R.I.P. 77 — Instructions for M-5 (Orange Diplomatic "B" Machine) — (PURPLE)

Source: NARA, College Park, Md., Record Group 38, Radio Intelligence Publications (R.I.P.), Reference: 370 27/18/06, Box 40

Editor: Frode Weierud, Crypto Cellar Research
Web Site: www.cryptocellar.org

Version: 19 February 2019

Reg #1

TABLE OF CONTENTS and List of Effective Pages

Table of Contents and List of Effective Pages - contd.

CHAPTER I

A. GENERAL

The cryptographic system covered by this publication has been arbitrarily labeled "Purple". It is a machine cipher system used by the Japanese Foreign Office and Diplomatic Officials on important foreign stations for diplomatic correspondence. In the instructions issued by the Japanese Foreign Office from time to time, this system has been designated "B" in order to distinguish it from a similar though less complex diplomatic system known as the "A". This latter system we have designated the "Red". It will be noted that the Japanese Foreign Office in issuing cryptographic changes and instructions from time to time, generally covers both "A" and "B" in the same dispatch. A list of the points holding the purple system is shown under Appendix 6B.

The Purple System was broken cryptographically to such an extent that it has been possible to reconstruct the cipher machine. Various printed data and instructions which are a part of the system are being compiled and where the information is complete enough, in the same form and manner as the originals held by the Japanese. The reconstructed cipher machine (built for deciphering only) is titled R.I.P. 72.

The Purple System as far as is known at present consists of the following elements:

1. The cipher machine.

2. A book, Section I containing instructions, indicators, etc. Section II contains random alphabets or sequences (OTU).

3. New instructions and modifications of existing instructions sent from Tokyo by dispatch to all points from time to time.

Of the elements listed above, the cipher machine may be considered a fixed quantity. This is due to the fact that permanently wired selector switches are used. Had interchangeable contact drums been used instead, it would be possible to substitute new drums or interchange drums thus radically changing the basic wiring pattern. As far as is known at this time, the only manner in which this could be accomplished with the existing Japanese machine is by rewiring the selector switches. This presents some major difficulties when it is considered that the machines are in use throughout the world. All of the methods of variation encountered thus far are inherent to the machine and are incorporated in R.I.P. 72.

The other elements have been recovered to such an extent that it is now possible to read about 99 percent of the intercepted traffic. On some days deciphering the traffic is just the mechanical process of decipherment. On others it is necessary to apply cryptanalytic methods of attack in order to fill in unrecovered portions of the elements of the system. The reason for this as well as the methods of attack are covered in succeeding chapters.

The following outline of the steps used by a Japanese operator in enciphering a dispatch is inserted in order to demonstrate how the elements of the system are actually employed.

To encipher a dispatch on a given day the Japanese operator first selects a sequence for that day from the part of a book which they refer to as "OTU",(Section II). (The section from which he takes the sequence is made up of fifty pages with twenty sequences on a page making a total of one thousand sequences. Each page and line is numbered). The manner of selecting the sequence is varied from time to time by instructions from Tokyo, but has consistently been some method of arriving at page and line from month and day of encipherment.

The sequence selected is then plugged into the plug board of the cipher machine. The manner of doing this is varied from time to time by instructions from Tokyo but is the same day by day for the periods between the effective dates of instructions from Tokyo. There are two variables in this process (1) The point in the selected sequence from which the plugging in is started and the direction in which the letters are taken, i.e., 5th letter from the left and proceed to the right, etc., etc. (2) The route on the plug board followed by the operator in plugging in from the designated starting point. The plug board of the Japanese machine is set up as follows and the route to be used is given as an alphabetic sequence i.e.,

I Y D H L P S W Z V R N K G C U E A O B F J M Q T X

PLUG BOARD OF JAPANESE MACHINE:

A O B F J M Q T X

E U C G K N R V Z

I Y D H L P S W

In the route above, the letter of the selected sequence designating the starting point is plugged into the "I" position, the

next letter into the "Y" position, etc. NOTE: The plug board of R.I.P. 72 does not correspond to that of the Japanese machine. Therefore, a conversion is necessary in order to plug a sequence from the Japanese book into R.I.P. 72.

The use of a different starting point or route of plugging in, even though the sequence be the same, completely changes the cipher text generated by the machine. For example, between November 1, 1940, and February 28, 1941, Tokyo used a different starting point from all other points. While the sequence used was the same, a machine set to decipher traffic from Tokyo would not decipher traffic to Tokyo.

Having plugged in the sequence for the day, the operator then selects an indicator at random from a list of 120. Accompanying this indicator which is composed of five digits all even or all odd (02648, 71395, etc) are numerals which designate the starting positions of the selector elements of the cipher machine. The machine is set up in accordance with these and the indicator to which an additive of five digits is applied is placed in the dispatch immediately preceding the cipher text. Additives to be used are established from time to time by Tokyo. Generally the same additive is used throughout a calendar month but there have been departuresfrom this practice.

CHAPTER I

B. CRYPTOGRAPHIC PRINCIPLES INVOLVED

The Purple machine produces a highly complicated form of heterogeneous polyalphabetic substitution. The Roman Alphabet of twentysix characters is divided into two sections - one of six letters commonly referred to as the six section and one of twenty letters known as the twenty section.

In the basic wiring of the machine the six section produces twenty five heterogeneous sequences. The cycle of the six section is therefore twenty five. The twenty five sequences are used over and over again and always in the same order. The only variable is the starting point which is determined from the indicator of the dispatch. The point most worthy of note in considering the six section is that each of the six letters connected thereto is replaced in the cipher text by itself or one of the remaining five letters of the six section. Another point is that the cycle of twentyfive resulting from the six section will have an effect upon the frequency characteristics of the cipher text. The extent of this effect is determined by the plain text frequency values of the six letters of the six section.

It will be seen from a study of R.I.P. 72 that while it is true that the twenty section selectors rotate through twentyfive points, the cycle of twentyfive has no bearing on the twenty section. Therefore, in a sufficient volume of text (about 150 groups minimum) the letters of the twenty section should produce a fairly flat frequency characteristic when counted on the basis of twentyfive while the six section will reveal a different characteristic. The frequency will tend to be flat but the average value of the six section will differ from that of the twenty section. If one or more letters of high plain text frequency are in the six section, the average frequency should be higher than that of the twenty section. If the six section is made up of low frequency letters the average frequency will have a lower value. In other words, in a frequency count based on a cycle of twentyfive, the letters of the six section will tend to have the same frequencies and of a value higher or lower than the twenty section. It is possible, though rare, for the plain text frequency values of the letters of the six section to be such that there is no marked difference in frequency between the six section and the twenty section. A difference in letter distribution will however be present.

The twenty section generates 15,625 (25x25x25) heterogeneous sequences. It is unnecessary to go into a detailed study of the cryptographic principles involved as R.I.P. 72 will reproduce all 15,625 sequences and further study is not necessary in order to recover the missing parts of the system.

In Appendix 5B is a form which converts the basic sequence to the one for R.I.P. 72 for various dates thus eliminating the step of arriving at the sequence as set up on the Japanese plug board by using starting point and route.

To decipher a dispatch for a given date first refer to Chapter II C "Chronological Index of Operating Instructions" and pick out the necessary data for that date. If this data is complete, decipherment is the routine operation of R.I.P. 72. If the sequence is missing, cryptanalytic attack is necessary.

Cryptanalytic attack is based mainly upon the assumption of plain text values. This is greatly facilitated by the stereotyped phraseology employed by the Japanese in drafting the beginnings of dispatches. Generally the opening groups are composed of enciphered expressions from a code used in connection with the Purple and other systems. This code, as recovered to date is in Appendix 6A.

Recovery of the sequence may be attacked by two methods:

A. Recovery of the six section by frequency analysis and from the plain-text values thus established, assumption of values in the twenty section and eventual recovery of the entire sequence. This method is particularly valuable where only one dispatch is on hand but it is necessary to have a minimum of about 150 groups in order to produce significant results.

B. Recovery of the six section and twenty section simultaneously by assumption of plain text values. This method is useful when a number of dispatches is on hand.

Recovery of the 6's Sequence by Frequency Analysis

The separate wiring of the leads to the 6's wheel separates the letters of that sequence from those of the 20's sequence and isolates their characteristics to such an extent that they can be identified by a frequency analysis of the cipher text. The most marked indications of these letters are evident when some of the letters in the 6's sequence have either very high or very low frequency counts in the underlying plain text. The presence of two or more high frequency letters will usually raise the frequency counts of all 6 letters into the high frequency level as compared with the letters in the 20's sequence. This is the most common case. Likewise, two or more low frequency letters will lower the counts of the others to a marked extent. A single high or low frequency letter may not be apparent in the over-all frequency analysis. Further detailed analysis is required to determine the order of the letters in the sequence and to identify the letters when the frequency distribution is regular.

CHAPTER II

A. INSTRUCTIONS FOR DECIPHERING CURRENT TRAFFIC

As stated in Chapter IA, by applying cryptanalytic methods of attack it is now possible to read about 99 percent of the intercepted traffic. This, with the Japanese custom of transmitting forthcoming changes in the system itself, enables us to keep well posted on indicator additives, indicators and selector starting points. It enables us to determine the route being used to select daily sequences in the Japanese book and to reduce recovered sequences to basic form. It enables us to reconstruct the original Section II and thus make use of recovered sequences when the route through the original crosses or follows previous routes. Therefore, we are reasonably certain to have all the information necessary to decipher traffic with the exception of some sequences.

As of April 1, 1941, about 50 percent of the sequences in the original Section II have been recovered. When the route through Section II is through recovered portions, solution is mechanical. When the route is through unrecovered portions, cryptanalytic attack generally gives the sequence, deciphers the traffic and adds another line to the book.

Before proceeding with the cryptanalytic methods of recovering sequences, it is essential to have a knowledge of basic sequences (as they appear in the original Section II) vs those that are used in R.I.P. 72. The Japanese plug board is arranged as follows:

```
A O B F J M Q T X

E U C G K N R V Z

I Y D H L P S W
```

The plug board of R.I.P. 72 in terms of the Japanese is as follows: (The electrical relationship - not the physical).

```
A O C L J V Q Z G

E U F T K X W B D

I Y R S N P M H
```

Knowing the sequence used on a given date in basic form and the starting point and route of plugging in (from translations of intercepted instructions), it is possible to obtain the sequence to use with R.I.P. 72 by performing the conversion indicated by the difference between the two plug boards.

2. The detailed analysis is based on the 25 step cycle of the 6's wheel. Worksheet 6-A (Appendix 5) is designed for this type of an analysis. The message is written (or marked off) in 25-letter units and a frequency count is made of each of the 25 columns (alphabets) on tally sheet 6-A (letter-column coordinates). This gives a horizontal frequency distribution for each of the 25 columns (alphabets) which are a graphic representation of the 25 secondary alphabets generated by the motion of the 6's wheel and an over-all distribution vertically for each individual letter. There will result, therefore, 6 vertical coulmns with frequency distribution differing in greater of lesser degree from the remaining 20 columns. Each cell represents only one plain text letter and the cells which represent the same letter will have the frequency characteristics of that letter. Therefore these columns take on the characteristic of peaking or bunching, as does any normal frequency distribution, and will have a different appearance than the flat distributions of the columns of letters in the 20's sequence. This is used to initially identify the letters in the 6's sequence.

The next step requires the use of Worksheet 6-B (Appendix 5). The table at the left of this sheet represents the wiring of the 6's wheel by listing vertically, under each incoming lead, the outlet lead to which it is connected for each position of the wheel. The letters in the 6's sequence correspond to the numbers in the table in their sequence position; i.e., at position #3 the letter connected to lead #3 (occupies #3 position in the 6's sequence) is the cipher equivalent of the letter which is connected to lead #4.

If the Wiring table (worksheet 6-B) is matched against the Tally sheet (worksheet 6-A) each wiring table column will indicate the identity of the cells in the tally column under its corresponding letter. At this point, that identity is expressed by the position numbers of the letters in the sequence. The two sheets can be matched by lining up the initial position (starting point) of the 6's wheel against the top row of the Tally sheet (worksheets should have the same vertical spacing). When each letter tally-column is matched against its proper wiring column a frequency count of the sequence positions will represent the frequency characteristics of the underlying plain text. Since each tally column under the letters in the 6's sequence can represent only the same 6 letters, then the six frequency distribution patterns will usually be similar. In actual practice this is qualified by the natural variations of frequency counts and will be most apparent when there is a peaked distribution among the letters in the 6's sequence.

By the foregoing an attempt has been made to show that the identity and order of the letters in the 6's sequence can be found by a search for evidences of the characteristic behavior of the letters when placed in the proper positions in the sequence. A typical solution might be carried out in the following manner:

1. Prepare a frequency tally-sheet (Worksheet 6-A) for the first 200 groups of a message. Add the vertical columns and enter the totals on the bottom of Worksheet 6-C (Appendix 5). Note any outstandingly high or low frequency letters.

2. Obtain the starting point for the 6's wheel from the key lists and check-mark that position on the wiring table on Worksheet 6-B. Enter the message cycle steps (1-25) on the right margin of the table (from the starting point) and fold the left edge of the sheet vertically along the left edge of the table to facilitate ease of comparison with the tally sheet.

3. Note the columns in the tally sheet which apparently vary from a flat distribution. Check these against the columns of the wiring table and note any repetitions of sequence position numbers which indicate high or low frequency letters. e.g. If there is a high frequency letter occupying number three position in the sequence, then each of the tally columns under the six letters in the 6's sequence should show bunching in the cells indicated as number three by the proper wiring column for each letter. Check probable letters in their sequence positions by making frequency distributions of the sequence positions using the forms provided by Worksheets 6-B and 6-C. Letters which are placed in their proper positions will show similar frequency distributions.

SECRET
R.I.P. 77

ORIGINAL
15 January 1941

Recovery of Entire Sequence

based on

Cryptographic Characteristics of RIP-72

As previously stated there are in this system three basic cryptographic elements which must be recovered before a given message can be read. The three elements are; 1) the basic wiring of the rotary switches effecting the cryptographic substitution; 2) the settings of those elements governed by the keys, and; 3) the plugboard sequence used for enciphering the message. The first of these elements, the basic wiring of the rotary switches, was determined in the solution of the first few messages and, since it is a fundamental part of the system, no change in it is possible. The second of these elements, the settings of the respective switches, is determined by the key and remains constant if is once determined from any one message, it is known for all messages bearing this key. The third of these elements, the sequence used for any particular message, changes from day to day. Therefore, in order to read all messages enciphered by means of this system (the basic wiring of the rotary switches having been recovered and the settings of the switches for each of the 120 keys determined) only the third of the basic elements has to be recovered cryptanalytically and, since this element is a function of the date, the problem resolves itself into the matter of solving a new sequence for each day's traffic. A method for recovery of these sequences, based on assuming the beginnings of the messages, was devised and is explained in subsequent paragraphs.

In view of the fact that it is a slow and trying process to follow through the circuits which effect the cryptographic substitution in the machine, for the purpose of deciphering a message, a method was evolved wherein a table of the complete substituttion alphabets for each of the first fifty settings of the rotary swtiches. These tables are called "Key Sequence Development Sheets" (Appendix 7) and by means of them the first fifty letters of any message for which the sequence is known may be deciphered without the use of any mechanical device or aid other than the Key Sequence Development Sheet for the key used in enciphering the message. In order to explain the theory underlying the construction of these sheets, the key for the message given in Chapter I as an example for setting up the machine will be used and the Key Sequence Development Sheet for this key will be developed.

SECRET
R.I.P. 77

ORIGINAL
15 January 1941

The true key for the message is 15973. It is sought in the table of keys (Appendix 2) and is found to correspond to the machine setting 12-12,12,1-(2-3-1). For the purpose of the illustration with which we are here concerned, the machine itself is now set up in accordance with instructions and the plugs and jacks are arranged to give the following arbitrary sequence on the plug board:

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z

If the garble switch is set to its inactive position so that the rotary switches will not move with the depression of a key, when the letter A is depressed on the cipher keyboard the letter U will be printed by the typewriter and when the letter E is struck O will be printed. The rotary switches do not move and, if the other letters of the alphabet are struck on the cipher keyboard, a complete deciphering alphabet for this setting of the rotary switches will be printed by the typewriter. For example, if the sequence A E I O U Y B C D F G H J K L M N P Q R S T V W X Z is typed out on the cipher keyboard, the typewriter will print out the sequence U O Y I E A W N Z P C F K M Q J T B D H R L V X G S. If the ~~garble~~ SET-UP switch is now thrown to ~~its active position~~ SET-UP (CH. NO. 2) and the space bar depressed, certain of the rotary switches will move forward one position in accordance with the motion determined by the setting of the manually operated setting switch. After a single depression of the space bar, the ~~garble~~ SET-UP switch is returned (CH. NO. 2) to ~~its inactive~~ OPERATE position and if the sequence A E I O U Y B C D F (CH. NO. 2) G H J K L M N P Q R S T V W X Z is typed on the cipher keyboard, the sequence I A E Y O U V B X W Z D H S K T J F P C G N L M Q R will be printed by the typewriter. It will be noted that this sequence is different from that obtained with the previous positions of the rotary switches. This operation may be continued for any number of steps for this key with the result that a table similar to the following may be developed on the typewriter by proper manipulation of the platen and carriage return between successive positions of the rotary switches on the cryptograph:

Sequence produced from first setting	U O Y I E A W N Z P C F K M Q J T B D H R L V X G S
SECOND	I A E Y O U V B X W Z D H S K T J F P C G N L M Q R
THIRD	O E U A I Y P G L B T N F V Z M W K R X J Q S C H D
FOURTH	A Y E I U O R F Q J D B W H C P S T X K N V G Z L M
FIFTH	U O I Y A E K L B N G Z R Q H D V W M P F X C J T S
	etc.

The first letters of each of the foregoing sequences are the successive decipherments of the letter A; the second letters are the decipherments of the letter E; the third corresponds to the letter I and so on in the order A E I O U Y B C D F G H J K L M N P Q R S T V W X Z to the final letters of each of these sequences which correspond to the successive decipherments of the letter Z. For convenience, therefore, this table could be arranged as a deciphering table for all messages enciphered by means of the plug-board sequence A E I O U Y B C D F G H J K L M N P Q R S T V W X Z with the machine set according to key 15973. The final form of this table is given in Fig. 1, below.

KEY SEQUENCE DEVELOPMENT SHEET FOR 15973

	A E I O U Y	B C D F G H J K L M N P Q R S T V W X Z	Cipher
1.	U O Y I E A	W N Z P C F K M Q J T B D H R L V X G S	PS
2.	I A E Y O U	V B X W Z D H S K T J F P C G N L M Q R	le
3.	O E U A I Y	P G L B T N F V Z M W K R X J Q S H C D	aq
4.	A Y E I U O	R F Q J D B W H C P S T X K N V G Z L M	iu
5.	U O I Y A E	K L B N G Z R Q H D V W M P F X C J T S	ne
6.	Y E U I O A	D V H C L S Z J T N R G Q B M K F W P X	n c e s

(Fig. 1)

It will be noted that in preparing the above table the vowels A E I O U Y were plugged into the circuits controlled by the rotary switch which effects the substitution for the 6-letter portion of the sequence, while the consonants B C D F G H J K L M N P Q R S T V W X Z were plugged into the circuits controlled by the three sets of rotary switches effecting the substitution for the 20-letter portion of the sequence. The table in this form shows very clearly the segregation of the two portions of the daily sequences into two separate substitution systems and, if it were extended far enough, it would be noted that the cycle of substitutions for the six letters A E I O U Y begins to repeat with the 26th alphabet, while it would be necessary to develope the table through approximately 25 cubed steps before the cycle of substitutions for the 20-letter portion of the sequence begins to repeat. It can also be seen from this table that nowhere will a letter of the 6-letter portion of the sequence be replaced by a letter from the 20-letter portion of the sequence or vice-versa

It should be stated at this time that the letters in the Key Sequence Development Sheets must not be confused with their alphabetical identities, but must be regarded as representing paths between the plugboard of the keyboard unit and the cryptographic unit. That is, the letters of the original sequence (A, E, I, O, U, Y, B, C, etc.) at the top of each development sheet represent the paths of all sequences from the plugboard to the cryptographic unit in the order of their connection there (1, 2, 3, 4, 5, 6, 7, 8, etc). The letters in each of the fifty rows of the body of the tables represent the paths from the cryptographic unit to the printer (through the plugboard) for each of the first fifty positions of the machine for each key set-up. e.g. For any message enciphered in the key 15973: the cipher letter which is the first letter of the daily sequence used will always be represented in the tables by the letter A. Therefore, for the first five positions of the machine it will be the cipher text equivalent of the letters in the daily sequence which are in the positions corresponding to U, I, O, A and U in the table sequence.

Now for the purpose of demonstration, the sequence M A F N Y D K W H B R Q Z E T V X L I G P U J S O C is set up on the plug-board and the foregoing procedure is followed with this sequence with a view to producing a similar table for the key 15973. This table will be as follows:

	M	A	F	N	Y	D	K	W	H	B	R	Q	Z	E	T	V	X	L	I	G	P	U	J	S	O	C	C-Cipher
1.	Y	N	D	F	A	M	S	X	C	L	W	B	E	V	I	Z	U	K	H	Q	G	T	J	O	R	P	P S
2.	F	M	A	D	N	Y	J	K	O	S	C	D	Q	P	E	U	Z	B	L	W	R	X	T	V	I	G	l e
3.	N	A	Y	M	F	D	L	R	T	K	U	X	B	J	C	V	S	E	G	O	Z	I	P	W	Q	H	a q
4.	M	D	A	F	Y	N	G	B	I	Z	H	K	S	Q	W	L	P	U	O	E	X	J	R	C	T	V	i u
5.	Y	N	F	D	M	A	E	T	K	X	R	C	G	I	Q	H	J	S	V	L	B	O	W	Z	U	P	n e
6.	D	A	Y	F	N	M	H	J	Q	W	T	P	C	Z	U	X	G	R	I	K	V	E	B	S	L	O	n c e s

(Fig, 2)

Reference will now be made to the message appearing in the example given in Chapter I. This message begins as follows:

WMTUP JKETI PVDQR OZEQN YHEOL, etc.

If the letter W, the first letter of the message, is sought in the line of the table labeled "Cipher", its equivalent in Alphabet No. 1 of the "Plain Sequences" is found to be the letter X. The letter M, the second letter of the message, is likewise sought in the "Cipher" sequence and its equivalent F is found in Alphabet No. 2 of the "Plain Sequences."

Likewise, the third, fourth and fifth letters, T, U, and P, respectively, are sought in the "Cipher" sequence and are found to correspond to C, J, and B in Alphabets 3, 4, and 5 of the the "Plain Sequences." If reference is made to that part of the instructions giving the deciphered version of this message, it will be found that the cipher-text group WMTUP equals plain-text group XFCJB. This procedure could be followed for the entire message had a sufficient number of sequences been developed in Figure 2 to accomodate all the positions of the rotary switches necessary for its decipherment.

If the table in Figure 2 is compared with that of Figure 1, it will be noted that wherever the letter A appears in Figure 1 the letter M appears in Figure 2. From this phenomenon it will be evident that the table of Figure 2 can be obtained from that of Figure 1 by simply effecting a monoalphabetic substitution on the table of Figure 1 using the following alphabet:

A	E	I	O	U	Y		B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z	Fig. 1 Sequence
M	A	F	N	Y	D		K	W	H	B	R	Q	Z	E	T	V	X	L	I	G	P	U	J	S	O	C	Fig. 2 Sequence

(Fig. 3)

Since the table of Figure 2 can be obtained from the table of Figure 1 by the monoalphabetic substitution given in Figure 3, it follows that the foregoing message may be deciphered by first converting the cipher letters of the message by means of the alphabet of Figure 3, deciphering the converted cipher text by means of the table of Figure 1, and then using the inverse of the alphabet of Figure 3 to reconvert the text resulting from this decipherment to obtain the original plain text of the message. The following is an example of this procedure:

W M T U P	etc.	Cipher text of the message
C A L T S	etc.	Converted cipher text

This conversion of the cipher text is accomplished by finding the cipher letters in that part of Figure 3 designated as "Sequence for Figure 2" and taking their equivalents from "Sequence for Figure 1". If this converted cipher text is now deciphered by means of the table of Figure 1, the following decipherment is obtained:

W M T U P	Cipher text of the message
C A L T S	Converted cipher text
N I Z V F	Decipherment of converted cipher text using table of Figure 1.

The foregoing decipherment of the converted cipher text is now reconverted by finding the letters appearing in it in that part of Figure 3 designated as "Sequence for Figure 1" and taking the corresponding letters from the "Sequence for Figure 2". From this the following is obtained:

W M T U P	Cipher text of the message
C A L T S	Converted cipher text
N I Z V F	Decipherment of converted cipher text using table of Figure 1.
X F C J B	Reconverted decipherment of converted cipher text.

It will be noted that the final resultant of this operation corresponds to the text of the message as it was deciphered by means of the cryptograph.

Therefore, if tables similar to that shown in Figure 1 are prepared for all of the 120 keys used in this system, and if they are all based on the same plug-board sequence, such tables can be used for rapidly checking the messages of any date against the sequence for that date. Such tables have been prepared under the heading "Key Sequence Development Sheets" and are included in Chapter III, Appendix 7. In preparing these tables the plug-board sequence

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z

was used because this gave a logical division of the 26 letters into 6-letter and 20-letter portions and, while it is suspected that the engraving on the plug-board of the machines actually used by the Japanese breaks the alphabet up into a similar division, their designations have no particular significance with reference to this phase of the solution of their machine.

The most important use to which these tables may be put is in the recovery of an unknown sequence. The method employed in this procedure is definitely a "Probable Word Method" and is based on the fact that the messages transmitted in this system, with very rare exception, begin with the message number. As a matter of fact, the appearance of a message without the usual stereotyped beginning is so unusual that for the purposes of solution it can be ignored.

For example, herewith are given the beginnings of six messages from Berlin to Tokyo which show this tendency toward stereotyped procedure.

1/12/41-F Y C B J B F O C K Y D G W P K S I K N S D O K U

1/11/41-X F C J K Z T X S I N S H C D E N M U K Y O K U C

1/10/41-F Y C J Y N K Y D S Y P K S I C C F H O N S H C H

1/9/41 -F Y C J B B F O C F O V D D N O B B F Y X O O S H

1/9/41 -F Y C J B B F O C F O V D D N O D D F Y X Y N C F

1/6/41 -F Y C G W F O C K A K U N E N K Y D S Y S Y S Y P

It will be noted in the foregoing list of beginnings that in five cases out of the six the first 3 letters of the messages are F Y C and that the letters immediately following these three letters give the message number. Fortunately, their practice is such that all messages originating at any one office are given serial numbers in the order of their filing for transmission regardless of the system used in their encipherment. If good intercept coverage is maintained on any given station and all its traffic is religiously indexed, it is possible to approximate the serial number of any message originated by that station and enciphered in this system.

Example: From: Rome
To : Tokyo 30 December 1940

74699 EYYIU IQRQI NFSTS STMGG ZCCRH EXQGM CIRHF EKGMP RBKPU

LDOPG, etc.

Indicator - 74699
Additive - 23320
Key - 51379

The traffic index indicates that this message's serial number is probably either 123_ or 124_ .

Therefore the probable beginnings are:

E Y Y I U I Q R Q I N F S T S S T M G G Z C C R H

F Y C J D D M S _ _ F O C F Y L C C F _ _ _ _ _ _ _
X F C Y N _ _ F O V
C F X _ _ C C F W D N _ _ _ _ _ _ _ _ _ _
C C F K Y D
F O C W D N
F O C K Y D

Previous traffic indicates that Rome most frequently begins its messages with 'FYC'. This will give in the second position of the message the identity: $Y_c - Y_p$. This can only be produced when there is a coincidence on the Sequence Development Sheet for key 51379 between the original sequence at the top and the sequence in Row #2 indicating the position of a letter which is its own plain text equivalent. In this case there are five such coincidences:

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z Top

A Y E I U O T X D W V S J M Z P F R Q B K C G L N H Row 2
1 2 3 4 5
Y Y Y Y Y

(Hereafter letters from the table representing paths between the cryptographic unit and the plugboard will be underlined)

There is no way of telling at this time which of these five cases correspond to the correct substitution, so it will be necessary to consider them all equally likely, and to carry through each until it can be definitely proved which is the correct one. This is done by assuming that the letter Y will occupy each of the five positions indicated in the following partially reconstructed alphabets:

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z (1)
Y

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z (2)
Y

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z (3)
Y

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z (4)
Y

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z (5)
Y

It will be noted that the third letter of the cipher text is a Y and that it represents the plain text letter C. The next step, therefore, is to locate the C in each of the foregoing sequences. In the third alphabet of the of the Sequence Development Sheet for key 51379 is found; $Y_c - \underline{U}_c - \underline{U}_p - C_p$; $Y_c - \underline{A}_c - \underline{A}_p - C_p$; $Y_c - \underline{K}_c - \underline{K}_p - C_p$; $Y_c - \underline{Q}_c - \underline{Q}_p - C_p$ and $Y_c - \underline{P}_c - \underline{P}_p - C_p$. In the above, $\underline{U}_c$ represents U in the alphabet, or Row, and $\underline{U}_p$ represents U in the top sequence. The letter C is now placed in the partially reconstructed alphabets in accordance with the positions indicated by these five equivalents as shown herewith:

```
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (1)
Y            C
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (2)
C            Y
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (3)
                 Y           C
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (4)
                       Y             C
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (5)
                                   C Y
```

The cipher text of the first few letters of the message is examined for other occurrrences of C or Y and, since none are noted which correspond to the assumed text, it becomes necessary to go to the plain text in order to add other values to the foregoing alphabets. In the seventh letter of the message there is a possible $Q_c - Y_p$ and in the seventh alphabet of the Sequence Development Sheet the five foregoing possibilities give; $Y_p - \underline{E}_p - \underline{E}_c - Q_c$; $Y_p - \underline{Y}_p - \underline{Y}_c - Q_c$; $Y_p - \underline{G}_p - \underline{G}_c - Q_c$; $Y_p - \underline{S}_p - \underline{S}_c - Q_c$ and $Y_p - \underline{R}_p - \underline{R}_c - Q_c$. These values are now entered into the foregoing alphabets to give:

```
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (1)
Y Q          C
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (2)
C            Y Q
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (3)
                 Y Q         C
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (4)
                       Y             C Q
A E I O U Y  B C D F G H J K L M N P Q R S T V W X Z  (5)
                                   C Y Q
```

Since the ninth letter of the message is a Q, an effort will be made to decipher it by means of the foregoing partially reconstructed alphabets. Only the second gives a known value; $Q_c - \underline{U}_c - \underline{U}_p - Y_p$. If the ninth letter of the plain text is a Y then the serial number of the message must be 1244 and, if all the assumptions previously made are correct, the second of the partially reconstructed alphabets is the correct one and the message begins as follows:

E Y Y I U I Q R Q I N F S T S S T M G G Z C C R H etc.
F Y C J D D Y N Y N F O C F Y L C C F
F O V
C C F W D N
C C F K Y D
C C F F O V

Note that two of the assumed beginnings have a Y occurring as the fifteenth letter of the message. If either of these are correct it will permit the letter S to be located in the partially reconstructed alphabet on which the last assumption is based. Reference to Alphabet (or Row) No. 15 of the Key Sequence Development Sheet for this key gives; $Y_p - \underline{E}_p - \underline{E}_c - S_c$ thereby locating the letter S in the second position of the sequence as shown herewith:

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z
C S Y Q (2)

The thirteenth letter of the cipher text is the letter S. Deciphering it by means of the Key Sequence Development Sheet gives; $S_c - \underline{A}_c - \underline{A}_p - C_p$. This looks very good because one of the two assumed beginnings used to locate the letter S in the sequence has the letter as a possibility for this position. It appears now that all the assumptions made up to this point are correct and that the message begins as follows:

E Y Y I U I Q R Q I N F S T S S T M G G Z C C R H
F Y C J D D Y N Y N F O C F Y L

The sixteenth letter of the message may now be used to locate the letter L in the sequence. This gives $S_c - \underline{E}_c - \underline{I}_p - L_p$ placing the L in the third position of the sequence as follows:

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z
C S L Y Q

SECRET
R.I.P. 77

ORIGINAL
15 January 1941

Five of the six letters of the 6-letter portion of the sequence have been determined and all the occurrences of these letters in the first 4 groups of the message have been deciphered. At this point it is desirable to decipher the other letters in the message in order; 1) to obtain definite corroboration of the assumptions made up to this point, and; 2) if these assumptions are correct, use the decipherment of these letters as a basis for other assumptions to be used to complete the reconstruction of the 20-letter portion of the sequence. The decipherment of the first ten groups of the message is as follows:

E Y Y I U I Q R Q I N F S T S S T M G G Z C C R H
F Y C J D D Y N Y N F O C F Y L ? S

E X Q G M C I R H F E K G M P R B K P U L D O P G
S C S

Now, since approximately one half of the messages in this system refer to previous messages, the message under study should be examined for a message reference. These references are usually made immediately after the serial number and will be either;

Re my (?) : WDN # # # P K S I C C F or

Re your (?) : KYD # # # P K S I C C F

In the beginning of the message under consideration, the S and C in the sixth and seventh groups of the message suggest the following possibility:

E Y Y I U I Q R Q I N F S T S S T M G G Z C C R H
F Y C J D D Y N Y N F O C F Y L W D N - - ? S - -
K Y D

E X Q G M C I R H F E K G M P R B K P U L D O P G
P K S I C C F

If this assumption is correct, the remaining letter of the 6-letter sequence must be the letter M, because the thirtieth letter of the message gives $M_c - C_p$. This is checked against the Sequence Development Sheet and $C_p - \underline{I}_p - \underline{I}_c - M_c$. When the letter M appearing as the eighteenth cipher letter of the message is deciphered Y_p is obtained, thus eliminating the W D N as a possibility. Also, the C in the twenty-second position deciphers as the letter M giving the combination MS, which is used to represent the number 3.

It is fairly evident now that the assumptions previously made are all correct and that the message actually begins as follows:

E Y Y I U I Q R Q I N F S T S S T M G G Z C C R H
F Y C J D D Y N Y N F O C F Y L K Y D - - M S - -

E X Q G M C I R H F E K G M P R B K P U L D O P G
P K S I X C F

It is now a fairly simple matter to reconstruct the 20-letter portion of the sequence. Note the three following sets of equivalents:

10th letter	$I_c - N_p$
11th letter	$N_c - F_p$
32nd letter	$I_c - F_p$

Reference is now made to the Sequence Development Sheet and a search is made for three letters satisfying these conditions in the tenth, eleventh and thirty-second alphabets of the sheet. Only two such cases are found, as follows:

10th alphabet	$B_c - K_p$	$P_c - G_p$
11th alphabet	$K_c - D_p$	$G_c - F_p$
32nd alphabet	$B_c - D_p$	$P_c - F_p$

These two cases give the two following possible arrangements of these letters in the sequence:

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z (1)
C S L M Y Q I F N

A E I O U Y B C D F G H J K L M N P Q R S T V W X Z (2)
C S L M Y Q F N I

Since only one of these two possibilities is correct, an effort will be made to eliminate the incorrect one. Note the following equivalents:

	(1)	(2)
Alphabet 6	$I_c - \underline{B}_c - \underline{N}_p - D_p$	$I_c - \underline{P}_c - \underline{C}_p - D_p$
Alphabet 19	$G_c - \overline{X}_c - \overline{N}_p - D_p$	$G_c - \overline{B}_c - \overline{C}_p - D_p$
Alphabet 29	$G_c - \overline{X}_c - \underline{B}_p - I_p$	$G_c - \overline{B}_c - \overline{V}_p - I_p$

Note that (2) gives a contradiction, placing both G and I in the same position in the sequence, while (1) is still possible.

These new equivalents are placed in the sequence to give the following:

A	E	I	O	U	Y	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z
C	S	L	M	Y	Q	I		F					N			D								G	

Five letters of the 20-letter portion of the sequence have now been located and it is only necessary to continue until all the letters of the assumed text have been added to the sequence:

A	E	I	O	U	Y	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Z
C	S	L	M	Y	Q	I	J	F	K	R	W	E	N	V	A	D	Z	O	U	B	H	P	T	G	X

The example above is a favorable case chosen to illustrate typical procedure. Normally, more than one message will be intercepted in the same day's traffic and partial recoveries from several messages can be used to complete the sequence.

Variations of this procedure are often used and are listed below:

1. Start with a letter going to itself. This is the method used to obtain the 6's sequence in the example above.

2. Use a complete chain of letters. This was the procedure followed in getting the start into the 20-letter sequence in the example above.

3. Use a fairly long incomplete chain of 7 or 8 different letters or more and assume for the value of one of the letters of the chain each of the 26 letters of the Sheet in succession. A wrong assumption will usually yield a contradiction; i.e., two different values for the same letter. Thus, the right set is found through a process of elimination.

4. Determine the values of the letters in the 6's sequence statistically. After these have been determined and their plain-text values substituted in the cipher text, sufficient additional plain-text may be filled in to enable the use of one of the first three methods.

5. Use two or more messages enciphered with the same sequence. If the messages to be used have the same sequence, a substitution made in one message is valid for the other and the procedure is much the same as for a single message. Suppose we have two messages whose first cipher groups are G X B E C and G D Y B Q. Assuming both messages start with XFC, we look for a letter in the cipher alphabet which goes to the same letter in the first plain-text alphabet in each of the two sheets. Let the letter be H and let it go to the plain-text letter Q. Then H = G and Q = X.

6. Use two messages, one going to Tokyo and one going from Tokyo. In this case the two sequences are different, but their relationship is known so that, if a value is assumed for a letter in one message, the value for this letter in the other message is uniquely determined. The following form is useful:

(1) A E I O U Y B C D F G H J K L M N P Q R S T V W X Z To Tokyo

(2) K X C T W L M F S B N R E G U Y Q I O J V Z A H D P .

(3) A E I O U Y B C D F G H J K L M N P Q R S T V W X Z Fm Tokyo

Suppose the letter G is assumed to have the value D in the message going TO Tokyo. It is placed under D in sequence (2) and its corresponding value in a message FROM Tokyo is given by the letter X which is directly under it in sequence (3).

SECRET
R.I.P. 77

ORIGINAL
15 January 1941

Recovery of Either "To" or "From" Sequence When Other is Known.
(for sequences subsequent to 1 November 1940)

The two daily sequences may be derived from each other, when one has been recovered, by transposition. The key for the transposition of the "From Tokyo" sequence to the "To Tokyo" sequence is:

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

Example: 5 December 1940

From: Q M E W K V G T N X A L R I J B F P S Z U O H D C Y

To : H R P S J B X E C T I D Z Q V G A Y F L N W U K M O

CHAPTER II

B. MACHINE OPERATING INSTRUCTIONS

R. I. P. 72 consists of the following three parts:

A. The selector unit.
B. The combination key board - plug board.
C. The printer.

All power units are designed for operation on 110 volts direct current only. Connections to power source are made by plugging the polarized leads of the selector and printer units into a 110 volt DC source.

The cryptographic function of the machine is performed in the selector unit by a series of 25 point interconnected selectors or rotary switches similar to those used in automatic telephone installations. By using different combinations of starting points of the various selectors and different orders of selector rotation, plus different orders of plugging sequences into the plug board, variation of the system is obtained. The selector unit is in reality a complex arrangement of switches which receive an impulse from a depressed key on the key board and return that impulse to a point on the plugboard and a letter of the printer. Due to the nature of the cryptographic system for which the selector unit is designed and wired, six of the twenty six plugs leading from the selector unit to the plug board are so wired within the selector unit that an impulse through one is always returned by that one or one of the other five. The same is true of the remaining twenty leads - an impulse through one is returned by that one or one of the other nineteen. The plugs connected with the six section are numbered 1 to 6 -- those connected with the twenty section 7 to 26.

The selectors are arranged within the selector unit from left to right as follows:

1. A pilot selector of three levels which runs in synchronism with the six section selector immediately to the right. It is the function of the pilot selector to regulate by metering action the motion of the selectors connected with the twenty section.

2. The six section selector which is of six levels and which as previously stated runs in synchronism with the pilot selector, This selector performs the switching operation between the six leads of the six section.

3. The twenty section selector bank which consists of twelve selectors of six levels each. The internal wiring is such that the first four rotate as a unit and produce the effect of a single selector of twenty levels. The second and third groups of four are

wired in the same manner. An impulse from a key connected with the twenty section passes through all three banks of selectors and thence to the plug board and the printer. The electrical path through the three banks of selectors depends upon the relative settings of the three banks at the time the key is depressed.

On the panel of the selector unit is a ten point manually operated rotary switch. Points 1 to 6 of this switch are so connected with the pilot selector that the order of rotation of the three banks of selectors in the twenty section may be varied i.e., 1-2-3, 2-1-3, etc. (Appendix 2A gives the complete operation of this switch.)

Each time a key on the key board is depressed, an impulse passes through the selector unit and the pilot and six section selectors move one step in order to be ready for the decipherment of the next letter. (All motion is in one direction - forward). One bank of the twenty section selectors will also move one step - the one that moves being governed by the setting of the 10 point rotary switch. This motion is repeated with the decipherment of each letter until the pilot and six section selectors reach step 25. At this point, the bank of twenty section selectors which has been in motion pauses for one step and the bank in the twenty section second in motion (as established by the setting of the 10 point switch) moves one step. Depressing the next key causes the pilot and six section selectors and the bank of twenty section selectors first in motion to again move one step. This motion continues until the pilot and six section selectors again reach 25 when they pause while the second bank in motion moves one step again. When the bank of twenty section selectors second in motion is on point 25 and the pilot and six section selectors reach point 25, the bank first in motion pauses for two steps while the bank third in motion moves one step and the bank second in motion moves one step. This is the basic motion of the selector unit.

The following five successive selector readings are inserted to show the order of selector motion at the time the second selector in motion reaches point 25:

Six section selector	Twenty section selector			order of motion
	1	2	3	
23	1	25	1	1-2-3
24	2	25	1	
25	2	25	2	
1	2	1	2	
2	3	1	2	

setting" designated in the table. Finally inspect the selectors to see that the pilot and six section selectors are synchronized and also that the four selectors in each of the three banks of the twenty section are synchronized. (Should any selector be out of synchronism, successively trip the pawl of that selector until it is in step.)

Throw the switch on the key board plug board unit to operate and turn on the printer unit switch. Insert message form in the printer and with the key board of the printer unit type in the reference data of the dispatch. Return the printer carriage to the starting point and type out the dispatch on the key board of the key board plug board unit.

The printer will print twenty five characters to the line. It is good practice to log the settings of each selector at the end of every four lines as a check as to whether or not the selectors remain synchronized. The figures logged should show the following pattern at the conclusion of each four lines:

A. The six section selector should be on its original starting point.

B. The selector bank first in motion in the twenty section will lose four points except when the selector second in motion reaches point 25 when it loses an additional point. (The reason for the apparent reverse motion of this selector is the pause each time the six section selector reaches point 25. The direction ofmotion is forward.)

C. The selector bank second in motion in the twenty section gains four points.

D. The selector bank third in motion in the twenty section gains one point when the selector second in motion reaches point 25.

Following are selector settings at the conclusion of each line (25 letters) of deciphered text with the following starting points and selector motion: - 19 - 22, 23, 23, 1-2-3:

While the basic motion and basic wiring of the selector unit remains the same, the system is varied by using various combinations of selector starting points and motions. To date only 120 of the large number of possible combinations have been used. Each is distinguished by a five digit indicator - all even or all odd. The system is further varied by changing daily the order of plugging the 26 leads from the selector unit into the plug board.

To decipher a dispatch for a given date first refer to the section in "Chronological Index of Operating Instructions" Chapter II C which applies to the date of encipherment of the dispatch. In the table of additives select the one applying to the date and subtract it from the five digit indicator which immediately precedes the text of the dispatch. If the figure obtained appears among the 120 listed in Appendix 2 the dispatch is in the Purple system. Read the paragraph in Chapter II C headed "Special Instructions" for any particular instructions applicable to that period.

Turn to Appendix 3A and select the sequence for the date. This sequence will appear in two sections - one of six letters and one of twenty letters. The leads from the selector unit are plugged in numerical order into the receptacles designated by the sequence. For example, the sequence for February 22, 1941 is Y V J N R D M B X etc. Plug #1 plug in the "Y" receptacle, #2 plug in the "V" receptacle and continue through all twenty six plugs in numerical order into the twenty six receptacles designated by the sequence. (Leads 1 to 6 are always plugged into receptacles designated by the 6 section of the sequence).

From the table of indicators and starting points in Appendix 2 select the data which applies to the indicator of the dispatch. This will appear as follows: (Example not actual)

6 section selector	20 Section selectors	Selector motion	Switch setting
12	9 14 7	2-3-1	4

Throw the toggle switch on the right hand side of the key board plug board unit to "Set Up" and the 10 point switch on the panel of the selector unit to point "7". Depress the space bar of the key board plug board unit successively until the starting point of the six section selector appears in the numbered jewels on the panel of the selector unit. Should the lights under the jewels fail to register starting points may be set up by referring to the numbers on the drums of each selector. Next throw the 10 point switch successively to points "8", "9", and "10" and set up the twenty section starting points in the order in which they appear in the table. Turn the 10 point switch to the "switch

Six Section	Twenty Section	Selector Motion
19	22 23 23	1-2-3
19	21 24 23	
19	20 25 23	
19	18 1 24	
19	17 2 24	
19	16 3 24	
19	15 4 24	
19	14 5 24	
19	13 6 24	
19	12 7 24	
19	11 8 24	
19	10 9 24	
19	9 10 24	
19	8 11 24	
19	7 12 24	
19	6 13 24	
19	5 14 24	
19	4 15 24	
19	3 16 24	
19	2 17 24	
19	1 18 24	
19	25 19 24	
19	24 20 24	
19	23 21 24	
19	22 22 24	
19	21 23 24	
19	20 24 24	
19	19 25 24	
19	17 1 25	

C. CHRONOLOGICAL INDEX OF OPERATING INSTRUCTIONS

Period from February 20, 1939 to October 31, 1940

Sequence:

For R.I.P. 72 ~~use pages A1 to A21 of Appendix 5~~

In Section II of original book:

From February 20, 1939 to November 30, 1940 start with page 10 row 10 and use row per day in succession.

From December 1, 1940 -
1st to 10th of month use pages 41 to 50.
11th to 31st use pages 11 to 31. Row equal to the number of the month.

STARTING POINT: Letter at extreme right.

DIRECTION: Left.

ROUTE ON JAPANESE PLUG BOARD:

IYDHLPSWEUCGKNRVZAOBFJMQXT

Additives: Refer to Chapter III, Appendix 1.

Indicators: Use data to the right of indicator.

Special Instructions:

If sequence is ~~not found on pages A1 to A21 of Appendix 5 but is~~ in original book use a form in Appendix A5 to convert.

Period from November 1, 1940 to February 28, 1941 (London to March 22, 1941

Sequence:

For R.I.P. 72 ~~see pages A22 to A29 of Appendix 3.~~

In Section II of original book:

PAGE: Number of the month multiplied by three.

ROW: To the page number add the day of the month. (Should the sum exceed twenty continue on the next page. If the sum is forty one or more subtract forty.)

STARTING POINT: From Tokyo: 5th letter from right.
To Tokyo: 10th letter from right.

DIRECTION: Left.

ROUTE ON JAPANESE PLUG BOARD:

IYDHLPSWZXTVRNKGCUEAOBFJMQ

Additives: Refer to Chapter III Appendix 1.

Indicators: Use data to the right of indicator.

Special Instructions:

A. These instructions effective for London only beyond February 28, 1941, and until March 22, 1941.
B. If sequence is ~~not found on pages A22 to A29 of Appendix 3 but is~~ in original book use a form in Appendix A5 to convert.
C. For certain subject matter the Japanese employ a plug board shift after enciphering ten letters. The selector settings are not changed. A form in Appendix 5 may be used to obtain the ten shift sequence from either a "From" or "To".

SECRET
R.I.P. 77

CHANGE NO. 1
1 April 1941

Period from March 1, 1941 to DECEMBER 31, 1941
(NOTE: These instructions not effective for London until March 23, 1941.)

Sequence:

For R.I.P. 72 ~~use pages A29 to ___ in Appendix 3:~~

In Section II of original book:

PAGE: Equal to the sum of the number of the day and the number of the month.

ROW: The day of the month counted up from the last line. On the 21st day and thereafter subtract 20.

STARTING POINT: 12th letter from right.

DIRECTION: Left.

ROUTE ON JAPANESE PLUG BOARD:

IDLSYHPWECKRZUGNVABJQXOFMT

Additives: Refer to Chapter III, Appendix 1.

Indicators: Use data to the left of indicator.

Special Instructions: SEE "E" EFFECTIVE APRIL 1, 1941. SEE "F" EFFECTIVE MAY 7, 1941 CH. # 2 C.B.H.

A. Use of "To" and "From" sequences discontinued except for London until March 22, 1941.
B. Commencing March 23, 1941 apply above data to London. From March 1, 1941 to March 22, 1941, inclusive, use operating instructions effective November 1, 1940. ~~Sequences listed on page A31 of Appendix 3.~~
C. If sequence is ~~not found on pages A29 to ___ of Appendix 3 but is~~ in original book use a form in Appendix A5 to convert.
D. For certain subject matter the Japanese employ a plug board shift after enciphering ten letters. The selector settings are not changed. A form in Appendix 5 may be used to obtain the ten shift. ~~Sequence from either a "From" or "To".~~ CH. # 2 C.B.H.

Period from January 1, 1942 to _____.

SEQUENCE:

In Section II of original book:

PAGE and ROW: In accordance with the method effective March 1, 1941 is used to determine the sequence which sets the plugging-in route.

STARTING POINT: 1st letter (at the left).

Direction: Right

ROUTE ON JAPANESE PLUG BOARD:

Two sequences are used each day. The sequence for the day determines method of plugging-in (scrambler) - the sequence below is the one that is plugged in.

In the event that the sequence for the day appears on line 20 of Section II, the line above (line 19) is used for the line below.

Form A5-B3 is provided for purpose of making conversions.

Additives: Refer to Chapter III, Appendix 1.

Indicators: Use data to the right of indicator.

(FOR EVEN INDICATORS - run encipher)
(FOR ODD INDICATORS - run decipher)

PERIOD FROM MARCH 1, 1941 TO DECEMBER 31, 1941 (CONTINUED)

E. In addition to the normal traffic on the TOKYO-BERLIN, BERLIN-TOKYO circuit, despatches were first intercepted in April bearing the group H I K A L before one of the 120 regular numerical indicators with the additive applied in the usual manner. Despatches so designated are enciphered in the Purple System but with a modification of the March 1, 1941, instructions. Briefly, the change consists of a minor change in the daily sequence and a radical change in selector starting points obtained by taking off the information in columns rather than lines. The sequence change has remained the same through April, May, and June but there has been a monthly change in starting points by varying the column used and the direction in taking off the data. Despatches prefixed HIKAL are usually in "CA" code. Following are instructions by months:

APRIL 1941

Change sequence for given day as follows:

NORMAL SEQUENCE -

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

HIKAL SEQUENCE -

D E F A B C G O I J K L W N H P Q R S T U V M X Y Z

ARRIVE AT STARTING POINTS AS FOLLOWS:

Apply April additive and seek starting points in data to the left of indicator as set forth in operating instructions effective March 1, 1941.

Set #6 selector on #1 selector setting of indicator.
Set #1 selector on #1 selector setting of indicator 3 below.
Set #2 selector on #1 selector setting of indicator 2 below.
Set #3 selector on #1 selector setting of indicator 1 below.

SELECTOR MOTION as called for by indicator.

MAY 1941

Change sequence for given day as follows:

Same as APRIL 1941.

NOTE: Commencing 7 May 1941 first perform the sequence shift indicated in Paragraph "F" below.

ARRIVE AT STARTING POINTS AS FOLLOWS:

Apply May additive and seek starting points in data to the left of indicator as set forth in operating instructions effective March 1, 1941.

Set #6 selector on #6 selector setting of indicator 3 above.
Set #1 selector on #6 selector setting of indicator.
Set #2 selector on #6 selector setting of indicator 1 above.
Set #3 selector on #6 selector setting of indicator 2 above.

SELECTOR MOTION as called for by indicator.

JUNE 1941

Change sequence for given day as follows:

Same as APRIL 1941.

ARRIVE AT STARTING POINTS AS FOLLOWS:

Apply June additive and seek starting points in data to the left of indicator as set forth in operating instructions effective March 1, 1941.

Set #6 selector on #3 selector setting of indicator 3 above.
Set #1 selector on #3 selector setting of indicator.
Set #2 selector on #3 selector setting of indicator 1 above.
Set #3 selector on #3 selector setting of indicator 2 above.

SELECTOR MOTION as called for by indicator.

JULY 1941

Sequence is derived from basic sequence for date with a daily change in plugging route. Starting point in basic same as March 1, 1941 instructions. See Para. E-1 this Chapter.

ARRIVE AT STARTING POINTS AS FOLLOWS:

Apply July additive and seek starting points in data to the left of indicator as set forth in operating instructions effective March 1, 1941.

Set #6 selector on #1 selector setting of indicator one below. Set #1, 2 and 3 selectors on #2, 3 and 6 selector settings respectively of indicator two below.

SELECTOR MOTION as called for by indicator.

SEQUENCES USED DURING JULY 1941.

July 2, 1941: C D X J Y N U V L H A E P B R Q T K G M I F Z S O W

July 4, 1941: R G Y T E F D N W C X S J U A V P O Z Q M I K L B H

July 5, 1941: D P R V Z Y Q M I J H U O C X K N L B S E F W A G T

AUGUST 1941

Sequence is derived from basic sequence for date with a daily change in plugging route. Starting point in basic same as March 1, 1941 instructions.

ARRIVE AT STARTING POINTS AS FOLLOWS:

Apply August additive and seek starting points in data to the left of indicator as set forth in operating instructions effective March 1, 1941.

Set #6, 1, 2 and 3 selectors on selector settings of indicator two below in that order.

SELECTOR MOTION as called for by indicator.

SEPTEMBER AND OCTOBER 1941

No H I K A L traffic during this period.

E-1. HIKAL sequences for the period July 1, 1941 to ____ are derived from the basic sequence for the day using the normal starting point in the sequence. The last letter of the basic covered by the following sets the point on the Japanese plug board at which plugging-in is started:

LAST LETTER IN BASIC

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

STARTING POINT

O T K H U B R G Y N S M C Z E W D F J L A P Q V I X

For example a basic sequence having "F" for a final letter would be plugged in starting with the "B" position as follows:

A O (B) F J M Q T X
E U C G K N R V Z
I Y D H L P S W

The normal starting point in the sequence for the period is the twelfth letter from the right and it is this letter that is plugged into the "B" position as above. The direction in the basic is the normal for the period (to the left) and the route to be followed varies with the point at plugging-in is started. In the example above, the route is from "B" to "X"; "A" to "O"; "E" to "Z"; "I" to "W". If the last letter in the basic had converted to "N" the route would have been "N" to "Z"; "E" to "K"; "A" to "X"; "I" to "W". If the last letter in the basic had converted to "S", the route would have been "S" to "W"; "I" to "P"; "A" to "X"; "E" to "Z".

A sequence plugged in as above is on the Japanese board. To convert to our board use the following:

A O C L J V Q Z G
E U F T K X W B D
I Y R S N P M H

NOVEMBER AND DECEMBER 1941

The following new method put into effect between November ___ and December ___ 1941.

The last letter of the basic sets the point on the plugboard at which plugging in is started. However, certain changes are necessary in order to adapt this to our machine. The original Japanese basic sequence is different from ours because of the difference in wiring of the two machines between the plugboard and the printer. This is, in effect, a simple substitution superimposed upon the output of the machine.

If we convert the last letter of the basic sequence as follows, the value thus established will give the starting point of plugging on the normal board:

LAST LETTER IN BASIC

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

STARTING POINT ON OUR BOARD

O T K H U B R G Y N S M C Z E W D F J L A P Q V I X

Having found the starting point on the board the method is to proceed to the right to the end of the line, fill in the balance of the line from the left and then the remaining two lines from left to right from top to bottom.

EXAMPLE

Basic for December 7: Starting point plugging in

D V B K G Q R V J I H Y E L N Z O C T X F S M A P (W),
converted becomes (Q))

Plug in

Normal Jap. Plug board: 2 : 1
A O B F J M Q T X
: 3
E U C G K N R V Z
: 4
I Y D H L P S W

In selecting starting points:

(1) Take off settings from left to right as follows:

JANUARY - 1, 2 and 3 wheels of indicator and 6-wheel of indicator one below.

FEBRUARY- 2 and 3 wheels of indicator and 6 and 1 wheels of indicator one below.

MARCH - 3 wheel of indicator and 6, 1 and 2 wheels of indicator one below.

APRIL - 6, 1, 2 and 3 wheels of indicator one below in regular order.

(2) Interchange the settings of the "1" and "3" wheels in all cases in which two indicators are involved.

For example, the step by step conversion to arrive at the starting points involved for the month of February, 1942 follows:

KEY	6 Wheel	20-wheels 1	2	3	
46028	25	20	3	2	Normal (listed in R.I.P. 77)
46028	25	2	3	20	Converted
46280	20	25	8	16	Normal below
46280	20	16	8	25	Converted
46028	3	20	20	16	Order in which taken off
46028	3	16	20	20	Converted for use with R.I.P. 72

MOTION as called for by indicator.

MACHINE OPERATION:

COMPLEMENTARY INDICATOR - operate machine for decipher.

NORMAL INDICATOR: (EVEN)-operate machine for encipher.

(ODD)-operate machine for decipher.

December 7 on Jap. Plug board	Y H I J V R N L E Q G K B U D W P A M S F X T C O Z
Difference between Jap. and our board	A O C L J V Q Z G E U F T K X W B D I Y R S N P M H

December 7
for our Machine

Y Q M H G S P I A K E Z V U J O T C N F X B R W D L

ARRIVE AT STARTING POINTS

Apply additive and seek starting points in data to the left of indicator as set forth in operating instructions effective March 1, 1941.

Set #6, 1, 2 and 3 selectors on selector settings of indicator three below in regular order.

SELECTOR MOTION as called for by indicator.

The new method put into effect between November ____ and December ____ 1941 has been continued into 1942 with the exception of the following additions:

The page and line used is determined by the indicator and date of message, ie.,

PAGE - The first two digits of the indicator after additive is applied equal the number of the page used. If over 50, the page number equals the first two digits minus 50.

ROW - Equal to the date of the message plus the month. If more than 20, subtract 20 and use row on following page.

ARRIVE AT STARTING POINTS

Apply monthly additive and seek starting points in data to the left of indicator.

Selector settings for the months of January, February, March and April as taken from the normal list of indicators follow:

JANUARY

Set #6 selector on #3 selector of indicator.
Set #1 selector on #6 selector of indicator one below.
Set #2 selector on #1 selector of indicator.
Set #3 selector on #2 selector of indicator.

FEBRUARY

Set #6 selector on #2 selector of indicator.
Set #1 selector on #3 selector of indicator one below.
Set #2 selector on #6 selector of indicator one below.
Set #3 selector on #1 selector of indicator.

MARCH

Set #6 selector on #1 selector of indicator.
Set #1 selector on #2 selector of indicator one below.
Set #2 selector on #3 selector of indicator one below.
Set #3 selector on #6 selector of indicator one below.

APRIL

Set #6, 1, 2 and 3 selectors on selector settings of indicator one below in regular order.

F. On May 7, 1941 a dispatch was sent from TOKYO to all points holding the purple system placing "1941 Instructions" in immediate effect. The change proved to be the use of the sequence shift after enciphering ten letters on all traffic. This shift, which had hitherto been reserved for despatches of greater secrecy than usual, is covered in paragraph "D" above. There is a form in Appendix 5 which gives the sequence shift. These instructions were later modified to the extent that the sequence shift was made before beginning the encipherment of the despatch. This became effective on May 15, 1941.

G. Washington, on traffic requiring a higher degree of secrecy, occasionally enciphers despatches in the Purple System which are prefixed by RED indicators. These are apparently a special series of starting points which have been applied to RED indicators and are employed with the Purple System without so designating externally in the despatch. Starting points and indicators recovered to date are on Page A2-A-4 entitled "Complementary Indicators."

H. On August 20, 1941 Tokyo instructed all holders of the Purple System to divide dispatches into two, three, four or five parts and to transmit the parts in irregular order. For example in a dispatch of 100 groups the originator might start enciphering at any point approximately the center of the dispatch, proceed to the end and insert "DDDD" indicating two parts in all and the end of the second part. Encipherment is continued at the actual beginning of the dispatch and when the point at which encipherment started is reached "DDBB" is inserted plus fillers to complete a five letter group as necessary.

CHAPTER III - Appendix 1

TABLE OF ADDITIVES

1939

From February 20 to April 30:

1st to 10th	32210
11th to 20th	23120
21st to 31st	12320
May	51230
June	52520
July	02120
August	33220
September	22110
October	21012
November	01223
December	50205

1940

January	12321
February	20502
March	05252
April	32023
May	22033
June	10203
July	52025
August	25250
September	32230
October	12320
November	22050
December	23320

1941

January	51230
February	52520
March	08083
March....(Tokyo-London-Tokyo)	02120
APRIL	32321
MAY	04140
JUNE	21215
July	50922
August	12213
September	90029
October	18112
November	82313
December	03210

CH. #2 C.O.H.

1942

January	20300
February	01230
March	91008
April	12123

INDICATORS
STARTING POINTS

Key	Initial Settings: Six Wheel	20 Wheels 1	2	3	20 Wheel Motion	Key	Initial Settings: Six Wheel	20 Wheels 1	2	3	20 Wheel Motion
02468	21	14	2	15	3-2-1	46028	25	20	3	2	1-2-3
02684	10	9	25	19	2-1-3	46280	20	25	~~19~~	16	2-3-1 CHG 2 C.B.H.
02846	14	3	10	14	3-1-2	46802	18	12	19	12	1-3-2
04286	15	16	23	11	2-1-3	48062	17	24	7	18	3-1-2
04628	11	21	22	17	1-3-2	48206	13	13	24	4	3-1-2
04862	12	5	9	9	1-3-2	48620	22	11	18	23	2-3-1
06248	19	2	12	10	2-3-1	60284	1	1	13	25	3-2-1
06482	9	7	17	1	1-3-2	60428	24	6	4	13	1-2-3
06824	6	10	15	24	2-1-3	60842	2	17	20	8	3-1-2
08264	16	8	5	22	3-1-2	62048	7	18	21	3	1-3-2
08426	4	23	6	5	2-3-1	62480	8	19	14	6	1-3-2
08642	23	4	11	21	2-3-1	62804	3	15	16	20	3-2-1
20486	5	22	1	7	3-2-1	64082	12	4	23	16	2-3-1
20648	7	16	18	8	1-2-3	64208	11	8	21	11	3-2-1
20864	16	19	16	19	2-3-1	64820	2	2	4	15	1-3-2
24068	9	23	9	25	3-2-1	68024	14	22	8	4	2-3-1
24680	18	5	7	7	1-2-3	68240	3	13	6	18	2-1-3
24806	10	12	14	21	1-2-3	68402	8	17	25	6	3-2-1
26084	6	21	11	17	3-1-2	80246	4	20	12	3	1-3-2
26408	20	1	10	22	2-1-3	80462	22	7	3	10	3-1-2
26840	21	6	2	1	2-3-1	80624	1	15	24	12	1-3-2
28046	5	9	13	20	3-1-2	82064	23	3	1	5	1-3-2
28460	25	18	5	14	2-1-3	82406	24	11	20	24	3-1-2
28604	17	25	22	13	2-1-3	82640	13	24	17	9	1-2-3
40268	15	14	15	23	1-3-2	84026	19	10	19	2	3-1-2
40682	7	8	21	24	2-3-1	84260	10	22	23	15	3-2-1
40826	13	6	20	23	1-2-3	84602	1	15	13	18	2-1-3
42086	4	14	13	12	3-2-1	86042	11	23	22	19	2-3-1
42608	2	4	5	2	1-2-3	86204	16	7	7	21	2-1-3
42860	24	2	16	5	1-3-2	86420	17	6	17	16	3-1-2

INDICATORS
STARTING POINTS
(cont'd)

Key	Six Wheel	1	2	3	20-Wheel Motion	Key	Six Wheel	1	2	3	20-Wheel Motion
13579	3	24	8	25	3-2-1	57139	19	20	6	4	2-3-1
13795	15	21	1	11	1-2-3	57391	25	10	25	20	2-1-3
13957	21	13	14	7	3-2-1	57913	23	16	19	13	1-2-3
15397	18	25	4	14	1-2-3	59173	6	19	15	10	3-2-1
15739	9	1	24	6	2-3-1	59317	20	18	2	17	3-2-1
15973	12	12	12	1	2-3-1	59731	14	5	3	3	1-3-2
17359	22	17	10	9	2-1-3	71395	8	3	11	8	1-2-3
17593	5	11	9	22	3-1-2	71539	5	6	2	23	3-2-1
17935	9	8	18	7	1-2-3	71953	6	1	22	4	2-1-3
19375	18	19	13	3	1-3-2	73159	23	5	20	1	2-3-1
19537	15	12	24	25	3-1-2	73591	19	18	19	20	3-2-1
19753	3	10	23	14	1-3-2	73915	24	3	4	19	2-3-1
31597	17	21	25	12	2-3-1	75193	10	20	9	5	3-2-1
31759	21	2	21	2	1-2-3	75319	25	24	10	24	1-3-2
31975	16	7	17	16	2-3-1	75931	2	4	16	18	3-2-1
35179	8	15	7	17	3-2-1	79135	22	23	12	9	1-2-3
35791	14	16	5	11	2-1-3	79351	12	9	1	13	2-3-1
35917	4	11	14	15	3-1-2	79513	11	25	3	6	1-3-2
37195	20	14	8	8	2-3-1	91357	1	22	6	10	1-3-2
37519	13	13	15	21	3-2-1	91573	7	17	11	22	3-1-2
37951	6	1	5	19	1-3-2	91735	8	23	1	9	2-3-1
39157	16	25	9	14	2-3-1	93175	25	7	6	12	1-3-2
39571	4	9	16	22	2-3-1	93517	10	13	18	15	3-2-1
39715	17	5	12	6	3-2-1	93751	20	3	25	8	1-2-3
51379	14	2	8	18	2-1-3	95137	19	4	7	21	2-3-1
51793	3	20	19	2	1-3-2	95371	12	21	20	11	3-1-2
51937	21	14	3	16	1-3-2	95713	11	6	22	20	3-1-2
53197	23	24	15	25	2-1-3	97153	18	22	11	17	2-3-1
53719	15	8	13	7	1-3-2	97315	22	10	4	24	3-1-2
53971	9	11	23	23	3-1-2	97531	24	12	2	10	1-3-2

COMPLEMENTARY INDICATORS

INITIAL SETTINGS

KEY	Six Wheel	20-Wheels 1	2	3	Wheel Motion
01234					- -
01342	7	I9	I4	3	I-3-2
01423					- - -
02143	-	-	-	-	- - -
02314					- - -
02431	4	2	I4	7	I-3-2
03124	13	5	5	24	3-2-1
03241	7	7	3	16	2-1-3
03412	20	24	7	11	1-3-2
04132	12	23	18	18	3-2-1
04213	3	8	11	6	1-2-3
04321					- -
10243	I8	I4	6	I4	3-I-2
10432	1	12	21	19	1-2-3
12034	4	21	4	3	3-1-2
12340					- - -
12403	-	-	-	-	- - -
13402		6	I5	I8	3-I-2
13204	24	8	22	6	2-1-3
13420					- -
14023	-	-	-	-	- - -
14230	-	-	-	-	- - -
14302	6	5	9	9	2-3-I
20134					- -
20341	-	-	-	-	- - -
20413	-	I4	-	-	- - -
21043	20	-	24	4	2-3-1
21304					- - -
21430	4	I3	I5	7	I-3-2

KEY	Six Wheel	20-Wheels 1	2	3	Wheel Motion
23014	1	18	17	5	3-1-2
23140	13	17	21	4	2-1-3
23401	2	19	13	4	2-1-3
24031	14	10	23	17	3-1-2
24103	25	4	2	25	2-3-1
24310					- - -
30142	-	-	-	-	- - -
30214	I7	25	20	2	3-I-2
30421					- -
31024	-	I	I0	8	2-3-I
31240	21	13	9	10	2-1-3
31402					- -
32041	I5	I5	I	9	I-3-2
32410	5	18	24	13	2-1-3
34012	16				- -
34120	10	I9	23	20	2-I-3
34201					1-2-3
40123	I2	I3	5	8	2-1-3
40231	6	-	-	-	- - -
40312					- -
41032	I	9	I8	I	3-I-2
41203					- -
41320	-	-	-	-	- - -
42013	-	-	-	-	- - -
42130	22	I8	8	I3	3-2-I
42301	5	-	-	24	- - -
43021					- -
43102	I0	I6	I4	21	3-I-2
43210	-	-	-	-	- - -

COMPLEMENTARY INDICATORS

INITIAL SETTINGS

KEY	Six Wheel	20-Wheels 1	2	3	Wheel Motion
56789	17	23	18	11	2-1-3
56897					- -
56978	21	22	17	19	3-2-1
57698					- -
57869	-	-	-	-	- - -
57986	-	-	-	-	- - -
58679	-	-	-	-	- - -
58796	22	-	-	-	- - -
58967	16	6	12	2	3-2-1
59687					- -
59768	-	-	-	-	- - -
59876	-	-	-	-	- - -
65798	-	-	-	-	- - -
65879	-	-	-	-	- - -
65987	-	-	-	-	1-3-2
67589	5	14	21	2	1-2-3
67895	25				- -
67958		-	-	-	- - -
68597	6	-	-	-	1-3-2
68759	18	13	5	21	3-2-1
68975					- -
69578	-	-	-	-	- - -
69785	-	-	-	-	- - -
69857	-	-	-	-	- - -
75689	-	-	-	-	- - -
75896	-	-	-	-	- -
75968	-	5	15	-	1-3-2
76598	7			10	- -
76859		-	-	-	- - -
76985	-	-	-	-	- - -
78569					- -
78695	-	-	-	-	1-2-3
78956	24	10	21	22	2-1-3
79586	7				1-2-3
79658	1	18	7	12	- - -
79865					- - -
85697	-	-	-	-	- - -
85769	4	-	-	-	- - -
85976	14	20	19	4	2-1-3
86579	2				- -
86795		-	-	-	- - -
86957	10	4	16	6	2-3-1
87596	17	7	15	19	3-2-1
87659					- -
87965	-	-	-	-	- - -
89567	13	10	13	1	3-2-1
89675					- -
89756	-	-	-	-	- - -
95678	-	-	-	-	- - -
95786	-	-	-	-	- - -
95867	-	-	-	-	- - -
96587	20	15	8	18	3-2-1
96758	14	3	4	13	3-2-1
96875	17				- -
97568	6	6	3	2	3-2-1
97685					- -
97856	-	-	-	-	- - -
98576	-	-	-	-	- - -
98657	-	-	-	-	- - -
98765	3	12	1	23	3-2-1

CHANGE NO. 2
1 July 1941

By NNP NARA Date 8/17/77

SECRET
R.I.P. 77

Line No.	Sequences	Date Used				
1	V L J Y K T M G Q C S R F H U A E D O I W N Z P B X	7/21/39	1/18/40			
2	L J C V N A B W G I M X U F R E D Y Z H Q P T K S O	7/22/39	2/18/40			
3	I H K P Y S F E O R B G N Z W T A V M C D L Q J U X	7/23/39	3/18/40			
4	K H N P Z E F V D T B S G Q X Y I L U C R A J O W M	7/24/39	4/18/40	1/17/42		
5	K M F V Y Z L N O J X P H E T Q B I U W S C A R G D	7/25/39	5/18/40	2/16/42		
6	R Z E V G L I B M H K U C N X F A Q T S W J Y D P O	7/26/39	6/18/40	3/15/41	3/15/42	
7	T O D U K G X S M H E W B R F P V C I Z N Y J Q L A	7/27/39	7/18/40	4/14/41	4/14/42	
8	E T I N Q K F Y W C Z G H V J X B S M U D R L O P A	7/28/39	8/18/40	5/13/41		
9	N E H X F A J Y C R K S Q O Z U M V I D T G W L B P	7/29/39	9/18/40	6/12/41		
10	T U X W R E Z J L Q H B O N M A D Y C G K F V I P S	7/30/39	10/18/40	7/11/41		
11	R Q X T G B Z I V N P U E H K D A J M L C F O W S Y	7/31/39		8/10/41		
12	K N W I D U O G C B A H F Q L Z E V S X R P J M T Y	8/1/39	12/18/39	9/9/41		
13	I Y V J C T O A E N S U R W H Z K F B G M L Q D X P	8/2/39	10/8/41			
14	L H G X Q N Z E O U J I Y R K C D P B W A V F S M T	8/3/39	11/7/41			
15	S U Q D I A K X Z V Y G M L O J R E N F W P T H B C	8/4/39	12/6/41			
16	W K D Z L Y G P T O Q X M I C N H E J A V F S R U B	8/5/39				
17	- -	8/6/39				
18	Z L N J D M T A F I Y S Q C V G B U R K W P H E O X	8/7/39				
19	N P C G I F T W E A L D R B O X J S U Y V K Z H Q M	8/8/39				
20	M G W C I U D J P X N L B R V O E K A Q Z Y H F S T	8/9/39				

A3-319

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

SECRET
R.I.P. 77

NO. 2 - ENCIPHER

ORIGINAL
JANUARY 15, 1941

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
1.	3	8	7	18	4	15	20	10	2	9	11	13	16	19	1	14	5	12	6	17	1.
2.	17	4	20	5	11	2	14	7	6	15	12	1	19	18	3	8	10	16	9	13	2.
3.	6	14	18	1	3	17	15	4	16	19	13	7	11	10	8	5	12	2	20	9	3.
4.	14	3	10	19	12	1	6	11	17	13	2	8	20	5	9	18	15	7	16	4	4.
5.	9	2	4	6	17	13	1	18	5	20	14	10	3	8	16	15	7	11	19	12	5.
6.	11	12	14	15	[illegible]	19	4	9	6	5	17	16	10	3	20	13	2	18	7	8	6.
7.	18	7	3	2	20	16	19	1	8	11	4	9	6	13	14	10	12	17	5	15	7.
8.	2	17	11	16	10	20	12	6	18	4	8	19	13	7	5	3	14	9	15	1	8.
9.	10	6	17	7	5	12	3	2	1	16	11	20	8	15	4	19	9	14	13	18	9.
10.	17	20	12	13	9	10	16	5	11	1	3	2	15	18	19	6	8	4	14	7	10.
11.	8	16	20	4	13	7	2	19	14	18	1	11	9	3	12	15	17	5	10	6	11.
12.	15	1	2	20	16	14	9	17	3	4	10	12	5	6	7	8	18	13	19	11	12.
13.	4	13	6	9	15	11	10	12	8	2	16	17	7	14	3	1	5	19	18	20	13.
14.	19	10	5	14	18	9	15	20	7	8	13	4	6	12	17	2	11	3	1	16	14.
15.	5	19	17	16	11	8	6	13	12	7	9	3	18	2	10	20	15	1	4	14	15.
16.	20	4	2	5	6	18	16	15	9	10	7	14	17	8	13	12	19	11	3	1	16.
17.	13	5	1	3	8	2	11	16	15	17	18	6	19	4	14	7	20	9	12	10	17.
18.	7	12	19	11	1	14	13	18	4	5	15	10	9	16	2	17	6	20	8	3	18.
19.	12	9	15	8	5	16	17	7	13	18	20	19	3	1	10	11	4	6	14	2	19.
20.	3	18	10	17	7	4	19	1	20	11	2	13	12	6	15	16	9	8	5	14	20.
21.	4	15	11	18	19	3	8	17	10	14	12	5	13	20	6	9	1	16	2	7	21.
22.	1	20	13	12	2	5	10	8	9	15	6	3	14	7	19	18	16	17	11	4	22.
23.	16	14	9	10	8	6	18	2	19	3	5	20	4	17	11	1	13	15	7	12	23.
24.	8	9	16	20	14	12	7	3	13	6	19	15	2	11	18	4	17	10	1	5	24.
25.	2	11	8	6	10	20	5	14	16	12	15	18	1	9	4	7	3	13	17	19	25.
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	

B55

SECRET
R.I.P. 77

NO. 3 - ENCIPHER

ORIGINAL
JANUARY 15, 1941

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

SECRET
R.I.P. 77

NO. 1 - DECIPHER

ORIGINAL
JANUARY 15, 1941

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

B56

SECRET
R.I.P. 77

NO. 2 - DECIPHER

ORIGINAL
JANUARY 15, 1941

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

SECRET
R.I.P. 77

NO. 3 - DECIPHER

ORIGINAL
JANUARY 15, 1941

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

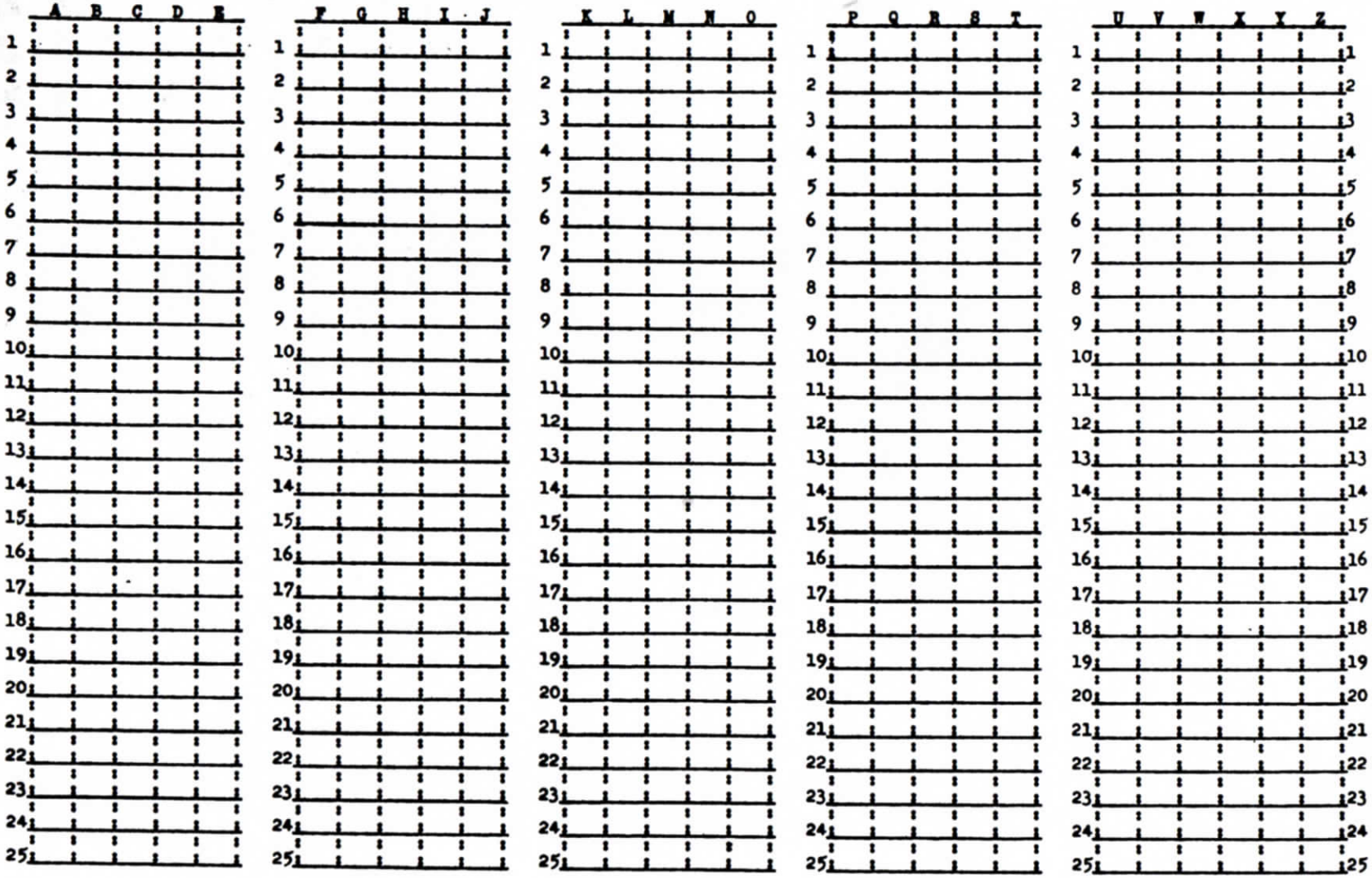
B57

CHAPTER III - Appendix 5

SECRET
R.I.P. 77

WORKSHEET 6-A
Cipher Text Frequency Tally Sheet.

ORIGINAL
15 January, 1941.



SECRET

WORKSHEET 6-B

DIRECT

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

REVERSE

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

SECRET
R.I.P. 77

WORKSHEET 6-C
6's Frequency Tally Sheet.

ORIGINAL
15 January, 1941

1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6
1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6
1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6
1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4 5 6

A5-3

Letters -
Frequencies - 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60

CIPHER TEXT LETTERS
(In order of frequencies)

PURPLE SEQUENCE CONVERSIONS - FEBRUARY 20, 1939, to OCTOBER 31, 1940.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
(A) BASIC																										
	9	18	26	8	17	25	11	7	10	16	1	19	5	14	6	20	22	21	3	24	23	15	4	12	13	2
(B) NORMAL																										

PURPLE SEQUENCE CONVERSIONS - NOVEMBER 1, 1940 to FEBRUARY 28, 1941 : : : : : : : : : : : : :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
(A) BASIC																										
	3	4	22	2	5	21	11	1	14	6	13	15	25	8	26	16	18	17	23	20	19	7	24	10	9	12
(B) NORMAL (FROM TOKYO)																										
	24	25	17	23	26	16	6	22	9	1	8	10	20	3	21	11	13	12	18	15	14	2	19	5	4	7
NORMAL (TO TOKYO)																										
	2	22	4	1	21	5	15	26	14	20	3	11	24	18	25	10	8	9	12	6	7	19	23	16	17	13
*(C) SHIFT (FROM TOKYO)																										
	23	17	25	22	16	26	10	21	9	15	24	6	19	13	20	5	3	4	7	1	2	14	18	11	12	8
SHIFT (TO TOKYO)																										

* Applied after enciphering the first TEN (10) letters of text of certain special dispatches. There is no external or internal indicator to designate dispatches employing the shift.

CHANGE NO. 2
July 1, 1941

PURPLE SEQUENCE CONVERSIONS (MARCH 1, 1941 to _____ _____)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
(A) BASIC																										
(B) NORMAL	24	7	15	19	2	11	25	23	3	6	20	8	22	5	18	12	13	9	21	14	10	1	17	4	26	16
(C) SHIFT	19	15	7	23	11	2	8	18	3	14	24	25	17	13	22	4	5	26	16	6	1	10	21	12	9	20
(D) NORMAL HIKAL	4	5	6	1	2	3	7	15	9	10	11	12	23	14	8	16	17	18	19	20	21	22	13	24	25	26
(E) SHIFT PLUS HIKAL	23	11	2	19	15	7	8	22	3	14	24	25	21	13	18	4	5	26	16	6	1	10	17	12	9	20

A5-B2

(A) Basic sequence from SECTION II.
(B) Normal sequence based on March 1, 1941, instructions.
(C) Shifted sequence - March 1, 1941 to May 7, 1941. Used for speical dispatches after enciphering two groups with normal sequence.
May 7, 1941 to May 15, 1941. Used for all dispatches after enciphering two groups with normal sequence.
May 15, 1941 to _____. Used for all disptaches from beginning of dispatch.
(D) Used for special dispatches Tokyo to Berlin and Berlin to Tokyo March 1, 1941 to May 15, 1941. HIKAL appears before indicator - selector starting points based on normal starting points - change monthly.
(E) Used for special dispatches Tokyo to Berlin and Berlin to Tokyo May 15, 1941 to _____ HIKAL appears before indicator - selector starting points based on normal starting points - change monthly.

SECRET
R.I.P. 77

CHANGE NO. 3
1 May 1942

PURPLE PREDICTIONS JANUARY 1, 1942 TO _____

	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
	O	T	K	H	U	B	R	G	Y	N	S	M	C	Z	E	W	D	F	J	L	A	P	Q	V	I	X
OUR BASIC - JAP BASIC																										

	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
	U	F	M	Q	O	R	H	D	Y	S	C	T	L	J	A	V	W	G	K	B	E	X	P	Z	I	N
JAP BASIC OUR BASIC																										

	A	E	I	O	U	Y	V	B	Z	C	X	W	J	K	F	S	L	P	Q	D	H	G	M	R	N	T
(A)																										
(B)																										
(C)																										
(D)																										

TO GET (B) = (C)(D) EQUALS (A)(B)
TO GET (C) = (B)(A) EQUALS (D)(C)
TO GET (D) = (A)(B) EQUALS (C)(D)

((B)) IS OUR SEQUENCE
((C)) IS BASIC FOR DAY CONVERTED TO JAP
((D)) IS BASIC BELOW NOT CONVERTED

SECRET

SECRET

SECRET
R.I.P. 77

A5-B3

CHAPTER LII - Appendix 6

JAPANESE DISTRIBUTION OF PURPLE SYSTEM

TOKYO	~~WASHINGTON~~
CANTON	
HANOI	HANKOW
SAIGON	
NANKING	SHANGHAI
HARBIN	
HONGKONG	HSINGKING
~~LONDON~~	~~MOSCOW~~
BERLIN	ROME
ANKARA	~~GENEVA~~
PEKING	BANGKOK
AMOY	BERNE
TIENTSIN	VICHY
~~MANILA~~	~~Mexico City~~
MADRID	BUENOS AIRES

CH #2 C.B.H.

BEFORE INVASION

BRUSSELLS

HAGUE

PARIS