

*for Navy*

CIPHER ATTACHMENT 42  
(SZ 42, Vol. III)

*NS*

Instructions for Use of Keys and Key Materials.

Contents:

- I. The Teleprinter Message Key, the Message Key Sheet and the Reading Table
- II. The Teleprinter Basic Key and the Motion Wheel Key
- III. The Plaintext Limitation.
- IV. Security Measures.

I. The Message Key, Message Key Sheet and Reading Table.

The Message Key serves to determine the initial setting of the 12 cipher wheels and a new key is selected for each secret transmission. The practical procedure is that given in the Instructions for Operation under III. The position of each of the 12 cipher wheels is designated by a number. This number appears in the appropriate window of the locking cover. Setting of each wheel is accomplished by turning the finger-wheel projecting through the cover.

The sending station selects the message key according to regulations and the receiving station must set its machine to correspond.

To transmit the selected initial setting to the correspondent the numbers are converted into letters.

This conversion is by use of the Message Key Sheet. This sheet has in the first column at the left the letters of the alphabet. Columns 1 - 12 at the right of this alphabet contain the possible settings of the 12 wheels expressed in numbers in random order. The initial position of the wheels is then represented by 12 letters. The first letter transmitted represents the setting of the 1st wheel, the second letter that of the 2nd wheel, &c.

To facilitate reading off the items and checking them the Message Key Sheet is placed in a frame called Reading Table 40. The riders, which can be slid along each column of figures, can be held in any position by the locking arrangement. Thus the association of key letters and numbers is easily set up and read off.

The selection by the sending station of Message Key letters according to "Provisional Operating Instructions for SZ 42" Section IIIa is accomplished by sliding all the riders in random fashion, transmitting the associated letters to the correspondent station which sets them up in order on its reading table and thus obtains the corresponding numbers for setting its cipher wheels.

II. The Basic Key and the Motion Wheel Key.

While the Message Key for SZ 42 can be set externally and the operating personnel makes the selection and setting, the other keying arrangements of the device are not accessible without further ado. This refers to the setting of the lugs on the 12 cipher wheels. To reach these the locking cover with safety lock must first be opened. The key to this lock is to be in the hands of the duty officer of the station and he alone is to have access to this keying part of the device and is to effect the settings at appointed times according to the following instructions. Involved are:

- The BASIC KEY, to be changed once a month, and
  - The Motion Wheel Key, to be changed daily.
- The requisite key material is distributed regularly to all offices concerned by the Key Office of C.K.H./In. 7. If necessary it should be requested from there.

Defol Entry, Form 10  
 5-52-473 TL 11.2

The keying mechanism is as follows:  
 Each of the 12 wheels has around its edge a series of lugs which may be "OUT" or "IN"; when OUT they are active and are then designated in the sheets of Basic and/or Motion Wheel Keys by †.

When "IN", i.e. inactive, they are represented by "o". On the Number strip of each wheel there is a number opposite each lug and this number on the key sheet shows a † or a "o" according to whether the lug is to be in active or inactive position.

The Basic Key is set on wheels 1 - 5 and 8 - 12.

The Motion Wheel Key is set on wheels 6 and 7 according to the group valid for the day on the Motion Wheel Sheet. The setting is as above.

The setting, which must be made in the presence of the officer in charge of the station is accomplished with least loss of time if the following rules are observed (because of illumination of the key field when the machine is operating setting should be made with the Operating Switch on "AUS" (off)). An officer dictates and a man sets the lugs using the stylus provided with the machine and repeating each setting as he makes it. A dictates, B sets; the Basic Key for wheel 1 is assumed to be:

Lug	:	01	.	02	.	03	.	04	.	05	.	06	.	07	.	08	.	09	.	10	&c
Wheel 1:		o		o		+		o		+		o		+		+		+		o	&c.

o = "No lug" (inactive position)  
 + = "Lug" (active position).

A: "Wheel 1, start with 01 - twice no lug"  
 B: "Twice no lug" (pushes two lugs in)

A: "Lug"  
 B: "Lug" (sets up one lug)

A: "No lug"  
 B: "No lug" (pushes lug in)

A: "Lug"  
 B: "Lug" (sets up lug)

A: "No lug"  
 B: "No lug" (pushes lug in)

A: "Thrice lug"  
 B: "Thrice lug" (sets up 3 lugs)

A: "No lug"  
 B: "No lug" (pushes lug in) &c.

All wheels to be set are treated in this fashion. Now and then the setter calls off the number of the lug he has just set as a check and the reader checks by his sheet. The setter must be careful not to let his stylus slip and disturb the lugs on an adjacent wheel already set.

When all wheels have been set the setter should call off all lugs while the officer checks by the sheet. This is very important since a single wrong lug in one's own or in correspondent's machine will result in several false letters of deciphered text or may even make the text entirely unintelligible.

When setting is completed, the lid is replaced and locked. The time for setting daily keys will be given in orders. at present 09.00 o'clock is found to be a period of relatively low traffic density.

## III. The Plaintext Limitation

The Plaintext Limitation (Klartextfunktion) represents an additional security measure. The machine is, however, secure against unauthorized decipherment even without the Plaintext Limitation if used strictly according to regulations. The Plaintext Limitation can be switched on or off by a switch located under the hood in a box at the upper right. This box has a screwed on lid marked "KT-Schalter".

When this switch is thrown to "KY" the Limitation is on. This setting must be used only by express command. When on, the movement of wheels 1 - 5 is affected by certain letters of the plaintext, hence the course of the wheels is different from what it would be without the Limitation. The KT switch must therefore be in the same position at both stations.

With the Plaintext Limitation switch on "KY"; without Limitation switch on "O".

It is better not to use the Limitation if there is any considerable interference. All machines are shipped from the factory with the KT switch off, however its position should always be checked before using a new machine.

## IV. Security measures.

If for any reason there is danger that the SZ 42 may fall into enemy hands and there is not adequate time to bring the whole machine to a safe place, the locked cover is to be opened, the two hexagonal screws at the front removed and the so-called Cipher Part taken out. This must be taken to safety or in any event not be permitted to fall into enemy hands. If no alternative remains this part must be destroyed (explosive charge, &c.)

Reference is made to Cipher Teleprinter Regulations (H.Dv.g.422 and/or L.Dv. 704/3b and/or M.Dv. 924a.)

Army High Command  
 (Chief or Army Ordnance and  
 Commander of Replacement Army)  
 Army Ordnance Office Testing Group 7  
 (signed) Henigst  
 Colonel and Section Chief.