Excerpt of TM-11-380, 1942

8. **Preparation of Cipher Key Lists**.

a. In order that Signal Operation Instructions may indicate in an absolutely clear and unambiguous manner the arrangement of the internal keying elements, it is essential that definite forms and procedures be followed in preparing the Cipher Key Lists.

b. To prepare a table of pin settings which will have a favorable randomizing effect on the shifting of the alphabets proceed as follows:

(1) Prepare a chart of the key wheels by listing in alphabetical order, starting with A, the letters appearing on the face of each wheel : the first wheel, A to Z, the second wheel A to Z omitting W, the third wheel A to X omitting W, the fourth wheel A to U, the fifth wheel A to S, and the sixth wheel A to Q.

(2) Prepare a set of 156 lettered cards or counters, 78 of which are marked R and the remainder L. Shuffle the cards or counters thoroughly and draw out one at a time, marking with a dash the position of the pins successively, starting with A on wheel number 1, in accordance with the letter drawn : if R, make a dash to the right of the letter, if L, make a dash to the left. (See sample table on page 17). This procedure insures a perfectly random assortment in which from 40 to 60 per cent of the pins are in the effective position

c. To prepare a table of favorable settings for the drum bar lugs proceed as follows :

(1) Mark off six columns of 1/4-inch cross-section paper and number the columns from 1 to 6. These numbers denote the effective positions for lug settings. Number the rows of the form

from 1 to 27, starting at the top. These numbers denote the drum bars in the order in which they become effective during an operating cycle of the machine.

(2) Select any set of six numbers, subject to the following limitations:

(a) Their sum must not be less than 28 nor more than 39;
(b) Three of the numbers should be odd and three even;
(c) No one number should be greater than 13;
(d) There should be a more or less uniform progression from the lowest to the highest number;
(e) The numbers must be so selected that the various combinations of one or more will, when added together, yield all the numbers from 1 to 27, inclusive, bearing in mind that the effect of two effective lugs on the same drum bar is 1. For example, the numbers 4 and 8 in columns 4 and 5, respectively, of Table 2 below total 11, not 12, because there are two effective lugs on bar number 10.

An example of such a set of numbers is 1, 2, 3, 4, 8, 11.

The foregoing limitations are imposed to prevent any tendencies toward monoalphabeticity in the shifting of the alphabets, and to add to the difficulties of enemy cryptanalysts in making a mathematical analysis of the messages.

(3) The numbers are now inserted in the chart in such a manner as to indicate the number of effective lugs, in each position from 1 to 6, on the bars forming the drum bar cage. Make an X in cell 1 of column 1, in cells 2 and 3 of column 2, in cells 4-6 of column 3, in cells 7-10 of column 4, in cells 10-17 of column 5, and in cells 17-27 of column 6. (See sample Table 2, below). Each X denotes the position of an effective lug. Unused lugs are left in the zero or ineffective position. The columns of the chart can be transposed in

any order to form additional keys which may all be used. It is preferable, however, not to use such keys in succession, but to space their use over several weeks.

d. Having prepared the tables of settings for both the key wheel pins and the drum bar lugs, it is desirable to provide a means by which holders of the machine can check the accuracy of their settings. This is done by adjusting the machine in accordance with the charts and enciphering the letter A twenty-six times, starting with the key wheels aligned on the letters AAAAAA. The twenty-six cipher equivalents are included with the two tables as a check, so that, having made his adjustments, the holder of a machine may test their accuracy by himself enciphering twenty-six A's with the key wheels set initially at AAAAAA. Any deviation from the 26-letter check indicates that an error was made in the settings and necessitates a recheck of the entire adjustment. The 26-letter check should be derived for and included with every pair of keying tables issued and will be given in the Cipher Key List merely as a sequence of letters such as the following:

26-letter check

T K H R X C U Y T K N O I K R J N T A D T A I V P M

e. An example of the form in which the two tables referred to in subparagraphs b and c above will appear in the Cipher Key Lists is shown in Tables 1 and 2 on pp. 17-18. In Table 1, "A-" indicates that the pin designated by the letter A on the key wheel in question is to be pushed to the right, while "-A" indicates that the pin designated by the letter A is to be placed in the left position. In Table 2 it is indicated that the left-hand lug on bar number 1 (see number ring (28)) is in the number 1 position, the left-hand lug on bars number 2 and 3 are in the number 2 position, etc. The zero positions are not shown on the table since it is obvious that a lug not in one of the numbered positions must be in a zero position. These positions are determined by reference to the number plate (27) at the rear of the drum bar cage.

TABLE 1- *Position of Key Wheel Pins*
Period of (date) to (date)

No.1 (26)	No.2 (25)	No.3 (23)	No.4 (21)	No.5 (19)	No.6 (17)
A-	-A	A-	-A	-A	A-
B-	-B	B-	-B	B-	B-
-C	-C	-C	C-	-C	-C
D-	D-	-D	-D	D-	D-
-E	E-	-E	E-	E-	-E
-F	-F	-F	F-	F-	-F
-G	G-	G-	-G	-G	-G
H-	-H	H-	H-	H-	H-
I-	-I	-I	I-	I-	-I
-J	J-	J-	-J	-J	-J
K-	K-	-K	-K	-K	K-
-L	L-	L-	-L	-L	-L
M-	-M	M-	M-	M-	-M
N-	-N	N-	N-	N-	N-
-O	O-	-O	-O	-O	O-
-P	-P	-P	P-	P-	-P
-Q	-Q	-Q	-Q	-Q	Q-
-R	R-	R-	-R	-R	
S-	S-	S-	S-	S-	
T-	-T	T-	T-		
-U	U-	U-	U-		
V-	-V	V-			
W-	X-	X-			
-X	-Y				
-Y	-Z				
-Z					

TABLE 2-*Position of Drum Bar Lugs*
Period of (date) to (date)

	1	2	3	4	5	6
1	X					
2		X				
3		X				
4			X			
5			X			
6			X			
7				X		
8				X		
9				X		
10				X	X	
11					X	
12					X	
13					X	
14					X	
15					X	
16					X	
17					X	X
18						X
19						X
20						X
21						X
22						X
23						X
24						X
25						X
26						X
27						X