## PREPARATION OF PIN AND LUG SETTINGS

## I. Pin Settings

a. Prepare a table of the rotors by listing, in alphabetical order, the letters appearing on the face of each rotor: the fist rotor, A to Z ; the second rotor A to Z , ommiting W ; the third rotor A to X , omitting W ; the fourth rotor A to U ; the fifth rotor A to S ; and the sixth rotor A to Q.
b. Prepare a set of 156 cards, 78 of which are marked R (right) and the remainder L (left). Shuffle the cards thoroughly and draw one at a time. Start with A on rotor number 1, and prepare the key list in accordance with the cards drawn: If a card bears an L , cross out the letter; if a card bears an R, do not cross the letter. Only letters with effective pins are then shown in the settings (tables I and IV). More than six consecutive effective or noneffective pins on any rotor must be rearranged in order to prevent use of such a sequence. A random arrangement, in which from 40 to 60 percent of the pins are in the effective position, is assured by this method.

## 2. Lug Settings *

To prepare a table of favorable lug settings, proceed with the following steps in the order given:
a. SELECTION OF NUMBERS. Select a set of six numbers from either group A or group B (pars. 1 and 2, app. III). Sets of numbers selected from group B must not exceed 10 percent of the total sets selected. The sets are selected at random from the table. Sets of numbers from group B should be used at irregular intervals and should not succeed each other in key lists.
b. REARRANGEMENT OF NUMBERS. Rearrange the numbers so that they appear in random order. Each number indicates the number of lugs to be placed in one of the effective positions on the drum. Lug placements may be randomized in each column as long as the necessary overlaps are obtained and all other requirements met.
c. DISTRIBUTION OF OVERLAPS. Although there are tow lugs on each bar, the bar can be moved to the left only once for each rotation of the drive knob. When both lugs of the same bar are in effective positions, the condition is described as an overlap. The total number of overlaps produced by a given set of numbers is found by substracting 27 (the number of bars on the drum) from the sum of the six numbers

[^0]In that set. The number of overlaps required for each set of numbers has been calculated, and is given with the sets (pars 1 and 2, app. III). The following rules offer a general guide for distributing the overlaps (some deviation may be made from all except the rule in (4) below, which must always be observed):
(1) Most of the six positions on the drum should be involved in the overlaps.
(2) Overlaps should occur between positions which are separated and between positions which are side by side.
(3) A small number of overlaps should occur between several positions rather than a large number of overlaps between only two positions.
(4) There will never be more than four overlaps between any two positions. It is permissible, however, for a position to have a combined overlap of more than four. (Positions 5 in table III has a combined overlap of 5.)

Note. When all the lugs in a particular position on the drum are overlapped, the condition is described as a complete overlap. Column 2 in table III illustrates a complete overlap. During one rotation of the drive knob, bars 6 and 7 may both be moved by the operation of either rotor 2 or 5 or by rotors 2 and 5 operating together. Thus when an effective pin on rotor 5 comes into play, rotor 2 can have no additional effect upon the process of encipherment. For this reason, the 26 -letter check cannot insure that all the pins on rotor 2 are
correctly set, and the rotor must be checked independly. Do not avoid the use of a complete overlap in lug settings; the occasional use of settings of this type adds to the security of the system. It is not advisable, however, to have more than one position on the drum completely ovelapped in any setting. Whenever a setting contains a complete ovelap, an asterisk will be placed beside the number of the corresponding rotor in the pin setting, directing attention to a footnote which warns the operator to "check this rotor thoroughly." (The symbol (*) is used in this manual.)

## d. CHECKING PLACEMENT OF OVERLAPS. The

 overlaps must be so placed that a single number (representing the number of lugs in a given position on the drum) or the sum of any two, three, four, five, or all six of the numbers, yields all the values from 1 to 27 , inclusive. Remember that the result of two effective lugs on the same drum bar is one. For example, in table III there are seven effective lugs in column 6, and eight effective lugs in column 5, given a total of fifteen. However, two of the effective lugs are on one bar; thus the effect of one lug is canceled, yielding a result of only fourteen. Hence, the proper total for columns 5 and 6 is fourteen (eight plus seven minus one) and not fifteen.e. PREPARING LUG SETTING WORK SHEET. The effective lugs (represented by X's) are now entered on a work sheet similar to that shown in table III; lugs in the same column are placed on successive drum bars in as many cases as the overlap condition permits. (If the overlap condition makes it necessary
or more convenient to place the lugs on bars which are separated, it is permissible to do so.) The completed work sheet should be checked carefully for accuracy with the results of the previous steps. The zero positions need not be shown on this chart.
f. PREPARING LUG SETTING TABLE. Convert the lug positions set up on the work sheet to a form similar to that illustrated in table IV, by writing the numbered positions of the lugs opposite the number representing the drum bar. Determine the positions by referring to the number plate (29) at the rear of the drum-bar cage.
g. COMPLETE PREPARATION OF LUG SETTING. The following example serves to illustrate the prepartion of a lug setting. The steps are numbered to correspond to the steps described in $a$ trough $d$ above.
(1) Select a set of numbers from group A.

$$
1,2,4,7,8,11 \quad \text { Overlaps }=6
$$

(2) Rearrange the numbers.

$$
11,2,4,1,8,7
$$

(3) Distribute the overlaps. Positions:

(a) Five of the six positions are involved.
(b) Positions side by side: Positions separated: 5 and 6

1 and 6
2 and 5
3 and 5
(c) A small number of overlaps occur between several positions rather than a large number of overlaps between only two positions.
(d) All values from 1 to 27, inclusive, are obtained. For example:

1 is given by position 4
2 is given by position 2
3 is given by positions 2 and 4
4 is given by position 3
5 is given by positions 3 and 4
6 is given by positions 2 and 3, and so on.

## 3. Purpose

The foregoing limitations are imposed to provide the greatest amount of security possible in the shifting of the alphabets, and to add to the difficulties of enemy cryptanalysts engaged in making a mathematical analysis of the messages.

Table III. Position of drum-bar lugs work sheet

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

Table IV. Suggested form publishing keying information contained in tables I and II
(SAMPLE) PIN AND LUG SETTING
(Effective date)
Rotor Pin Setting
Drum-Bar
Lug Setting
Drum $\quad$ Lug bar Position

| 1 | $0-4$ | 1 | $2^{*}$ | 3 | 4 | 5 | 6 |
| ---: | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 2 | $3-0$ | A | A | A | -- | -- | A |
| 3 | $3-0$ | B | -- | B | -- | B | B |
| 4 | $3-5$ | -- | -- | -- | C | -- | -- |
| 5 | $3-5$ | D | D | -- | -- | D | D |
| 6 | $2-5$ | -- | E | -- | E | E | -- |
| 7 | $2-5$ | -- | -- | -- | F | F | -- |
| 8 | $0-5$ | -- | G | G | -- | -- | -- |
| 9 | $0-5$ | H | -- | H | H | H | H |
| 10 | $0-5$ | I | -- | -- | I | I | -- |
| 11 | $5-6$ | -- | J | J | -- | -- | -- |
| 12 | $0-6$ | K | K | -- | -- | -- | K |
| 13 | $0-6$ | -- | L | L | -- | -- | -- |
| 14 | $0-6$ | M | -- | M | M | M | -- |
| 15 | $0-6$ | N | -- | N | N | N | N |
| 16 | $0-6$ | -- | O | -- | -- | P | O |
| 17 | $1-6$ | -- | -- | -- | P | -- | -- |
| 18 | $1-0$ | -- | -- | -- | -- | -- | Q |
| 19 | $1-0$ | -- | R | R | -- | S |  |
| 20 | $1-0$ | S | S | S | S |  |  |
| 21 | $1-0$ | T | -- | T | T |  |  |
| 22 | $1-0$ | -- | U | U | U |  |  |
| 23 | $1-0$ | V | -- | -- |  |  |  |
| 24 | $1-0$ | W | X | X |  |  |  |
| 25 | $1-0$ | -- | -- |  |  |  |  |
| 26 | $1-0$ | -- | -- |  |  |  |  |
| 27 | $1-0$ | -- |  |  |  |  |  |

26-Letter Check:

## NIHTZ DXAJJ KVSIT HKNKO NAGZR I

* Check this rotor thoroughly. An error in setting the pins on this rotor may not appear in the 26 -letter check but will appear as an error in the message; therefore, it is important that the operator check the position of each pin on this rotor to insureits conforming to the position shown in this pin setting.
The indicator for this "Pin and Lug Setting" is VC.


# SETS OF NUMBERS AND OVERLAPS FOR LUG SETTINGS 

## I Group A



| Sets | Overlaps | Sets | Overlap |
| :---: | :---: | :---: | :---: |
| 1235912 | 5 | 12351013 | 7 |
| 1235813 | 5 | 12361012 | 7 |
| 1236911 | 5 | 1236913 | 7 |
| 1236812 | 5 | 12371011 | 7 |
| 1236713 | 5 | 1237912 | 7 |
| 1237910 | 5 | 1237813 | 7 |
| 1237811 | 5 | 12451012 | 7 |
| 1245911 | 5 | 1245913 | 7 |
| 1245812 | 5 | 1246813 | 7 |
| 1245713 | 5 | 1246912 | 7 |
| 1246910 | 5 | 12461011 | 7 |
| 1246811 | 5 | 1247911 | 7 |
| 1246712 | 5 | 1247812 | 7 |
| 1247810 | 5 | 1248910 | 7 |
| 12341112 | 6 | 12351113 | 8 |
| 12341013 | 6 | 12361112 | 8 |
| 12351012 | 6 | 12361013 | 8 |
| 1235913 | 6 | 12371012 | 8 |
| 12361011 | 6 | 1237913 | 8 |
| 1236912 | 6 | 12451112 | 8 |
| 1236813 | 6 | 12451013 | 8 |
| 1237911 | 6 | 1246913 | 8 |
| 1237812 | 6 | 12461012 | 8 |
| 12451011 | 6 | 12471011 | 8 |
| 1245912 | 6 | 1247912 | 8 |
| 1245813 | 6 | 1247813 | 8 |
| 1246812 | 6 | 1248911 | 8 |
| 1246911 | 6 | 12351213 | 9 |
| 1246713 | 6 | 12361113 | 9 |
| 1247910 | 6 | 12371112 | 9 |
| 1247811 | 6 | 12371013 | 9 |
| 12341113 | 7 | 12451113 | 9 |
| 12351112 | 7 | 12461013 | 9 |


|  | rlaps |  |  | Sets | Overlaps |
| :---: | :---: | :---: | :---: | :---: | :---: |
|  | 2461112 | 9 | 12 | 2471013 | 10 |
|  | 2471012 | 9 |  | 248913 | 10 |
|  | 247913 | 9 | 12 | 2481012 | 10 |
|  | 2481011 | 9 |  | 2371213 | 11 |
|  | 248912 | 9 | 12 | 2461213 | 11 |
| 12 | 2361213 | 10 | 12 | 247113 | 11 |
|  | 2371113 | 10 | 12 | 2481112 | 11 |
| 12 | 2451213 | 10 | 12 | 2481013 | 11 |
|  | 2461113 | 10 |  | 2471213 | 12 |
|  | 2471112 | 10 |  | 2481113 |  |

## 2. Group B

|  |  | Sets |  | Overlap |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 1 | 1 | 2 | 4 | 9 | 12 | 2 |
| 1 | 1 | 2 | 4 | 8 | 13 | 2 |
| 1 | 1 | 2 | 5 | 9 | 11 | 2 |
| 1 | 1 | 2 | 5 | 8 | 12 | 2 |
| 1 | 1 | 2 | 5 | 7 | 13 | 2 |
| 1 | 1 | 3 | 4 | 9 | 11 | 2 |
| 1 | 1 | 3 | 4 | 8 | 12 | 2 |
| 1 | 1 | 3 | 4 | 7 | 13 | 2 |
| 1 | 1 | 3 | 5 | 9 | 10 | 2 |
| 1 | 1 | 3 | 5 | 8 | 11 | 2 |
| 1 | 1 | 3 | 5 | 7 | 12 | 2 |
| 1 | 1 | 3 | 5 | 6 | 13 | 2 |
| 1 | 1 | 3 | 6 | 8 | 10 | 2 |
| 1 | 1 | 3 | 6 | 7 | 11 | 2 |
| 1 | 2 | 2 | 3 | 9 | 12 | 2 |
| 1 | 2 | 2 | 3 | 8 | 13 | 2 |
| 1 | 2 | 2 | 4 | 9 | 11 | 2 |
| 1 | 2 | 2 | 4 | 7 | 13 | 2 |
| 1 | 2 | 2 | 5 | 9 | 10 | 2 |

Sets Overlaps


| Sets | Overlaps | Sets O | Overlap |
| :---: | :---: | :---: | :---: |
| 11341011 | 3 | 124779 | 3 |
| 1134912 | 3 | 11251012 | 4 |
| 1134813 | 3 | 1125913 | 4 |
| 1135911 | 3 | 11341012 | 4 |
| 1135812 | 3 | 1134913 | 4 |
| 1135713 | 3 | 11351011 | 4 |
| 1136910 | 3 | 1135912 | 4 |
| 1136811 | 3 | 1135813 | 4 |
| 1136712 | 3 | 1136911 | 4 |
| 1223913 | 3 | 1136812 | 4 |
| 12241011 | 3 | 1136713 | 4 |
| 1224912 | 3 | 1224913 | 4 |
| 1224813 | 3 | 12251011 | 4 |
| 1225911 | 3 | 1225912 | 4 |
| 1225812 | 3 | 1225813 | 4 |
| 1225713 | 3 | 1226911 | 4 |
| 1226910 | 3 | 1226713 | 4 |
| 1226811 | 3 | 12331012 | 4 |
| 1226712 | 3 | 1233913 | 4 |
| 12331011 | 3 | 12351010 | 4 |
| 1233912 | 3 | 1236613 | 4 |
| 1233813 | 3 | 1237711 | 4 |
| 12341010 | 3 | 123799 | 4 |
| 1236612 | 3 | 1244911 | 4 |
| 123699 | 3 | 1244713 | 4 |
| 1237710 | 3 | 124699 | 4 |
| 1244910 | 3 | 1247710 | 4 |
| 1244811 | 3 | 11251013 | 5 |
| 1244712 | 3 | 11341013 | 5 |
| 1244613 | 3 | 11351012 | 5 |
| 1245513 | 3 | 1135913 | 5 |
| 124599 | 3 | 11361011 | 5 |
| 1246611 | 3 | 1136912 | 5 |


| Sets Overlaps |  | Sets O | Overlap |
| :---: | :---: | :---: | :---: |
| 236813 | 5 | 11361112 | 7 |
| 12241013 | 5 | 11361013 | 7 |
| 12251012 | 5 | 12241213 | 7 |
| 1225913 | 5 | 12251113 | 7 |
| 1226912 | 5 | 12261112 | 7 |
| 1226813 | 5 | 12261013 | 7 |
| 12331013 | 5 | 12361111 | 7 |
| 12341111 | 5 | 12441112 | 7 |
| 12361010 | 5 | 12441013 | 7 |
| 1237712 | 5 | 12451111 | 7 |
| 12441011 | 5 | 1247713 | 7 |
| 1244912 | 5 | 12471010 | 7 |
| 1244813 | 5 | 1248811 | 7 |
| 1246613 | 5 | 11361113 | 8 |
| 1247711 | 5 | 12261113 | 8 |
| 124799 | 5 | 12351212 | 8 |
| 12488 | 5 | 12441113 | 8 |
| 11351112 | 6 | 12461111 | 8 |
| 11351013 | 6 | 11361213 | 9 |
| 11361012 | 6 | 12261213 |  |
| 1136913 | 6 | 12361212 | 9 |
| 12241113 | 6 | 12441213 | 9 |
| 12251112 | 6 | 12451212 | 9 |
| 12251013 | 6 | 12471111 | 9 |
| 1226913 | 6 | 1248813 | 9 |
| 12331113 | 6 | 12261313 | 10 |
| 12351111 | 6 | 12351313 | 10 |
| 1237713 | 6 | 12481111 | 10 |
| 12371010 | 6 | 12361313 | 11 |
| 1247712 | 6 | 12471212 | 11 |
| 124899 | 6 | 12371313 | 12 |
| 11351113 | 7 |  |  |


[^0]:    * This dicussion pressuposes a thorough understanding of paragrahs 63 and 64c.

