Excerpt of TM-11-380, 1943

15. **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. (Table 1, page 36). 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) Of the six numbers selected, at least two, and no more than four, must be even; a set of five even numbers and one odd number (or five odd numbers and one even number) must never be choosen.

(c) The six numbers must be well scattered from 1 to 13, inclusive.

(d) The same set of six numbers must not be used a second time as long as other sets are available.

(3) Rearrange the numbers so that they will appear in random order.

(4) Substract 27 (the number of bars on the drum) from the total of the six numbers. The condition is described as overlap when the two lugs (paragraph 4a(2)) on the same bar are placed in effective positions.

(5) Distribute the overlaps among the numbers according to the following rubes:

(6) The numbers must be so selected and the overlaps so placed that a number or the sum of certain numbers will yield all the values from 1 to 27 incluse. The numbers 1 and 2 must always be choosen, otherwise all numbers from 1 to 27 inclusive cannot be obtained.

(7) The effective lugs are now entered on the prepared chart, lugs in the same column being placed on successive drum bars as far as possible.

d. After the tables of settings for both the key wheel pins and the drum bar lugs are prepared, it is desirable to provide a means by which operators of the machine can check the accuracy of their settings. This is done by adjusting the machine according to 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, after his adjustments have been made, the operator of a machine may test his accuracy by enciphering twenty-six A's himself, 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 a recheck of the entire adjustment must be made. The 26-letter check should be derived for, and included with every pair of keying tables issued. It 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 15b and 15c above will appear in the Cipher Key Lists is shown in Tables 1 and 2 on pp. 36-37. In Table 1, "A-" indicates that the pin designated by the letter A on the key wheel 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 3 position, and the right-hand lug on bars number 2 is in the number 6 position, but the left-hand lug not being shown is in the zero or non-effective position, etc. The zero positions are not shown on the table—a lug not in one of the numbered positions is in a zero position. These positions are

determined by reference to the number plate (27) at the rear of the drum bar cage.

SIGNAL COPRS

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					

Converter M-209-B

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

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

Steps as in paragraph 15c.

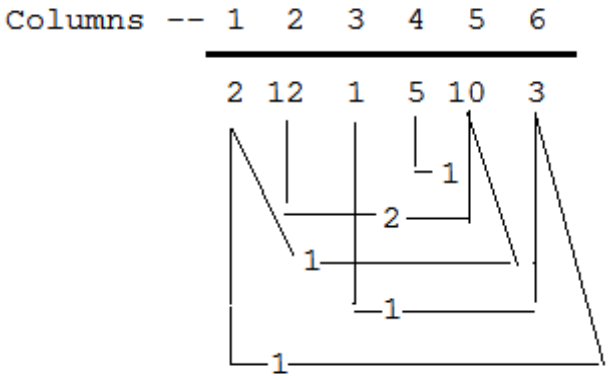
(1) See box, table 2.

(2) Numbers chosen at random : 1, 2, 3, 5, 10, 12.

(3) Numbers are transposed : 2, 12, 1, 5, 10, 3.

(4) 27 is substracted from their total to find number of overlaps : 2 + 12 + 1 + 5 + 10 + 3 = 33 – 27 = 6.

(5) Overlaps are distributed :



(*a*) All of the six numbers are involved.

(*b*) Column 1 is overlapped with Column 5 and 6 (columns separated).

Column 2 is overlapped with Column 5 (columns separated).

Column 3 is overlapped with Column 6 (columns seaparated).

Column 4 is overlapped with Column 5 (columns side by side).

(*c*) Small overlaps are used in preference to one large one.

(6) Notice that from the numbers, or combinations of them, it is

possible to obtain all values from 1 to 27 inclusive.

(7) Effective lugs are marked on the chart prepared in step 1. (Table 2).