the bottom border of the cipher page. (Writing cells should be chosen as starting cells for the message key just as often as empty cells.) The letter pairs bb in the column watchword and ae in the row watchword are crossed out on the raster pattern with a pencil. The starting cell is then marked by pencil lines as upper limit of the writing area and by one vertical **arrow** on the cipher page, as shown in the image. After that the plain message key bbae needs to be enciphered with the character exchange table on the front side of the pattern. According to the character exchange table (compare number 16b) b can be replaced by any of the letters **t q x u r**, also, a and e can can be replaced by any of the characters **g e b z l** and respectively **d y n v p**. However, it is necessary to keep in mind that the enciphered message key has to consist of four different characters. Hence, the twice appearing b has to be replaced by two different – apart from that arbitrary – of the letters **t q x u r**.

This yields, e. g.:

b b a e = t u z d

that is written in this form on the bottom border of the cipher page.

After that the message is entered row-wise into the writing cells of the cipher page.

30. Once the message has been entered into the cipher page, the tactical time, character count, and the message key are written as message head into a message blank.

    Message head: **1 2 0 3 – 7 7 – t u z d –** *(not readable)*

    The cross sum is calculated from the minute count 03 and the letter count 77:

    0 + 3 + 7 + 7 = 17.

    Following that in the column watchword 17 cells are counted to the right starting at **bb**. The first cell to be counted is the cell to the right of bb. The counting finishes in column **ee** which is to be **instantly** marked as take-out column by a **cross** with pencil.

31. The take-out begins in by **ee** labeled column 19, then follow the columns 20, 21, 22, …, 25, 1, 2, …, 18. When the characters of one column are taken out and written down, then this column on the cipher page will be stricken out vertically.

32. The resulting **cipher text** is:

1 2 0 3 – 7 7 t u z d – *(not readable)*
d i a n m r q t v f n n r i s i f f g p
u e f z g n a e e h a e u t a i i e a d
a g q q l w i b s f f x u t i t e e a a
e n i q s s i r l i e f e s e l t

VIII. Deciphering

(compare image 3)

33. The message key is deciphered according to the character exchange table by looking up the characters **t u z d** in the exchange table one after the other and by replacing them by the characters that are found above them in the head of the table:

t u z d = b b a e

34. The starting cell that is located in column **bb** and in row **ae** is looked up on the raster pattern. The message has to begin in this cell or resp. in the first writing cell that follows to the right of this cell.

35. Starting from cell **bbae** 77 writing cells are counted according to the message length, which is facilitated by the fact that **each row contains 10 writing cells**. Hence, counted are in row **ae**, beginning at the starting cell, 4 writing cells and then row-wise 14, 24, 34, 44, 54, 64, 74 cells and in row **dd** the writing cells from 75 to 77. Therefore the last character has to be entered in cell **dbdd**.

36. The writing area, in which the message has to be entered according to number 34 and 35, needs to be framed with pencil. For this purpose the writing cells, which precede the starting cell, and the cells, which are located behind the last writing cell and below the last row, are crossed out.

37. According to number 30 the cross sum 17 is calculated from the minute count of the tactical time and the character count. In the column watchword, starting at **bb,** 17 cells are counted to the right, which takes you to column **ee**.

38. Starting at column 19, which is marked by **ee**, the cipher text is to be entered column-wise into the framed writing area, whereas you follow the order 19, 20, 21, …, 25, 1, …, 18.

39. After entering, the plain text is row-wise taken out of the cipher page while the cipher position, which is framed in **aa** and **ee**, has to be deciphered according to the place name alphabet (compare number 16c).

40. In case that counting the writing cells according to number 35 reaches the bottom row in the cipher page and the counting is

continued on the first writing cell on the top row, then between the last writing cell and the starting cell of the message an empty space appears in the middle of the cipher page. In this case, during the column-wise entering of the cipher text, which always begins in the top row of the cipher page, in each column the empty space in the middle of the cipher page has to be skipped. Compare image 4 that is based on the following **example**:

Plain text:
1721 –
Auflärungsflieger meldet vor Bataillons-
abschnitt feindliche Bereitstellung.

Message key: **accc - bwak**

Text to be entered into the plain text:

saturrnn aufklflieger meldet vor btl
absqnitt fdl bereitstellung kkaaese.

Message length:	64 characters
Cross sum:	2 + 1 + 6 + 4 = 13
Take-out column:	12
Cipher text:	**1721 – 64 – bwak –**
	gdesl llllr itnia uenbl
	etekm teare nabtu sknrr
	alege tafto sfetf budik
	rvqs

Deciphering:

Message key: **bwak = accc**

The starting cell **accc** is looked up in the cipher page and the line **ad** crossed out as the upper limit of the writing area. Beginning at the starting cell 64 writing cells are counted according to the character count. Hereby **eeca** is found to be the last writing cell of the message. Hence, for the downward limitation of the writing

area the row **ca,** beginning at column **db**, and the row **ea**, from its beginning to column **db**, are crossed out.

Cross sum: 2 + 1 + 6 + 4 = 13
Take-out column: 12

Now, beginning with column 12, the cipher text is entered column-wise into the cipher page. The entering begins in each column at the top border of the cipher page. In each column the area in the middle of the cipher page between the lower and the upper limitation of the writing area needs to remain blank. When the entering is finished, beginning with the row of the starting cell, the plain text will be taken out row-wise.

IX. Labeling of the Cipher Keys

41. **Indicator groups**, which can be extracted from the raster patterns, serve for the labeling of **certain** keys.

42. As a matter of principle, indicator groups are to be used as rarely as possible. Per cipher key type and day four indicator groups are available, which have to be used alternately.

43. If the labeling of an in a message supplied key is necessary then this message receives an indicator group, which is entered unchanged into the message head behind the character count. The same indicator group has to be used in all parts of multipart messages.

44. Example of a message head with indicator group:

Tactical Time	Character Count		Indicator Group	Message Key
1203	- 77	-	k a x	t u z d - *(not readable)*

X. Penal Provisions

H. Dv. 99, M. Dv. Nr. 9, L. Dv. 99, Ziffer 24.

45. Breaches of this order and the additional orders are to be prosecuted. If no judicial prosecution is necessary it needs to be investigated if a disciplinary punishment has to happen according to the Armed Forces Disciplinary Punishment System (H. Dv. 3/9, M. Dv. Nr. 130,L. Dv. 3/9) or the Government Authorities Punishment System.

§ 88 R St GB.

46. State secrets in terms of the regulations of this chapter are writings, drawings, other items, facts or news about it, whose confidentiality is from foreign governments is necessary for the wellbeing of the empire, particularly in the interest of national defense.

    Treason in terms of the regulations of this chapter is committed by somebody who endangers the wellbeing of the empire on purpose, who lets the state secret reach others, particularly foreign governments or somebody, who is active for a foreign government or informs publicly.

§ 92 M St GB.

47. He, who purposely does not follow orders in official businesses and by doing so purposely or negligently causes considerable detriment, a danger for human lives or to a significant extent for other's property or danger for the security of the empire or the repercussiveness of the armed forces, will be punished with aggravated arrest for no less than one week or with imprisonment or fortress detention for up to 10 years, away at wars for up to 15 years or for life.

    A negligently committed act leads to imprisonment for up to two years, away at wars for up to three years.

Image 1 for number 24

Image 2 for numbers 28 – 32

Image 3 for numbers 33 – 39

Image 4 for number 40

Armed Forces High Command (not readable), 18 October 1944
Chief Armed Forces Communication
Ag WNV Nr.1908/44 geh.

Conc.: Simplification of the cipher system ***Secret!***

To

2. The determination of the take-out column by using the cross sum out of minute count and character count has to be omitted everywhere. The cipher clerk chooses the take-out column always freely in the future.
3. For the communication units of the armed forces the minimum length of messages will be reduced from 60 to 45 characters.

Hereto is ordered:

To 1: a) The enciphering is started with the take out of the secret text from the cipher page in an arbitrary, from message to message changing column. However, the column of the starting cell must not be used as the take-out column.

Apart from that, for the selection of the take-out column by the cipher clerk apply the same principles as for the selection of the starting cell. There must not at all be any preference for certain columns (e. g., the first column in the raster pattern or the column number 1). Also, following a certain sequence for the selection of the take-out column is most strictly prohibited.

b) The take-out column is given in the message key by the letter pair of the column watchword above it (5th and 6th character of the message key).

c) The plain message key, that consequently indicates the position of the message's starting cell and the take-out column

e. g.	b b a e	c a
	|	|
	starting cell	take-out column

are enciphered by using the character exchange table, and namely so that the encrypted message key consists of six different characters.

Example:

b b a e c a	=	t u z d o b
plain message key	:	enciphered message key

d) The encrypted message key is entered into the message head, namely the 6 characters of the message key are split into a group of 4 characters and one of 2 characters.

notation of the message head: 1203 – 77 – t u z d ob –

keying: 1203 1203 – 77 77 – tuzd tuzd ob ob –

To 2: a) The minimum length of the messages has to be 60 characters for the communication of the communication troops and 45 characters for the communication of the communication units of the armed forces. Messages that don't reach the minimum length have to be filled up to at least 60 resp. 45 characters by adding optional words.

b) A dropping below the minimum length of 45 characters endangers the security of the key to a large extent. For that reason, under any circumstances the compliance to the numbers above has to be enforced.

per pro

(signature not readable)

General of the Communications Troop and
Chief of Communications of the Armed Forces

Distributor:

Bis z.d.Div.Kdos. *(partially not readable)*

Ob West: Distributor C.