~~SECRET~~ Register No. 11

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

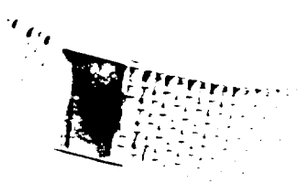
WASHINGTON

ANALYSIS

OF A

MECHANICO-ELECTRICAL CRYPTOGRAPH

PART II



~~SECRET~~

Register No. 11

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

ANALYSIS
OF A
MECHANICO-ELECTRICAL CRYPTOGRAPH

PART II

▼

TECHNICAL PAPER
OF
SIGNAL INTELLIGENCE SECTION
WAR PLANS AND TRAINING DIVISION

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON: 1935

TABLE OF CONTENTS

ANALYSIS OF A MECHANICO-ELECTRICAL CRYPTOGRAPH

PART II

SECTION I

INTRODUCTORY REMARKS

1. **Nature of investigation.**—In April 1932, there was submitted to the Chief Signal Officer a modified form of the Hebern Cipher Machine with a view to testing it for its cryptographic security.[1] It was desired that the test be of the utmost severity, exceeding in severity what could be expected from an attack under the most favorable conditions.

With this in view, there was furnished, with the machine, 55 messages with plain text and 110 messages without the equivalent plain text; also the general system employed in setting up message indicators. (See Appendix I.)

[1] This test was made at request of the Code and Signal Section, Office of Naval Communications, Navy Department. The test was conducted by Mr. F. B. Rowlett, Dr. S. Kullback, and Dr. A. Sinkov, under the supervision of Mr. W. F. Friedman, Chief of Signal Intelligence Section.

SECTION II

DESCRIPTION OF MACHINE AND ITS OPERATION

2. General description.—The 1932 model of the Hebern Cipher Machine consists of a keyboard, a set of five cipher wheels, a set of five pawls for controlling the angular displacements of the cipher wheels, an arrangement for governing the action of the pawls, a mechanical drive for angularly displacing the cipher wheels, and an automatic printer. This model requires a current supply of 110 volts direct current.

3. Motion of the wheels.—From a cryptographic standpoint, the essential difference between this and the previous model rests almost entirely on the difference in the type of cipher-wheel

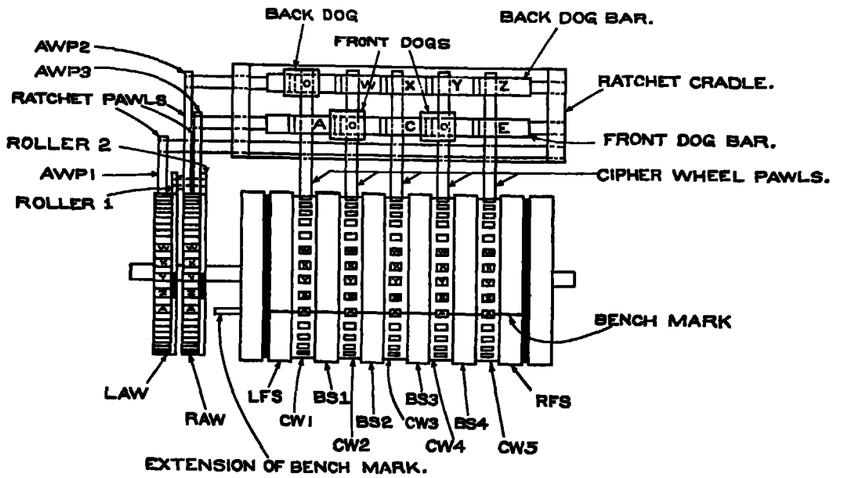


FIGURE 1

displacement utilized by the two machines. (See W. F. Friedman, *Analysis of a Mechanico-Electrical Cryptograph, Part I*, Technical Publication S. I. S., 1934.) In the earlier model, the displacements of the cipher wheels are definitely fixed and invariable, being similar to the movements of the wheels in a recording meter. Only the fifth (or extreme right-hand) wheel steps forward continuously once per depression on the keyboard; the first wheel steps forward once per 26 depressions; and the middle wheel steps forward once per 650 depressions. Wheels 2 and 4 are displaceable only by hand, and not automatically. In the 1932 model the arrangement is no longer meterlike—any two of the five cipher wheels (depending upon the action selected) may move continuously, a third wheel moves one step per 26 depressions on the keyboard, and the two remaining wheels move one step after 650 depressions on the keyboard.

4. Ratchet cradle.—The accompanying diagram, figure 1, shows the mechanical means which causes the wheels to move forward.

This means consists of a rachet cradle upon which are mounted two dog bars carrying three dogs, five cipher-wheel pawls, three aluminum-wheel pawls, and an arrangement (not shown in the diagram) for releasing all the pawls while the wheels are being set. The action of the dogs is controlled by two aluminum wheels, LAW and RAW, which are mounted on the left-hand side of the machine in a line with and on an extension of the shaft upon which revolve the cipher wheels. LAW and RAW, however, move independently of the cipher wheels.

The front dog bar has two dogs mounted upon it and provides five active positions which are designated by the first 5 letters of the alphabet, A, B, C, D, E, as is shown in figure 1. The back dog bar has only one dog mounted upon it, and also provides five active positions designated by the last 5 letters of the alphabet, V, W, X, Y, and Z.

The construction of the two aluminum wheels, LAW and RAW, is identical and is such that the periphery of each of the two wheels is divided into two bands. The left-hand band of each wheel has 26 teeth, each tooth being designated by a letter of the alphabet. The right-hand band is smooth throughout the entire circumference of the wheel except for a notch which extends from the letter Y to the letter Z.

The five cipher-wheel pawls, CWP1 to 5, are mounted upon a shaft which is located underneath the two dog bars. Each pawl has two notches on it (not shown in fig. 1), one situated for acting in association with a dog on the front bar, the other situated for acting in association with a dog on the rear bar. Since the dogs are individually slidable on their bars, the five pawls may act independently. When a dog situated either on the front or the rear bar is in position, the pawl immediately beneath it is withdrawn from its active position and is prevented from stepping the cipher wheel forward, except in those special cases when the action of the dog is neutralized by the action of either the LAW or RAW, as will now be discussed.

5. Functions of LAW and RAW.—The three aluminum-wheel pawls, AWP1, AWP2, and AWP3, are mounted upon an extension of the shaft holding the cipher-wheel pawls. The first aluminum-wheel pawl, AWP1, acts each time a key is depressed and moves the LAW forward one space; that is its only function. The action of AWP2 is controlled by the LAW in the following manner. On the left side of AWP2 there is a projection upon which is mounted a small roller, designated roller 1 in the sketch. This roller normally rests upon the smooth band on the right-hand side of the LAW and, when such is the case, AWP2 is out of action. However, when the LAW moves to the position where roller 1 falls into the notch in the right-hand band, AWP2 acts in two ways: (1) It engages the RAW and moves it forward one space; (2) AWP2 is connected to the back-dog bar by a lever, and the arrangement is such that the action of the back dog is neutralized when roller 1 of AWP2 has dropped into the notch. This allows the cipher-wheel pawl that is temporarily associated with the back dog to engage its cipher wheel and move it forward one space. The roller of the AWP is so placed that when the peripheral letter I on the LAW is at the bench mark, AWP2 engages the RAW, and the cipher-wheel pawl that is temporarily associated with the back dog engages its cipher wheel. Since the notch in the right-hand band on LAW must present itself to roller 1 once per complete revolution of LAW, and since this will happen once per 26 depressions on the keyboard, it follows that the cipher-wheel pawl that is temporarily associated with the dog on the rear bar will step the associated cipher wheel forward one step per 26 depressions on the keyboard.

AWP3 acts both upon the RAW and the front-dog bar. On the right-hand side of the AWP3 there is a roller (roller 2) similar to that on AWP2. Roller 2 rests upon the smooth band of the RAW, except when the RAW is so set that its peripheral letter I is at the bench mark. At this point roller 2 drops into the notch and allows AWP3 to engage the RAW and also neutralize the action of the front dogs, allowing the two cipher-wheel pawls temporarily associated with these dogs to engage the proper two cipher wheels.

6. Detailed study of a particular dog setting.—The consequences of the foregoing arrangement of dogs, pawls, and ratchets can now be made clear. Suppose the two front dogs are set into positions B and D, and the rear dog into position V, as shown in figure 1. Taking the elements of the dog-action setting BDV in alphabetical order, B means that, in general, CW2 will not be allowed to step forward; D means that CW4 also will not be allowed to step forward. Hence, there remain CW1, CW3, and CW5 free to step forward so far as the front dogs are concerned. But since the dog on the rear bar is set at V, and this will affect CW1, it follows that only CW3 and CW5 are free to step forward for each depression of a key, so far as the dogs on both front and rear bars are concerned. Further, whenever the dog on the rear bar, now set at V, is neutralized by the action of roller 1 and AWP2, the result will be that CW1 will be allowed to step forward; and whenever the dogs on the front bar, now at B and D, are simultaneously neutralized by the action of roller 2 and AWP3, then CW2 and CW4 will be allowed to step forward.

The foregoing explanation of dog action and wheel displacements will now be set forth in connection with detailed observations on the actual sequence of events and results. It should be observed at this point that the wheels may be inserted in the machine in either a direct or a reversed position, the two cases yielding entirely different results. As a consequence, any single wheel may be made to serve the part of two if the reversed position be included. The letter d or r will be written after the number of the wheel (as below) to distinguish between these two cases. Thus CW1d and CW1r will mean cipher wheel 1 in the direct and reversed positions respectively. It should also be observed in this connection that the letters on the periphery of a direct wheel progress in reverse order as the wheel moves forward whereas the progression is normal for a reversed wheel. Let us suppose that the wheels are brought to the following initial setting:

LAW	RAW	CW1d	CW2d	CW3d	CW4d	CW5d
H	I	A	A	A	A	A

Let the dog action be BDV. The following represent the successive settings of the wheels as the keys of the keyboard are depressed:

TABLE I.—*Successive settings of all wheels*

[Initial setting, HI–AAAAA; dog action, BDV]

Cycle	Depression number	LAW	RAW	CW1	CW2	CW3	CW4	CW5
1st	1	H	I	A	A	A	A	A
	2	G	H	A	Z	Z	Z	Z
	3	F	H	A	Z	Y	Z	Y
	4	E	H	A	Z	X	Z	X
	5	D	H	A	Z	W	Z	W
	6	C	H	A	Z	V	Z	V
	7	B	H	A	Z	U	Z	U
	8	A	H	A	Z	T	Z	T
	9	Z	H	A	Z	S	Z	S
	10	Y	H	A	Z	R	Z	R
	11	X	H	A	Z	Q	Z	Q
	12	W	H	A	Z	P	Z	P
	13	V	H	A	Z	O	Z	O
	14	U	H	A	Z	N	Z	N
	15	T	H	A	Z	M	Z	M
	16	S	H	A	Z	L	Z	L
	17	R	H	A	Z	K	Z	K
	18	Q	H	A	Z	J	Z	J
	19	P	H	A	Z	I	Z	I
	20	O	H	A	Z	H	Z	H
	21	N	H	A	Z	G	Z	G
	22	M	H	A	Z	F	Z	F
	23	L	H	A	Z	E	Z	E
	24	K	H	A	Z	D	Z	D
	25	J	H	A	Z	C	Z	C
	26	I	H	A	Z	B	Z	B
2d	27	H	G	Z	Z	A	Z	A
	28	G	G	Z	Z	Z	Z	Z
	29	F	G	Z	Z	Y	Z	Y
	30	E	G	Z	Z	X	Z	X
	31	D	G	Z	Z	W	Z	W
	32	C	G	Z	Z	V	Z	V
	33	B	G	Z	Z	U	Z	U
	34	A	G	Z	Z	T	Z	T
	35	Z	G	Z	Z	S	Z	S
	36	Y	G	Z	Z	R	Z	R
	37	X	G	Z	Z	Q	Z	Q
	38	W	G	Z	Z	P	Z	P
	39	V	G	Z	Z	O	Z	O
	40	U	G	Z	Z	N	Z	N
	41	T	G	Z	Z	M	Z	M
	42	S	G	Z	Z	L	Z	L
	43	R	G	Z	Z	K	Z	K
	44	Q	G	Z	Z	J	Z	J
	45	P	G	Z	Z	I	Z	I
	46	O	G	Z	Z	H	Z	H
	47	N	G	Z	Z	G	Z	G
	48	M	G	Z	Z	F	Z	F
	49	L	G	Z	Z	E	Z	E
	50	K	G	Z	Z	D	Z	D
	51	J	G	Z	Z	C	Z	C
	52	I	G	Z	Z	B	Z	B
	3d	53	H	F	Y	Z	A	Z	A
		..	.	.	.	.	.	.	.
	4th	79	H	E	X	Z	A	Z	A
	5th	105	H	D	W	Z	A	Z	A
	6th	131	H	C	V	Z	A	Z	A
	7th	157	H	B	U	Z	A	Z	A
	8th	183	H	A	T	Z	A	Z	A
	9th	209	H	Z	S	Z	A	Z	A
	10th	235	H	Y	R	Z	A	Z	A
	11th	261	H	X	Q	Z	A	Z	A
	12th	287	H	W	P	Z	A	Z	A
	13th	313	H	V	O	Z	A	Z	A
	14th	339	H	U	N	Z	A	Z	A
	15th	365	H	T	M	Z	A	Z	A
	16th	391	H	S	L	Z	A	Z	A
	17th	417	H	R	K	Z	A	Z	A
	18th	443	H	Q	J	Z	A	Z	A
	19th	469	H	P	I	Z	A	Z	A
	20th	495	H	O	H	Z	A	Z	A
	21st	521	H	N	G	Z	A	Z	A
	22d	547	H	M	F	Z	A	Z	A
	23d	573	H	L	E	Z	A	Z	A
	24th	599	H	K	D	Z	A	Z	A
	25th	625	H	J	C	Z	A	Z	A
		626	G	J	C	Z	Z	Z	Z
		7	F	J	C	Z	Y	Z	Y
		8	E	J	C	Z	X	Z	X
		9	D	J	C	Z	W	Z	W
		630	C	J	C	Z	V	Z	V
		1	B	J	C	Z	U	Z	U
		2	A	J	C	Z	T	Z	T
		3	Z	J	C	Z	S	Z	S
		4	Y	J	C	Z	R	Z	R
		5	X	J	C	Z	Q	Z	Q
		6	W	J	C	Z	P	Z	P
		7	V	J	C	Z	O	Z	O
		8	U	J	C	Z	N	Z	N
		9	T	J	C	Z	M	Z	M
		640	S	J	C	Z	L	Z	L
		1	R	J	C	Z	K	Z	K
		2	Q	J	C	Z	J	Z	J
		3	P	J	C	Z	I	Z	I
		4	O	J	C	Z	H	Z	H
		5	N	J	C	Z	G	Z	G
		6	M	J	C	Z	F	Z	F
		7	L	J	C	Z	E	Z	E
		8	K	J	C	Z	D	Z	D
		9	J	J	C	Z	C	Z	C
		650	I	J	C	Z	B	Z	B
	26th	1	H	I	B	Z	A	Z	A
		2	G	H	B	Y	Z	Y	Z
		3	F	H	B	Y	Y	Y	Y
	4	E	H	B	Y	X	Y	X
	5	D	H	B	Y	W	Y	W
	6	C	H	B	Y	V	Y	V
	7	B	H	B	Y	U	Y	U
	8	A	H	B	Y	T	Y	T
	9	Z	H	B	Y	S	Y	S
660	1	Y	H	B	Y	R	Y	R
	2	X	H	B	Y	Q	Y	Q
	3	W	H	B	Y	P	Y	P
	4	V	H	B	Y	O	Y	O
	5	U	H	B	Y	N	Y	N
	6	T	H	B	Y	M	Y	M
	7	S	H	B	Y	L	Y	L
	8	R	H	B	Y	K	Y	K
	9	Q	H	B	Y	J	Y	J
670	1	P	H	B	Y	I	Y	I
	2	O	H	B	Y	H	Y	H
	3	N	H	B	Y	G	Y	G
	4	M	H	B	Y	F	Y	F
	5	L	H	B	Y	E	Y	E
	6	K	H	B	Y	D	Y	D
	7	J	H	B	Y	C	Y	C
	8	I	H	B	Y	B	Y	B
680	9	H	F	Z	Y	A	Y	A
	1	G	F	Z	Y	Z	Y	Z
	2	F	F	Z	Y	Y	Y	Y
	3	E	H	B	Y	X	Y	X
	4	D	H	B	Y	W	Y	W
	5	C	H	B	Y	V	Y	V
	6	B	H	B	Y	U	Y	U
	7	A	H	B	Y	T	Y	T
	8	Z	H	B	Y	S	Y	S
	9	Y	H	B	Y	R	Y	R
690	1	X	H	B	Y	Q	Y	Q
	2	W	H	B	Y	P	Y	P
	3	V	H	B	Y	O	Y	O
	4	U	H	B	Y	N	Y	N
	5	T	H	B	Y	M	Y	M
	6	S	H	B	Y	L	Y	L
	7	R	H	B	Y	K	Y	K
	8	Q	H	B	Y	J	Y	J
	9	P	H	B	Y	I	Y	I
700	1	O	H	B	Y	H	Y	H
	2	N	H	B	Y	G	Y	G
	3	M	H	B	Y	F	Y	F
	4	L	H	B	Y	E	Y	E
	5	K	H	B	Y	D	Y	D
	6	J	H	B	Y	C	Y	C
	7	I	H	B	Y	B	Y	B
710	8	H	F	Z	Y	A	Y	A
	9	G	F	Z	Y	Z	Y	Z
	1	F	F	Z	Y	Y	Y	Y

In the foregoing listing of successive settings, it will be noted that all the wheels progress in accordance with the sequence of letters in the reversed standard alphabet, and that

(1) LAW progresses one step per depression;

(2) RAW progresses one step per 26 depressions except in the first and twenty-sixth cycles, about which more will subsequently be said;

(3) CW1 progresses one step per 26 depressions;

(4) CW2 moves one step immediately after the 1st depression and is stationary thereafter until immediately after the 651st depression;

(5) CW3 progresses one step per depression;

(6) CW4 acts similarly to CW2;

(7) CW5 acts similarly to CW3.

A diagrammatic representation of the displacements of LAW and RAW, coordinated with the foregoing, will be useful. In discussing the diagram it will be convenient to refer to the two cipher wheels which are displaced after every depression on the keyboard as the "1" wheels; the cipher wheel which is displaced after each series of 26 depressions as the "26" wheel; and the two cipher wheels which are displaced after the series of 650 depressions as the "650" wheels.

Cycle	RAW	LAW																									Wheel in position 1
		H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	
1	I	1	(1)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	A
2	G	27	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Z
3	F	53	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Y
4	E	79	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	X
5	D	105	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	W
6	C	131	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	V
7	B	157	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	U
8	A	183	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	T
9	Z	209	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	S
10	Y	235	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	R
11	X	261	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Q
12	W	287	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	P
13	V	313	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	O
14	U	339	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	N
15	T	365	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	M
16	S	391	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	L
17	R	417	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	K
18	Q	443	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	J
19	P	469	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	I
20	O	495	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	H
21	N	521	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	G
22	M	547	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	F
23	L	573	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	E
24	K	599	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	D
25	J	625 (2)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	C
26	I	[3] 651	(4)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	B
27	G	677 (5)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	A
28	F	703 (6)	(7)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	Z

[1] GH–AZZZZ.
[2] CZZZZ.
[3] HI–BZAZA.
[4] GH–BYZYZ=652d letter of message.
[5] AYZYZ.
[6] ZYZYZ (704).
[7] ZYYYY (705).

FIGURE 2

N.B.—The letter I appears on RAW for only one depression of the keyboard. The wheels for the 2d and 705th letters are in the same positions relative to each other. Similarly for the 3d and 706th, 4th and 707th, etc. With the exception of the 1st letter, any two wheel settings separated by 703 letters are in the same relative alignment.

In figure 2 the letters indicated are the letters at the bench mark. The notch in the LAW which controls the motion of the "26" wheel comes into play when the letters opposite the bench mark pass from I to H. Therefore, for each line of the diagram the "26" wheel remains stationary. The "1" wheels move, of course, from column to column but remain fixed in any single column. The RAW is so constructed that no matter what the position of LAW, RAW will move from I to H after one depression instead of after 26 depressions, as is the case in all other letters on RAW. The movement of RAW from I to H induces the movement of the "650" wheels. For the block of 650 outlined, the motion then is as follows: The "1" wheel moves for each letter; the "26" wheel moves in passing from line to line; the "650" wheels move in passing from block to block.

The figure illustrates the most general complete block. A message may, of course, start anywhere within the block.[1]

The diagrammatic scheme of the motions of the wheels enables one to find readily the length of cycle required for the wheels to return to their original relative setting.

Since the "650" wheels move before the "26" wheel has made a complete revolution, the "650" wheels and the "26" wheel will be in the same relative setting *after* $1+\frac{1}{26}$ revolutions of the "26" wheels, i.e., on line 28. The "1" wheels must move one space to catch up to the other wheels. The letters which come from the same relative settings are therefore 27 lines of 26 apart and one column over to the right; that is, the length of this cyclic period is 703 letters $[(27\times26)+1]$.

The importance of a thorough understanding of figure 2 is, that if it is possible to determine exactly when in the course of encipherment of a message the "650" wheels were displaced, it is possible to determine the exact initial settings of LAW and RAW (save for the two exceptional cases referred to in footnote 1 below).

7. Study of cryptographic action.—We may now proceed with a discussion of an actual example of encipherment. Let it be assumed for this example that the initial setting is as follows:

	LAW	RAW	CW1d	CW2d	CW3d	CW4d	CW5d
Permutation of wheels:							
Alignment of wheels:	A	A	A	A	A	A	A

Dog action: BDV
Switch lever setting: "CODE"

[The above setting is that depicted in figure 1]

FIGURE 3

The machine is ready for operation at the instant the current is turned on. Let it be assumed that the message begins

RELIA BLERE PORTS INDIC ATETH ATJAP ANESE
FORCE SHAVE ADVAN CEDON CHINE SEFOR TIFIC
ATION SINTH EWOOS UNGAR EA... .....

[1] There are two exceptions to the situation depicted in figure 2. If the control wheels were set originally at HH, the first block would contain 651 letters, although thereafter the motion would be as in figure 2. If the control wheels were set originally at θI (in which θ is not H), the "650" wheels would move after the first letter was enciphered and thereafter the motion would conform to figure 2.

When the encipherer depresses the key R, two switches are closed. One of these controls the printing circuit and the other the mechanical device which steps the wheels forward. In the printing circuit, the current leaves the contact corresponding to key R, passes to the letter R on the RFS;[1] from R on the RFS it goes through the cipher wheels to E on the LFS; from E on the LFS the circuit goes to the solenoid corresponding to E in the back of the printer where it is translated into a mechanical action, and the letter E is printed.

While the cipher letter is being printed, the magnet controlling the mechanical device is energized and causes the motor to move the ratchet cradle downward and back to its original position. When the cradle has reached its lowest point, CWP3, CWP5, and AWP1 engage their respective wheels and step them forward on the upward thrust. The machine is now in position to encipher the second letter of the message. The setting for the second letter will be ZA–AAZAZ. The enciphering operation is the same for the following 18 letters. However, at the encipherment of the nineteenth letter, the LAW will be so set that I is at the bench mark, and the roller of AWP2 will fall into the notch on the periphery, causing the RAW to move forward. The action of the back dog will be neutralized during this instant, and the cipher wheel pawl governed by it will be permitted to act. Since the back dog is set at V, CWP1 will be liberated and CW1 will move forward one step accompanied by CW3 and CW5. At the *end* of the encipherment of this letter the setting is

LAW	RAW	CW1d	CW2d	CW3d	CW4d	CW5d
H	Z	Z	A	H	A	H

FIGURE 4

For the next 26 letters, CW3 and CW5 will move forward continuously and, with the encipherment of the forty-fifth letter, the action described immediately above will be duplicated.

From this point on, the RAW and CW1 will move forward one step with each 26 letters. However, after $17\times26+18$ letters have been enciphered from the initial setting, the alignment of the wheels will have become

LAW	RAW	CW1d	CW2d	CW3d	CW4d	CW5d
J	J	J	A	J	A	J

FIGURE 5

[1] In the earlier model of the machine when the switch is at the "direct" or enciphering position, the keyboard is connected to the LFS. In the 1932 model, however, the reverse of this is true. The current flows from the key contact to the RFS, through the cipher wheels to the LFS, and from the LFS to the proper solenoid of the printer. For the RFS, LFS, and wiring of the wheels, see pages 12 and 13.

When the key corresponding to the next plain-text letter is depressed, the CWP3, CWP5, and AWP1 will engage their respective wheels and move them forward to the setting

LAW	RAW	CW1d	CW2d	CW3d	CW4d	CW5d
I	J	J	A	I	A	I

FIGURE 6

On the next letter, the roller of AWP2 will fall into the notch of LAW and will cause RAW and CW1 to move forward with CW3 and CW5. The setting is

LAW	RAW	CW1d	CW2d	CW3d	CW4d	CW5d
H	I	I	A	H	A	H

FIGURE 7

Now for the next letter the roller of AWP3 will fall into the notch of RAW and the CWP2 and CWP4 will be liberated so that they may engage CW2 and CW4. The AWP3 will also engage the RAW, moving it forward along with cipher wheels 2, 3, 4, and 5, and the LAW giving

LAW	RAW	CW1d	CW2d	CW3d	CW4d	CW5d
G	H	I	Z	G	Z	G

FIGURE 8

for the encipherment of the next letter. Now CW2 and CW5 will not move forward again until the RAW has been rotated to I. It will be noted in the case considered above, that the RAW on reaching J moves forward two spaces for one revolution of the LAW. This particular setting of the RAW is the only one which allows such a motion.

8. **Action of possible dog settings.**—The displacements of cipher wheels in the example thus far studied corresponded to those for a BDV setting of the dogs. What would happen for other settings? The following table shows the displacements for each of the 50 possible settings of the three dogs:

TABLE II.—*Showing cipher-wheel displacements for all dog settings*

Setting of dogs	Moving per depression					Moving per 26 depressions					Moving per 650 depressions				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
ABV			3	4	5	1					1	2			
W			3	4	5		2				1	2			
X				4	5			3			1	2			
Y			3		5				4		1	2			
Z			3	4						5	1	2			
ACV		2		4	5	1					1		3		
W				4	5		2				1		3		
X		2		4	5			3			1		3		
Y		2			5				4		1		3		
Z		2		4						5	1		3		
ADV		2	3		5	1					1			4	
W			3		5		2				1			4	
X		2			5			3			1			4	
Y		2	3		5				4		1			4	
Z		2	3							5	1			4	
AEV		2	3	4		1					1				5
W			3	4			2				1				5
X		2		4				3			1				5
Y		2	3						4		1				5
Z		2	3	4						5	1				5
BCV				4	5	1						2	3		
W	1			4	5		2					2	3		
X	1			4	5			3				2	3		
Y	1				5				4			2	3		
Z	1			4						5		2	3		
BDV			3		5	1						2		4	
W	1		3		5		2					2		4	
X	1				5			3				2		4	
Y	1		3		5				4			2		4	
Z	1		3							5		2		4	
BEV			3	4		1						2			5
W	1		3	4			2					2			5
X	1			4				3				2			5
Y	1		3						4			2			5
Z	1		3	4						5		2			5
CDV		2			5	1							3	4	
W	1				5		2						3	4	
X	1	2			5			3					3	4	
Y	1	2			5				4				3	4	
Z	1	2								5			3	4	
CEV		2		4		1							3		5
W	1			4			2						3		5
X	1	2		4				3					3		5
Y	1	2							4				3		5
Z	1	2		4						5			3		5
DEV		2	3			1								4	5
W	1		3				2							4	5
X	1	2						3						4	5
Y	1	2	3						4					4	5
Z	1	2	3							5				4	5

Not all the settings shown in table II, however, were used in the test messages, as will be noted from a careful reading of the instructions set forth in Appendix I. Informally, it was stated that a limited number was employed, but the basic principles followed in the selection of settings actually used were not disclosed.

Section III

CRYPTOGRAPHIC ANALYSIS OF THE MACHINE

9. Preliminary preparation.—The first step in the analysis is, of course, to record the exact wiring of the LFS, RFS, and the various cipher wheels, so that the mixed-alphabet sequences may be transcribed upon sliding strips which may be employed in tracing through the exact paths followed by the electric current in encipherment or decipherment.[1] The wiring of the six cipher wheels was kindly furnished by the Navy Code and Signal Section, to eliminate the small amount of labor that would be involved in this determination. The wiring of the LFS and the RFS was determined in collaboration with a representative of the Navy Code and Signal Section, with a simple testing circuit including a voltmeter. The wiring of the foregoing elements is as shown below:

Cipher wheel 1d

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

Cipher wheel 2d

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

Cipher wheel 3d

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

Cipher wheel 4d

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

Cipher wheel 5d

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

[1] See Section III of Part I.

Cipher wheel 6d

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

Bench mark ↓ RFS (right fixed sequence)

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

Bench mark ↓ LFS (left fixed sequence)

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

Figure 9

The foregoing alphabets of the cipher wheels, for purposes of analysis, must be converted into their reciprocals (see par. 8 of Part I), and are then as follows:

NAL_1	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
MAL_1	F	B	Q	M	P	L	N	R	C	H	Z	E	W	A	S	G	T	J	O	V	K	D	I	Y	X	U
NAL_2	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
MAL_2	L	Q	I	E	W	D	X	U	H	R	A	F	O	N	T	K	Z	B	V	P	Y	C	G	J	M	S
NAL_3	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
MAL_3	K	T	R	H	Q	P	Z	X	J	F	N	L	O	E	M	W	D	A	G	Y	C	B	V	I	S	U
NAL_4	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
MAL_4	O	R	A	X	K	M	S	P	L	W	V	H	E	G	J	Q	F	T	B	D	U	Z	N	C	I	Y
NAL_5	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
MAL_5	M	W	J	V	F	K	G	Q	H	A	U	T	P	L	B	Z	E	C	I	X	N	R	Y	D	S	O
NAL_6	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
MAL_6	W	P	A	U	L	F	B	R	O	N	C	Q	X	V	H	E	K	T	I	S	D	Y	G	J	Z	M

Figure 10

The foregoing alphabets are now transcribed upon sliding strips and made ready for use.

10. Classification of messages.—In what follows we shall refer to and classify messages according to the final letter of the dog-action setting, V, W, X, Y, or Z. By a "V" message, for example, we mean one in which the dog-action setting is $\theta_1\theta_2$V; by a "Z" message we mean one in which the setting is $\theta_1\theta_2$Z.

In respect to the foregoing classification, the types of messages which lend themselves most readily to study belong to the "V" or "Z" classes, for reasons which will now be explained. We first take up "V" messages.

11. Conversion of "V" messages.—Suppose that the cipher wheel in position 1[1] has been determined, together with its initial setting and motion. It is then possible to convert the message into a new cipher from which the effect of the LFS and the first cipher wheel has been removed. In fact, if the motion and identity of any number of consecutive cipher wheels begin-

[1] We number the wheel positions from left to right.

71836—35——2

ning from the left have been completely determined, the effect of the LFS and these wheels may be removed from the particular message so that only the remaining cipher wheels have any effect in producing the converted message.

To illustrate, suppose it is known that a particular cipher letter Q representing E_p was obtained with CW1d set at F in position 1. The permutation and settings of the remaining wheels are temporarily of no consequence. Then, since Q on the LFS is opposite position 10 on BS1, the current must have come from the tenth letter on MAL1, viz, S. The S of NAL1 is opposite position 14 on BS2, and it may therefore be concluded that the current producing the letter Q in question passed through the fourteenth contact of the second bakelite separator. This information may be diagrammatically represented as follows:

BS2	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
NAL1	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
MAL1	L	N	R	C	H	Z	E	W	A	S	G	T	J	O	V	K	D	I	Y	X	U	F	B	Q	M	P
BS1	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
LFS	T	E	G	D	N	S	X	U	P	Q	Y	V	H	A	M	B	K	R	F	J	L	Z	I	W	O	C

FIGURE 11

If the successive contacts of BS2 were identified by means of a normal sequence, position 14 would correspond to letter N, and the current could be said to have come from N on BS2. In other words, the action of the last four cipher wheels, i.e., those in positions 2, 3, 4, and 5, may be considered to have resulted in a replacement of E_p by N_c.

If the setting of the second wheel were also known, the conversion, i.e., the elimination of the cipher wheel in position 2, could be carried over to BS3.

Of course, the foregoing applies to a single letter only. But, if the left-end wheels were known not only as to identity and position but also as to motion, then the motion could be taken account of and the conversion carried through for the entire message.

Returning then to a consideration of a "V" motion in connection with the foregoing reasoning; suppose it possible to determine the first cipher wheel and its initial setting. Then, since a "V" motion means that the cipher wheel in position 1 steps forward once every 26 letters, a complete conversion to BS2 can be carried out. Moreover, no difficulty can arise in connection with the exact place in the message where this cipher wheel steps forward, because the initial setting of the first wheel gives the initial setting of the left control wheel and hence determines just where each line of 26 letters begins.[1]

If the converted message is written out in lines of 26 letters, then in each column we have letters which have been enciphered with the last four cipher wheels in exactly the same position; hence all letters within the same column belong to the same monoalphabet. It is thus seen that a "V" message whose first wheel is known, when correctly converted, becomes a polyalphabetic substitution cipher of 26 alphabets. The latter may be recognized or detected by the usual tests based upon repetitions and the normal appearance of monoalphabetic distributions.

12. General observations on "V" messages.—A method of attack is thus indicated. If a message is suspected to be in a "V" motion, a conversion can be carried through for every possible wheel in every possible bench-mark setting. *The correct assumption will yield a message arranged in 26 alphabets*, which may be recognized by the usual external phenomena. Since there are six wheels, each of which may assume two positions and 26 settings on each wheel, the total

[1] See Appendix I, instructions issued with Hebern, par. 2 (c) (2).

number of trials necessary for any single message is $6 \times 2 \times 26 = 312$. For each of these trials the converted message must be tested to determine whether or not it is now in the form of a set of 26 monoalphabets from left to right in the successive columns.

Naturally, for such tests the length of the message is very important, for unless there are enough elements in a frequency distribution it is very difficult to tell whether we are dealing with a random or a polyalphabetic distribution. Consequently, we should make our tests first upon the longest message we can find and then, if no "V" message is indicated, try the next longest message, and so on. Accordingly, Serial No. 183, with 1,420 letters, the longest in the set of 110 cipher messages, was the first one selected for experiment The results were negative, i.e., the tests indicated that the message was not a "V" message. Since the steps followed are the same as in a successful test, the details in connection with this negative experiment can be omitted in favor of those in connection with a successful experiment.

13. Application of principles to a suspected "V" message.—Consider the second longest message, Serial No. 210, with 1,325 letters.

This message begins as follows:

OCRYP HWKON QCPJI MUNDK GZLYY JLFZG . . .

Let us assume that CW1d occupies position 1. Let us further assume that the initial bench-mark setting for CW1 is A, so that 19 letters will be enciphered before CW1 moves. Then the conversion equivalents (to eliminate LFS and CW1) for the first line of cipher text are obtained by setting MAL1–NAL1–BS2 against the LFS so that A on NAL1 is opposite T of LFS (the initial or bench-mark setting).

The diagram of sliding-strip alphabets for the conversion is as follows:

	BS2	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
CW1	NAL1	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
	MAL1	F	B	Q	M	P	L	N	R	C	H	Z	E	W	A	S	G	T	J	O	V	K	D	I	Y	X	U
	LFS	T	E	G	D	N	S	X	U	P	Q	Y	V	H	A	M	B	K	R	F	J	L	Z	I	W	O	C

FIGURE 12

By tracing each cipher letter back from LFS to BS2 on the foregoing diagram, we get the following conversion equivalents:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Cipher	O	C	R	Y	P	H	W	K	O	N	Q	C	P	J	I	M	U	N	D
Conversion equivalents	X	U	J	Z	C	W	Y	T	X	P	H	U	C	V	I	S	R	P	M

FIGURE 13

To obtain the equivalents for the second line of cipher text, we must now shift MAL1–NAL1 one interval forward, to take into account the fact that CW1 has stepped forward one interval. BS2 remains stationary. The diagram of alphabets for this conversion is as follows:

	BS2	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
CW1	NAL1	Z	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
	MAL1	U	F	B	Q	M	P	L	N	R	C	H	Z	E	W	A	S	G	T	J	O	V	K	D	I	Y	X
	LFS	T	E	G	D	N	S	X	U	P	Q	Y	V	H	A	M	B	K	R	F	J	L	Z	I	W	O	C

FIGURE 14

The conversion equivalents for the second line are then as follows:

	1	2	3	4	5	6	7	8	9	10	11	
Cipher	K	G	Z	L	Y	Y	J	L	F	Z	G	. . .
Conversion equivalents	H	C	L	W	I	I	P	W	K	L	C	. . .

FIGURE 15

To obtain the equivalents for the third line of cipher text, NAL1–MAL1 is displaced one more interval (forward) to the right, and so on.

14. **Index of monoalphabeticity.**—When this has been done for the whole message, the columns of conversion equivalents are examined from the point of view of their possible monoalphabeticity. Of course, one could study the columns for repetitions of single letters within columns, as well as for repetitions of digraphs, trigraphs, and polygraphs. But this would require much time and the compilation of many frequency distributions. A better way is to try to establish monoalphabeticity by statistical methods. For this purpose we may set up, theoretically, or by calculation on actual plain text, an index of monoalphabeticity with which a calculation for unknown text should agree within limits of variation due to chance. The plain text should be arranged in horizontal lines and the frequency distributions for individual columns then prepared; in order to have accurate results, the number of columns and the number of elements in each column should be fairly large.

In each distribution the sums of the squares of the frequencies should be found. The index itself and the limits of variation should then be obtained by finding the mean and standard deviation for all frequency distributions. For a monoalphabet of T letters the mean of the sum of the squares of the absolute frequencies is, theoretically, given by $S^2=0.066\ T^2+0.934\ T$. (For a more complete statistical discussion of monoalphabeticity, see S. Kullback, *Statistical Methods in Cryptanalysis*, Technical Publication of the Signal Intelligence Section, 1934.)

To apply these results to the problem in hand however, a slight modification is necessary. The foregoing index applies to the case where a frequency distribution contains T letters and is *strictly* monoalphabetic. In our problem, however, we can never expect these two conditions to obtain, because, firstly, at a maximum there can be only 25 letters in each monoalphabet (for after 25 lines have been enciphered the "650" wheels move and consequently the twenty-sixth letter in the column belongs to a different alphabet than do the first 25 letters); secondly, we do not know where this "650" break occurs in the message. It may occur after the very first line, or after the second, third . . . line. Consequently, it can easily happen that in taking only 26 letters per column we may be assimilating 10 letters of one monoalphabet with 16 of another, or 11 of one and 15 of another, and so on, so that the index for pure monoalphabeticity would never be closely approximated. We may, however, be sure of one thing: If we should

take columns of 36 letters, the number of letters that may fall in the respective alphabets can be only as follows:

TABLE III

Case	First alphabet	Second alphabet	Third alphabet	Case	First alphabet	Second alphabet	Third alphabet
1	0	25	11	14	13	23	0
2	1	25	10	15	14	22	0
3	2	25	9	16	15	21	0
4	3	25	8	17	16	20	0
5	4	25	7	18	17	19	0
6	5	25	6	19	18	18	0
7	6	25	5	20	19	17	0
8	7	25	4	21	20	16	0
9	8	25	3	22	21	15	0
10	9	25	2	23	22	14	0
11	10	25	1	24	23	13	0
12	11	25	0	25	24	12	0
13	12	24	0	26	25	11	0

The worst possible cases for our purposes are those in which three different alphabets enter. The best possible cases are those in which only two alphabets enter.

We may, however, assume theoretically that those ten cases in which the 36 letters fall into three different alphabets would not distort the index for monoalphabeticity very much, since the letters falling in one alphabet (25) are much more numerous than those falling into each of the two other alphabets. In fact, the index may perhaps not be distorted any more in those cases than in the ones where the distribution is 18 in each alphabet, or 17 in one and 19 in the other, or 16 in one and 20 in the other. Consequently, if we consider that the case in which the letters are divided equally between two alphabets is perhaps the worst for our purposes, even then we have only bialphabeticity to deal with.

Our problem is therefore now one not of strict monoalphabeticity but of approximate bialphabeticity. What is the index for that? Actual calculations upon several distributions of sets of 36 letters in two different alphabets gave an average index of 94 for the sum of the squares of occurrences of letters for the case where the 36 letters were evenly divided between two alphabets.

For our purposes, therefore, we may assume an index of 94 to be the minimum permissible in studying columns of 36 letters.

15. **Application to Serial No. 210.**—When the calculations pertaining to this index of bialphabeticity were applied to the various conversions of Serial No. 210, according to the different cipher wheels, the calculation applicable to the case where CW2r was in position 1, with H at the bench-mark setting gave, for the first five columns, indices that seemed conclusive. Thus:

[Index 112]

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
		2	2			3		3	3	2	2		1		4	3		1	3	1	2	2			

FIGURE 16.—*Distribution for column 1*

and similar results for the columns 2, 3, 4, and 5.

The message was accordingly completely converted and transcribed. In this transcription we may place the very first letter of the message under H of the LAW sequence, since under the specifications it is known that the initial setting of LAW and the cipher wheel in position 1 must coincide. Note the repetitions that appear:

FIGURE 17.—*Serial no. 210, converted*

FROM: NAVAL STATION GUAM
TO: OPNAV 3 MARCH, 1932
INDICATOR: 1003 EHHBE VGBKL

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

FIGURE 17.—*Serial no. 210, converted*—Continued

FROM: NAVAL STATION GUAM 3 MARCH, 1932
TO: OPNAV
INDICATOR: 1003 EHHBE VGBKL

	1 H	2 G	3 F	4 E	5 D	6 C	7 B	8 A	9 Z	10 Y	11 X	12 W	13 V	14 U	15 T	16 S	17 R	18 Q	19 P	20 O	21 N	22 M	23 L	24 K	25 J	26 I	
25		D	F	F	R	L	G	O	D	U	Q	N	L	J	S	C	K	W	R	Z	L	D	Z	K	J	S	7
26	Q	V	L	L	A	P	A	Z	L	K	Q	G	A	I	O	P	U	V	F	W	G	U	G	V	C	K	8
27	J	O	E	R	U	S	F	Z	G	I	J	L	N	V	M	S	Q	G	P	J	L	O	M	W	C	X	9
28	N	P	E	H	X	X	B	I	L	C	Q	Q	X	I	S	X	M	V	O	M	Z	H	X	A	C	K	10
29	J	Y	P	C	D	S	D	K	Q	R	H	A	K	I	K	U	I	H	I	A	F	R	W	T	K	I	11
30	P	G	G	Y	O	Z	Q	B	O	K	S	W	B	I	C	L	U	J	K	S	O	J	G	O	P	I	12
31	I	T	Y	D	L	H	S	Q	E	N	C	Z	P	W	S	Q	J	H	X	Y	F	F	W	Y	S	I	13
32	Q	J	T	V	U	F	W	S	T	P	Y	G	B	Z	M	F	Z	K	X	Y	P	B	X	A	I	P	14
33	U	D	P	Z	O	F	E	V	N	I	Z	R	M	F	R	F	B	K	K	X	H	K	P	N	U	U	15
34	T	X	C	R	E	Z	G	I	U	N	Y	C	Q	W	S	C	F	E	Z	S	O	Q	R	U	V	A	16
35	T	V	U	V	E	N	D	H	T	U	O	V	R	T	S	Q	M	J	K	Z	R	Q	W	L	H	I	17
36	T	X	C	R	U	B	P	Q	A	U	N	Y	X	Y	I	C	K	O	D	S	O	W	G	A	W	I	18
37	B	W	R	X	J	G	S	M	L	G	C	L	A	Z	S	U	I	M	P	J	L	U	M	E	D	Y	19
38	A	G	K	D	A	X	W	C	J	H	H	D	D	V	M	S	U	E	F	M	H	Z	D	Y	V	P	20
39	L	W	E	U	O	B	Q	M	L	G	C	L	A	Z	S	U	U	G	P	M	S	U	Y	C	O	G	21
40	E	N	P	C	I	B	G	I	X	B	Q	Q	X	M	K	F	I	M	P	H	P	M	M	D	D	G	22
41	O	Q	E	K	N	N	G	I	U	E	R	J	B	Q	C	I	S	J	I	X	Z	N	D	L	Y	I	23
42	W	D	G	X	Z	N	S	B	O	M	Q	U	P	O	R	F	U	V	O	Z	L	U	C	D	O	L	24
43	W	D	P	C	S	C	S	O	L	G	U	X	A	Z	N	A	J	E	F	S	O	F	W	L	I	K	25
44	A	T	F	D	L	N	S	J	L	N	Y	G	L	E	C	I	I	P	B	Z	C	Q	P	V	B	X	26
45	W	G	L	E	W	G	E	K	X	Z	N	Q	R	E	Y	M	Y	J	W	T	D	K	C	A	V	I	1
46	Q	V	H	U	U	R	H	H	O	M	N	E	H	I	T	C	F	E	B	L	E	R	N	D	Q	X	2
47	X	J	H	C	R	P	F	K	V	G	N	A	B	A	S	X	P	O	A	Q	M	U	A	F	G	E	3
48	T	J	T	X	X	K	Z	R	G	U	B	H	B	G	K	Y	B	K	B	M	O	M	W	D	I	I	4
49	D	T	P	C	P	C	Y	S	T	I	O	Z	P	J	T	Q	X	E	F	U	D	U	Z	W	F	K	5
50	X	J	H	C	L	X	D	Q	O	J	Q	D	U	W	S	I	S	K	P	S	O	R	R	W	V	I	6
51	S	K																									7
51			J	P	D	B	J	R	V	E	S	O	X	X	P	V	A	P	O	B	T	R	F	P	O		7

16. **Relation between alphabets in different blocks.**—It is clear that all the 51 letters in any one column of this converted cryptogram cannot belong to the same monoalphabet. At most, only 25 of them can do so. There may be two or three monoalphabets involved in each column, depending upon where the "650" breaks occur. Thus, we may outline the distribution of the 51 letters as follows:

TABLE IV

Case	"650" break occurs on lines	Number of letters in—			
		First alphabet	Second alphabet	Third alphabet	Fourth alphabet
1	1, 26, 51	0	25	25	1
2	2, 27	1	25	25	0
3	3, 28	2	25	24	0
4	4, 29	3	25	23	0
5	5, 30	4	25	22	0
6	6, 31	5	25	21	0
7	7, 32	6	25	20	0
8	8, 33	7	25	19	0
9	9, 34	8	25	18	0
10	10, 35	9	25	17	0
11	11, 36	10	25	16	0
12	12, 37	11	25	15	0
13	13, 38	12	25	14	0
14	14, 39	13	25	13	0
15	15, 40	14	25	12	0
16	16, 41	15	25	11	0
17	17, 42	16	25	10	0
18	18, 43	17	25	9	0
19	19, 44	18	25	8	0
20	20, 45	19	25	7	0
21	21, 46	20	25	6	0
22	22, 47	21	25	5	0
23	23, 48	22	25	4	0
24	24, 49	23	25	3	0
25	25, 50	24	25	2	0

The question now arises: Can we tell exactly or even approximately where the "650" break or breaks occur? Why not use the repetitions of digraphs and trigraphs as a test? For example, note the long repetition on lines 37 and 39; obviously, the break cannot occur on line 38 or 39, nor, for that matter, on line 37 after the repetition MLG . . . . Nor can the break occur between lines 27 and 37, because the trigraph VMS is common to these lines. Again, it looks as though the break cannot occur between lines 26 and 28, because the digraph CK is common to these two lines. We may now study repetitions within the first half of the message, working toward the middle, lines 25–26, and try to localize the section where the break may be.

By a careful study of what repetitions do appear, we are led to believe that the break occurs on line 25 and we may tentatively block out the message as shown herewith:

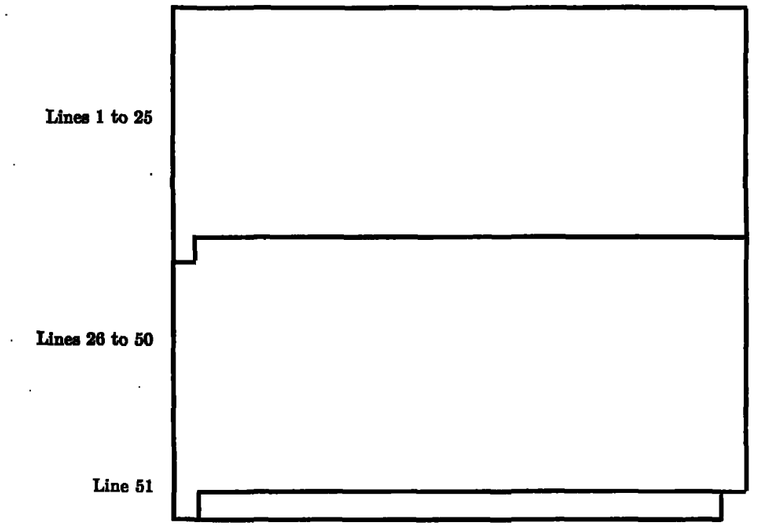


FIGURE 18

If the foregoing is correct, then the second letter of the message indicator (VGBKL) equals I_p. (Refer, in this connection, to fig. 2.)

The following two points in procedure should be carefully observed since they are of frequent application in the solution of the messages submitted.

(1) The method of message indicators is essentially a polyalphabet of five alphabets. As a result, if the letter D in the indicator DMSCH enciphers F_p, then an initial D in any other indicator will also represent F_p. Similarly the determination of the equivalent of any letter in a given indicator gives the equivalent of that same letter in the same position in any other indicator.

(2) The initial setting of a wheel determines whether it is to be inserted in a direct or reversed position. Hence, if it has once been determined that CW1 originally set at F is direct, then any other wheel set at F must also be direct.

We have before us now not one but two independent problems, each involving 26 mixed alphabets, with but 25 letters in each alphabet. (The single letter at the beginning of the message and the last line can be of very little help.) The difficulties of reaching a solution under these circumstances require no further comment.

If we could relate the two blocks in some way, perhaps the difficulties could be reduced. Why not take advantage of the "703" cycle mentioned in paragraph 6, if possible?

Under the conditions of the system we know that after 703 letters have been enciphered the five cipher wheels have returned to their original positions relative to one another. The only change that has occurred in the setting of the machine between the 2d and the 705th letters is that the five cipher wheels have, as though they were permanently fixed on the horizontal shaft, been displaced one step forward between the LFS and the RFS. This is equivalent to a forward step of all the paths which the electric current traces out between the wheels. Consequently, if on the 2d depression a current enters the wheels from the RFS at Y, for example, and emerges from the wheels at T on the LFS, on the 705th depression a cur-

rent entering the wheels from the RFS at L (the letter that follows Y on the RFS) must emerge from the wheels at E (the letter that follows T) on the LFS. Since all letters 703 intervals apart are related in the same manner, we can use this fact to advantage. But, first we must take into account the fact that our transcribed message represents the conversion text, not the original cipher text. How are sequent letters of the LFS related in the converted text? Obviously, the method of establishing the conversion text indicates that if T_c of the original text is replaced by Z in the conversion text, then E_c of the original text will be replaced by A in the conversion text, since T is followed by E on the LFS, and Z is followed by A on the BS2 sequence. (The reader should refer to the sliding strips with CW2r set at H in position 1.)

Now refer to the second letter of the conversion text. It is F, and there are five of them in column 2 of the first block. Whatever θ_p the letter F represents, it is the same for all five occurrences. Suppose for a moment that θ=E. If the letter G which follows F on the bakelite separator were the 705th letter of the converted text, its plain-text equivalent would be K, because K follows E on the LFS. But one can say even more. Since the conversion has produced monoalphabets in the columns of each block, any G_c in the third column of the second block would have the same value as a G_c in position 705. There are two G's in this third column; if the assumption θ=E is correct, then both of these letters must represent K. Such a result is not very likely as we would not expect K_p to occur two times in but 25 letters, hence the assumption θ=E is not a good one. If $\theta=T_p$, then $G=U_p$, which is again unlikely. Thus, we examine all the possibilities and pick out these as most likely:

$F=O_p$	$F=A_p$	$F=N_p$	$F=S_p$
$G=I_p$	$G=M_p$	$G=S_p$	$G=E_p$

FIGURE 19

Enough has been indicated to show the procedure. Were the message long enough, say about 600 words, then there would be available at least four blocks of "703" cycles for comparison and check on assumed values and there is hardly any doubt but that such a message could be solved within a reasonable length of time. One could tabulate the frequencies of A_c in the first alphabet of block I; the frequencies of B_c in the second alphabet of block II; the frequencies of C_c in the third alphabet of block III; and so on. Suppose A_c represents E_p; then B_c, C_c . . . would represent K_p, D_p, . . . in sequence. The weight assigned to a particular arrangement is given by the product of the frequency of each cipher letter and its corresponding plain-text letter. If A_c is assumed to represent T_p, then a different set of plain-text letters and consequently a new total frequency would be obtained. The correct result will be theoretically determined as that one which yields the greatest weight. Letters obtained on this basis can then be inserted in the message. Here, however, we have only two such blocks; sufficient material is not at hand to permit of solution within a reasonable length of time. However, it must be stated that an earnest attempt was made to solve this cryptogram on the basis of the observable repetitions and the "703" phenomenon but without success. It seemed necessary to elaborate better methods of attack if the problem were to be solved at all.

17. **Résumé.**—Let us set down the difficulties in their broad outlines. First, there are those connected with the determination as to whether a given cryptogram is in a "V" motion. We saw that long messages are necessary for this determination and that the process may involve a maximum of 312 different trials, each quite lengthy. Next there come the difficulties of determining just where the "650" break occurs in a message that has been found to be in a "V" motion. Then there come the difficulties involved in attempts to solve a polyalphabetic substitution cipher of 26 nonrelated, random-mixed alphabets, or, at most, of two related sets of such alphabets.

Let us see if we can eliminate some of the difficulties of the first sort and facilitate the discovery of "V" messages.

SECTION IV

SYNOPTIC TABLES

18. **"V" messages with known plain text.**—Suppose we make the problem more easy by studying certain phenomena in a known "V" message with known plain text. Let the message indicator (enciphered) be MCDDU.

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

FIGURE 20

Let us now study certain plain-cipher relationships, in connection with our sliding alphabets. Consider H_p in line 3P, column 3 and H_p in line 4P, column 3; the plain-text letters are the same, the cipher equivalents, different. This difference in cipher equivalents for two similar letters in the same column is occasioned solely[1] by the displacement of the cipher wheel in position 1, for the cipher wheels in positions 2 to 5 are in exactly the same setting in the two cases (since we are dealing with a known "V" message). The same is the case with the following pairs in the same lines:

S_p (line 3P, column 14)=A_c	E_p (line 3P, column 19)=V_c
S_p (line 4P, column 14)=Z_c	E_p (line 4P, column 19)=C_c

FIGURE 21

[1] We assume the "650" break not to occur in the first four lines of the message.

The question arises: Can we find by experiment with the various cipher wheels (or their equivalent sliding strips) which wheel will produce the cipher equivalents indicated above, under the conditions noted there? Consider the case of the two plain-text letters H in lines 3P and 4P. The current corresponding to H_p in both cases entered the cipher wheels from the twenty-third contact of the RFS; its path through the cipher wheels in positions 5, 4, 3, and 2 is unknown, but whatever it is, it left the cipher wheel in position 2 at exactly the same contact in both cases, so that the contact on BS2 from which the current entered the cipher wheel in position 1 is the same in both cases. Now consider what happens at the LFS and the cipher wheel in position 1 (for both cases). The only reason the cipher equivalent for the first H is different from that for the second H is that the cipher wheel in position 1 has advanced one interval, and the current entering it from BS2 in the first instance emerges from the cipher wheel at V on the LFS, in the second instance, at C.

We may take one of the sliding alphabets, say CW1, and place it in position 1, between the LFS and BS2; we may arbitrarily set CW1d at A. We then locate V on the LFS and trace the path of the current from V, through NAL1–MAL1, to a contact on BS2, making note of the latter. We then advance CW1 one interval and repeat the operation, beginning with C on the LFS. If the contact to which the second tracing leads (on BS2) is different from that to which it led in the first tracing, then obviously CW1d cannot be the correct wheel for position 1 if the setting must be A. If CW1d is correct it is not at the correct setting, and we must try another setting. If, however, the two paths lead to the same contact on BS2, then we have an indication that CW1 *may be* the correct wheel for position 1. We say "*may be*" because, unless we can get some further corroboration, this coincidence of exits from CW1 for both cases may simply be accidental and not causal. Therefore, we should try another case where the cipher letters are different for identical plain-text letters in the same two lines, but in another column, e.g., S_p in column 14, yielding A_c in the first encipherment, Z_c in the second. We replace NAL1–MAL1 in its A setting against LFS and BS2 and trace the path of the current from A_c on LFS to BS2; slide the alphabet one interval forward, and trace the path from Z_c on LFS to BS2. If again the current leads to the same contact for both encipherments, a corroboration is obtained for CW1 at the setting and position indicated; if not, then we consider the first coincidence to be purely accidental, and proceed with further tests of the same kind.

These tests would require much time if carried out exactly as indicated above, but we may very materially shorten the work by constructing certain synoptic tables which will, by inspection, yield possibilities for correct cipher wheels and at the same time give the exact setting.

19. **First-interval data, cipher-text relationships.**—Consider CW1d set at A in position 1, and suppose the plain-text letter being enciphered is E.

LFS	T	E	G	D	N	S	X	U	P	Q	Y	V	H	A	M	B	K	R	F	J	L	Z	I	W	O	C
MAL1	F	B	Q	M	P	L	N	R	C	H	Z	E	W	A	S	G	T	J	O	V	K	D	I	Y	X	U
NAL1	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
BS1	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

[4 intervening wheels]

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

FIGURE 22

The current leaves E on the RFS and passes through the wheels in positions 2, 3, 4, 5. The exact path is not known; it depends on the identity and relative position of the intervening wheels. Suppose the path traced leads to position 15 on BS1 opposite O on NAL1. Then the resulting cipher letter is F. After 26 letters have been enciphered, the wheels will be in the following position:

LFS	T	E	G	D	N	S	X	U	P	Q	Y	V	H	A	M	B	K	R	F	J	L	Z	I	W	O	C
MAL1	U	F	B	Q	M	P	L	N	R	C	H	Z	E	W	A	S	G	T	J	O	V	K	D	I	Y	X
NAL1	Z	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
BS1	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

[4 intervening wheels]

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

FIGURE 23

If in this position E is again enciphered, the path traced by the current will again lead to position 15 on BS1, because the four intervening wheels are in the same position as before. Since now, position 15 on BS1 is opposite N on NAL1, the resulting cipher letter is U.

These results indicate that for CW1d set at A, the cipher digraph FU corresponds to a plain-text repetition at an interval of 26 letters or interval 1 down a column. We obtained this digraph by considering the letter E and assuming that the identity and settings of the intervening wheels were such as to carry the current to position 15 on BS1. For a different arrangement of the intervening wheels some other plain-text letter would have led to position 15 and the same cipher digraph would have resulted. Consequently, the identity of the plain-text repetition is not an essential element. For CW1d at A, any plain-text repetition which leads to position 15 on BS1 will correspond to the cipher digraph FU.

Had we assumed a position on BS1 other than 15, a different cipher digraph would have resulted, e.g.:

TABLE V

Position	Digraph	Position	Digraph	Position	Digraph
1	AV	10	RW	19	MP
2	EM	11	LF	20	KB
3	PG	12	SZ	21	CR
4	ZQ	13	DX	22	JT
5	VI	14	XN	23	HL
6	TH	15	FU	24	OA
7	BE	16	NJ	25	WC
8	QK	17	GS	26	YO
9	IY	18	UD		

For CW1d at A, these 26 digraphs represent the only combinations which can correspond to plain-text repetitions at interval 1. Any digraph, not contained in the above set, cannot correspond to a plain-text repetition.

This procedure can be carried out in detail for every wheel and every setting, yielding 26 digraphs for each case. The results can be set up in a series of tables (one for each wheel) which give the correct digraphs for each setting. It must be observed that these results will hold for

interval 1 only. It is possible in the same way to construct tables to correspond to any required interval. On the other hand, it is possible to obtain information about any desired interval from tables for interval 1. To illustrate, we know that FU for CW1d at A is a correct possibility. The correct digraph beginning with U for CW1d at Z is US. Consequently, FS is a correct digraph for interval 2 for CW1d at A. In the same way, since SP is a possibility for interval 1 when CW1d is set at Y, FP is a correct digraph for interval 3 with CW1d at A. The extension to any interval follows along the same lines. One must be careful in working with a reverse wheel to remember that the wheel settings progress in the normal order and not in the reverse order as for direct wheels. These tables are given in Appendix II, basic cipher-text sequences.

Our chief interest in these tables is to be able to pass from a known digraph to a set of possible wheels and settings. To get this information, the tables just described must be rearranged in the following way: Instead of listing the digraphs corresponding to wheels and their settings, we list separately each digraph and the positions for which it is a possibility. This has been done for interval 1 in Appendix III entitled "first-interval data, cipher-text relationships."

20. **Application of first-interval data to a known "V" message.**—Let us now proceed to make use of these tables to try to find which cipher wheel is the one involved in the test message employed as an illustrative example on page 23.

Take the first pair of equivalents:

$$\left.\begin{matrix} H_p \text{ (locus 3P–3)}=V_c \\ H_p \text{ (locus 4P–3)}=C_c \end{matrix}\right\} \text{Case 1}$$

FIGURE 24

Refer now to Appendix III, table V, line C; there are found the following cipher wheels and positions indicated for the digraph VC:

Wheel	Setting	Wheel	Setting	Wheel	Setting
1d	K, L, Z	6d	P	4r	I
3d	V	1r	R	5r	M
4d	N	2r	F	6r	K
5d	A, B, P	3r	G		

FIGURE 25

Take another pair in the same lines of the message:

$$\left.\begin{matrix} S_p \text{ (locus 3P–14)}=A_c \\ S_p \text{ (locus 4P–14)}=Z_c \end{matrix}\right\} \text{Case 2}$$

FIGURE 26

Again referring to Appendix III, table A, line Z, there are found the following cipher wheels and positions indicated:

Wheel	Setting	Wheel	Setting	Wheel	Setting
1d	Z	5d	C, D, Q	2r	F
2d	U	6d	D, O	5r	U
3d	C, S	1r	X	6r	N, J
4d	Z				

FIGURE 27

The only indications common to cases 1 and 2 are CW1d, set at Z and CW2r, set at F for line 3P. This means that if CW1d, set at Z is correct for line 3P, then for the line 1P, CW1 must have been set at B; if, on the other hand, CW2r, set at F for line 3P is correct, then for the first line CW2 must have been set at D. Let us seek corroboration for one or the other of these two possibilities:

$$\left.\begin{matrix} D_p \text{ (locus 1P–13)}=N_c \\ D_p \text{ (locus 2P–13)}=D_c \end{matrix}\right\} \text{Case 3}$$

FIGURE 28

Refer to Appendix III and we find corroboration, for on table N, line D, CW2r at D is indicated as a possibility, whereas CW1d set at B is not so indicated.

For lines 2P and 3P, we should find CW2r set at E indicated for the following pairs:

$$\left.\begin{matrix} A_p \text{ (locus 2P–9)}=X_c \\ A_p \text{ (locus 3P–9)}=D_c \end{matrix}\right\} \text{Case 4}$$

$$\left.\begin{matrix} E_p \text{ (locus 2P–12)}=D_c \\ E_p \text{ (locus 3P–12)}=Y_c \end{matrix}\right\} \text{Case 5}$$

$$\left.\begin{matrix} A_p \text{ (locus 2P–26)}=L_c \\ A_p \text{ (locus 3P–26)}=K_c \end{matrix}\right\} \text{Case 6}$$

FIGURE 29

Referring to Appendix III, it is found that CW2r set at E is indicated for the first two of the three cases, but for the third case, CW2r set at F, not E, is indicated. This is not a contradiction, as will be explained later (p. 37), but it indicates that the "26" break in the lines occurs either at or before column 26. At any rate, there is now no question but that we have located the cipher wheel in position 1, together with its initial setting.

All the foregoing was, however, predicated upon known facts: First the message was known to be a "V" message, and secondly, the plain text was available, so that identical letters in columns were known. What if these two facts were not known?

In order to answer the questions proposed, a slight digression must be made.

21. **Statistical study of "V" messages.**—Consider [1] a large amount of plain text to be at hand. It is desired to determine the probability that two letters chosen at random from it shall be the same. The probability that one of the letters is an E is the normal frequency of E. The probability that both are E's is the square of the normal frequency of E. Similarly, the chance that both are A's is given by the square of the normal frequency of A. The sum of these two numbers gives the chance that the two letters are either both E or both A. The probability that both letters are the same, regardless of what particular plain-text letter they may happen to be, is the sum of the probabilities for each pair of identical letters and hence the sum of the squares of the normal frequencies of all the letters in the alphabet. The calculation on page 27 of Part I shows this result to be 0.066.

If, instead of plain text, one were given a monoalphabetic substitution, the reasoning would still be the same. For the particular identity of the repetition was of no consequence in the reasoning. Moreover, two like cipher letters correspond to two like plain-text letters. Hence, the probability for a repetition of two cipher letters in a monoalphabetic substitution cipher is 0.066.

[1] The reader is advised to review the mathematical analysis contained in the discussion in Part I (pp. 26–31).

Suppose now that a polyalphabetic message is being studied. If the number of alphabets is known, it is possible to rewrite the message so as to break it up into its constituent monoalphabets. If now the number of coincidences is tabulated in each monoalphabet, the situation is still the same. The total number of coincidences for all the alphabets should still correspond to a probability of 0.066.

What happens if the number of alphabets is not known and the message is incorrectly written out? What kind of result will be obtained from a tabulation of the total number of coincidences in such a case? To answer this question completely, it will be assumed that the message under consideration is homogeneous, i.e., that each cipher letter has practically the same probability of appearance as every other one. Such an assumption is not a very great restriction since any fairly good cipher satisfies it. Even a polyalphabetic message with as few as six alphabets has a very flat frequency table. In such a case then, two like cipher letters in a column may represent any plain-text letters whatever. Select a particular cipher letter in a column, say θ_c. The chances that any other letter in that column is θ_c are the same for every cipher letter, i.e., 1/26=0.038. This number is so much less than 0.066 that it should therefore be a simple matter statistically to determine the proper number of alphabets in a polyalphabetic message; for an incorrect assumption will yield only three-fifths as many coincidences as a correct one. The difference between the numbers 0.038 and 0.066 is significant enough to show up very plainly.[1]

22. **Résumé.**—Summarizing what has been said up to this point in connection with "V" motions, it appears that every "V" cipher message can be determined provided only that it be at least 125 or 150 letters long.[2] In determining a message to be "V", the identity and position of the first wheel are obtained as incidental items of information. Moreover, if the message is of sufficient length, the "650" break may be determined by the same analytical test, for that break defines the beginning of a new set of alphabets. The letters above the break will not yield the proper percentage of coincidences with the letters below it and if the message is long enough this property permits the break to be definitely located. This additional information gives the initial setting of the second control wheel and the initial setting of the second wheel. However, it does not determine the identity of the second wheel except in very special cases. (For instance, it might happen that the first wheel in a particular message has been determined to be CW2d set at I. If the second wheel is found to begin at any letter between A and H, it must be CW1, because in the numerical key that letter would have to correspond to 1. Such cases are however very unusual.)

The actual application of the test for "V" messages can now be explained by using a message whose motion and plain text are unknown.

23. **Application of statistical method to an unknown message (Serial No. 169).**—To begin with, the message was written out in lines of 26 letters; only 12 lines were actually used in the test, inasmuch as it was felt that this amount of text was quite sufficient. Twelve lines of text afford 11×26=286 pair of letters (at interval 1) that may be employed to find the cipher wheel—if a "V" motion is involved. According to theory, we should find 286×0.066=18.88, or approximately 19, coincidences; hence, we should find one wheel in one position (all indications being

[1] The advantage of such a method of determining the number of alphabets involved in a polyalphabetic message over the commonly used one based upon repetitions is that a much smaller amount of text is necessary to obtain unquestionable results. It is possible in this way to determine the number of alphabets with only 5 or 6 letters in each alphabet, provided the number of alphabets is fairly large. An illustration of this and other applications will be found in S. Kullback, *Statistical Methods in Cryptanalysis*, Technical Publication, Signal Intelligence Section, 1934.

[2] The total number of possible coincidences will be about $26\times{}^{4}C_{2}=260$; large enough to give fairly reliable results.

reduced to yield the initial setting) indicated about 19 tines. Incorrect wheels should yield 286×0.038=10.8, or approximately 11 indications.

Serial No. 169

INDICATOR: 0003 EHHBE DMSCH

	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
1	F	M	E	I	W	I	G	C	V	C	W	G	F	Q	C	D	V	G	G	L	N	X	V	S	V	P
2	B	W	O	T	C	M	K	F	J	C	E	S	P	O	C	H	P	F	O	L	V	M	O	J	V	A
3	U	Y	R	P	P	S	Y	I	H	I	E	Q	O	N	W	I	M	V	P	B	G	N	J	G	Z	W
4	A	N	C	I	E	K	L	C	B	V	G	V	T	G	D	B	R	K	F	Y	B	Y	Q	X	K	Z
5	C	X	Z	V	B	O	P	M	L	U	B	L	D	Q	X	I	D	W	T	E	H	Z	M	F	D	U
6	N	G	S	G	J	L	N	C	Z	R	M	L	M	X	Q	I	S	U	I	X	M	A	T	R	K	D
7	D	C	W	L	Z	O	T	H	R	G	Z	P	E	Y	K	Y	R	X	R	S	J	P	Z	H	H	Q
8	Z	W	G	E	I	L	A	Y	V	V	E	O	Z	V	Q	P	U	F	E	E	U	S	S	E	A	R
9	Z	W	L	G	B	X	N	S	G	B	E	Y	L	E	A	R	U	C	M	Y	J	P	X	V	R	V
10	H	T	X	N	T	Q	S	X	H	T	Z	H	M	T	H	V	Y	V	A	E	Z	V	Z	Q	S	G
11	U	M	A	H	B	A	B	W	W	O	M	Q	U	D	U	N	I	Y	B	S	F	X	D	W	F	P
12	B	V	E	D	Y	Y	M	O	L	Z	Z	J	S	Y	N	U	G	T	K	R	K	X	W	S	C	C

FIGURE 30

A digraphic table was constructed of the pairs in adjacent lines; thus, for the first and second lines, FB, MW, EO, etc., for the second and third lines, BU, WY, OR, etc.

Referring then to Appendix III, the indications for FB, MW, EO, etc., were distributed in the following manner:

TABLE VI.—*Table for the interval between lines 1 and 2*

	Setting																									
	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
CW1d	2	2		2		3	1		1	1				1		2	2	1		1	1	1				
CW1r		1		2	1	2	1	2	1	1	2	2	1	2	3				1	2	1	3	1	2	2	
CW2d	1	3	1	1	1		1		2	1	2		2			1	1				2	1	1		2	1
CW2r		1	1	2	1	1		2		1	1	2		3			2		1	2	2		2			3
CW3d	2	3	1	1	3		1	1	1	1	2	1	1			1	3	1		3	3		2	3		2
CW3r	2	1		2	1	1	2			2			1	1		1	1	1			1	1		1		3
CW4d		1			1	1		1	2	2		1	1	1		4	3		1	1		1	1	1	1	3
CW4r			1	2	2						1			2	1	1	1		1	1			2	2		1
CW5d					1	3	1	1		1	2		1	2	1		2		1	1		1		1	1	1
CW5r	2	3		1	1	1	1	1							1		1	1	3					1	2	.
CW6d	2	1		1		2		1	1	1	2	2			1	1	1	2	1	1	1	3			1	2
CW6r		1		1	3		1	2			1	2		3	1	1		1			1			1		1

71836—35——3

The indications for BU, WY, OR, etc., were then distributed in the same table, but the positions indicated were reduced to initial settings.

This process was continued for all the other pairs in the digraphic table, with this final result:

TABLE VII

	Setting																							
	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
CW1d	13	12	13	15	16	24	5	7	13	10	8	10	11	9	9	16	10	8	7	10	7	6	10	11	11	10
CW1r	9	16	11	9	7	18	5	12	9	8	10	12	11	10	9	10	7	7	11	10	8	12	14	12	15	19
CW2d	11	15	7	10	16	9	7	14	10	14	10	9	9	10	11	8	6	8	18	9	9	8	13	6	17	8
CW2r	10	13	9	14	15	19	7	15	9	7	16	12	13	15	15	16	10	10	8	4	12	5	11	6	7	16
CW3d	18	13	11	9	17	5	10	9	12	9	12	9	11	9	4	11	14	6	14	14	6	11	7	13	11	13
CW3r	5	13	8	12	13	9	9	10	5	8	14	8	11	11	11	12	8	13	9	16	10	17	8	10	17	10
CW4d	7	13	11	16	12	13	6	17	7	10	13	16	15	13	10	14	8	7	8	8	10	12	8	13	13	12
CW4r	9	9	9	13	12	15	9	10	8	8	11	11	10	12	16	14	15	9	14	10	6	9	10	13	10	13
CW5d	16	17	10	16	11	15	10	11	10	13	12	12	11	6	12	10	14	6	13	7	15	20	10	11	7	9
CW5r	12	19	14	13	17	12	7	9	13	11	14	6	7	13	15	9	13	4	12	14	8	13	12	8	15	16
CW6d	13	12	12	11	11	13	11	18	6	12	12	8	10	12	10	10	11	9	12	8	11	15	7	11	17	8
CW6r	8	9	9	6	10	9	7	10	14	12	11	14	9	13	14	14	12	11	9	12	7	12	12	13	7	15

Note now the number of indications for CW1d at F; it is 24 as against an average of 11.0 for all other alphabets and positions. This means that not only are we dealing with a "V" message, but also the theoretical expectancy, 19, was really lower than the actual, 24, and that there are more repetitions in columns than was anticipated.

As a check on this result the same process was carried out for interval 2, that is, the letters of line 1 taken to form pairs with the letters in the same columns of line 3; those of line 2 with those of line 4, etc. The total number of tabulations is 260, the expected number of coincidences, 17. The actual number found for the setting F, CW1d was 20. The percentage of coincidences for 286+260=546 digraphs for the setting F, CW1d is therefore 8.1 percent instead of the theoretical 6.6 percent.

This result is really better than was anticipated. There can hardly be any doubt but that the right wheel and setting have been found. In less-fortunate cases, it may be necessary to tabulate and sum the data for several intervals before a conclusive result can be obtained.

It should be observed here that the occurrence of the "650" break in a message may cause some difficulty in the actual test. Any two lines which have the break between them will not furnish correct information. However, for small intervals the degree of error introduced is practically negligible. For example, in using interval 1 only one pair of lines at most will be incorrect, viz, those with the break between them; for interval 2 only two pairs, etc. In a message of at least six lines, the correct result will still be obtainable.

Having found the correct setting for the cipher wheel in position 1, it follows that the letter D in message indicator DMSCH must equal F_p; also F indicates that a wheel is in the direct position.

When message Serial No. 169 was converted so as to remove the first cipher wheel from consideration, the following polyalphabetic message resulted:

FIGURE 31.—Serial No. 169 converted

1	D Z T U C U R O Q O C R D P O G Q R R Y V H Q E
2	Q A W G R C T O B L E T I N J R T Y J L R D V O R E
3	V S U G I X X H G W N W R D M Q V W B Y X C T Q S T
4	E V L C H A O R B H I M P M Q P K I D R T E I E V F
5	R U L Z I A J D B S V X J V Q M Z G Q U F Y H I S E
6	Q X Y Z C Z A O Y E N K J O J P I T C W T P J F S K
7	D R W M K U C H A S E V C J B T I T E R E.Z Y J C S
8	S N G S I U R Z B L K K U O G K D Y P A U U P Q Q U
9	B T W P R G H Y L D G H F E R F V A J C I E U Q Y S
10	A S B R E K R Y S E B R P B N R B A W A C V P A P Y
11	S X A R I U L I L D D F R E A V A H Q Z L O S B V D
12	S W P W K L A A T E M R R B F A N I Q Z S O S C Y F
13	X X B I C K C D W V R Z X R B G E Z V H I O F L B L
14	V T E R M C K V L B P I G X H Q A L Q C I E P V Y F
15	V X G W M H W C V N S Z F T Y A V Y Q S M O K G W R
16	M O A S S G J E Y T G Z W T V Z J J S C E C L A Q Q
17	B G M U Q G S Q N D X N C U N Z J S V C I E N Q V X
18	S P H I V N L A E J M A U Y K Q B P D C N Z U U G Z
19	J U J T T K S M S K S Z E T R A V T Y J K V C T N Y
20	V U Q I N K V G

A study of the repetitions in the message and of the monoalphabets down each column seemed to indicate that the "650" break occurred between lines 6 and 9. On using the analytical test based on coincidences, it turned out that the break was either on line 7 or 8 and consequently the second letter of the message indicator must be either P or Q. The number of coincidences obtained when lines 7 and 8 were tested with the preceding lines were so nearly alike as to yield no definite information. Hence, in the message indicator DMSCH, M_c=P or Q.

Enough has been shown, it is thought, to indicate the procedure that was followed with unknown cipher messages to determine whether or not they were "V" messages; when encountered, the value of the first letter of the message indicator, and whether its plain-text equivalent meant "direct" or "reversed" constituted important collateral information.

After testing out the method on several unknown cipher messages and finding it to be efficacious, there seemed to be no point in spending further time with similar cipher messages with unknown plain text. After all, the cipher messages with known plain text would yield identical results in much shorter time, since identities of plain-text letters were indicated in the messages themselves when transcribed in lines of 26 letters. Consequently, all the plain-text messages were studied in connection with their cipher versions in order to shorten the time required for a complete solution. The possession of the 55 "known" cryptograms admittedly facilitated solution of the 110 "unknown." Nevertheless, the solution was not made possible by, and would not in practice require possession of, plain-text messages with their

cryptographic equivalents. After several days' work along these lines, many values and determinations were obtained from the procedure.

24. **Consideration of "W" messages.**—The foregoing methods are applicable to "V" motions. How about "W" motions? In a "W" motion the first wheel is either stationary or moves continuously; the second wheel moves every 26. The proper assumptions regarding the setting of the first wheel and its motion together with a correct assumption as to the second wheel makes the problem equivalent to the one just discussed. This procedure is a bit more complicated since it involves trials on two wheels and the number of necessary trials is therefore greatly increased but otherwise the two problems are identical. There is no reason why such messages cannot be picked out by the above procedure. In the present test such a situation did not arise because it was found possible to get sufficient information from "V" motions and "Z" motions (to be discussed) to obtain a complete solution of the problem.

A particular idea in this connection should be emphasized. Suppose that in a given series of messages all of the "V" messages are found before a search is begun for "W" messages. In such a case, the number of trials mentioned above is considerably reduced, since in many of the "W" messages the first letter will be known. Any wheel assumed in the first position will then be entered in only one possible setting and the determination of "W" messages will not be of much greater difficulty than the determination of "V" messages.

Similarly, after all the "W" messages have been found, a search can be made for "X" messages by assuming the first three wheels, two of which will in some cases be known.

A general solution can be arrived at by such a procedure.

25. **First interval data, plain-text relationships.**—It has already been remarked that the messages most amenable to study are those whose motions are either "V" or "Z", but as yet nothing has been said about the latter. In such a motion, if the message is written out in lines of 26, and letters down a column are considered, the fifth wheel is the only one which has moved. This property may be put to use in a manner similar to that employed for "V" messages.

Suppose that the wheel in position 5 is CW5d set at A, and that the plain-text letter being enciphered is E. The current passes from E on the RFS to Y on MAL5 thence to Y on NAL5.

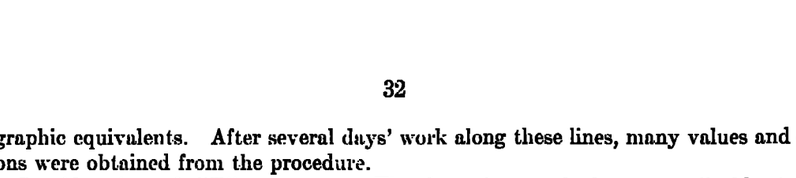


FIGURE 32

From this point on, it goes through the remaining four wheels, finally emerging at some cipher letter θ_e. After the encipherment of 26 letters, CW5 has moved to setting Z.

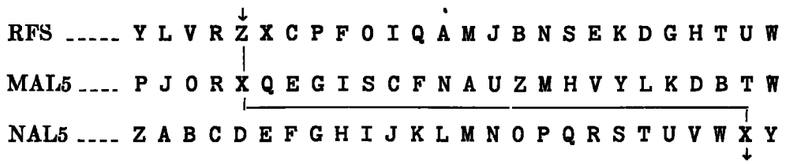


FIGURE 33

If now the plain-text letter be Z, the current passes from Z on RFS to X on MAL5 thence to X on NAL5. The current is now at the same point on BS4 as the current for the preceding E. Since the other four wheels are in identically the same position as before the path traversed through

them by the current is the same in both cases and the same cipher letter will result. It thus follows that for CW5d set at A, the sequence EZ of plain-text letters at a distance of 26 will yield a cipher repetition. Similarly the sequence AB will yield a cipher repetition. Continuing in this way, it becomes possible to set up 26 digraphs which represent all the possibilities of plain-text pairs which shall yield like cipher letters when CW5d is in the fifth position at A. These digraphs are:

TABLE VIII

AB	HM	NP	UE
BD	IC	OT	VX
CQ	JK	PS	WV
DL	KG	QN	XH
EZ	LA	RW	YF
FR	MU	SJ	ZY
GI		TO	

It is to be observed that it makes no difference just what the cipher letter is. That will depend on the first four wheels. The essential element is the fact that the cipher letter repeats. Any digraph not contained in the above 26 cannot yield a cipher repetition for CW5d set at A.

Let this procedure be carried out for every wheel in every setting. A series of tables will then be obtained which will give the 26 digraphs corresponding to cipher repetitions for any particular wheel in any given setting. It is, of course, understood that this information will apply only to interval 1, i.e., to letters which are 26 apart in the plain text.

For intervals other than 1, a similar procedure can be followed which will give the same type of information. Thus, one can construct tables which will give the correct digraphs for interval 2 or interval 3. It is, however, possible to derive all of these further tables from the tables for interval 1. For if P_1P_2 is a possibility for CW1d at Y and P_2P_3 is a possibility for CW1d at X, both being considered for interval 1, then P_1P_3 is a possibility for CW1d at Y for interval 2. Similarly if P_4P_5 is a possibility for CW1r at A and P_5P_6 for CW1r at B, both for interval 1, then P_4P_6 is a possibility for interval 2 on CW1r at A.

It is possible in this way to combine digraphs for different intervals and get desired information about any interval whatever. All of this information can be conveniently combined into one set of tables (one for each wheel) which have been designated "Basic Plain-Text Sequences" (Appendix IV). To explain just how these tables are used, reference is made to the square for CW1d. The letters down the outside of the box represent the settings of the wheel. If, for CW1d, digraphs are desired for interval 1 at setting A, the first letter is read from line A, and the second is found by reading diagonally to the right, thus YT, HX, ZY, etc. For interval 2 at setting A, the first letter is again found on line A, the second is one removed along the diagonal, e.g., YC, HL, etc. In every case, the first letter is found on the line corresponding to the desired setting and the second letter is obtained by reading diagonally downward and to the right. The distance between the first and second letters of the digraph is the interval under consideration.

Suppose the tables for interval 1 are inverted, i.e., suppose that the data above obtained is arranged with respect to the digraphs and not with respect to the wheels and their settings. This will be found in Appendix V, "First-Interval Data, Plain-Text Relationships". Then the

tables will give information of a different character. Thus, under the letter B, it is found that the digraph BJ will yield a cipher repetition for each of the following settings:

d	r
1Y	1D
2M	2T
3F	3Z
4O	5T
4R	5V
4Y	

FIGURE 34

The diagraph BN will yield a cipher repetition only for CW4r at 0; there is no other possibility. Similarly, any particular digraph is associated with a definite set of possibilities for the wheels and their settings. It is interesting to note that the wheels are so constructed that no plain-text doublet can ever yield a cipher doublet for interval 1.

26. Application of plain-text relationships to messages with known plain text.—The application of the above information to the discovery of "Z" messages when the plain text is known is very simple. Consider Serial No. 155.

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

	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
11	F	O	U	R	T	H	C	O	M	M	A	B	U	T	L	A	R	G	E	C	R	O	W	D	S	W
	V	N	S	G	K	Q	P	G	O	R	P	K	A	U	M	C	Y	J	J	R	V	M	B	B	S	W
12	E	R	E	D	I	S	P	E	R	S	E	D	B	Y	P	O	L	I	C	E	A	N	D	N	O	S
	Z	S	A	K	G	D	F	H	W	S	W	L	E	J	G	Q	D	D	U	D	Z	R	N	N	C	E
13	E	R	I	O	U	S	D	I	S	T	U	R	B	A	N	C	E	T	O	O	K	P	L	A	C	E
	D	A	E	J	G	O	P	K	M	Q	L	S	G	I	W	Q	Q	W	O	E	K	F	R	L	C	N
14	P	E	R	I	O	D	S	H	A	N	G	H	A	I	I	S	S	H	O	W	I	N	G	S	O	M
	V	R	L	F	M	I	R	D	W	H	U	W	S	Z	I	L	V	H	U	A	E	A	J	G	A	U
15	E	S	I	G	N	S	O	F	G	R	A	D	U	A	L	L	Y	R	E	S	U	M	I	N	G	N
	N	N	U	W	D	M	A	B	E	L	B	R	N	G	N	T	L	U	I	K	Q	C	C	F	C	S
16	O	R	M	A	L	C	O	N	D	I	T	I	O	N	S	P	E	R	I	O	D	A	D	M	I	R
	Q	D	N	Q	F	T	H	R	A	L	E	L	C	V	J	C	X	D	X	M	B	I	T	G	B	Z
17	A	L	K	E	L	L	Y	I	N	F	O	R	M	S	M	E	T	H	A	T	H	E	H	A	S	B
	N	T	D	O	Q	K	M	A	Z	Q	R	D	I	M	U	B	P	X	B	Y	B	O	T	E	P	N
18	E	E	N	A	S	K	E	D	B	Y	H	I	S	G	O	V	E	R	N	M	E	N	T	W	H	Y
	K	Z	T	A	G	I	F	I	V	Q	W	D	H	X	U	B	E	J	G	A	A	U	D	J	J	L
19	H	I	S	R	E	L	A	T	I	O	N	S	W	I	T	H	M	E	W	E	R	E	N	O	T	C
	D	L	E	Z	Z	C	P	E	A	J	U	R	M	U	D	W	R	U	J	A	M	D	J	M	D	P
20	L	O	S	E	R	P	E	R	I	O	D	O	U	R	R	E	L	A	T	I	O	N	S	H	A	V
	B	L	M	B	U	D	Z	G	K	H	E	F	X	A	B	V	K	N	H	Y	Q	T	F	E	L	R
21	E	B	E	E	N	C	L	O	S	E	A	N	D	C	O	R	D	I	A	L	A	N	D	H	E	H
	B	T	Q	U	W	C	P	V	C	E	W	K	L	L	M	J	O	K	L	R	W	S	E	B	A	F
22	A	S	K	E	P	T	U	S	F	U	L	L	Y	I	N	F	O	R	M	E	D	O	F	A	L	L
	D	Z	L	M	K	V	K	Z	V	T	R	X	V	L	M	Z	F	H	P	U	P	U	Z	G	C	X
23	S	T	E	P	S	H	E	H	A	S	T	A	K	E	N											
	E	H	Z	L	C	P	L	Z	R	X	L	O	W	Q	P	G	O	P								

FIGURE 35

On lines 1 and 2, the plain-text digraph EI corresponds to the cipher repetition VV in column 6 and to the repetition RR in column 16. If the message is a "Z" message, then the only possibilities for the last wheel are

d	r
2G	1I
2I	3B
2W	6E
3B	
3Y	
4I	
6B	

FIGURE 36

Now consider the digraph GE which in column 18, lines 2 and 3 corresponds to the cipher repetition HH. The possibilities which it yields for the fifth wheel are

d	r
1W	2M
1F	3M
2H	4H
2L	4R
3H	4Z
5W	6B
	6J
	6T
	6X

FIGURE 37

But it must be remembered that in passing from line 1 to line 2, the setting of wheel 5 has changed in the reversed direction for a direct wheel and in the normal direction for a reversed wheel. To compare the second set of possibilities with the first, it is therefore necessary to compensate for this shift. The second set of possibilities will then become

d	r
1X	2L
1G	3L
2I	4G
2M	4Q
3I	4Y
5X	6A
	6I
	6S
	6W

FIGURE 38

It is now found that only one entry is common to both sets, viz: CW2d at I. If the message is a "Z" message and the fifth wheel is 2d set at I, it should be possible to check this fact by using other cipher repetitions, for example, WW in column 12, lines 3–4. The plain-text digraph to which it corresponds is EI and one would expect 2G to be listed as a possibility under this digraph. This is found to be the case. Similarly, the digraph TH in column 15, lines 5–6 is found to check. The necessary conclusion must then be that we are dealing with a "Z" message whose fifth wheel is CW2d initially set at I.

If a procedure such as has been outlined above does not result in one setting common to all the possibilities, the message cannot be a "Z" message.[1]

It is thus seen that if the plain text is known, the discovery of "Z" messages is a matter of relative simplicity and that each time such a message is found the identity and position of the fifth wheel are determined. But this is not all the information which is obtainable. The same test that has already been applied will give information about the first two wheels.

[1] If only one or two of several yield apparent contradictions, they may be the result of factors which are explained in what follows.

To see how this comes about we proceed as follows: Consider the cipher repetition BB on lines 20–21 in column 1. The corresponding plain-text digraph is LE. Since the fifth wheel is originally set at I and progresses in a reverse direction, it should have arrived at R for line 20. In other words, one of the possibilities which should appear under LE in the tables of interval 1 is 2Rd. But, on reference to the tables, this entry is not found opposite LE, although 2Qd is found. The explanation for this appearance is not difficult. When a message is written out in lines of 26, the first column should be that one which corresponds to H on the first control wheel. This was not taken into account when the cipher message was set down, and it would consequently be expected that some of the columns would be out of place. That is exactly what happens in this case. Column 1 really belongs on the right of column 26 and the digraph BB should appear on lines 19–20 rather than on lines 20–21. For these lines, it would be expected that LE would correspond to 2Qd, as it actually does. (One must be careful not to overlook this fact in searching for "Z" messages.)

The question now arises: "Does column 2 belong on the left or right?" In order to answer it, one must first find a cipher repetition in column 2 and check the corresponding plain-text digraph against the tables. When this is done with LL on lines 19–20, it is found that column 2 really belongs to the right of column 1.

The continuation of this reasoning introduces the use of other intervals than 1 since neither column 3 nor column 4 contains a cipher repetition at that interval. But this is not an essential difficulty. The use of interval 1 up to this point has been purely a matter of convenience; any other single interval or even any combination of intervals would have given the same results. It is found by this procedure that columns 3 and 4 also belong on the right leaving column 5 as the H column of the final set-up.

These results have two important consequences. In the first place, the letters $\begin{matrix} J & A & P & A \\ K & C & M & I \end{matrix}$ at the beginning of the message must stand alone at the right end of line 1. They correspond to a different setting from that indicated by the letters beginning $\begin{matrix} N & E & S & E & \cdot & \cdot & \cdot \\ Z & V & U & F & \cdot & \cdot & \cdot \end{matrix}$. But it was these latter letters which corresponded to the setting 2Id. Consequently the message really begins with the fifth wheel 2d at J and not I.

Secondly, since the fifth column corresponds to H on the left control wheel, it follows that the initial setting of the control wheel is L. Moreover, that initial setting gives the setting of the first cipher wheel. This means that the indicator EQPRZ of Serial No. 155 is deciphered as L...J.

This is not yet all the information which might be obtained from this message. Suppose it were long enough to contain the "650" break. Could not that break be located by the same procedure? To this end let us theoretically consider the line on which the break takes place. This break is due to a motion of two of the first four wheels which had been stationary throughout. The relative setting of all four as a unit is therefore changed and it is no longer correct to say that the first four wheels remain unchanged down a column. But that was the very property which permitted us to make use of the tables of plain-text relationships, and since it no longer holds, the line on which the break takes place will not check with those above it. It will check only with those below it.

The application of this notion is quite simple. It is merely a matter of finding the first line which does not check with those above it. Serial No. 115, indicator R3PVQ, furnishes a good example of this procedure.

SERIAL NO. 115

	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
1	E	S	T	I	M	A	T	E	S	I	T	U	A	T	I	O	N	T	W	E	L	V	E	H	U	N
	G	Q	C	B	F	H	A	N	W	J	I	P	D	N	A	C	U	M	I	I	K	L	P	L	A	V
2	D	R	E	D	T	W	E	N	T	Y	O	N	E	F	E	B	R	U	A	R	Y	J	A	P	A	N
	B	E	G	C	L	L	L	V	C	O	F	Q	G	O	Z	A	B	X	O	R	B	O	U	E	M	F
3	E	S	E	F	O	R	C	E	S	A	S	H	O	R	E	I	N	C	L	U	D	I	N	G	N	A
	D	U	P	W	D	E	K	T	D	V	U	U	D	M	O	B	T	W	U	J	P	D	O	M	F	X
4	V	Y	T	W	E	N	T	Y	T	W	O	T	H	O	U	S	A	N	D	T	H	R	E	E	H	U
	D	X	H	C	P	W	X	P	M	K	R	M	U	K	S	Y	R	P	J	T	F	L	H	G	L	K
5	N	D	R	E	D	O	F	T	H	E	S	E	T	W	E	N	T	Y	F	I	V	E	H	U	N	D
	U	V	K	K	Y	P	L	V	E	F	M	F	S	S	D	J	A	N	N	L	W	P	C	L	P	Y
6	R	E	D	I	N	W	O	O	S	U	N	G	A	R	E	A	O	P	P	O	S	I	N	G	C	H
	J	R	C	E	G	X	W	G	M	I	B	A	V	T	I	G	P	C	C	V	Z	Y	P	L	B	C
7	I	N	E	S	E	F	O	R	C	E	S	A	B	O	U	T	F	I	F	T	Y	F	I	V	E	T
	O	S	D	K	O	B	A	R	Z	A	P	H	O	N	M	G	M	K	M	X	T	J	J	R	T	D
8	H	O	U	S	A	N	D	J	A	P	A	N	E	S	E	F	O	R	C	E	S	M	O	V	I	N
	G	I	J	H	B	Y	K	E	V	L	I	G	F	Z	V	X	Y	A	J	C	O	L	G	J	E	Z
9	G	A	B	O	U	T	S	H	A	N	G	H	A	I	A	R	E	A	F	I	F	T	Y	S	E	V
	P	K	D	H	N	D	F	R	Z	L	Z	L	W	J	W	R	G	U	C	Y	K	N	D	H	M	N
10	E	N	V	E	S	S	E	L	S	I	N	J	A	P	A	N	E	S	E	A	D	V	A	N	C	E
	H	B	Z	D	T	L	A	D	J	I	T	F	F	Z	V	C	T	C	K	C	Y	A	K	O	I	K
11	O	N	K	I	A	N	G	W	A	N	Y	E	S	T	E	R	D	A	Y	V	E	R	Y	L	I	T
	N	K	Z	A	N	Q	K	J	L	Z	K	M	I	O	A	L	F	O	X	F	Z	P	T	O	T	T
12	T	L	E	P	R	O	G	R	E	S	S	M	A	D	E	A	N	D	A	T	T	W	E	L	V	E
	Y	F	M	M	X	Y	A	Y	L	L	A	N	Z	G	X	A	Z	P	Q	O	F	L	E	R	S	I
13	H	U	N	D	R	E	D	C	H	I	N	E	S	E	S	T	I	L	L	H	O	L	D	I	N	G
	J	F	H	N	P	G	G	W	Y	K	L	M	U	H	A	B	J	L	O	R	J	P	D	A	H	H
14	W	E	S	T	E	R	N	E	N	D	O	F	T	O	W	N	C	H	I	N	E	S	E	E	N	T
	P	Q	W	I	Z	R	S	T	F	Y	J	Y	X	Z	I	Y	S	T	P	A	Q	G	H	T	U	G
15	R	E	N	C	H	E	D	W	E	S	T	O	F	R	A	I	L	W	A	Y	A	N	D	Y	E	S
	M	D	J	L	P	Z	K	O	B	O	C	H	I	D	S	H	H	Q	B	C	N	C	L	P	C	S
16	T	E	R	D	A	Y	H	A	D	O	N	L	Y	A	F	E	W	O	U	T	P	O	S	T	S	I
	K	N	R	R	Y	N	C	X	O	H	J	D	G	E	K	I	E	E	I	N	E	X	W	G	V	A
17	N	K	I	A	N	G	W	A	N	B	A	T	T	L	E	A	R	E	A	I	T	I	S	E	V	I
	L	V	E	U	E	O	S	T	M	M	E	P	L	G	Z	R	L	O	I	F	G	W	S	A	A	G
18	D	E	N	T	I	N	T	E	N	T	I	O	N	O	F	J	A	P	A	N	E	S	E	I	S	T
	W	U	V	F	S	S	H	G	U	M	Y	E	F	Y	H	E	D	U	K	N	P	C	T	X	F	X
19	O	E	X	E	C	U	T	E	A	N	E	N	V	E	L	O	P	I	N	G	M	O	V	E	M	E
	U	A	W	J	K	S	A	W	Q	Q	W	C	Z	C	P	F	H	Z	X	K	K	B	U	P	P	B
20	N	T	S	O	U	T	H	W	E	S	T	T	O	C	U	T	O	F	F	C	H	I	N	E	S	E
	K	W	M	H	V	Y	Y	B	M	G	F	L	T	Y	V	L	E	N	K	V	M	M	A	E	E	Z

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

Etc.

FIGURE 39

The message is found to be a "Z" message with the first wheel originally set at I and CW6r at V in the last place. If it is written out as in figure 39, it will be found that line 14 checks with those below it but not with those above it. Consequently line 14 represents I on the second control wheel. On counting back to line 1, it is found that the second control wheel was originally at V. This gives the setting V for the second cipher wheel and shows that the indicator RSPVQ is deciphered as IV..V .

Returning to Serial No. 155, it is found that every line of the message checks with every other, and the break does not appear anywhere in the message. As a result it would seem that the initial position of the second control wheel is unobtainable, and in general, this would be true. It happens though that the particular message under consideration proves to be an exception because of its length. Since the last line checks with all the others above it, it must correspond to a setting of the control wheel other than I. Suppose this setting were any other letter than J or K. Then it is found by counting back that some line in the message would represent I and would have to contain the break. Consequently, the last line must be either J or K and the initial setting of the second control wheel must be either H or G. This reduction to two possibilities is as far as one may go with the method given above.

It may be useful to summarize what has been said up to this point about "Z" messages with known plain text. In the first place, it can be determined by the use of the tables of plain-text relationships whether or not the message is in a "Z" motion. This procedure results in a knowledge of the identity and original position of the fifth wheel. Secondly, the original position of the first control wheel can be determined and if the message is long enough, that of the second control wheel can also be found. The information about the control wheels gives the original settings of the corresponding cipher wheels.

27. **Application of plain-text relationships to messages with unknown plain text.**—The next element to consider is the study of messages for which no plain text is available. For them, some statistical method must be devised which will indicate the correct result by a study of frequencies. Suppose that the machine is set for a "Z" motion with wheel 4 direct at S in the last position. If the plain-text letter E is hit 26 times in succession a series of cipher letters will result. If the next 26 plain-text letters are all C, the second cipher line will be identical with the first because, according to the table, an E and a C at a distance of 26 will yield the same cipher letter.

Suppose now that the first line had been all E's but the second line ordinary plain text. Then in any column where the cipher letters are identical the second letter must represent C. If the cipher letters in the column are not the same, the second letter cannot be C. Hence, the number of coincidences is the same as the relative frequency of C in the second line.

If the first 26 letters had been plain text the number of E's on the top line would have corresponded to the normal frequency of E. The chances of finding on these two lines a cipher coincidence which represents EC are given by the product of the normal frequencies of E and C. The chances of finding a cipher coincidence whose first plain-text equivalent shall

be A are represented by the product of the normal frequencies of A and N since, according to the table, AN is one of the digraphs to be sought for at interval 1.

It now follows that the chance for the appearance of any cipher repetition regardless of what plain-text digraph it may represent, is obtained by summing the results for all 26 correct digraphs. The calculations are given below:

AN=0.072×0.076=0.0055	JM=0.002×0.025=0.0001	SB=0.058×0.012=0.0007
BZ= .012× .001= .0000	KU= .004× .030= .0001	TL= .090× .036= .0032
CS= .034× .058= .0020	LJ= .036× .002= .0001	UE= .030× .126= .0038
DK= .040× .004= .0002	MW= .025× .014= .0004	VA= .013× .072= .0009
EC= .126× .034= .0043	NQ= .076× .003= .0002	WT= .014× .090= .0013
FY= .030× .021= .0006	OV= .074× .013= .0010	XO= .005× .074= .0004
GF= .018× .030= .0005	PR= .027× .083= .0022	YG= .021× .018= .0004
HP= .033× .027= .0009	QI= .003× .076= .0002	ZD= .001× .040= .0000
IH= .076× .033= .0025	RX= .083× .005= .0004	

FIGURE 40

The expected theoretical number of cipher coincidences at interval 1 is 0.032 of the total number of tabulations. The average incorrect result is $\frac{1}{26}$, since it may be assumed that all cipher digraphs have an equal probability of appearance. Hence, the average incorrect result is 0.038 against a correct result of 0.032.

In considering cipher repetitions on the first and third lines, it is necessary to use interval 2. Similarly, in comparing line 1 with other lines of the message, new intervals must be introduced. The correct results for CW4d at S (as calculated above) are given here for a few intervals with the corresponding incorrect result in each case.

TABLE IX

Interval	Correct result	Incorrect result	Interval	Correct result	Incorrect result	Interval	Correct result	Incorrect result
2	0. 043	0. 038	7	0. 048	0. 038	12	0. 034	0. 038
3	. 034	. 038	8	. 043	. 038	13	. 034	. 038
4	. 038	. 038	9	. 037	. 038	14	. 043	. 038
5	. 031	. 038	10	. 048	. 038	15	. 033	. 038
6	. 038	. 038	11	. 045	. 038	16	. 043	. 038

Should one wish to study repetitions between line 2 and the lines below it, it would be necessary to consider wheel 4 as being set at R. The results obtained for the first 15 intervals of this setting are:

TABLE X

Interval	Correct result	Incorrect result	Interval	Correct result	Incorrect result	Interval	Correct result	Incorrect result
1	0. 042	0. 038	6	0. 036	0. 038	11	0. 041	0. 038
2	. 033	. 038	7	. 032	. 038	12	. 030	. 038
3	. 031	. 038	8	. 045	. 038	13	. 033	. 038
4	. 042	. 038	9	. 032	. 038	14	. 036	. 038
5	. 043	. 038	10	. 040	. 038	15	. 030	. 038

These results seem to indicate that the incorrect result is often larger than the correct one and that even in those cases where the correct one is greater, the difference is not very appreciable. In other words, a mere count of cipher repetitions cannot give any information as to whether or not a message is in a "Z" motion.

However, it is to be expected that the distribution of the repetitions will vary with the probability. For example, if the correct result for two lines is 0.045, it is natural to expect more cipher repetitions between them than between two lines whose probability is 0.030. It seems reasonable then to multiply the number of repetitions between two lines by the corresponding probability and to sum the results for all possible pairs of lines. Such a procedure was followed in several tests and the following results were obtained. (In most cases the ncorrect settings were picked at random. The correct one is the first one listed.)

Serial No. 139 (10 lines)

1Cd	1Dd	4Sd
17771	17596	17903

Serial No. 131 (10 lines beginning as in cipher message)

4Sd	1Bd	1Ed
14519	14597	14735

Serial No. 131 (10 lines beginning at proper position)

[This test assumes a knowledge of first control wheel]

4Sd	1Ad	1Bd	1Cd	1Ed
14108	13098	13941	13488	13929

Serial No. 131 (17 lines beginning at proper position)

[This test assumed that there was no break in the first 17 lines]

4Sd	1Ed
58491	58192

FIGURE 41

The results obtained above do not seem very satisfactory. In several cases, an incorrect setting gave a larger total than the correct setting. Even in those cases where the correct setting gave a larger result than the few incorrect positions used, the percentage difference was very small. Consider the final test, where 17 lines were used. The difference between the correct and incorrect settings is $\frac{299}{58491}$ which is one-half of 1 percent. It appears that one cannot determine "Z" motions by comparing the cipher repetitions between pairs of lines only. One must use more than just two lines.

It is not difficult to see how this can be done. It has already been shown that for a given wheel in a given position a cipher repetition between two lines, at any interval whatever, can represent only 1 of 26 possible digraphic combinations. To put it differently, if the plain-text equivalent of the first of the two cipher letters is arbitrarily assigned, the equivalent of the second is completely determined. In exactly the same way then, if three or more like cipher letters appear down any one column, and a plain-text equivalent is assigned to any one of them, the equivalents of the others will be fixed. Naturally, these equivalents will vary with the different wheels and their different settings.

To illustrate this notion, consider Serial No. 155. If this message is written out in lines of 26, the cipher letter D is found to appear five times in column 1, the first appearance corresponding to the setting H on the correct wheel, 2 direct. The positions of the other letters D correspond to the settings, C, X, R, O. These letters H, C, X, R, O give the intervals between the repeated cipher letters, viz, 5, 5, 6, 3. If we assume the first D to be represented by A, then the second must be B, because the tables give AB as a correct digraph for interval 5 when wheel 2d is set at H. If the second D is supposed to be B, then the third must be W because BW is a correct digraph for interval 5 and for wheel 2d set at C. The fourth and fifth letters in this same way become G and J, so that finally if the first of the set is A, the entire set is ABWGJ. This same procedure can be carried out by assigning each of the 26 letters in turn to the first of the cipher letters D and as a result, the following sets of 5 letters are obtained:

K I Y M N H B T L O Z Q X V W G S F J D E R A C P U
L D V C J O N I P Z Y H M K W T F S Q A R U B X E G
J G B A O X L E U Z V M H N S F R D I T Y C W P Q K
P U Z I F K V H T J O Y N R C A X M S W D L G E B Q
M Q H X W Y S A R K C O B F N D V T Z U G E J I L P
93 167 79 211 196 136 194 397 266 81 142 156 150 205 195 250 189 243 140 246 288 308 117 267 203 81

FIGURE 42

The number at the foot of each column represents the sum of the relative frequencies of the letters in it. The highest of these sums, 397, which comes from the set TIEHA is found on comparison with the known plain text of the message to be the correct set of letters.

Given any set of repeated cipher letters in a column, it is possible in this way to relate to it 26 sets of plain-text letters, provided, of course, that the entire set of cipher letters is contained within one block of 650.

This notion can be extended still further. Suppose a fairly long message is being studied and that the original positions of the control wheels are known. (Such an assumption is not unreasonable, since this information is obtainable from a study of "V" messages.) In such a message one can relate cipher letters in one block of 650 to letters in other blocks by using the properties of the "703" cycle, in which as has already been shown a shift of one letter arises in both of the fixed sequences.

To illustrate the procedure, consider Serial No. 115, on which the proper breaks have been indicated.

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

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

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

FIGURE 43

In column 1 of block 1, the letter G is found repeated at interval 7. For wheel 6 reversed, set at V, this pair can represent one of 26 possible digraphs, obtainable from the tables for that wheel. These digraphs are

KJ	PD	MB	FE
BI	RL	DV	GF
QX	US	IN	OM
LA	XG	JP	YT
CU	SO	VZ	TC
NR	HQ	ZY	
WK	AW	EH	

FIGURE 44

Let us recall just how these digraphs were obtained. Suppose that the first of the cipher letters G had represented the plain-text letter E. Then with wheel 6 reversed, set at V, the current would have traversed the following path:

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

NAL6..... V U T S R Q P O N M L K J I H G F E D C B A Z Y X W

MAL6r.... N D R T H L B I J Z E Q X S O W F P U K G C Y V M A

[4 intervening wheels]

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

FIGURE 45

Just what path is traversed through the first four wheels is of no concern since those wheels remain fixed down the column.

To see what plain-text letter the second G represents, it is first necessary to shift the last wheel to the setting C, 7 places removed from V. Then in this position the strips appear as follows:

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

NAL6..... C B A Z Y X W V U T S R Q P O N M L K J I H G F E D

MAL6r.... K G C Y V M A N D R T H L B I J Z E Q X S O W F P U

[4 intervening wheels]

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

FIGURE 46

The last four wheels are in identically the same position as before. Consequently, if the current emerged at G, it must have followed the same path as before and must have come from G on CW6r. G on NAL6 is opposite H on RFS. It is thus seen that the second of the cipher letters represents H. This result checks with the results as shown in the table.

Suppose now that the letters in the second block are being considered. Since 703 leaves a remainder of 1 on being divided by 26, it is necessary to relate the letters of column 1 in the first block to those of column 2 in the second block. Moreover, as a result of the shift in the fixed sequences, the letter G of block 1 must be related to D in block 2. The second column of block 2 is found to contain the letter D three times. The second of the letters G having been supposed to be on line C, the first D will be on line K. For this line, the setting of the strips becomes

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

NAL6..... K J I H G F E D C B A Z Y X W V U T S R Q P O N M L

MAL6r.... Q X S O W F P U K G C Y V M A N D R T H L B I J Z E

[4 intervening wheels]

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

FIGURE 47

In this setting the first four wheels are in the same position as before, but have been shifted one place as a unit relative to the LFS. The path of the current to D on the LFS from MAL6r will be the path previously followed to G on LFS from MAL6r but will be shifted down one place along its entire length. This means that the current to D on LFS must have come from S on MAL6r and therefore from E on RFS. D_c on line C must therefore represent E_p.

The equivalents of the remaining D_c's in column 2 block 2 can now be obtained without difficulty.

71836—35——4

If the cipher letter N appeared in column 3 of block 3, a similar procedure to the one described above would determine the corresponding plain-text letters. Here again a shift of the fixed sequences must be introduced in the same way as before. This method of relating letters in each of two or three blocks of 650 makes it possible to study larger sets of letters than would otherwise be obtained. For example, in Serial No. 115, more than 25 sets of such letters were found where each set contained at least 5 letters. In a message of but one block, the occurrence of even four or five such sets is rare.

For each assumption as to the identity and original setting of the fifth wheel, 26 combinations of plain-text letters can be assigned to each set. For, by the above procedure, after any one of the cipher letters in such a set has been arbitrarily assigned a plain-text value, the equivalents of all the others can be determined. To illustrate, consider the cipher letters G, D, and N in columns 16, 17, and 18 of blocks 1, 2, and 3, respectively. The total number of occurrences of these letters is 7 and the sets of plain-text letters obtained on the assumption that the fifth wheel is CW6r at V are given below:

```
B  G S P A H X M O Z Q T V E K Y N D F I U J L B C R W
C  E F M T C J I X A U R K D L S G O Q W B V N P Z Y H
   . . . . . . . . . . . . . . . . . . . . . . . . . .
N  J Z X A V C D H I O M L E B Q P R K U F S W G N T O
Q  B X O T W M R N Z G E J I C H L Q D V U K Y A S P F
R  C I U Y J Z S X H K B Q P T V A G R W D L M E F O N
   . . . . . . . . . . . . . . . . . . . . . . . . . .
M  H F M R Z Q L X K G O W A Y S J I C V E T P N U D B
Q  F B X O T W M R N Z G E J I C H L Q D V U K Y A S P
      502    343      427  459
```

FIGURE 48.—Columns 16, 17, 18—GDN

Of these sets, the combination ATATYRO represents the greatest total frequency, viz, 502. On reference to the known plain text, this set is found to be the correct set.

It now appears that for a correct assumption of the fifth wheel, the proper letters will be found from a set of 26 possibilities by a summation of frequencies. That the correct letters correspond to the greatest sum is substantiated by the fact that only one exception was found in more than ten tests of this nature. Hence, it may be assumed that in each group of 26 sets the column giving the greatest sum is the only one to be considered. Suppose such a procedure were carried out for every set containing at least 5 letters, not only for the correct setting but also for all incorrect settings. How would the grand total of the frequencies of all the sets in the correct case compare with an incorrect case? If the former should be the greatest of all or among the greatest, one would then have a method of testing unknown messages for "Z" motions. Moreover, there is no question about the fact that such will be the case for messages which are sufficiently long. Unfortunately, this is not true for a message of the size of

Serial No. 115. A series of tests carried out on the latter message gave negative results as follows:

TABLE XI

Cipher letters	Columns	Correct setting	Incorrect setting
GDN	16	502	560
ZIW	17	417	471
HAM	19	383	415
FJL	26	468	436
EGD	25	455	383
KRF	7	210	414
JLZ	19	308	505
		2,743	3,184

Unless one can obtain longer messages, the methods herein discussed will not permit the discovery of "Z" messages whose plain text is unknown. Some other plan of attack will have to be devised for use in such cases.

APPENDIX I

INSTRUCTIONS

TEST OF HCM

APRIL 1, 1932.

1. There are four sets of variables in the HCM which must be adjusted before a message can be enciphered or deciphered, namely:

(*a*) Code-wheel arrangement
(*b*) Code-wheel lineup
(*c*) Control-wheel setting
(*d*) Ratchet action

The code-wheel wirings and end wirings are semipermanent, but remain unchanged for long periods of time. They will remain fixed for this test.

2. The method by which the above listed variable adjustments are set is as follows:

(*a*) Each message contains an external indicator which shows, by reference to a printed cipher or list for the date in question, the initial key and hence the set-up of the HCM. It also shows which one of the six cipher wheels is to be omitted from consideration for that day. Ordinarily, the initial key would change daily, but for this test it will remain the same throughout.

(*b*) In each message, a message indicator follows the external indicator. With the HCM set up as determined by the external indicator, the message indicator (5 letters) is enciphered on the HCM. This encipherment produces the message key. By the use of a simple code, the message key determines an entire new set-up for the HCM. The set-up thus obtained is made and the encipherment or decipherment of the message proper now begins.

The message indicator, and therefore the message key, changes with every message.

(*c*) The actual set-up of the four variables is derived from the key as follows:

(1) *Code-wheel arrangement.*—If the key were YSRIP, for example, the order of the wheels would be 5, 4, 3, 1, 2. A table in the cipher shows whether each wheel is to be used in the direct or reverse position. If the table were

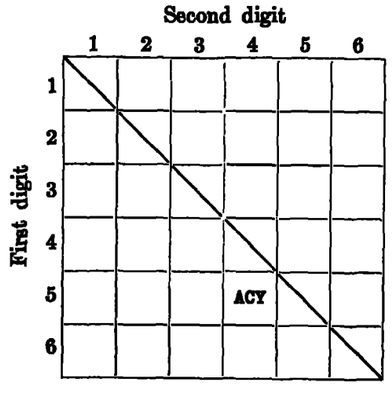
Direct_____	A	B	C	D	E	F	G	H	I	J	K	L	M
Reversed____	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

the code-wheel arrangement would be 5R, 4R, 3R, 1D, 2R, since Y, S, R, and P in the table show that the wheels are to be used in the reversed position, and I in table shows that its wheel is to be used in the direct position. The wheels are then placed in the HCM in that order and position, from left to right.

(2) *Code-wheel line-up.*—The key itself is used as the line-up setting of the code wheels. Thus, wheel 5R, which is now installed as the left-hand wheel, is set with the Y (on the wheel periphery) against the bench mark; wheel 4R is set with S against the bench mark, etc.

(3) *Control-wheel setting.*—The first two letters of the key are used as the control-wheel setting. Thus, the left-hand control wheel is set at Y; the right-hand wheel at S.

(4) *Ratchet action.*—The arrangement of the code wheels has already been derived as 5R, 4R, 3R, 1D, 2R. The first two digits, 5 and 4, are applied to a table in the cipher to find the ratchet-action setting. Such a table would be



The setting of the ratchet action from the table is ACY.

Appendix II

BASIC CIPHER-TEXT SEQUENCES

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

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

BASIC CIPHER-TEXT SEQUENCES FOR CW2 DIRECT

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

BASIC CIPHER-TEXT SEQUENCES FOR CW3 DIRECT

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

BASIC CIPHER-TEXT SEQUENCES FOR CW4 DIRECT

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

BASIC CIPHER-TEXT SEQUENCES FOR CW5 DIRECT

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

BASIC CIPHER-TEXT SEQUENCES FOR CW6 DIRECT

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

BASIC CIPHER-TEST SEQUENCES FOR CW1 REVERSED

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

BASIC CIPHER-TEXT SEQUENCES FOR CW2 REVERSED

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

BASIC CIPHER-TEXT SEQUENCES FOR CW3 REVERSED

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

BASIC CIPHER-TEXT SEQUENCES FOR CW4 REVERSED

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

BASIC CIPHER-TEXT SEQUENCES FOR CW5 REVERSED

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

BASIC CIPHER-TEXT SEQUENCES FOR CW6 REVERSED

Appendix III

FIRST-INTERVAL DATA—CIPHER-TEXT RELATIONSHIPS

Table A

A																									
H	1D	2T	3Z	5V	5T	1Y	2M	3F	40	4R	4Y														
V	1T	1H	1A	30	3B	4H	5S	5L	5J	5E	6L	1Z	2T	2W	3Y	4B	4T	6T							
Y	2I	3I	4V	4N	4D	6X	6F	6P	6T	1A	1J	2L	2P	3L	5A										
Q	1U	4T	4K	5M	5B	6K	1M	1P	1Q	1W	2N	2Y	4H	5L	5N	5S									
P	5K	2A	2Z	3N	4P	4Z	5P	6R																	
U	1V	1B	2G	2E	4U	4P	1B	2S	3S	4W	5E	6D													
X	2Y	2W	20	4C	5A	3R	3S	4G	6L																
S	1M	3F	6I	2C	2E	2S	3U	3X	4E	6X															
N	2S	5P	5F	6Y	6W	6H	6A	2U	3C	3V	3Z	5I	5T	5Z	6V	6Z									
D	1S	2N	2J	2F	3Y	3V	3Q	3E	4E	1E	1H	4Y	6C	6F											
G	1R	1L	1F	2V	2R	3G	40	6Z	6Q	6G	3K	4I	5W	6I											
E	1X	1J	1I	3T	4L	5Z	5Y	5N	6N	1T	2H	3I	4K	5J	6M										
T	10	2H	5R	5I	6R	1F	4M	4S	6P																
C	1N	1C	2B	2A	1I	10	2X	4A	4D	5Q	5V	6A	6G												
O	1Y	2M	4X	4R	4F	4B	6S	1G	1V	3B	3E	3H	4L	4V	5K	5Y	60	6W							
W	4J	6J	2G	4Q	5D	6H																			
I	2C	3U	3N	5G	6B	1N	1R	1U	2D	2R	3T														
Z	1Z	2U	3S	3C	4Z	5Q	5D	5C	60	6D	1X	2F	5U	6J	6N										
L	1W	1G	2X	2P	3K	4Q	5W	5H	2I	20	2Q	30	5N	6Y											
J	1E	2K	5U	6M	6C	6Q																			
F	2D	3X	3W	3L	3D	4I	4G	6U	1D	1C	1S	2V	3W	4C	5C	5F	5G	5X	6S						
R	3J	3A	4S	4Z	1K	2K	3Q	4F	4N	4U	6E	6U													
K	1Q	1P	2Q	2L	3P	3M	4Y	50	6E	3A	3G	3M	5B	50	5R	6K									
B	1K	2Z	3R	3H	4W	5X	6V	1L	2B	3D	3P	4J	5H	6B											
M	4M																								

Underlined type denotes wheels in reversed positions.

Table H

A	4N																							
H																								
V	1E	2U	3A	5W	5U	1X	2L	3E	4N	4Q	4X													
Y	1U	1I	1B	3P	3C	4I	5T	5M	5K	5F	6M	1Y	2S	2V	3X	4A	4S	6S						
Q	2J	3J	4W	40	4E	6Y	6G	6Q	6U	1Z	1I	2K	20	3K	5Z									
P	1V	4U	4L	5N	5C	6L	1L	1P	10	1V	2M	2X	4G	5K	5L	5R								
U	5L	2Z	2Y	3M	40	4Y	50	6Q																
X	1W	1C	2H	2F	4V	4Q	1A	2I	3I	4V	6C	5D												
S	2Z	2X	2P	4D	5B	3Q	3R	4F	6K															
N	1N	3G	6J	2B	2D	2R	3T	3W	4D	6W														
D	2T	5Q	5G	6Z	6X	6I	6B	2T	3B	3U	3Y	5H	5S	5Y	6U	6Y								
G	1T	20	2K	2G	3Z	3W	3R	3F	4F	1D	1G	4X	6B	6E										
E	1S	1M	1G	2W	2S	3H	4P	6A	6R	6H	3J	4H	5V	6H										
T	1Y	1K	1J	3U	4M	5A	5Z	50	60	1S	2G	3H	4J	5I	6L									
C	1P	2I	5S	5J	6S	1E	4L	4R	60															
O	10	1D	2C	2B	1H	1N	2W	4Z	4C	5P	5U	6F	6Z											
W	1Z	2N	4Y	4S	4G	4C	6T	1F	1U	3A	3D	3G	4K	4U	5J	5X	6N	6V						
I	4K	6K	2F	4P	5C	6G																		
Z	2D	3V	30	5H	6C	1M	1Q	1T	2C	2Q	3S													
L	1A	2V	3T	3D	4A	5R	5E	5D	6P	6E	1W	2E	5T	6I	6M									
J	1X	1H	2Y	2Q	3L	4R	5X	5I	2H	2N	2P	3N	5M	6X										
F	1F	2L	5V	6N	6D	6P																		
R	2E	3Y	3X	3M	3E	4J	4H	6V	1C	1B	1R	2U	3V	4B	5B	5E	5F	5W	6R					
K	3K	3B	4T	4A	1J	2J	3P	4E	4M	4T	6D	6T												
B	1R	1Q	2R	2M	3Q	3N	4Z	5P	6F	3F	3L	3Z	5A	5N	5Q	6J								
M	1L	2A	3S	3I	4X	5Y	6W	1K	2A	3C	30	4I	5G	6A										

Underlined type denotes wheels in reversed positions.

Table V

A	1M	2B	3T	3J	4Y	5Z	6X	1J	2Z	3B	3N	4H	5F	6Z										
H	40																							
V																								
Y	1F	2V	3B	5X	5V	1W	2K	3D	4M	4P	4W													
Q	1V	1J	1C	3Q	3D	4J	5U	5N	5L	5G	6N	1X	2R	2U	3W	4R	4Z	6R						
P	2K	3K	4X	4P	4F	6Z	6H	6R	6V	1Y	1H	2J	2N	3J	5Y									
U	1W	4V	4M	50	5D	6M	1K	10	1N	1U	2L	2W	4F	5J	5K	5Q								
X	5M	2Y	2X	3L	4N	4X	5N	6P																
S	1X	1D	2I	2G	4W	4R	1Z	2H	3H	4U	5C	6B												
N	2A	2Y	2Q	4E	5C	3P	3Q	4E	6J															
D	10	3H	6K	2A	2C	2Q	3S	3V	4C	6V														
G	2U	5R	5H	6A	6Y	6J	6C	2S	3A	3T	3X	5G	5R	5X	6T	6X								
E	1U	2P	2L	2H	3A	3X	3S	3G	4G	1C	1F	4W	6A	6D										
T	1T	1N	1H	2X	2T	3I	4Q	6B	6S	6I	3I	4G	5U	6G										
C	1Z	1L	1K	3V	4N	5B	5A	5P	6P	1R	2F	3G	4I	5H	6K									
O	1Q	2J	5T	5K	6T	1D	4K	4Q	6N															
W	1P	1E	2D	2C	1G	1M	2V	4Y	4B	50	5T	6Y	6E											
I	1A	20	4Z	4T	4H	4D	6U	1E	1T	3Z	3C	3F	4J	4T	5I	5W	6M	6U						
Z	4L	6L	2E	40	5B	6F																		
L	2E	3W	3P	5I	6D	1L	1P	1S	2B	2P	3R													
J	1B	2W	3U	3E	4B	5S	5F	5E	6Q	6F	1V	2D	5S	6H	6L									
F	1Y	1I	2Z	2R	3M	4S	5Y	5J	2G	2M	20	3M	5L	6W										
R	1G	2M	5W	60	6E	60																		
K	2F	3Z	3Y	3N	3F	4K	4I	6W	1B	1A	1Q	2T	3U	4A	5A	5D	5E	5V	6Q					
B	3L	3C	4U	4B	1I	2I	30	4D	4L	4S	6C	6S												
M	1S	1R	2S	2N	3R	30	4A	5Q	6G	3E	3K	3Y	5M	5P	5Z	6I								

Underlined type denotes wheels in reversed positions.

Table Y

A	1T	1S	2T	2O	3S	3P	4B	5R	6H	3X	3D	3J	5Y	5L	5O	6H
H	1N	2C	3U	3K	4Z	5A	6Y	1I	2Y	3A	3M	4G	5E	6Y		
V	4P															
Y																
Q	1G	2W	3C	5Y	5W	1V	2J	3C	4L	4O	4V					
P	1W	1K	1D	3R	3E	4K	5V	5O	5M	5H	6O	1W	2Q	2T	3V	4Y	4Q	6Q
U	2L	3L	4Y	4Q	4G	6A	6I	6S	6W	1X	1G	2I	2M	3I	5X			
X	1X	4W	4N	5P	5E	6N	1J	1N	1M	1T	2K	2V	4E	5I	5J	5P		
S	5N	2X	2W	3K	4M	4W	5M	6O										
N	1Y	1E	2J	2H	4X	4S	1Y	2G	3G	4T	5B	6A						
D	2B	2Z	2R	4F	5D	3O	3P	4D	6I									
G	1P	3I	6L	2Z	2B	2P	3R	3U	4B	6U								
E	2V	5S	5I	6B	6Z	6K	6D	2R	3Z	3S	3W	5F	5Q	5W	6S	6W		
T	1V	2Q	2M	2I	3B	3Y	3T	3H	4H	1B	1E	4V	6Z	6C				
C	1U	1O	1I	2Y	2U	3J	4R	6C	6T	6J	3H	4F	5T	6F				
O	1A	1M	1L	3W	4O	5C	5B	5Q	6Q	1Q	2E	3F	4H	5G	6J			
W	1R	2K	5U	5L	6U	1C	4J	4P	6M									
I	1Q	1F	2E	2D	1F	1L	2U	4X	4A	5N	5S	6X	6D					
Z	1B	2P	4A	4U	4I	4E	6V	1D	1S	3Y	3B	3E	4I	4S	5H	5V	6L	6T
L	4M	6M	2D	4N	5A	6E												
J	2F	3X	3Q	5J	6E	1K	1O	1R	2A	2O	3Q							
F	1C	2X	3V	3F	4C	5T	5G	5F	6R	6G	1U	2C	5R	6G	6K			
R	1Z	1J	2A	2S	3N	4T	5Z	5K	2F	2L	2N	3L	5K	6V				
K	1H	2N	5X	6P	6F	6N												
B	2G	3A	3Z	3O	3G	4L	4J	6X	1A	1Z	1P	2S	3T	4Z	5Z	5C	5D	5U	6P
M	3M	3D	4V	4C	1H	2H	3N	4C	4K	4R	6B	6R						

Underlined type denotes wheels in reversed positions.

Table Q

A	3N	3E	4W	4D	1G	2G	3M	4B	4J	4Q	6A	6Q			
H	1U	1T	2U	2P	3T	3Q	4C	5S	6I	3W	3C	3I	5X	5K	5N	6G
V	1O	2D	3V	3L	4A	5B	6Z	1H	2X	3Z	3L	4F	5D	6X		
Y	4Q															
Q																
P	1H	2X	3D	5Z	5X	1U	2I	3B	4K	4N	4U					
U	1X	1L	1E	3S	3F	4L	5W	5P	5N	5I	6P	1V	2P	2S	3U	4X	4P	6P
X	2M	3M	4Z	4R	4H	6B	6J	6T	6X	1W	1F	2H	2L	3H	5W			
S	1Y	4X	4O	5Q	5F	6O	1I	1M	1L	1S	2J	2U	4D	5H	5I	5O		
N	5O	2W	2V	3J	4L	4V	5L	6N										
D	1Z	1F	2K	2I	4Y	4T	1X	2F	3F	4S	5A	6Z						
G	2C	2A	2S	4G	5E	3N	3O	4C	6H									
E	1Q	3J	6M	2Y	2A	2O	3Q	3T	4A	6T								
T	2W	5T	5J	6C	6A	6L	6E	2Q	3Y	3R	3V	5E	5P	5V	6R	6V		
C	1W	2R	2N	2J	3C	3Z	3U	3I	4I	1A	1D	4U	6Y	6B				
O	1V	1P	1J	2Z	2V	3K	4S	6D	6U	6K	3G	4E	5S	6E				
W	1B	1N	1M	3X	4P	5D	5C	5R	6R	1P	2D	3E	4G	5F	6I			
I	1S	2L	5V	5M	6V	1B	4I	4O	6L									
Z	1R	1G	2F	2E	1E	1K	2T	4W	4Z	5M	5R	6W	6C					
L	1C	2Q	4B	4V	4J	4F	6W	1C	1R	3X	3A	3D	4H	4R	5G	5U	6K	6S
J	4N	6N	2C	4M	5Z	6D												
F	2G	3Y	3R	5K	6F	1J	1N	1Q	2Z	2N	3P							
R	1D	2Y	3W	3G	4D	5U	5H	5G	6S	6H	1T	2B	5Q	6F	6J			
K	IA	1K	2B	2T	3O	4U	5A	5L	2E	2K	2M	3K	5J	6U				
B	1I	2O	5Y	6Q	6G	6M												
M	2H	3B	3A	3P	3H	4M	4K	6Y	1Z	1Y	1O	2R	3S	4Y	5Y	5B	5C	5T	6O

Underlined type denotes wheels in reversed positions.

Table P

A	2I	3C	3B	3Q	3I	4N	4L	6Z	1Y	1X	1N	2Q	3R	4X	5X	5A	5B	5S	6N
H	3O	3F	4X	4E	1F	2F	3L	4A	4I	4P	6Z	6P							
V	1V	1U	2V	2Q	3U	3R	4D	5T	6J	3V	3B	3H	5W	5J	5M	6F			
Y	1P	2E	3W	3M	4B	5C	6A	1G	2W	3Y	3K	4E	5C	6W					
Q	4R																		
P																			
U	1I	2Y	3E	5A	5Y	1T	2H	3A	4J	4M	4T								
X	1Y	1M	1F	3T	3G	4M	5X	5Q	5O	5J	6Q	1U	2O	2R	3T	4W	4O	6O	
S	2N	3N	4A	4S	4I	6C	6K	6U	6Y	1V	1E	2G	2K	3G	5V				
N	1Z	4Y	4P	5R	5G	6P	1H	1L	1K	1R	2I	2T	4C	5G	5H	5N			
D	5P	2V	2U	3I	4K	4U	5K	6M											
G	1A	1G	2L	2J	4Z	4U	1W	2E	3E	4R	5Z	6Y							
E	2D	2B	2T	4H	5F	3M	3N	4B	6G										
T	1R	3K	6N	2X	2Z	2N	3P	3S	4Z	6S									
C	2X	5U	5K	6D	6B	6M	6F	2P	3X	3Q	3U	5D	5O	5U	6Q	6U			
O	1X	2S	2O	2K	3D	3A	3V	3J	4J	1Z	1C	4T	6X	6A					
W	1W	1Q	1K	2A	2W	3L	4T	6E	6V	6L	3F	4D	5R	6D					
I	1C	1O	1N	3Y	4Q	5E	5D	5S	6S	1O	2C	3D	4F	5E	6H				
Z	1T	2M	5W	5N	6W	1A	4I	4N	6K										
L	1S	1H	2G	2F	1D	1J	2S	4V	4Y	5L	5Q	6V	6B						
J	1D	2R	4C	4W	4K	4G	6X	1B	1Q	3W	3Z	3C	4G	4Q	5F	5T	6J	6R	
F	4O	6O	2B	4L	5Y	6C													
R	2H	3Z	3S	5L	6G	1I	1M	1P	2Y	2M	3O								
K	1E	2Z	3X	3H	4E	5V	5I	5H	6T	6I	1S	2A	5P	6E	6I				
B	1B	1L	2C	2U	3P	4V	5B	5M	2D	2J	2L	3J	5I	6T					
M	1J	2P	5Z	6R	6H	6L													

Underlined type denotes wheels in reversed positions.

Table U

A	1K	2Q	5A	6S	6I	6K												
H	2J	3D	3C	3R	3J	4O	4M	6A	1X	1W	1M	2P	3Q	4W	5W	5Z	5A	5R	6M
V	3P	3G	4Y	4F	1E	2E	3K	4Z	4H	4O	6Y	6O							
Y	1W	1V	2W	2R	3V	3S	4E	5U	6K	3U	3A	3G	5V	5I	5L	6E			
Q	1Q	2F	3X	3N	4C	5D	6B	1F	2V	3X	3J	4D	5B	6V					
P	4S																		
U																			
X	1J	2Z	3F	5B	5Z	1S	2G	3Z	4I	4L	4S								
S	1Z	1N	1G	3U	3H	4N	5Y	5R	5P	5K	6R	1T	2N	2Q	3S	4V	4N	6N	
N	2Q	3O	4B	4T	4J	6D	6L	6V	6Z	1U	1D	2F	2J	3F	5U				
D	1A	4Z	4Q	5S	5H	6Q	1G	1K	1J	1Q	2H	2S	4B	5F	5G	5M			
G	5Q	2U	2T	3H	4J	4T	5J	6L											
E	1B	1H	2M	2K	4A	4V	1V	2D	3D	4Q	5Y	6X							
T	2E	2C	2U	4I	5G	3L	3M	4A	6F										
C	1S	3L	6O	2W	2Y	2M	3O	3R	4Y	6R									
O	2Y	5V	5L	6E	6C	6N	6G	2Q	3W	3P	3T	5C	5N	5T	6P	6T			
W	1Y	2T	2P	2L	3E	3B	3W	3K	4K	1Y	1B	4S	6W	6Z					
I	1X	1R	1L	2B	2X	3M	4U	6F	6W	6M	3E	4C	5Q	6C					
Z	1D	1P	1O	3Z	4R	5F	5E	5T	6T	1N	2B	3C	4E	5D	6G				
L	1U	2N	5X	5O	6X	1Z	4G	4M	6J										
J	1T	1I	2H	2G	1C	1I	2R	4U	4X	5K	5P	6U	6A						
F	1E	2S	4D	4X	4L	4H	6Y	1A	1P	3V	3Y	3B	4F	4P	5E	5S	6I	6Q	
R	4P	6P	2A	4K	5X	6B													
K	2I	3A	3T	5M	6H	1H	1L	1O	2X	2L	3N								
B	1F	2A	3Y	3I	4F	5W	5J	5I	6U	6J	1R	2Z	5O	6D	6H				
M	1C	1M	2D	2V	3Q	4W	5C	5N	2C	2I	2K	3I	5H	6S					

Underlined type denotes wheels in reversed positions.

Table X

A	1D	1N	2E	2W	3R	4X	5D	5O	2B	2H	2J	3H	5G	6R										
H	1L	2R	5B	6T	6J	6J																		
V	2K	2S	3E	3D	3K	4P	4N	6B	1W	1V	1L	2O	3P	4V	5V	5Y	5Z	5Q	6L					
Y	3Q	3H	4Z	4G	1D	2D	3J	4Y	4G	4N	6X	6N												
Q	1X	1W	2X	2S	3W	3T	4F	5V	6L	3T	3Z	3F	5U	5H	5K	6D								
P	1R	2G	3Y	3O	4D	5E	6C	1E	2U	3W	3I	4C	5A	6U										
U	4T																							
X																								
S	1K	2A	3G	5C	5A	1R	2F	3Y	4H	4K	4R													
N	1A	1O	1H	3V	3I	4O	5Z	5S	5Q	5L	6S	1S	2M	2P	3R	4U	4M	6M						
D	2P	3P	4C	4U	4K	6E	6M	6W	6A	1T	1C	2E	2I	3E	5T									
G	1B	4A	4R	5T	5I	6R	1F	1J	1I	1P	2G	2R	4A	5E	5F	5L								
E	5R	2T	2S	3G	4I	4S	5I	6K																
T	1C	1I	2N	2L	4B	4W	1U	2C	3C	4P	5X	6W												
C	2F	2D	2V	4J	5H	3K	3L	4Z	6E															
O	1T	3M	6P	2V	2X	2L	3N	3Q	4X	6Q														
W	2Z	5W	5M	6F	6D	6O	6H	2N	3V	3O	3S	5B	5M	5S	6O	6S								
I	1Z	2U	2Q	2M	3F	3C	3X	3L	4L	1X	1A	4R	6V	6Y										
Z	1Y	1S	1M	2C	2Y	3N	4V	6G	6X	6N	3D	4B	5P	6B										
L	1E	1Q	1P	3A	4S	5G	5F	5U	6U	1M	2A	3B	4D	5C	6F									
J	1V	2O	5Y	5P	6Y	1Y	4F	4L	6I															
F	1U	1J	2I	2H	1B	1H	2Q	4T	4W	5J	5O	6T	6Z											
R	1F	2T	4E	4Y	4M	4I	6Z	1Z	1O	3U	3X	3A	4E	4O	5D	5R	6H	6P						
K	4Q	6Q	2Z	4J	5W	6A																		
B	2J	3B	3U	5N	6I	1G	1K	1N	2W	2K	3M													
M	1G	2B	3Z	3J	4G	5X	5K	5J	6V	6K	1Q	2Y	5N	6C	6G									

Underlined type denotes wheels in reversed positions.

Table S

A	1H	2C	3A	3K	4H	5Y	5L	5K	6W	6L	1P	2X	5M	6B	6F									
H	1E	1O	2F	2X	3S	4Y	5E	5P	2A	2G	2I	3G	5F	6Q										
V	1M	2S	5C	6U	6K	6I																		
Y	2L	2T	3F	3E	3L	4Q	4O	6C	1V	1U	1K	2N	3O	4U	5U	5X	5Y	5P	6K					
Q	3R	3I	4A	4H	1C	2C	3I	4X	4F	4M	6W	6M												
P	1Y	1X	2Y	3T	3X	3U	4G	5W	6M	3S	3Y	3E	5T	5G	5J	6C								
U	1S	2H	3Z	3P	4E	5F	6D	1D	2T	3V	3H	4B	5Z	6T										
X	4U																							
S																								
N	1L	2B	3H	5D	5B	1Q	2E	3X	4G	4J	4Q													
D	1B	1P	1I	3W	3J	4P	5A	5T	5R	5M	6T	1R	2L	2O	3Q	4T	4L	6L						
G	2Q	3Q	4D	4V	4L	6F	6N	6X	6B	1S	1B	2D	2H	3D	5S									
E	1C	4B	4S	5U	5J	6S	1E	1I	1H	1O	2F	2Q	4Z	5D	5E	5K								
T	5S	2S	2R	3F	4H	4R	5H	6J																
C	1D	1J	2O	2M	4C	4X	1T	2B	3B	4Q	5W	6V												
O	2G	2E	2W	4K	5I	3J	3K	4Y	6D															
W	1U	3N	6Q	2U	2W	2K	3M	3P	4W	6P														
I	2A	5X	5N	6G	6E	6P	6I	2M	3U	3N	3R	5A	5L	5R	6N	6R								
Z	1A	2V	2R	2N	3G	3D	3Y	3M	4M	1W	1Z	4Q	6U	6X										
L	1Z	1T	1N	2D	2Z	3O	4W	6H	6Y	6O	3C	4A	5O	6A										
J	1F	1R	1Q	3B	4T	5H	5G	5V	6V	1L	2Z	3A	4C	5B	6E									
F	1W	2P	5Z	5Q	6Z	1X	4E	4K	6H															
R	1V	1K	2J	2I	1A	1G	2P	4S	4V	5I	5N	6S	6Y											
K	1G	2U	4F	4Z	4N	4J	6A	1Y	1N	3T	3W	3Z	4D	4N	5C	5Q	6G	6O						
B	4R	6R	2Y	4I	5V	6Z																		
M	2K	3C	3V	5O	6J	1F	1J	1M	2V	2J	3L													

Underlined type denotes wheels in reversed positions.

Table N

A	2L	3D	3W	5P	6K	1E	1I	1L	2U	2I	3K												
H	1I	2D	3B	3L	4I	5Z	5M	5L	6X	6M	10	2W	5L	6A	6E								
V	1F	1P	2G	2Y	3T	4Z	5F	5Q	2Z	2F	2H	3F	5E	6P									
Y	1N	2T	5D	6V	6L	6H																	
Q	2M	2U	3G	3F	3M	4R	4P	6D	1U	1T	1J	2M	3N	4T	5T	5W	5X	5Q	6J				
P	3S	3J	4B	4I	1B	2B	3H	4W	4E	4L	6V	6L											
U	1Z	1Y	2Z	3U	3Y	3V	4H	5X	6N	3R	3X	3D	5S	5F	5I	6B							
X	1T	2I	3A	3Q	4F	5G	6E	1C	2S	3U	3G	4A	5Y	6S									
S	4V																						
N																							
D	1M	2C	3I	5E	5C	1P	2D	3W	4F	4I	4P												
G	1C	1Q	1J	3X	3K	4Q	5B	5U	5S	5N	6U	1Q	2K	2N	3P	4S	4K	6K					
E	2R	3R	4E	4W	4M	6G	60	6Y	6C	1R	1A	2C	2G	3C	5R								
T	1D	4C	4T	5V	5K	6T	1D	1H	1G	1N	2E	2P	4Y	5C	5D	5J							
C	5T	2R	2Q	3E	4G	4Q	5G	6I															
O	1E	1K	2P	2N	4D	4Y	1S	2A	3A	4N	5V	6U											
W	2H	2F	2X	4L	5J	3I	3J	4X	6C														
I	1V	30	6R	2T	2V	2J	3L	30	4V	60													
Z	2B	5Y	50	6H	6F	6Q	6J	2L	3T	3M	3Q	5Z	5K	5Q	6M	6Q							
L	1B	2W	2S	20	3H	3E	3Z	3N	4N	1V	1Y	4P	6T	6W									
J	1A	1U	10	2E	2A	3P	4X	6I	6Z	6P	3B	4Z	5N	6Z									
F	1G	1S	1R	3C	4U	5I	5H	5W	6W	1K	2Y	3Z	4B	5A	6D								
R	1X	2Q	5A	5R	6A	1W	4D	4J	6G														
K	1W	1L	2K	2J	1Z	1F	20	4R	4U	5H	5M	6R	6X										
B	1H	2V	4G	4A	40	4K	6B	1X	1M	3S	3V	3Y	4C	4M	5B	5P	6F	6N					
M	4S	6S	2X	4H	5U	6Y																	

Underlined type denotes wheels in reversed positions.

Table D

A	4T	6T	2W	4G	5T	6X																	
H	2M	3E	3X	5Q	6L	1D	1H	1K	2T	2H	3J												
V	1J	2E	3C	3M	4J	5A	5N	5M	6Y	6N	1N	2V	5K	6Z	6D								
Y	1G	1Q	2H	2Z	3U	4A	5G	5R	2Y	2E	2G	3E	5D	60									
Q	10	2U	5E	6W	6M	6G																	
P	2N	3H	3G	2V	3N	4S	4Q	6E	1T	1S	1I	2L	3M	4S	5S	5V	5W	5N	6I				
U	3T	3K	4C	4J	1A	2A	3G	4V	4D	4K	6U	6K											
X	1A	1Z	2A	3V	3Z	3W	4I	5Y	60	3Q	3W	3C	5R	5E	5H	6A							
S	1U	2J	3B	3R	4G	5H	6F	1B	2R	3T	3F	4Z	5X	6R									
N	4W																						
D																							
G	1N	2D	3J	5F	5D	10	2C	3V	4E	4H	40												
E	1D	1R	1K	3Y	3L	4R	5C	5V	5T	50	6V	1P	2J	2M	30	4R	4J	6J					
T	2S	3S	4F	4X	4N	6H	6P	6Z	6D	1Q	1Z	2B	2F	3B	5Q								
C	1E	4D	4U	5W	5L	6U	1C	1G	1F	1M	2D	20	4X	5B	5C	5I							
O	5U	2Q	2P	3D	4F	4P	5F	6H															
W	1F	1L	2Q	20	4E	4Z	1R	2Z	3Z	4M	5U	6T											
I	2I	2G	2Y	4M	5K	3H	3I	4W	6B														
Z	1W	3P	6S	2S	2U	2I	3K	3N	4U	6N													
L	2C	5Z	5P	6I	6G	6R	6K	2K	3S	3L	3P	5Y	5J	5P	6L	6P							
J	1C	2X	2T	2P	3I	3F	3A	30	40	1U	1X	40	6S	6V									
F	1B	1V	1P	2F	2B	3Q	4Y	6J	6A	6Q	3A	4Y	5M	6Y									
R	1H	1T	1S	3D	4V	5J	5I	5X	6X	1J	2X	3Y	4A	5Z	6C								
K	1Y	2R	5B	5S	6B	1V	4C	4I	6F														
B	1X	1M	2L	2K	1Y	1E	2N	4Q	4T	5G	5L	6Q	6W										
M	1I	2W	4H	4B	4P	4L	6C	1W	1L	3R	3U	3X	4B	4L	5A	50	6E	6M					

Underlined type denotes wheels in reversed positions.

TABLE G

A 1J 2X 4I 4C 4Q 4M 6D 1V 1K 3Q 3T 3W 4A 4K 5Z 5N 6D 6L
H 4U 6U 2V 4F 5S 6W
V 2N 3F 3Y 5R 6M 1C 1G 1J 2S 2G 3I
Y 1K 2F 3D 3N 4K 5B 50 5N 6Z 60 1M 2U 5J 6Y 6C
Q 1H 1R 2I 2A 3V 4B 5H 5S 2X 2D 2F 3D 5C 6N
P 1P 2V 5F 6X 6N 6F
U 20 2W 3I 3H 30 4T 4R 6F 1S 1R 1H 2K 3L 4R 5R 5U 5V 5M 6H
X 3U 3L 4D 4K 1Z 2Z 3F 4U 4C 4J 6T 6J
S 1B 1A 2B 3W 3A 3X 4J 5Z 6P 3P 3V 3B 5Q 5D 5G 6Z
N 1V 2K 3C 3S 4H 5I 6G 1A 2Q 3S 3E 4Y 5W 6Q
D 4X
G
E 10 2E 3K 5G 5E 1N 2B 3U 4D 4G 4N
T 1E 1S 1L 3Z 3M 4S 5D 5W 5U 5P 6W 10 2I 2L 3N 4Q 4I 6I
C 2T 3T 4G 4Y 40 6I 6Q 6A 6E 1P 1Y 2A 2E 3A 5P
O 1F 4E 4V 5X 5M 6V 1B 1F 1E 1L 2C 2N 4W 5A 5B 5H
W 5V 2P 20 3C 4E 40 5E 6G
I 1G 1M 2R 2P 4F 4A 1Q 2Y 3Y 4L 5T 6S
Z 2J 2H 2Z 4N 5L 3G 3H 4V 6A
L 1X 3Q 6T 2R 2T 2H 3J 3M 4T 6M
J 2D 5A 5Q 6J 6H 6S 6L 2J 3R 3K 30 5X 5I 50 6K 60
F 1D 2Y 2U 2Q 3J 3G 3B 3P 4P 1T 1W 4N 6R 6U
R 1C 1W 1Q 2G 2C 3R 4Z 6K 6B 6R 3Z 4X 5L 6X
K 1I 1U 1T 3E 4W 5K 5J 5Y 6Y 1I 2W 3X 4Z 5Y 6B
B 1Z 2S 5C 5T 6C 1U 4B 4H 6E
M 1Y 1N 2M 2L 1X 1D 2M 4P 4S 5F 5K 6P 6V

Underlined type denotes wheels in reversed positions.

TABLE E

A 1Z 10 2N 2M 1W 1C 2L 40 4R 5E 5J 60 6U
H 1K 2Y 4J 4D 4R 4N 6E 1U 1J 3P 3S 3V 4Z 4J 5Y 5M 6C 6K
V 4V 6V 2U 4E 5R 6V
Y 20 3G 3Z 5S 6N 1B 1F 1I 2R 2F 3H
Q 1L 2G 3E 30 4L 5C 5P 50 6A 6P 1L 2T 5I 6X 6B
P 1I 1S 2J 2B 3W 4C 5I 5T 2W 2C 2E 3C 5B 6M
U 1Q 2W 5G 6Y 60 6E
X 2P 2X 3J 3I 3P 4U 4S 6G 1Q 1R 1G 2J 3K 4Q 5Q 5T 5U 5L 6G
S 3V 3M 4E 4L 1Y 2Y 3E 4T 4B 4I 6S 6I
N 1C 1B 2C 3X 3B 3Y 4K 5A 6Q 30 3U 3A 5P 5C 5F 6Y
D 1W 2L 3D 3T 4I 5J 6H 1Z 2P 3R 3D 4X 5V 6P
G 4Y
E
T 1P 2F 3L 5H 5F 1M 2A 3T 4C 4F 4M
C 1F 1T 1M 3A 3N 4T 5E 5X 5V 5Q 6X 1N 2H 2K 3M 4P 4H 6H
O 2U 3U 4H 4Z 4P 6J 6R 6B 6F 10 1X 2Z 2D 3Z 50
W 1G 4F 4W 5Y 5N 6W 1A 1E 1D 1K 2B 2M 4V 5Z 5A 5G
I 5W 20 2N 3B 4D 4N 5D 6F
Z 1H 1N 2S 2Q 4G 4B 1P 2X 3X 4K 5S 6R
L 2K 2I 2A 40 5M 3F 3G 4U 6Z
J 1Y 3R 6U 2Q 2S 2G 3I 3L 4S 6L
F 2E 5B 5R 6K 6I 6T 6M 2I 3Q 3J 3N 5W 5H 5N 6J 6N
R 1E 2Z 2V 2R 3K 3H 3C 3Q 4Q 1S 1V 4M 6Q 6T
K 1D 1X 1R 2H 2D 3S 4A 6L 6C 6S 3Y 4W 5K 6W
B 1J 1V 1U 3F 4X 5L 5K 5Z 6Z 1H 2V 3W 4Y 5X 6A
M 1A 2T 5D 5U 6D 1T 4A 4G 6D

Underlined type denotes wheels in reversed positions.

TABLE T

A 1B 2U 5E 5V 6E 1S 4Z 4F 6C
H 1A 1P 20 2N 1V 1B 2K 4N 4Q 5D 5I 6N 6T
V 1L 2Z 4K 4E 4S 40 6F 1T 1I 30 3R 3U 4Y 4I 5X 5L 6B 6J
Y 4W 6W 2T 4D 5Q 6U
Q 2P 3H 3A 5T 60 1A 1E 1H 2Q 2E 3G
P 1M 2H 3F 3P 4M 5D 5Q 5P 6B 6Q 1K 2S 5H 6W 6A
U 1J 1T 2K 2C 3X 4D 5J 5U 2V 2B 2D 3B 5A 6L
X 1R 2X 5H 6Z 6P 6D
S 2Q 2Y 3K 3J 3Q 4V 4T 6H 1P 1Q 1F 2I 3J 4P 5P 5S 5T 5K 6F
N 3N 3W 4F 4M 1X 2X 3D 4S 4A 4H 6R 6H
D 1D 1C 2D 3Y 3C 3Z 4L 5B 6R 3N 3T 3Z 50 5B 5E 6X
G 1X 2M 3E 3U 4J 5K 6I 1Y 20 3Q 3C 4W 5U 60
E 4Z
T
C 1Q 2G 3M 5I 5G 1L 2Z 3S 4B 4E 4L
O 1G 1U 1N 3B 3Q 4U 5F 5Y 5W 5R 6Y 1M 2G 2J 3L 4Q 4G 6G
W 2V 3V 4I 4A 4Q 6K 6S 6C 6G 1N 1W 2Y 2C 3Y 5N
I 1H 4G 4X 5Z 50 6X 1Z 1D 1C 1J 2A 2L 4U 5Y 5Z 5F
Z 5X 2N 2M 3A 4C 4M 5C 6E
L 1I 10 2T 2R 4H 4C 10 2W 3W 4J 5R 6Q
J 2L 2J 2B 4P 5N 3E 3F 4T 6Y
F 1Z 3S 6V 2P 2R 2F 3H 3K 4R 6K
R 2F 5C 5S 6L 6J 6U 6N 2H 3P 3I 3M 5V 5G 5M 6I 6M
K 1F 2A 2W 2S 3L 3I 3D 3R 4R 1R 1U 4L 6P 6S
B 1E 1Y 1S 2I 2E 3T 4B 6M 6D 6T 3X 4V 5J 6V
M 1K 1W 1V 3G 4Y 5M 5L 5A 6A 1G 2U 3V 4X 5W 6Z

Underlined type denotes wheels in reversed positions.

TABLE C

A 1L 1X 1W 3H 4Z 5N 5M 5B 6B 1F 2T 3U 4W 5V 6Y
H 1C 2V 5F 5W 6F 1R 4Y 4E 6B
V 1B 1Q 2P 20 1U 1A 2J 4M 4P 5C 5H 6M 6S
Y 1M 2A 4L 4F 4T 4P 6G 1S 1H 3N 3Q 3T 4X 4H 5W 5K 6A 6I
Q 4X 6X 2S 4C 5P 6T
P 2Q 3I 3B 5U 6P 1Z 1D 1G 2P 2D 3F
U 1N 2I 3G 3Q 4N 5E 5R 5Q 6C 6R 1J 2R 5G 6V 6Z
X 1K 1U 2L 2D 3Y 4E 5K 5V 2U 2A 2C 3A 5Z 6K
S 1S 2Y 5I 6A 6Q 6C
N 2R 2Z 3L 3K 3R 4W 4U 6I 10 1P 1E 2H 3I 40 50 5R 5S 5J 6E
D 3X 30 4G 4N 1W 2W 3C 4R 4Z 4G 6Q 6G
G 1E 1D 2E 3Z 3D 3A 4M 5C 6S 3M 3S 3Y 5N 5A 5D 6W
E 1Y 2N 3F 3V 4K 5L 6J 1X 2N 3P 3B 4V 5T 6N
T 4A
C
O 1R 2H 3N 5J 5H 1K 2Y 3R 4A 4D 4K
W 1H 1V 10 3C 3P 4V 5G 5Z 5X 5S 6Z 1L 2F 2I 3K 4N 4F 6F
I 2W 3W 4J 4B 4R 6L 6T 6D 6H 1M 1V 2X 2B 3X 5M
Z 1I 4H 4Y 5A 5P 6Y 1Y 1C 1B 1I 2Z 2K 4T 5X 5Y 5E
L 5Y 2M 2L 3Z 4B 4L 5B 6D
J 1J 1P 2U 2S 4I 4D 1N 2V 3V 4I 5Q 6P
F 2M 2K 2C 4Q 50 3D 3E 4S 6X
R 1A 3T 6W 20 2Q 2E 3G 3J 4Q 6J
K 2G 5D 5T 6M 6K 6V 60 2G 30 3H 3L 5U 5F 5L 6H 6L
B 1G 2B 2X 2T 3M 3J 3E 3S 4S 1Q 1T 4K 60 6R
M 1F 1Z 1T 2J 2F 3U 4C 6N 6E 6U 3W 4U 5I 6U

Underlined type denotes wheels in reversed positions.

71836—35——6

Table O

A	1G	1A	1U	2K	2G	3V	4D	60	6F	6V	3V	4T	5H	6T
H	1M	1Y	1X	3I	4A	50	5N	5C	6C	1E	2S	3T	4V	5U	6X
V	1D	2W	5G	5X	6G	1Q	4X	4D	6A						
Y	1C	1R	2Q	2P	1T	1Z	2I	4L	40	5B	5G	6L	6R		
Q	1N	2B	4M	4G	4U	4Q	6H	1R	1G	3M	3P	3S	4W	4G	5V	5J	6Z	6H
P	4Y	6Y	2R	4B	50	6S												
U	2R	3J	3C	5V	6Q	1Y	1C	1F	20	2C	3E							
X	10	2J	3H	3R	40	5F	5S	5R	6S	6D	1I	2Q	5F	6U	6Y			
S	1L	1V	2M	2E	3Z	4F	5L	5W	2T	2Z	2B	3Z	5Y	6J				
N	1T	2Z	5J	6B	6R	6B												
D	2S	2A	3M	3L	3S	4X	4V	6J	1N	10	1D	2G	3H	4N	5N	5Q	5R	5I	6D
G	3Y	3P	4H	40	1V	2V	3B	4Q	4Y	4F	6P	6F							
E	1F	1E	2F	3A	3E	3B	4N	5D	6T	3L	3R	3X	5M	5Z	5C	6V			
T	1Z	20	3G	3W	4L	5M	6K	1W	2M	30	3A	4U	5S	6M					
C	4B																		
O																			
W	1S	2I	30	5K	5I	1J	2X	3Q	4Z	4C	4J								
I	1I	1W	1P	3D	3Q	4W	5H	5A	5Y	5T	6A	1K	2E	2H	3J	4M	4E	6E	
Z	2X	3X	4K	4C	4S	6M	6U	6E	6I	1L	1U	2W	2A	3W	5L				
L	1J	4I	4Z	5B	5Q	6Z	1X	1B	1A	1H	2Y	2J	4S	5W	5X	5D			
J	5Z	2L	2K	3Y	4A	4K	5A	6C											
F	1K	1Q	2V	2T	4J	4E	1M	2U	3U	4H	5P	60							
R	2N	2L	2D	4R	5P	3C	3D	6W	4R										
K	1B	3U	6X	2N	2P	2D	3F	3I	4P	6I									
B	2H	5E	5U	6N	6L	6W	6P	2F	3N	3G	3K	5T	5E	5K	6G	6K			
M	1H	2C	2Y	2U	3N	3K	3F	3T	4T	1P	1S	4J	6N	6Q					

Underlined type denotes wheels in reversed positions.

Table W

A	1I	2D	2Z	2V	30	3L	3G	3U	4U	10	1R	4I	6M	6P	
H	1H	1B	1V	2L	2H	3W	4E	6P	6G	6W	3U	4S	5G	6S	
V	1N	1Z	1Y	3J	4B	5P	50	5D	6D	1D	2R	3S	4U	5T	6W
Y	1E	2X	5H	5Y	6H	1P	4W	4C	6Z						
Q	1D	1S	2R	2Q	1S	1Y	2H	4K	4N	5A	5F	6K	6Q		
P	10	2C	4N	4H	4V	4R	6I	1Q	1F	3L	30	3R	4V	4F	5U	5I	6Y	6G
U	4Z	6Z	2Q	4A	5N	6R												
X	2S	3K	3D	5W	6R	1X	1B	1E	2N	2B	3D							
S	1P	2K	3I	3S	4P	5G	5T	5S	6T	6E	1H	2P	5E	6T	6X			
N	1M	1W	2N	2F	3A	4G	5M	5X	2S	2Y	2A	3Y	5X	6I				
D	1U	2A	5K	6C	6S	6A												
G	2T	2B	3N	3M	3T	4Y	4W	6K	1M	1N	1C	2F	3G	4M	5M	5P	5Q	5H	6C
E	3Z	3Q	4I	4P	1U	2U	3A	4P	4X	4E	60	6E							
T	1G	1F	2G	3B	3F	3C	40	5E	6U	3K	3Q	3W	5L	5Y	5B	6U			
C	1A	2P	3H	3X	4M	5N	6L	1V	2L	3N	3Z	4T	5R	6L					
O	4C																		
W																			
I	1T	2J	3P	5L	5J	1I	2W	3P	4Y	4B	4I								
Z	1J	1X	1Q	3E	3R	4X	5I	5B	5Z	5U	6B	1J	2D	2G	3I	4L	4D	6D	
L	2Y	3Y	4L	4D	4T	6N	6V	6F	6J	1K	1T	2V	2Z	3V	5K				
J	1K	4J	4A	5C	5R	6A	1W	1A	1Z	1G	2X	2I	4R	5V	5W	5C			
F	5A	2K	2J	3X	4Z	4J	5Z	6B											
R	1L	1R	2W	2U	4K	4F	1L	2T	3T	4G	50	6N							
K	20	2M	2E	4S	5Q	3C	3B	4Q	6V										
B	1C	3V	6Y	2M	20	2C	3E	3H	40	6H									
M	2I	5F	5V	60	6M	6X	6Q	2E	3M	3F	3J	5S	5D	5J	6F	6J			

Underlined type denotes wheels in reversed positions.

TABLE I

A	2J	5G	5W	6P	6N	6Y	6R	2D	3L	3E	3I	5R	5C	5I	6E	6I
H	1J	2E	2A	2W	3P	3M	3H	3V	4V	1N	1Q	4H	6L	60		
V	1I	1C	1W	2M	2I	3X	4F	6Q	6H	6X	3T	4R	5F	6R		
Y	10	1A	1Z	3K	4C	5Q	5P	5E	6E	1C	2Q	3R	4T	5S	6V	
Q	1F	2Y	5I	5Z	6I	10	4V	4B	6Y							
P	1E	1T	2S	2R	1R	1X	2G	4J	4M	5Z	5E	6J	6P			
U	1P	2D	40	4I	4W	4S	6J	1P	1E	3K	3N	3Q	4U	4E	5T	5H	6X	6F
X	4A	6A	2P	4Z	5M	6Q										
S	2T	3L	3E	5X	6S	1W	1A	1D	2M	2A	3C					
N	1Q	2L	3J	3T	4Q	5H	5U	5T	6U	6F	1G	20	5D	6S	6W	
D	1N	1X	20	2G	3B	4H	5N	5Y	2R	2X	2Z	3X	5W	6H		
G	1V	2B	5L	6D	6T	6Z										
E	2U	30	3N	2C	3U	4Z	4X	6L	1L	1M	1B	2E	3F	4L	5L	50	5P	5G	6B
T	3A	3R	4J	4Q	1T	2T	3Z	40	4W	4D	6N	6D							
C	1H	1G	2H	3C	3G	3D	4P	5F	6V	3J	3P	3V	5K	5X	5A	6T			
O	1B	2Q	3I	3Y	4N	50	6M	1U	2K	3M	3Y	4S	5Q	6K					
W	4D																		
I																			
Z	1U	2K	3Q	5M	5K	1H	2V	30	4X	4A	4H								
L	1K	1Y	1R	3F	3S	4Y	5J	5C	5A	5V	6C	1I	2C	2F	3H	4K	4C	6C	
J	2Z	3Z	4M	4E	4U	60	6W	6G	6K	1J	1S	2U	2Y	3U	5J				
F	1L	4K	4B	5D	5S	6B	1V	1Z	1Y	1F	2W	2H	4Q	5U	5V	5B			
R	5B	2J	2I	3W	4Y	4I	5Y	6A											
K	1M	1S	2X	2V	4L	4G	1K	2S	3S	4F	5N	6M							
B	2P	2N	2F	4T	5R	3A	3B	4P	6U										
M	1D	3W	6Z	2L	2N	2B	3D	3G	4N	6G									

Underlined type denotes wheels in reversed positions.

TABLE Z

A	1E	3X	6A	2K	2M	2A	3C	3F	4M	6F						
H	2K	5H	5X	6Q	60	6Z	6S	2C	3K	3D	3H	5Q	5B	5H	6D	6H
V	1K	2F	2B	2X	3Q	3N	3I	3W	4W	1M	1P	4G	6K	6N		
Y	1J	1D	1X	2N	2J	3Y	4G	6R	6I	6Y	3S	4Q	5E	6Q		
Q	1P	1B	1A	3L	4D	5R	5Q	5F	6F	1B	2P	3Q	4S	5R	6U	
P	1G	2Z	5J	5A	6J	1N	4U	4A	6X							
U	1F	1U	2T	2S	1Q	1W	2F	4I	4L	5Y	5D	6I	60			
X	1Q	2E	4P	4J	4X	4T	6K	10	1D	3J	3M	3P	4T	4D	5S	5G	6W	6E
S	4B	6B	20	4Y	5L	6P										
N	2U	3M	3F	5Y	6T	1V	1Z	1C	2L	2Z	3B					
D	1R	2M	3K	3U	4R	5I	5V	5U	6V	6G	1F	2N	5C	6R	6V	
G	10	1Y	2P	2H	3C	4I	50	5Z	2Q	2W	2Y	3W	5V	6G		
E	1W	2C	5M	6E	6U	6Y										
T	2V	3P	30	2D	3V	4A	4Y	6M	1K	1L	1A	2D	3E	4K	5K	5N	50	5F	6A
C	3B	3S	4K	4R	1S	2S	3Y	4N	4V	4C	6M	6C							
O	1I	1H	2I	3D	3H	3E	4Q	5G	6W	3I	30	3U	5J	5W	5Z	6S			
W	1C	2R	3J	3Z	40	5P	6N	1T	2J	3L	3X	4R	5P	6J					
I	4E																		
Z																			
L	1V	2L	3R	5N	5L	1G	2U	3N	4W	4Z	4G								
J	1L	1Z	1S	3G	3T	4Z	5K	5D	5B	5W	6D	1H	2B	2E	3G	4J	4B	6B	
F	2A	3A	4N	4F	4V	6P	6X	6H	6L	1I	1R	2T	2X	3T	5I				
R	1M	4L	4C	5E	5T	6C	1U	1Y	1X	1E	2V	2G	4P	5T	5U	5A			
K	5C	2I	2H	3V	4X	4H	5X	6Z											
B	1N	1T	2Y	2W	4M	4H	1J	2R	3R	4E	5M	6L							
M	2Q	20	2G	4U	5S	3Z	3A	40	6T										

Underlined type denotes wheels in reversed positions.

TABLE L

A 2R 2P 2H 4V 5T 3Y 3Z 4N 6S

H 1F 3Y 6B 2J 2L 2Z 3B 3E 4L 6E

V 2L 5I 5Y 6R 6P 6A 6T 2B 3J 3C 3G 5P 5A 5G 6C 6G

Y 1L 2G 2C 2Y 3R 30 3J 3X 4X 1L 10 4F 6J 6M

Q 1K 1E 1Y 20 2K 3Z 4H 6S 6J 6Z 3R 4P 5D 6P

P 1Q 1C 1B 3M 4E 5S 5R 5G 6G 1A 20 3P 4R 5Q 6T

U 1H 2A 5K 5B 6K 1M 4T 4Z 6W

X 1G 1V 2U 2T 1P 1V 2E 4H 4K 5X 5C 6H 6N

S 1R 2F 4Q 4K 4Y 4U 6L 1N 1C 3I 3L 30 4S 4C 5R 5F 6V 6D

N 4C 6C 2N 4X 5K 60

D 2V 3N 3G 5Z 6U 1U 1Y 1B 2K 2Y 3A

G 1S 2N 3L 3V 4S 5J 5W 5V 6W 6H 1E 2M 5B 6Q 6U

E 1P 1Z 2Q 2I 3D 4J 5P 5A 2P 2V 2X 3V 5U 6F

T 1X 2D 5N 6F 6V 6X

C 2W 2E 3Q 3P 3W 4B 4Z 6N 1J 1K 1Z 2C 3D 4J 5J 5M 5N 5E 6Z

O 3C 3T 4L 4S 1R 2R 3X 4M 4U 4B 6L 6B

W 1J 1I 2J 3E 3I 3F 4R 5H 6X 3H 3N 3T 5I 5V 5Y 6R

I 1D 2S 3K 3A 4P 5Q 60 1S 2I 3K 3W 4Q 50 6I

Z 4F

L

J 1W 2M 3S 50 5M 1F 2T 3M 4V 4Y 4F

F 1M 1A 1T 3H 3U 4A 5L 5E 5C 5X 6E 1G 2A 2D 3F 4I 4A 6A

R 2B 3B 40 4G 4W 6Q 6Y 6I 6M 1H 1Q 2S 2W 3S 5H

K 1N 4M 4D 5F 5U 6D 1T 1X 1W 1D 2U 2F 40 5S 5T 5Z

B 5D 2H 2G 3U 4W 4G 5W 6Y

M 10 1U 2Z 2X 4N 4I 1I 2Q 3Q 4D 5L 6K

Underlined type denotes wheels in reversed positions.

TABLE J

A 1P 1V 2A 2Y 40 4J 1H 2P 3P 4C 5K 6J

H 2S 2Q 2I 4W 5U 3X 3Y 4M 6R

V 1G 3Z 6C 2I 2K 2Y 3A 3D 4K 6D

Y 2M 5J 5Z 6S 6Q 6B 6U 2A 3I 3B 3F 50 5Z 5F 6B 6F

Q 1M 2H 2D 2Z 3S 3P 3K 3Y 4Y 1K 1N 4E 6I 6L

P 1L 1F 1Z 2P 2L 3A 4I 6T 6K 6A 3Q 40 5C 60

U 1R 1D 1C 3N 4F 5T 5S 5H 6H 1Z 2N 30 4Q 5P 6S

X 1I 2B 5L 5C 6L 1L 4S 4Y 6V

S 1H 1W 2V 2U 10 1U 2D 4G 4J 5W 5B 6G 6M

N 1S 2G 4R 4L 4Z 4V 6M 1M 1B 3H 3K 3N 4R 4B 5Q 5E 6U 6C

D 4D 6D 2M 4W 5J 6N

G 2W 30 3H 5A 6V 1T 1X 1A 2J 2X 3Z

E 1T 20 3M 3W 4T 5K 5X 5W 6X 6I 1D 2L 5A 6P 6T

T 1Q 1A 2R 2J 3E 4K 5Q 5B 20 2U 2W 3U 5T 6E

C 1Y 2E 50 6G 6W 6W

O 2X 3R 3Q 2F 3X 4C 4A 60 1I 1J 1Y 2B 3C 4I 5I 5L 5M 5D 6Y

W 3D 3U 4M 4T 1Q 2Q 3W 4L 4T 4A 6K 6A

I 1K 1J 2K 3F 3J 3G 4S 5I 6Y 3G 3M 3S 5H 5U 5X 6Q

Z 1E 2T 3L 3B 4Q 5R 6P 1R 2H 3J 3V 4P 5N 6H

L 4G

J

F 1X 2N 3T 5P 5N 1E 2S 3L 4U 4X 4E

R 1N 1B 1U 3I 3V 4B 5M 5F 5D 5Y 6F 1F 2Z 2C 3E 4H 4Z 6Z

K 2C 3C 4P 4H 4X 6R 6Z 6J 6N 1G 1P 2R 2V 3R 5G

B 10 4N 4E 5G 5V 6E 1S 1W 1V 1C 2T 2E 4N 5R 5S 5Y

M 5E 2G 2F 3T 4V 4F 5V 6X

Underlined type denotes wheels in reversed positions.

Table F

A	5F	2F	2E	3S	4U	4E	5U	6W
H	1Q	1W	2B	2Z	4P	4K	1G	2O	3O	4B	5J	6I
V	2T	2R	2J	4X	5V	3W	3X	4L	6Q
Y	1H	3A	6D	2H	2J	2X	3Z	3C	4J	6C
Q	2N	5K	5A	6T	6R	6C	6V	2Z	3H	3A	3E	5N	5Y	5E	6A	6E
P	1N	2I	2E	2A	3T	3Q	3L	3Z	4Z	1J	1M	4D	6H	6K
U	1M	1G	1A	2Q	2M	3B	4J	6U	6L	6B	3P	4N	5B	6N
X	1S	1E	1D	3O	4G	5U	5T	5I	6I	1Y	2M	3N	4P	5O	6R
S	1J	2C	5M	5D	6M	1K	4R	4X	6U
N	1I	1X	2W	2V	1N	1T	2C	4F	4I	5V	5A	6F	6L
D	1T	2H	4S	4M	4A	4W	6N	1L	1A	3G	3J	3M	4Q	4A	5P	5D	6T	6B
G	4E	6E	2L	4V	5I	6M
E	2X	3P	3I	5B	6W	1S	1W	1Z	2I	2W	3Y
T	1U	2P	3N	3X	4U	5L	5Y	5X	6Y	6J	1C	2K	5Z	6O	6S
C	1R	1B	2S	2K	3F	4L	5R	5C	2N	2T	2V	3T	5S	6D
O	1Z	2F	5P	6H	6X	6V
W	2Y	2G	3S	3R	3Y	4D	4B	6P	1H	1I	1X	2A	3B	4H	5H	5K	5L	5C	6X
I	3E	3V	4N	4U	1P	2P	3V	4K	4S	4Z	6J	6Z
Z	1L	1K	2L	3G	3K	3H	4T	5J	6Z	3F	3L	3R	5G	5T	5W	6P
L	1F	2U	3M	3C	4R	5S	6Q	1Q	2G	3I	3U	4O	5M	6G
J	4H
F	
R	1Y	2O	3U	5Q	5O	1D	2R	3K	4T	4W	4D
K	1O	1C	1V	3J	3W	4C	5N	5G	5E	5Z	6G	1E	2Y	2B	3D	4G	4Y	6Y
B	2D	3D	4Q	4I	4Y	6S	6A	6K	6O	1F	1O	2Q	2U	3Q	5F
M	1P	4O	4F	5H	5W	6F	1R	1V	1U	1B	2S	2D	4M	5Q	5R	5X

Underlined type denotes wheels in reversed positions.

Table R

A	1Q	4P	4G	5I	5X	6G	1Q	1U	1T	1A	2R	2C	4L	5P	5Q	5W
H	5G	2E	2D	3R	4T	4D	5T	6V
V	1R	1X	2C	2A	4Q	4L	1F	2N	3N	4A	5I	6H
Y	2U	2S	2K	4Y	5W	3V	3W	4K	6P
Q	1I	3B	6E	2G	2I	2W	3Y	3B	4I	6B
P	2O	5L	5B	6U	6S	6D	6W	2Y	3G	3Z	3D	5M	5X	5D	6Z	6D
U	1O	2J	2F	2B	3U	3R	3M	3A	4A	1I	1L	4C	6G	6J
X	1N	1H	1B	2R	2N	3C	4K	6V	6M	6C	3O	4M	5A	6M
S	1T	1F	1E	3P	4H	5V	5U	5J	6J	1X	2L	3M	4O	5N	6Q
N	1K	2D	5N	5E	6N	1J	4Q	4W	6T
D	1J	1Y	2X	2W	1M	1S	2B	4E	4H	5U	5Z	6E	6K
G	1U	2I	4T	4N	4B	4X	6O	1K	1Z	3F	3I	3L	4P	4Z	5O	5C	6S	6A
E	4F	6F	2K	4U	5H	6L
T	2Y	3Q	3J	5C	6X	1R	1V	1Y	2H	2V	3X
C	1V	2Q	3O	3Y	4V	5M	5Z	5Y	6Z	6K	1B	2J	5Y	6N	6R
O	1S	1C	2T	2L	3G	4M	5S	5D	2M	2S	2U	3S	5R	6C
W	1A	2G	5Q	6I	6Y	6U
I	2Z	3T	3S	3H	3Z	4E	4C	6Q	1G	1H	1W	2Z	3A	4G	5G	5J	5K	5B	6W
Z	3F	3W	4O	4V	1O	2O	3U	4J	4R	4Y	6I	6Y
L	1M	1L	2M	2H	3L	3I	4U	5K	6A	3E	3K	3Q	5F	5S	5V	6O
J	1G	2V	3N	3D	4S	5T	6R	1P	2F	3H	3T	4N	5L	6F
F	4I
R	
K	1Z	2P	3V	5R	5P	1C	2Q	3J	4S	4V	4C
B	1P	1D	1W	3K	3X	4D	5O	5H	5F	5A	6H	1D	2X	2A	3C	4F	4X	6X
M	2E	3E	4R	4J	4Z	6T	6B	6L	6P	1E	1N	2P	2T	3P	5E

Underlined type denotes wheels in reversed positions.

Table K

A	2F	3F	4S	4K	4A	6U	6C	6M	6Q	1D	1M	2O	2S	3O	5D
H	1R	4Q	4H	5J	5Y	6H	1P	1T	1S	1Z	2Q	2B	4K	5O	5P	5V
V	5H	2D	2C	3Q	4S	4C	5S	6U								
Y	1S	1Y	2D	2B	4R	4M	1E	2M	3M	4Z	5H	6G				
Q	2V	2T	2L	4Z	5X	3U	3V	4J	6O							
P	1J	3C	6F	2F	2H	2V	3X	3A	4H	6A						
U	2P	5M	5C	6V	6T	6E	6X	2X	3F	3Y	3C	5L	5W	5C	6Y	6C
X	1P	2K	2G	2C	3V	3S	3N	3B	4B	1H	1K	4B	6F	6I		
S	1O	1I	1C	2S	2O	3D	4L	6W	6N	6D	3N	4L	5Z	6L		
N	1U	1G	1F	3Q	4I	5W	5V	5K	6K	1W	2K	3L	4N	5M	6P	
D	1L	2E	5O	5F	6O	1I	4P	4V	6S							
G	1K	1Z	2Y	2X	1L	1R	2A	4D	4G	5T	5Y	6D	6J			
E	1V	2J	4U	4O	4C	4Y	6P	1J	1Y	3E	3H	3K	4O	4Y	5N	5B	6R	6Z
T	4G	6G	2J	4T	5G	6K										
C	2Z	3R	3K	5D	6Y	1Q	1U	1X	2G	2U	3W					
O	1W	2R	3P	3Z	4W	5N	5A	5Z	6A	6L	1A	2I	5X	6M	6Q	
W	1T	1D	2U	2M	3H	4N	5T	5E	2L	2R	2T	3R	5Q	6B		
I	1B	2H	5R	6J	6Z	6T										
Z	2A	3U	3T	3I	3A	4F	4D	6R	1F	1G	1V	2Y	3Z	4F	5F	5I	5J	5A	6V
L	3G	3X	4P	4W	1N	2N	3T	4I	4Q	4X	6H	6X							
J	1N	1M	2N	2I	3M	3J	4V	5L	6B	3D	3J	3P	5E	5R	5U	6N			
F	1H	2W	3O	3E	4T	5U	6S	1O	2E	3G	3S	4M	5K	6E					
R	4J																		
K																			
B	1A	2Q	3W	5S	5Q	1B	2P	3I	4R	4U	4B								
M	1Q	1E	1X	3L	3Y	4E	5P	5I	5G	5B	6I	1C	2W	2Z	3B	4E	4W	6W	

Underlined type denotes wheels in reversed positions.

Table B

A	1R	1F	1Y	3M	3Z	4F	5Q	5J	5H	5C	6J	1B	2V	2Y	3A	4D	4V	6V
H	2G	3G	4T	4L	4B	6V	6D	6N	6R	1C	1L	2N	2R	3N	5C			
V	1S	4R	4I	5K	5Z	6I	1O	1S	1R	1Y	2P	2A	4J	5N	5O	5U		
Y	5I	2C	2B	3P	4R	4B	5R	6T										
Q	1T	1Z	2E	2C	4S	4N	1D	2L	3L	4Y	5G	6F						
P	2W	2U	2M	4A	5Y	3T	3U	4I	6N									
U	1K	3D	6G	2E	2G	2U	3W	3Z	4G	6Z								
X	2Q	5N	5D	6W	6U	6F	6Y	2W	3E	3X	3B	5K	5V	5B	6X	6B		
S	1Q	2L	2H	2D	3W	3T	3O	3C	4C	1G	1J	4A	6E	6H				
N	1P	1J	1D	2T	2P	3E	4M	6X	6O	6E	3M	4K	5Y	6K				
D	1V	1H	1G	3R	4J	5X	5W	5L	6L	1V	2J	3K	4M	5L	6O			
G	1M	2F	5P	5G	6P	1H	4O	4U	6R									
E	1L	1A	2Z	2Y	1K	1Q	2Z	4C	4F	5S	5X	6C	6I					
T	1W	2K	4V	4P	4D	4Z	6Q	1I	1X	3D	3G	3J	4N	4X	5M	5A	6Q	6Y
C	4H	6H	2I	4S	5F	6J												
O	2A	3S	3L	5E	6Z	1P	1T	1W	2F	2T	3V							
W	1X	2S	3Q	3A	4X	5O	5B	5A	6B	6M	1Z	2H	5W	6L	6P			
I	1U	1E	2V	2N	3I	4O	5U	5F	2K	2Q	2S	3Q	5P	6A				
Z	1C	2I	5S	6K	6A	6S												
L	2B	3V	3U	3J	3B	4G	4E	6S	1E	1F	1U	2X	3Y	4E	5E	5H	5I	5Z	6U
J	3H	3Y	4Q	4X	1M	2M	3S	4H	4P	4W	6G	6W							
F	1O	1N	2O	2J	3N	3K	4W	5M	6C	3C	3I	3O	5D	5Q	5T	6M			
R	1I	2X	3P	3F	4U	5V	6T	1N	2D	3F	3R	4L	5J	6D					
K	4K																		
B																			
M	1B	2R	3X	5T	5R	1A	2O	3H	4Q	4T	4A								

Underlined type denotes wheels in reversed positions.

TABLE M

A	1C	2S	3Y	5U	5S	1Z	2N	3G	4P	4S	4Z	
H	1S	1G	1Z	3N	3A	4G	5R	5K	5I	5D	6K	1A	2U	2X	3Z	4C	4U	6U
V	2H	3H	4U	4M	4C	6W	6E	6O	6S	1B	1K	2M	2Q	3M	5B			
Y	1T	4S	4J	5L	5A	6J	1N	1R	1Q	1X	2O	2Z	4I	5M	5N	5T		
Q	5J	2B	2A	3O	4Q	4A	5Q	6S										
P	1U	1A	2F	2D	4T	4O	1C	2K	3K	4X	5F	6E						
U	2X	2V	2N	4B	5Z	3S	3T	4H	6M									
X	1L	3E	6H	2D	2F	2T	3V	3Y	4F	6Y								
S	2R	5O	5E	6X	6V	6G	6Z	2V	3D	3W	3A	5J	5U	5A	6W	6A		
N	1R	2M	2I	2E	3X	3U	3P	3D	4D	1F	1I	4Z	6D	6G				
D	1Q	1K	1E	2U	2Q	3F	4N	6Y	6P	6F	3L	4J	5X	6J				
G	1W	1I	1H	3S	4K	5Y	5X	5M	6M	1U	2I	3J	4L	5K	6N			
E	1N	2G	5Q	5H	6Q	1G	4N	4T	6Q									
T	1M	1B	2A	2Z	1J	1P	2Y	4B	4E	5R	5W	6B	6H					
C	1X	2L	4W	4Q	4E	4A	6R	1H	1W	3C	3F	3I	4M	4W	5L	5Z	6P	6X
O	4I	6I	2H	4R	5E	6I												
W	2B	3T	3M	5F	6A	1O	1S	1V	2E	2S	3U							
I	1Y	2T	3R	3B	4Y	5P	5C	5B	6C	6N	1Y	2G	5V	6K	6O			
Z	1V	1F	2W	2O	3J	4P	5V	5G	2J	2P	2R	3P	5O	6Z				
L	1D	2J	5T	6L	6B	6R												
J	2C	3W	3V	3K	3C	4H	4F	6T	1D	1E	1T	2W	3X	4D	5D	5G	5H	5Y	6T
F	3I	3Z	4R	4Y	1L	2L	3R	4G	4O	4V	6F	6V						
R	1P	1O	2P	2K	3O	3L	4X	5N	6D	3B	3H	3N	5C	5P	5S	6L		
K	1J	2Y	3Q	3G	4V	5W	6U	1M	2C	3E	3Q	4K	5I	6C				
B	4L																	
M																		

Underlined type denotes wheels in reversed positions.

APPENDIX IV

BASIC PLAIN-TEXT SEQUENCES

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

BASIC PLAIN-TEXT SEQUENCES FOR CW1 DIRECT

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

BASIC PLAIN-TEXT SEQUENCES FOR CW2 DIRECT

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

BASIC PLAIN-TEXT SEQUENCES FOR CW3 DIRECT

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

BASIC PLAIN-TEXT SEQUENCES FOR CW4 DIRECT

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

BASIC PLAIN-TEXT SEQUENCES FOR CW5 DIRECT

71836—35——7

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

BASIC PLAIN-TEXT SEQUENCES FOR CW6 DIRECT

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

BASIC PLAIN-TEXT SEQUENCES FOR CW1 REVERSED

Setting

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

BASIC PLAIN-TEXT SEQUENCES FOR CW2 REVERSED

Setting

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

BASIC PLAIN-TEXT SEQUENCES FOR CW3 REVERSED

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

BASIC PLAIN-TEXT SEQUENCES FOR CW4 REVERSED

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

BASIC PLAIN-TEXT SEQUENCES FOR CW5 REVERSED

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

BASIC PLAIN-TEXT SEQUENCES FOR CW6 REVERSED

APPENDIX V

FIRST-INTERVAL DATA—PLAIN-TEXT RELATIONSHIPS

TABLE B

B																										
J	1Y	2M	3F	4O	4R	4Y	1D	2T	3Z	5V	5T															
M	1A	2U	2X	3Z	4C	4U	6U	1S	1G	1Z	3N	3A	4G	5R	5K	5I	5D	6K								
A	1C	1L	2N	2R	3N	5C	2G	3G	4T	4L	4B	6V	6D	6N	6R											
Q	1P	1T	1S	1Z	2Q	2B	4K	5O	5P	5V	1R	4Q	4H	5J	5Y	6H										
I	2E	2D	3R	4T	4D	5T	6V	5G																		
O	1G	2O	3O	4B	5J	6I	1Q	1W	2B	2Z	4P	4K														
F	3X	3Y	4M	6R	2S	2Q	2I	4W	5U																	
P	2J	2L	2Z	3B	3E	4L	6E	1F	3Y	6B																
C	2C	3K	3D	3H	5Q	5B	5H	6D	6H	2K	5H	5X	6Q	6O	6Z	6S										
X	1N	1Q	4H	6L	6O	1J	2E	2A	2W	3P	3M	3H	3V	4V												
Z	3U	4S	5G	6S	1H	1B	1V	2L	2H	3W	4E	6P	6G	6W												
R	1E	2S	3T	4V	5U	6X	1M	1Y	1X	3I	4A	5O	5N	5C	6C											
V	1R	4Y	4E	6B	1C	2V	5F	5W	6F																	
L	1V	1B	2K	4N	4Q	5D	5I	6N	6T	1A	1P	2O	2N													
Y	1U	1J	3P	3S	3V	4Z	4J	5Y	5M	6C	6K	1K	2Y	4J	4D	4R	4N	6E								
W	2V	4F	5S	6W	4U	6U																				
U	1D	1H	1K	2T	2H	3J	2M	3E	3X	5Q	6L															
T	1O	2W	5L	6A	6E	1I	2D	3B	3L	4I	5Z	5M	5L	6X	6M											
H	2A	2G	2I	3G	5F	6Q	1E	1O	2F	2X	3S	4Y	5E	5P												
G	6J	1L	2R	5B	6T	6J																				
D	1X	1W	1M	2P	3Q	4W	5W	5Z	5A	5R	6M	2J	3D	3C	3R	3J	4O	4M	4S	6A						
K	1F	2F	3L	4A	4I	4P	6Z	6P	3O	3F	4X	4F														
E	3W	3C	3I	5X	5K	5N	6G	1U	1T	2U	2P	3T	3Q	4C	5S	6I										
S	1I	2Y	3A	3M	4G	5E	6Y	1N	2C	3U	3K	4Z	5A	6Y												
N																										

Underlined type denotes wheels in reversed positions.

TABLE J

B																							
J																							
M	1Z	2N	3G	4P	4S	4Z	1C	2S	3Y	5U	5S												
A	1B	2V	2Y	3A	4D	4V	6V	1R	1F	1Y	3M	3Z	4F	5Q	5J	5H	5C	6J					
Q	1D	1M	20	2S	30	5D	2F	3F	4S	4K	4A	6U	6C	6M	6Q								
I	1Q	1U	1T	1A	2R	2C	4L	5P	5Q	5W	1Q	4P	4G	5I	5X	6G							
O	2F	2E	3S	4U	4E	5U	6W	5F															
F	1H	2P	3P	4C	5K	6J	1P	1V	2A	2Y	40	4J											
P	3Y	3Z	4N	6S	2R	2P	2H	4V	5T														
C	2K	2M	2A	3C	3F	4M	6F	1E	3X	6A													
X	2D	3L	3E	3I	5R	5C	5I	6E	6I	2J	5G	5W	6P	6N	6Y	6R							
Z	10	1R	4I	6M	6P	1I	2D	2Z	2V	30	3L	3G	3U	4U									
R	3V	4T	5H	6T	1G	1A	1U	2K	2G	3V	4D	60	6F	6V									
V	1F	2T	3U	4W	5V	6Y	1L	1X	1W	3H	4Z	5N	5M	5B	6B								
L	1S	4Z	4F	6C	1B	2U	5E	5V	6E														
Y	1W	1C	2L	40	4R	5E	5J	60	6U	1Z	10	2N	2M										
W	1V	1K	3Q	3T	3W	4A	4K	5Z	5N	6D	6L	1J	2X	4I	4C	4Q	4M	6D					
U	2W	4G	5T	6X	4T	6T																	
T	1E	1I	1L	2U	2I	3K	2L	3D	3W	5P	6K												
H	1P	2X	5M	6B	6F	1H	2C	3A	3K	4H	5Y	5L	5K	6W	6L								
G	2B	2H	2J	3H	5G	6R	1D	1N	2E	2W	3R	4X	5D	50									
D	6K	1K	2Q	5A	6S	6I																	
K	1Y	1X	1N	2Q	3R	4X	5X	5A	5B	5S	6N	2I	3C	3B	3Q	3I	4N	4L	4R	6Z			
E	1G	2G	3M	4B	4J	4Q	6A	6Q	3N	3E	4W	4E											
S	3X	3D	3J	5Y	5L	50	6H	1T	1S	2T	20	3S	3P	4B	5R	6H							
N	1J	2Z	3B	3N	4H	5F	6Z	1M	2B	3T	3J	4Y	5Z	6X									

Underlined type denotes wheels in reversed positions.

TABLE M

B	1K	2A	3C	30	4I	5G	6A	1L	2A	3S	3I	4X	5Y	6W									
J																							
M																							
A	1A	20	3H	4Q	4T	4A	1B	2R	3X	5T	5R												
Q	1C	2W	2Z	3B	4E	4W	6W	1Q	1E	1X	3L	3Y	4E	5P	5I	5G	5B	6I					
I	1E	1N	2P	2T	3P	5E	2E	3E	4R	4J	4Z	6T	6B	6L	6P								
O	1R	1V	1U	1B	2S	2D	4M	5Q	5R	5X	1P	40	4F	5H	5W	6F							
F	2G	2F	3T	4V	4F	5V	6X	5E															
P	1I	2Q	3Q	4D	5L	6K	10	1U	2Z	2X	4N	4I											
C	3Z	3A	40	6T	2Q	20	2G	4U	5S														
X	2L	2N	2B	3D	3G	4N	6G	1D	3W	6Z													
Z	2E	3M	3F	3J	5S	5D	5J	6F	6J	2I	5F	5V	60	6M	6X	6Q							
R	1P	1S	4J	6N	6Q	1H	2C	2Y	2U	3N	3K	3F	3T	4T									
V	3W	4U	5I	6U	1F	1Z	1T	2J	2F	3U	4C	6N	6E	6U									
L	1G	2U	3V	4X	5W	6Z	1K	1W	1V	3G	4Y	5M	5L	5A	6A								
Y	1T	4A	4G	6D	1A	2T	5D	5U	6D														
W	1X	1D	2M	4P	4S	5F	5K	6P	6V	1Y	1N	2M	2L										
U	1W	1L	3R	3U	3X	4B	4L	5A	50	6E	6M	1I	2W	4H	4B	4P	4L	6C					
T	2X	4H	5U	6Y	4S	6S																	
H	1F	1J	1M	2V	2J	3L	2K	3C	3V	50	6J												
G	1Q	2Y	5N	6C	6G	1G	2B	3Z	3J	4G	5X	5K	5J	6V	6K								
D	2C	2I	2K	3I	5H	6S	1C	1M	2D	2V	3Q	4W	5C	5N									
K	6L	1J	2P	5Z	6R	6H																	
E	1Z	1Y	10	2R	3S	4Y	5Y	5B	5C	5T	60	2H	3B	3A	3P	3H	4M	4K	4Q	6Y			
S	1H	2H	3N	4C	4K	4R	6B	6R	3M	3D	4V	4D											
N	3Y	3E	3K	5Z	5M	5P	6I	1S	1R	2S	2N	3R	30	4A	5Q	6G							

Underlined type denotes wheels in reversed positions.

Table A

B	3Z	3F	3L	5A	5N	5Q	6J	1R	1Q	2R	2M	3Q	3N	4Z	5P	6F
J	1L	2B	3D	3P	4J	5H	6B	1K	2Z	3R	3H	4W	5X	6V		
M																
A																
Q	1B	2P	3I	4R	4U	4B	1A	2Q	3W	5S	5Q					
I	1D	2X	2A	3C	4F	4X	6X	1P	1D	1W	3K	3X	4D	5O	5H	5F	5A	6H
O	1F	1O	2Q	2U	3Q	5F	2D	3D	4Q	4I	4Y	6S	6A	6K	6Q			
F	1S	1W	1V	1C	2T	2E	4N	5R	5S	5Y	1O	4N	4E	5G	5V	6E		
P	2H	2G	3U	4W	4G	5W	6Y	5D										
C	1J	2R	3R	4E	5M	6L	1N	1T	2Y	2W	4M	4H						
X	3A	3B	4P	6U	2P	2N	2F	4T	5R									
Z	2M	2O	2C	3E	3H	4O	6H	1C	3V	6Y								
R	2F	3N	3G	3K	5T	5E	5K	6G	6K	2H	5E	5U	6N	6L	6W	6P		
V	1Q	1T	4K	6O	6R	1G	2B	2X	2T	3M	3J	3E	3S	4S				
L	3X	4V	5J	6V	1E	1Y	1S	2I	2E	3T	4B	6M	6D	6T				
Y	1H	2V	3W	4Y	5X	6A	1J	1V	1U	3F	4X	5L	5K	5Z	6Z			
W	1U	4B	4H	6E	1Z	2S	5C	5T	6C									
U	1Y	1E	2N	4Q	4T	5G	5L	6Q	6W	1X	1M	2L	2K					
T	1X	1M	3S	3V	3Y	4C	4M	5B	5P	6F	6N	1H	2V	4G	4A	4O	4K	6B
H	2Y	4I	5V	6Z	4R	6R												
G	1G	1K	1N	2W	2K	3M	2J	3B	3U	5N	6I							
D	1R	2Z	5O	6D	6H	1F	2A	3Y	3I	4F	5W	5J	5I	6U	6J			
K	2D	2J	2L	3J	5I	6T	1B	1L	2C	2U	3P	4V	5B	5M				
E	6M	1I	2O	5Y	6Q	6G												
S	1A	1Z	1P	2S	3T	4Z	5Z	5C	5D	5U	6P	2G	3A	3Z	3O	3G	4L	4J	4P	6X
N	1I	2I	3O	4D	4L	4S	6C	6S	3L	3C	4U	4C						

Underlined type denotes wheels in reversed positions.

Table Q

B	1J	2J	3P	4E	4M	4T	6D	6T	3K	3B	4T	4B				
J	3A	3G	3M	5B	5O	5R	6K	1Q	1P	2Q	2L	3P	3M	4Y	5O	6E
M	1M	2C	3E	3Q	4K	5I	6C	1J	2Y	3Q	3G	4V	5W	6U		
A																
Q																
I	1C	2Q	3J	4S	4V	4C	1Z	2P	3V	5R	5P					
O	1E	2Y	2B	3D	4G	4Y	6Y	1O	1C	1V	3J	3W	4C	5N	5G	5E	5Z	6G
F	1G	1P	2R	2V	3R	5G	2C	3C	4P	4H	4X	6R	6Z	6J	6N			
P	1T	1X	1W	1D	2U	2F	4O	5S	5T	5Z	1N	4M	4D	5F	5U	6D		
C	2I	2H	3V	4X	4H	5X	6Z	5C										
X	1K	2S	3S	4F	5N	6M	1M	1S	2X	2V	4L	4G						
Z	3B	3C	4Q	6V	2O	2M	2E	4S	5Q									
R	2N	2P	2D	3F	3I	4P	6I	1B	3U	6X								
V	2G	3O	3H	3L	5U	5F	5L	6H	6L	2G	5D	5T	6M	6K	6V	6O		
L	1R	1U	4L	6P	6S	1F	2A	2W	2S	3L	3I	3D	3R	4R				
Y	3Y	4W	5K	6W	1D	1X	1R	2H	2D	3S	4A	6L	6C	6S				
W	1I	2W	3X	4Z	5Y	6B	1I	1U	1T	3E	4W	5K	5J	5Y	6Y			
U	1V	4C	4I	6F	1Y	2R	5B	5S	6B									
T	1Z	1F	2O	4R	4U	5H	5M	6R	6X	1W	1L	2K	2J					
H	1Y	1N	3T	3W	3Z	4D	4N	5C	5Q	6G	6O	1G	2U	4F	4Z	4N	4J	6A
G	2Z	4J	5W	6A	4Q	6Q												
D	1H	1L	1O	2X	2L	3N	2I	3A	3T	5M	6H							
K	1S	2A	5P	6E	6I	1E	2Z	3X	3H	4E	5V	5I	5H	6T	6I			
E	2E	2K	2M	3K	5J	6U	1A	1K	2B	2T	3O	4U	5A	5L				
S	6N	1H	2N	5X	6P	6F												
N	1B	1A	1Q	2T	3U	4A	5A	5D	5E	5V	6Q	2F	3Z	3Y	3N	3F	4K	4I	4O	6W

Underlined type denotes wheels in reversed positions.

TABLE I

B	1C	1B	1R	2U	3V	4B	5B	5E	5F	5W	6R	2E	3Y	3X	3M	3E	4J	4H	4N	6V
J	1K	2K	3Q	4F	4N	4U	6E	6U	3J	3A	4S	4A								
M	3B	3H	3N	5C	5P	5S	6L	1P	10	2P	2K	30	3L	4X	5N	6D				
A	1N	2D	3F	3R	4L	5J	6D	1I	2X	3P	3F	4U	5V	6T						
Q																				
I																				
O	1D	2R	3K	4T	4W	4D	1Y	20	3U	5Q	50									
F	1F	2Z	2C	3E	4H	4Z	6Z	1N	1B	1U	3I	3V	4B	5M	5F	5D	5Y	6F		
P	1H	1Q	2S	2W	3S	5H	2B	3B	40	4G	4W	6Q	6Y	6I	6M					
C	1U	1Y	1X	1E	2V	2G	4P	5T	5U	5A	1M	4L	4C	5E	5T	6C				
X	2J	2I	3W	4Y	4I	5Y	6A	5B												
Z	1L	2T	3T	4G	50	6N	1L	1R	2W	2U	4K	4F								
R	3C	3D	4R	6W	2N	2L	2D	4R	5P											
V	20	2Q	2E	3G	3J	4Q	6J	1A	3T	6W										
L	2H	3P	3I	3M	5V	5G	5M	6I	6M	2F	5C	5S	6L	6J	6U	6N				
Y	1S	1V	4M	6Q	6T	1E	2Z	2V	2R	3K	3H	3C	3Q	4Q						
W	3Z	4X	5L	6X	1C	1W	1Q	2G	2C	3R	4Z	6K	6B	6R						
U	1J	2X	3Y	4A	5Z	6C	1H	1T	1S	3D	4V	5J	5I	5X	6X					
T	1W	4D	4J	6G	1X	2Q	5A	5R	6A											
H	1A	1G	2P	4S	4V	5I	5N	6S	6Y	1V	1K	2J	2I							
G	1Z	10	3U	3X	3A	4E	40	5D	5R	6H	6P	1F	2T	4E	4Y	4M	4I	6Z		
D	2A	4K	5X	6B	4P	6P														
K	1I	1M	1P	2Y	2M	30	2H	3Z	3S	5L	6G									
E	1T	2B	5Q	6F	6J	1D	2Y	3W	3G	4D	5U	5H	5G	6S	6H					
S	2F	2L	2N	3L	5K	6V	1Z	1J	2A	2S	3N	4T	5Z	5K						
N	60	1G	2M	5W	60	6E														

Underlined type denotes wheels in reversed positions.

TABLE O

B	6P	1F	2L	5V	6N	6D													
J	1D	1C	1S	2V	3W	4C	5C	5F	5G	5X	6S	2D	3X	3W	3L	3D	4I	4G	4M	6U
M	1L	2L	3R	4G	40	4V	6F	6V	3I	3Z	4R	4Z								
A	3C	3I	30	5D	5Q	5T	6M	10	1N	20	2J	3N	3K	4W	5M	6C				
Q	10	2E	3G	3S	4M	5K	6E	1H	2W	30	3E	4T	5U	6S						
I																				
O																				
F	1E	2S	3L	4U	4X	4E	1X	2N	3T	5P	5N									
P	1G	2A	2D	3F	4I	4A	6A	1M	1A	1T	3H	3U	4A	5L	5E	5C	5X	6E		
C	1I	1R	2T	2X	3T	5I	2A	3A	4N	4F	4V	6P	6X	6H	6L					
X	1V	1Z	1Y	1F	2W	2H	4Q	5U	5V	5B	1L	4K	4B	5D	5S	6B				
Z	2K	2J	3X	4Z	4J	5Z	6B	5A												
R	1M	2U	3U	4H	5P	60	1K	1Q	2V	2T	4J	4E								
V	3D	3E	4S	6X	2M	2K	2C	4Q	5O											
L	2P	2R	2F	3H	3K	4R	6K	1Z	3S	6V										
Y	2I	3Q	3J	3N	5W	5H	5N	6J	6N	2E	5B	5R	6K	6I	6T	6M				
W	1T	1W	4N	6R	6U	1D	2Y	2U	2Q	3J	3G	3B	3P	4P						
U	3A	4Y	5M	6Y	1B	1V	1P	2F	2B	3Q	4Y	6J	6A	6Q						
T	1K	2Y	3Z	4B	5A	6D	1G	1S	1R	3C	4U	5I	5H	5W	6W					
H	1X	4E	4K	6H	1W	2P	5Z	5Q	6Z											
G	1B	1H	2Q	4T	4W	5J	50	6T	6Z	1U	1J	2I	2H							
D	1A	1P	3V	3Y	3B	4F	4P	5E	5S	6I	6Q	1E	2S	4D	4X	4L	4H	6Y		
K	2B	4L	5Y	6C	40	60														
E	1J	1N	1Q	2Z	2N	3P	2G	3Y	3R	5K	6F									
S	1U	2C	5R	6G	6K	1C	2X	3V	3F	4C	5T	5G	5F	6R	6G					
N	2G	2M	20	3M	5L	6W	1Y	1I	2Z	2R	3M	4S	5Y	5J						

Underlined type denotes wheels in reversed positions.

TABLE F

B	2H	2N	2P	3N	5M	6X	1X	1H	2Y	2Q	3L	4R	5X	5I
J	6Q	1E	2K	5U	6M	6C								
M	1E	1D	1T	2W	3X	4D	5D	5G	5H	5Y	6T	2C	3W	3V	3K	3C	4H	4F	4L	6T
A	1M	2M	3S	4H	4P	4W	6G	6W	3H	3Y	4Q	4Y								
Q	3D	3J	3P	5E	5R	5U	6N	1N	1M	2N	2I	3M	3J	4V	5L	6B				
I	1P	2F	3H	3T	4N	5L	6F	1G	2V	3N	3D	4S	5T	6R						
O																				
F																				
P	1F	2T	3M	4V	4Y	4F	1W	2M	3S	5O	5M									
C	1H	2B	2E	3G	4J	4B	6B	1L	1Z	1S	3G	3T	4Z	5K	5D	5B	5W	6D		
X	1J	1S	2U	2Y	3U	5J	2Z	3Z	4M	4E	4U	6O	6W	6G	6K					
Z	1W	1A	1Z	1G	2X	2I	4R	5V	5W	5C	1K	4J	4A	5C	5R	6A				
R	2L	2K	3Y	4A	4K	5A	6C	5Z												
V	1N	2V	3V	4I	5Q	6P	1J	1P	2U	2S	4I	4D								
L	3E	3F	4T	6Y	2L	2J	2B	4P	5N											
Y	2Q	2S	2G	3I	3L	4S	6L	1Y	3R	6U										
W	2J	3R	3K	30	5X	5I	50	6K	6O	2D	5A	5Q	6J	6H	6S	6L				
U	1U	1X	40	6S	6V	1C	2X	2T	2P	3I	3F	3A	30	40						
T	3B	4Z	5N	6Z	1A	1U	1O	2E	2A	3P	4X	6I	6Z	6P						
H	1L	2Z	3A	4C	5B	6E	1F	1R	1Q	3B	4T	5H	5G	5V	6V					
G	1Y	4F	4L	6I	1V	20	5Y	5P	6Y											
D	1C	1I	2R	4U	4X	5K	5P	6U	6A	1T	1I	2H	2G							
K	1B	1Q	3W	3Z	3C	4G	4Q	5F	5T	6J	6R	1D	2R	4C	4W	4K	4G	6X		
E	2C	4M	5Z	6D	4N	6N														
S	1K	10	1R	2A	20	3Q	2F	3X	3Q	5J	6E									
N	1V	2D	5S	6H	6L	1B	2W	3U	3E	4B	5S	5F	5E	6Q	6F					

Underlined type denotes wheels in reversed positions.

TABLE P

B	1W	2E	5T	6I	6M	1A	2V	3T	3D	4A	5R	5E	5D	6P	6E
J	2I	20	2Q	30	5N	6Y	1W	1G	2X	2P	3K	4Q	5W	5H	
M	6R	1D	2J	5T	6L	6B									
A	1F	1E	1U	2X	3Y	4E	5E	5H	5I	5Z	6U	2B	3V	3U	3J	3B	4G	4E	4K	6S
Q	1N	2N	3T	4I	4Q	4X	6H	6X	3G	3X	4P	4X								
I	3E	3K	3Q	5F	5S	5V	60	1M	1L	2M	2H	3L	3I	4U	5K	6A				
O	1Q	2G	3I	3U	40	5M	6G	1F	2U	3M	3C	4R	5S	6Q						
F																				
P																				
C	1G	2U	3N	4W	4Z	4G	1V	2L	3R	5N	5L									
X	1I	2C	2F	3H	4K	4C	6C	1K	1Y	1R	3F	3S	4Y	5J	5C	5A	5V	6C		
Z	1K	1T	2V	2Z	3V	5K	2Y	3Y	4L	4D	4T	6N	6V	6F	6J					
R	1X	1B	1A	1H	2Y	2J	4S	5W	5X	5D	1J	4I	4Z	5B	5Q	6Z				
V	2M	2L	3Z	4B	4L	5B	6D	5Y												
L	10	2W	3W	4J	5R	6Q	1I	10	2T	2R	4H	4C								
Y	3F	3G	4U	6Z	2K	2I	2A	40	5M											
W	2R	2T	2H	3J	3M	4T	6M	1X	3Q	6T										
U	2K	3S	3L	3P	5Y	5J	5P	6L	6P	2C	5Z	5P	6I	6G	6R	6K				
T	1V	1Y	4P	6T	6W	1B	2W	2S	20	3H	3E	3Z	3N	4N						
H	3C	4A	50	6A	1Z	1T	1N	2D	2Z	30	4W	6H	6Y	60						
G	1M	2A	3B	4D	5C	6F	1E	1Q	1P	3A	4S	5G	5F	5U	6U					
D	1Z	4G	4M	6J	1U	2N	5X	50	6X											
K	1D	1J	2S	4V	4Y	5L	5Q	6V	6B	1S	1H	2G	2F							
E	1C	1R	3X	3A	3D	4H	4R	5G	5U	6K	6S	1C	2Q	4B	4V	4J	4F	6W		
S	2D	4N	5A	6E	4M	6M														
N	1L	1P	1S	2B	2P	3R	2E	3W	3P	5I	6D									

Underlined type denotes wheels in reversed positions.

71836—35——8

Table C

B	1M	1Q	1T	2C	2Q	3S	2D	3V	3O	5H	6C											
J	1X	2F	5U	6J	6N	1Z	2U	3S	3C	4Z	5Q	5D	5C	6O	6D							
M	2J	2P	2R	3P	5O	6Z	1V	1F	2W	2O	3J	4P	5V	5G								
A	6S	1C	2I	5S	6K	6A																
Q	1G	1F	1V	2Y	3Z	4F	5F	5I	5J	5A	6V	2A	3U	3T	3I	3A	4F	4D	4J	6R		
I	1O	2O	3U	4J	4R	4Y	6I	6Y	3F	3W	4O	4W										
O	3F	3L	3R	5G	5T	5W	6P	1L	1K	2L	2G	3K	3H	4T	5J	6Z						
F	1R	2H	3J	3V	4P	5N	6H	1E	2T	3L	3B	4Q	5R	6P								
P																						
C																						
X	1H	2V	3O	4X	4A	4H	1U	2K	3Q	5M	5K											
Z	1J	2D	2G	3I	4L	4D	6D	1J	1X	1Q	3E	3R	4X	5I	5B	5Z	5U	6B				
R	1L	1U	2W	2A	3W	5L	2X	3X	4K	4C	4S	6M	6U	6E	6I							
V	1Y	1C	1B	1I	2Z	2K	4T	5X	5Y	5E	1I	4H	4Y	5A	5P	6Y						
L	2N	2M	3A	4C	4M	5C	6E	5X														
Y	1P	2X	3X	4K	5S	6R	1H	1N	2S	2Q	4G	4B										
W	3G	3H	4V	6A	2J	2H	2Z	4N	5L													
U	2S	2U	2I	3K	3N	4U	6N	1W	3P	6S												
T	2L	3T	3M	3Q	5Z	5K	5Q	6M	6Q	2B	5Y	5O	6H	6F	6Q	6J						
H	1W	1Z	4Q	6U	6X	1A	2V	2R	2N	3G	3D	3Y	3M	4M								
G	3D	4B	5P	6B	1Y	1S	1M	2C	2Y	3N	4V	6G	6X	6N								
D	1N	2B	3C	4E	5D	6G	1D	1P	1O	3Z	4R	5F	5E	5T	6T							
K	1A	4H	4N	6K	1T	2M	5W	5N	6W													
E	1E	1K	2T	4W	4Z	5M	5R	6W	6C	1R	1G	2F	2E									
S	1D	1S	3Y	3B	3E	4I	4S	5H	5V	6L	6T	1B	2P	4A	4U	4I	4E	6V				
N	2E	4O	5B	6F	4L	6L																

Underlined type denotes wheels in reversed positions.

Table X

B	2F	4P	5C	6G	4K	6K																
J	1N	1R	1U	2D	2R	3T	2C	3U	3N	5G	6B											
M	1Y	2G	5V	6K	6O	1Y	2T	3R	3B	4Y	5P	5C	5B	6N	6C							
A	2K	2Q	2S	3Q	5P	6A	1U	1E	2V	2N	3I	4O	5U	5F								
Q	6T	1B	2H	5R	6J	6Z																
I	1H	1G	1W	2Z	3A	4G	5G	5J	5K	5B	6W	2Z	3T	3S	3H	3Z	4E	4C	4I	6Q		
O	1P	2P	3V	4K	4S	4Z	6J	6Z	3E	3V	4N	4V										
F	3G	3M	3S	5H	5U	5X	6Q	1K	1J	2K	2F	3J	3G	4S	5I	6Y						
P	1S	2I	3K	3W	4Q	5O	6I	1D	2S	3K	3A	4P	5Q	6O								
C																						
X																						
Z	1I	2W	3P	4Y	4B	4I	1T	2J	3P	5L	5J											
R	1K	2E	2H	3J	4M	4E	6E	1I	1W	1P	3D	3Q	4W	5H	5A	5Y	5T	6A				
V	1M	1V	2X	2B	3X	5M	2W	3W	4J	4B	4R	6L	6T	6D	6H							
L	1Z	1D	1C	1J	2A	2L	4U	5Y	5Z	5F	1H	4G	4X	5Z	5O	6X						
Y	2O	2N	3B	4D	4N	5D	6F	5W														
W	1Q	2Y	3Y	4L	5T	6S	1G	1M	2R	2P	4F	4A										
U	3H	3I	4W	6B	2I	2G	2V	4M	5K													
T	2T	2V	2J	3L	3O	4V	6O	1V	3O	6R												
H	2M	3U	3N	3R	5A	5L	5R	6N	6R	2A	5X	5N	6G	6E	6P	6I						
G	1X	1A	4R	6V	6Y	1Z	2U	2Q	2M	3F	3C	3X	3L	4L								
D	3E	4C	5Q	6C	1X	1R	1L	2B	2X	3M	4U	6F	6W	6M								
K	1O	2C	3D	4F	5E	6H	1C	1O	1N	3V	4Q	5E	5D	5S	6S							
E	1B	4I	4O	6L	1S	2L	5V	5M	6V													
S	1F	1L	2U	4X	4A	5N	5S	6X	6D	1Q	1F	2E	2D									
N	1E	1T	3Z	3C	3F	4J	4T	5I	5W	6M	6U	1A	2O	4Z	4T	4H	4D	6U				

Underlined type denotes wheels in reversed positions.

Table Z

B	1F	1U	3A	3D	3G	4K	4U	5J	5X	6N	6V	1Z	2N	4Y	4S	4G	4C	6T
J	2G	4Q	5D	6H	4J	6J												
M	10	1S	1V	2E	2S	3U	2B	3T	3M	5F	6A							
A	1Z	2H	5W	6L	6P	1X	2S	3Q	3A	4X	5Q	5B	5A	6M	6B			
Q	2L	2R	2T	3R	5Q	6B	1T	1D	2U	2M	3H	4N	5T	5E				
I	6U	1A	2G	5Q	6I	6Y												
O	1I	1H	1X	2A	3B	4H	5H	5K	5L	5C	6X	2Y	3S	3R	3G	3Y	4D	4B	4H	6P
F	1Q	2Q	3W	4L	4T	4A	6K	6A	3D	3U	4M	4U						
P	3H	3N	3T	5I	5V	5Y	6R	1J	1I	2J	2E	3I	3F	4R	5H	6X		
C	1T	2J	3L	3X	4R	5P	6J	1C	2R	3J	3Z	40	5P	6N				
X																		
Z																		
R	1J	2X	3Q	4Z	4C	4J	1S	2I	30	5K	5I							
V	1L	2F	2I	3K	4N	4F	6F	1H	1V	10	3C	3P	4V	5G	5Z	5X	5S	6Z
L	1N	1W	2Y	2C	3Y	5N	2V	3V	4I	4A	4Q	6K	6S	6C	6G			
Y	1A	1E	1D	1K	2B	2M	4V	5Z	5A	5G	1G	4F	4W	5Y	5N	6W		
W	2P	20	3C	4E	40	5E	6G	5V										
U	1R	2Z	3Z	4M	5U	6T	1F	1L	2Q	20	4E	4Z						
T	3I	3J	4X	6C	2H	2F	2X	4L	5J									
H	2U	2W	2K	3M	3P	4W	6P	1U	3N	6Q								
G	2N	3V	30	3S	5B	5M	5S	60	6S	2Z	5W	5M	6F	6D	60	6H		
D	1Y	1B	4S	6W	6Z	1Y	2T	2P	2L	3E	3B	3W	3K	4K				
K	3F	4D	5R	6D	1W	1Q	1K	2A	2W	3L	4T	6E	6V	6L				
E	1P	2D	3E	4G	5F	6I	1B	1N	1M	3X	4P	5D	5C	5R	6R			
S	1C	4J	4P	6M	1R	2K	5U	5L	6U									
N	1G	1M	2V	4Y	4B	50	5T	6Y	6E	1P	1E	2D	2C					

Underlined type denotes wheels in reversed positions.

Table R

B	1H	1N	2W	4Z	4C	5P	5U	6Z	6F	10	1D	2C	2B					
J	1G	1V	3B	3E	3H	4L	4V	5K	5Y	60	6W	1Y	2M	4X	4R	4F	4B	6S
M	2H	4R	5E	6I	4I	6I												
A	1P	1T	1W	2F	2T	3V	2A	3S	3L	5E	6Z							
Q	1A	2I	5X	6M	6Q	1W	2R	3P	3Z	4W	5N	5A	5Z	6L	6A			
I	2M	2S	2U	3S	5R	6C	1S	1C	2T	2L	3G	4M	5S	5D				
O	6V	1Z	2F	5P	6H	6X												
F	1J	1I	1Y	2B	3C	4I	5I	5L	5M	5D	6Y	2X	3R	3Q	3F	3X	4C	4A	4G	60
P	1R	2R	3X	4M	4U	4B	6L	6B	3C	3T	4L	4T						
C	3I	30	3U	5J	5W	5Z	6S	1I	1H	2I	2D	3H	3E	4Q	5G	6W		
X	1U	2K	3M	3Y	4S	5Q	6K	1B	2Q	3I	3Y	4N	50	6M				
Z																		
R																		
V	1K	2Y	3R	4A	4D	4K	1R	2H	3N	5J	5H							
L	1M	2G	2J	3L	40	4G	6G	1G	1U	1N	3B	30	4U	5F	5Y	5W	5R	6Y
Y	10	1X	2Z	2D	3Z	50	2U	3U	4H	4Z	4P	6J	6R	6B	6F			
W	1B	1F	1E	1L	2C	2N	4W	5A	5B	5H	1F	4E	4V	5X	5M	6V		
U	2Q	2P	3D	4F	4P	5F	6H	5U										
T	1S	2A	3A	4N	5V	6U	1E	1K	2P	2N	4D	4Y						
H	3J	3K	4Y	6D	2G	2E	2W	4K	5I									
G	2V	2X	2L	3N	3Q	4X	6Q	1T	3M	6P								
D	20	3W	3P	3T	5C	5N	5T	6P	6T	2Y	5V	5L	6E	6C	6N	6G		
K	1Z	1C	4T	6X	6A	1X	2S	20	2K	3D	3A	3V	3J	4J				
E	3G	4E	5S	6E	1V	1P	1J	2Z	2V	3K	4S	6D	6U	6K				
S	1Q	2E	3F	4H	5G	6J	1A	1M	1L	3W	40	5C	5B	5Q	6Q			
N	1D	4K	4Q	6N	1Q	2J	5T	5K	6T									

Underlined type denotes wheels in reversed positions.

TABLE V

B	1E	4L	4R	60	1P	2I	5S	5J	6S															
J	1I	10	2X	4A	4D	5Q	5V	6A	6G	1N	1C	2B	2A											
M	1H	1W	3C	3F	3I	4M	4W	5L	5Z	6P	6X	1X	2L	4W	4Q	4E	4A	6R						
A	2I	4S	5F	6J	4H	6H																		
Q	1Q	1U	1X	2G	2U	3W	2Z	3R	3K	5D	6Y													
I	1B	2J	5Y	6N	6R	1V	2Q	30	3Y	4V	5M	5Z	5Y	6K	6Z									
O	2N	2T	2V	3T	5S	6D	1R	1B	2S	2K	3F	4L	5R	5C										
F	6W	1Y	2E	50	6G	6W																		
P	1K	1J	1Z	2C	3D	4J	5J	5M	5N	5E	6Z	2W	3Q	3P	3E	3W	4B	4Z	4F	6N				
C	1S	2S	3Y	4N	4V	4C	6M	6C	3B	3S	4K	4S												
X	3J	3P	3V	5K	5X	5A	6T	1H	1G	2H	2C	3G	3D	4P	5F	6V								
Z	1V	2L	3N	3Z	4T	5R	6L	1A	2P	3H	3X	4M	5N	6L										
R																								
V																								
L	1L	2Z	3S	4B	4E	4L	1Q	2G	3M	5I	5G													
Y	1N	2H	2K	3M	4P	4H	6H	1F	1T	1M	3A	3N	4T	5E	5X	5V	5Q	6X						
W	1P	1Y	2A	2E	3A	5P	2T	3T	4G	4Y	40	6I	6Q	6A	6E									
U	1C	1G	1F	1M	2D	20	4X	5B	5C	5I	1E	4D	4U	5W	5L	6U								
T	2R	2Q	3E	4G	4Q	5G	6I	5T																
H	1T	2B	3B	40	5W	6V	1D	1J	20	2M	4C	4X												
G	3K	3L	4Z	6E	2F	2D	2V	4J	5H															
D	2W	2Y	2M	30	3R	4Y	6R	1S	3L	60														
K	2P	3X	3Q	3U	5D	50	5U	6Q	6U	2X	5U	5K	6D	6B	6M	6F								
E	1A	1D	4U	6Y	6B	1W	2R	2N	2J	3C	3Z	3U	3I	4I										
S	3H	4F	5T	6F	1U	10	1I	2Y	2U	3J	4R	6C	6T	6J										
N	1R	2F	3G	4I	5H	6K	1Z	1L	1K	3V	4N	5B	5A	5P	6P									

Underlined type denotes wheels in reversed positions.

TABLE L

B	1S	2G	3H	4J	5I	6L	1Y	1K	1J	3U	4M	5A	5Z	50	60									
J	1F	4M	4S	6P	10	2H	5R	5I	6R															
M	1J	1P	2Y	4B	4E	5R	5W	6B	6H	1M	1B	2A	2Z											
A	1I	1X	3D	3G	3J	4N	4X	5M	5A	6Q	6Y	1W	2K	4V	4P	4D	4Z	6Q						
Q	2J	4T	5G	6K	4G	6G																		
I	1R	1V	1Y	2H	2V	3X	2Y	3Q	3J	5C	6X													
O	1C	2K	5Z	60	6S	1U	2P	3N	3X	4U	5L	5Y	5X	6J	6Y									
F	20	2U	2W	3U	5T	6E	1Q	1A	2R	2J	3E	4K	5Q	5B										
P	6X	1X	2D	5N	6F	6V																		
C	1L	1K	1A	2D	3E	4K	5K	5N	50	5F	6A	2V	3P	30	3D	3V	4A	4Y	4E	6M				
X	1T	2T	3Z	40	4W	4D	6N	6D	3A	3R	4J	4R												
Z	3K	3Q	3W	5L	5Y	5B	6U	1G	1F	2G	2B	3F	3C	40	5E	6U								
R	1W	2M	30	3A	4U	5S	6M	1Z	20	3G	3W	4L	5M	6K										
V																								
L																								
Y	1M	2A	3T	4C	4F	4M	1P	2F	3L	5H	5F													
W	10	2I	2L	3N	4Q	4I	6I	1E	1S	1L	3Z	3M	4S	5D	5W	5U	5P	6W						
U	1Q	1Z	2B	2F	3B	5Q	2S	3S	4F	4X	4N	6H	6P	6Z	6D									
T	1D	1H	1G	1N	2E	2P	4Y	5C	5D	5J	1D	4C	4T	5V	5K	6T								
H	2S	2R	3F	4H	4R	5H	6J	5S																
G	1U	2C	3C	4P	5X	6W	1C	1I	2N	2L	4B	4W												
D	3L	3M	4A	6F	2E	2C	2U	4I	5G															
K	2X	2Z	2N	3P	3S	4Z	6S	1R	3K	6N														
E	2Q	3Y	3R	3V	5E	5P	5V	6R	6V	2W	5T	5J	6C	6A	6L	6E								
S	1B	1E	4V	6Z	6C	1V	2Q	2M	2I	3B	3Y	3T	3H	4H										
N	3I	4G	5U	6G	1T	1N	1H	2X	2T	3I	4Q	6B	6S	6I										

Underlined type denotes wheels in reversed positions.

TABLE Y

B 3J 4H 5V 6H 1S 1M 1G 2W 2S 3H 4P 6A 6R 6H
J 1T 2H 3I 4K 5J 6M 1X 1J 1I 3T 4L 5Z 5Y 5N 6N
M 1G 4N 4T 6Q 1N 2G 5Q 5H 6Q
A 1K 1Q 2Z 4C 4F 5S 5X 6C 6I 1L 1A 2Z 2Y
Q 1J 1Y 3E 3H 3K 40 4Y 5N 5B 6R 6Z 1V 2J 4U 40 4C 4Y 6P
I 2K 4U 5H 6L 4F 6F
O 1S 1W 1Z 2I 2W 3Y 2X 3P 3I 5B 6W
F 1D 2L 5A 6P 6T 1T 20 3M 3W 4T 5K 5X 5W 6I 6X
P 2P 2V 2X 3V 5U 6F 1P 1Z 2Q 2I 3D 4J 5P 5A
C 6Y 1W 2C 5M 6E 6U
X 1M 1L 1B 2E 3F 4L 5L 50 5P 5G 6B 2U 30 3N 3C 3U 4Z 4X 4D 6L
Z 1U 2U 3A 4P 4X 4E 60 6E 3Z 3Q 4I 4Q
R 3L 3R 3X 5M 5Z 5C 6V 1F 1E 2F 2A 3E 3B 4N 5D 6T
V 1X 2N 3P 3B 4V 5T 6N 1Y 2N 3F 3V 4K 5L 6J
L
Y
W 1N 2B 3U 4D 4G 4N 10 2E 3K 5G 5E
U 1P 2J 2M 30 4R 4J 6J 1D 1R 1K 3Y 3L 4R 5C 5V 5T 50 6V
T 1R 1A 2C 2G 3C 5R 2R 3R 4E 4W 4M 6G 60 6Y 6C
H 1E 1I 1H 10 2F 2Q 4Z 5D 5E 5K 1C 4B 4S 5U 5J 6S
G 2T 2S 3G 4I 4S 5I 6K 5R
D 1V 2D 3D 4Q 5Y 6X 1B 1H 2M 2K 4A 4V
K 3M 3N 4B 6G 2D 2B 2T 4H 5F
E 2Y 2A 20 3Q 3T 4A 6T 1Q 3J 6M
S 2R 3Z 3S 3W 5F 5Q 5W 6S 6W 2V 5S 5I 6B 6Z 6K 6D
N 1C 1F 4W 6A 6D 1U 2P 2L 2H 3A 3X 3S 3G 4G

Underlined type denotes wheels in reversed positions.

TABLE W

B 1D 1G 4X 6B 6E 1T 20 2K 2G 3Z 3W 3R 3F 4F
J 3K 4I 5W 6I 1R 1L 1F 2V 2R 3G 40 6Z 6Q 6G
M 1U 2I 3J 4L 5K 6N 1W 1I 1H 3S 4K 5Y 5X 5M 6M
A 1H 40 4U 6R 1M 2F 5P 5G 6P
Q 1L 1R 2A 4D 4G 5T 5Y 6D 6J 1K 1Z 2Y 2X
I 1K 1Z 3F 3I 3L 4P 4Z 50 5C 6S 6A 1U 2I 4T 4N 4B 4X 60
O 2L 4V 5I 6M 4E 6E
F 1T 1X 1A 2J 2X 3Z 2W 30 3H 5A 6V
P 1E 2M 5B 6Q 6U 1S 2N 3L 3V 4S 5J 5W 5V 6H 6W
C 2Q 2W 2Y 3W 5V 6G 10 1Y 2P 2H 3C 4I 50 5Z
X 6Z 1V 2B 5L 6D 6T
Z 1N 1M 1C 2F 3G 4M 5M 5P 5Q 5H 6C 2T 3N 3M 3B 3T 4Y 4W 4C 6K
R 1V 2V 3B 4Q 4Y 4F 6P 6F 3Y 3P 4H 4P
V 3M 3S 3Y 5N 5A 5D 6W 1E 1D 2E 2Z 3D 3A 4M 5C 6S
L 1Y 20 3Q 3C 4W 5U 60 1X 2M 3E 3U 4J 5K 6I
Y
W
U 10 2C 3V 4E 4H 40 1N 2D 3J 5F 5D
T 1Q 2K 2N 3P 4S 4K 6K 1C 1Q 1J 3X 3K 4Q 5B 5U 5S 5N 6U
H 1S 1B 2D 2H 3D 5S 2Q 3Q 4D 4V 4L 6F 6N 6X 6B
G 1F 1J 1I 1P 2G 2R 4A 5E 5F 5L 1B 4A 4R 5T 5I 6R
D 2U 2T 3H 4J 4T 5J 6L 5Q
K 1W 2E 3E 4R 5Z 6Y 1A 1G 2L 2J 4Z 4U
E 3N 30 4C 6H 2C 2A 2S 4G 5E
S 2Z 2B 2P 3R 3U 4B 6U 1P 3I 6L
N 2S 3A 3T 3X 5G 5R 5X 6T 6X 2U 5R 5H 6A 6Y 6J 6C

Underlined type denotes wheels in reversed positions.

Table U

B	2T	3B	3U	3Y	5H	5S	5Y	6U	6Y	2T	5Q	5G	6Z	6X	6I	6B
J	1E	1H	4Y	6C	6F	1S	2N	2J	2F	3Y	3V	3Q	3E	4E		
M	3L	4J	5X	6J	1Q	1K	1E	2U	2Q	3F	4N	6Y	6P	6F		
A	1V	2J	3K	4M	5L	6O	1V	1H	1G	3R	4J	5X	5W	5L	6L	
Q	1I	4P	4V	6S	1L	2E	5O	5F	6O							
I	1M	1S	2B	4E	4H	5U	5Z	6E	6K	1J	1Y	2X	2W			
O	1L	1A	3G	3J	3M	4Q	4A	5P	5D	6T	6B	1T	2H	4S	4M	4A	4W	6N
F	2M	4W	5J	6N	4D	6D										
P	1U	1Y	1B	2K	2Y	3A	2V	3N	3G	5Z	6U					
C	1F	2N	5C	6R	6V	1R	2M	3K	3U	4R	5I	5V	5U	6G	6V	
X	2R	2X	2Z	3X	5W	6H	1N	1X	2O	2G	3B	4H	5N	5Y		
Z	6A	1U	2A	5K	6C	6S										
R	1O	1N	1D	2G	3H	4N	5N	5Q	5R	5I	6D	2S	3M	3L	3A	3S	4X	4V	4B	6J
V	1W	2W	3C	4R	4Z	4G	6Q	6G	3X	3O	4G	4O								
L	3N	3T	3Z	5O	5B	5E	6X	1D	1C	2D	2Y	3C	3Z	4L	5B	6R				
Y	1Z	2P	3R	3D	4X	5V	6P	1W	2L	3D	3T	4I	5J	6H						
W																				
U																				
T	1P	2D	3W	4F	4I	4P	1M	2C	3I	5E	5C									
H	1R	2L	2O	3Q	4T	4L	6L	1B	1P	1I	3W	3J	4P	5A	5T	5R	5M	6T		
G	1T	1C	2E	2I	3E	5T	2P	3P	4C	4U	4K	6E	6M	6W	6A					
D	1G	1K	1J	1Q	2H	2S	4B	5F	5G	5M	1A	4Z	4Q	5S	5H	6Q				
K	2V	2U	3I	4K	4U	5K	6M	5P												
E	1X	2F	3F	4S	5A	6Z	1Z	1F	2K	2I	4Y	4T								
S	3O	3P	4D	6I	2B	2Z	2R	4F	5D											
N	2A	2C	2Q	3S	3V	4C	6V	1O	3H	6K										

Underlined type denotes wheels in reversed positions.

Table T

B	2B	2D	2R	3T	3W	4D	6W	1N	3G	6J						
J	2U	3C	3V	3Z	5I	5T	5Z	6V	6Z	2S	5P	5F	6Y	6W	6H	6A
M	1F	1I	4Z	6D	6G	1R	2M	2I	2E	3X	3U	3P	3D	4D		
A	3M	4K	5Y	6K	1P	1J	1D	2T	2P	3E	4M	6X	6O	6E		
Q	1W	2K	3L	4N	5M	6P	1U	1G	1F	3Q	4I	5W	5V	5K	6K	
I	1J	4Q	4W	6T	1K	2D	5N	5E	6N							
O	1N	1T	2C	4F	4I	5V	5A	6F	6L	1I	1X	2W	2V			
F	1M	1B	3H	3K	3N	4R	4B	5Q	5E	6U	6C	1S	2G	4R	4L	4Z	4V	6M
P	2N	4X	5K	6O	4C	6C										
C	1V	1Z	1C	2L	2Z	3B	2U	3M	3F	5Y	6T					
X	1G	2O	5D	6S	6W	1Q	2L	3J	3T	4Q	5H	5U	5T	6F	6U	
Z	2S	2Y	2A	3Y	5X	6I	1M	1W	2N	2F	3A	4G	5M	5X		
R	6B	1T	2Z	5J	6B	6R										
V	1P	1O	1E	2H	3I	4O	5O	5R	5S	5J	6E	2R	3L	3K	3Z	3R	4W	4U	4A	6I
L	1X	2X	3D	4S	4A	4H	6R	6H	3W	3N	4F	4N								
Y	3O	3U	3A	5P	5C	5F	6Y	1C	1B	2C	2X	3B	3Y	4K	5A	6Q				
W	1A	2Q	3S	3E	4Y	5W	6Q	1V	2K	3C	3S	4H	5I	6G						
U																				
T																				
H	1Q	2E	3X	4G	4J	4Q	1L	2B	3H	5D	5B									
G	1S	2M	2P	3R	4U	4M	6M	1A	1O	1H	3V	3I	4O	5Z	5S	5Q	5L	6S		
D	1U	1D	2F	2J	3F	5U	2O	3O	4B	4T	4J	6D	6L	6V	6Z					
K	1H	1L	1K	1R	2I	2T	4C	5G	5H	5N	1Z	4Y	4P	5R	5G	6P				
E	2W	2V	3J	4L	4V	5L	6N	5O												
S	1Y	2G	3G	4T	5B	6A	1Y	1E	2J	2H	4X	4S								
N	3P	3Q	4E	6J	2A	2Y	2Q	4E	5C											

Underlined type denotes wheels in reversed positions.

TABLE H

B	3Q 3R 4F 6K <u>2Z</u> <u>2X</u> <u>2P</u> <u>4D</u> <u>5B</u>
J	2C 2E 2S 3U 3X 4E 6X <u>1M</u> <u>3F</u> <u>6I</u>
M	2V 3D 3W 3A 5J 5U 5A 6W 6A <u>2R</u> <u>50</u> <u>5E</u> <u>6X</u> <u>6V</u> <u>6G</u> <u>6Z</u>
A	1G 1J 4A 6E 6H <u>1Q</u> <u>2L</u> <u>2H</u> <u>2D</u> <u>3W</u> <u>3T</u> <u>30</u> <u>3C</u> <u>4C</u>
Q	3N 4L 5Z 6L <u>10</u> <u>1I</u> <u>1C</u> <u>2S</u> <u>20</u> <u>3D</u> <u>4L</u> <u>6W</u> <u>6N</u> <u>6D</u>
I	1X 2L 3M 40 5N 6Q <u>1T</u> <u>1F</u> <u>1E</u> <u>3P</u> <u>4H</u> <u>5V</u> <u>5U</u> <u>5J</u> <u>6J</u>
O	1K 4R 4X 6U <u>1J</u> <u>2C</u> <u>5M</u> <u>5D</u> <u>6M</u>
F	10 1U 2D 4G 4J 5W 5B 6G 6M <u>1H</u> <u>1W</u> <u>2V</u> <u>2U</u>
P	1N 1C 3I 3L 30 4S 4C 5R 5F 6V 6D <u>1R</u> <u>2F</u> <u>4Q</u> <u>4K</u> <u>4Y</u> <u>4U</u> <u>6L</u>
C	20 4Y 5L 6P <u>4B</u> <u>6B</u>
X	1W 1A 1D 2M 2A 3C <u>2T</u> <u>3L</u> <u>3E</u> <u>5X</u> <u>6S</u>
Z	1H 2P 5E 6T 6X <u>1P</u> <u>2K</u> <u>3I</u> <u>3S</u> <u>4P</u> <u>5G</u> <u>5T</u> <u>5S</u> <u>6E</u> <u>6T</u>
R	2T 2Z 2B 3Z 5Y 6J <u>1L</u> <u>1V</u> <u>2M</u> <u>2E</u> <u>3Z</u> <u>4F</u> <u>5L</u> <u>5W</u>
V	6C <u>1S</u> <u>2Y</u> <u>5I</u> <u>6A</u> <u>6Q</u>
L	1Q 1P 1F 2I 3J 4P 5P 5S 5T 5K 6F <u>2Q</u> <u>3K</u> <u>3J</u> <u>3Y</u> <u>3Q</u> <u>4V</u> <u>4T</u> <u>4Z</u> <u>6H</u>
Y	1Y 2Y 3E 4T 4B 4I 6S 6I <u>3V</u> <u>3M</u> <u>4E</u> <u>4M</u>
W	3P 3V 3B 5Q 5D 5G 6Z <u>1B</u> <u>1A</u> <u>2B</u> <u>2W</u> <u>3A</u> <u>3X</u> <u>4J</u> <u>5Z</u> <u>6P</u>
U	1B 2R 3T 3F 4Z 5X 6R <u>1U</u> <u>2J</u> <u>3B</u> <u>3R</u> <u>4G</u> <u>5H</u> <u>6F</u>
T	
H	
G	1R 2F 3Y 4H 4K 4R <u>1K</u> <u>2A</u> <u>3G</u> <u>5C</u> <u>5A</u>
D	1T 2N 2Q 3S 4V 4N 6N <u>1Z</u> <u>1N</u> <u>1G</u> <u>3U</u> <u>3H</u> <u>4N</u> <u>5Y</u> <u>5R</u> <u>5P</u> <u>5K</u> <u>6R</u>
K	1V 1E 2G 2K 3G 5V <u>2N</u> <u>3N</u> <u>4A</u> <u>4S</u> <u>4I</u> <u>6C</u> <u>6K</u> <u>6U</u> <u>6Y</u>
E	1I 1M 1L 1S 2J 2U 4D 5H 5I 50 <u>1Y</u> <u>4X</u> <u>40</u> <u>5Q</u> <u>5F</u> <u>60</u>
S	2X 2W 3K 4M 4W 5M 60 <u>5N</u>
N	1Z 2H 3H 4U 5C 6B <u>1X</u> <u>1D</u> <u>2I</u> <u>2G</u> <u>4W</u> <u>4R</u>

Underlined type denotes wheels in reversed positions.

TABLE G

B	1A 2I 3I 4V 5D 6C <u>1W</u> <u>1C</u> <u>2H</u> <u>2F</u> <u>4V</u> <u>4Q</u>
J	3R 3S 4G 6L <u>2Y</u> <u>2W</u> <u>20</u> <u>4C</u> <u>5A</u>
M	2D 2F 2T 3V 3Y 4F 6Y <u>1L</u> <u>3E</u> <u>6H</u>
A	2W 3E 3X 3B 5K 5V 5B 6X 6B <u>2Q</u> <u>5N</u> <u>5D</u> <u>6W</u> <u>6U</u> <u>6F</u> <u>6Y</u>
Q	1H 1K 4B 6F 6I <u>1P</u> <u>2K</u> <u>2G</u> <u>2C</u> <u>3V</u> <u>3S</u> <u>3N</u> <u>3B</u> <u>4B</u>
I	30 4M 5A 6M <u>1N</u> <u>1H</u> <u>1B</u> <u>2R</u> <u>2N</u> <u>3C</u> <u>4K</u> <u>6V</u> <u>6M</u> <u>6C</u>
O	1Y 2M 3N 4P 50 6R <u>1S</u> <u>1E</u> <u>1D</u> <u>30</u> <u>4G</u> <u>5U</u> <u>5T</u> <u>5I</u> <u>6I</u>
F	1L 4S 4Y 6V <u>1I</u> <u>2B</u> <u>5L</u> <u>5C</u> <u>6L</u>
P	1P 1V 2E 4H 4K 5X 5C 6H 6N <u>1G</u> <u>1V</u> <u>2U</u> <u>2T</u>
C	10 1D 3J 3M 3P 4T 4D 5S 5G 6W 6E <u>1Q</u> <u>2E</u> <u>4P</u> <u>4J</u> <u>4X</u> <u>4T</u> <u>6K</u>
X	2P 4Z 5M 6Q <u>4A</u> <u>6A</u>
Z	1X 1B 1E 2N 2B 3D <u>2S</u> <u>3K</u> <u>3D</u> <u>5W</u> <u>6R</u>
R	1I 2Q 5F 6U 6Y <u>10</u> <u>2J</u> <u>3H</u> <u>3R</u> <u>40</u> <u>5F</u> <u>5S</u> <u>5R</u> <u>6D</u> <u>6S</u>
V	2U 2A 2C 3A 5Z 6K <u>1K</u> <u>1U</u> <u>2L</u> <u>2D</u> <u>3Y</u> <u>4E</u> <u>5K</u> <u>5V</u>
L	6D <u>1R</u> <u>2X</u> <u>5H</u> <u>6Z</u> <u>6P</u>
Y	1R 1Q 1G 2J 3K 4Q 5Q 5T 5U 5L 6G <u>2P</u> <u>3J</u> <u>3I</u> <u>3X</u> <u>3P</u> <u>4U</u> <u>4S</u> <u>4Y</u> <u>6G</u>
W	1Z 2Z 3F 4U 4C 4J 6T 6J <u>3U</u> <u>3L</u> <u>4D</u> <u>4L</u>
U	3Q 3W 3C 5R 5E 5H 6A <u>1A</u> <u>1Z</u> <u>2A</u> <u>2V</u> <u>3Z</u> <u>3W</u> <u>4I</u> <u>5Y</u> <u>60</u>
T	1C 2S 3U 3G 4A 5Y 6S <u>1T</u> <u>2I</u> <u>3A</u> <u>3Q</u> <u>4F</u> <u>5G</u> <u>6E</u>
H	
G	
D	1S 2G 3Z 4I 4L 4S <u>1J</u> <u>2Z</u> <u>3F</u> <u>5B</u> <u>5Z</u>
K	1U 20 2R 3T 4W 40 60 <u>1Y</u> <u>1M</u> <u>1F</u> <u>3T</u> <u>3G</u> <u>4M</u> <u>5X</u> <u>5Q</u> <u>50</u> <u>5J</u> <u>6Q</u>
E	1W 1F 2H 2L 3H 5W <u>2M</u> <u>3M</u> <u>4Z</u> <u>4R</u> <u>4H</u> <u>6B</u> <u>6J</u> <u>6T</u> <u>6X</u>
S	1J 1N 1M 1T 2K 2V 4E 5I 5J 5P <u>1X</u> <u>4W</u> <u>4N</u> <u>5P</u> <u>5E</u> <u>6N</u>
N	2Y 2X 3L 4N 4X 5N 6P <u>5M</u>

Underlined type denotes wheels in reversed positions.

TABLE D

B	2Z 2Y 3M 40 4Y 50 6Q 5L
J	1B 2J 3J 4W 5E 6D 1V 1B 2G 2E 4U 4P
M	3S 3T 4H 6M 2X 2V 2N 4B 5Z
A	2E 2G 2U 3W 3Z 4G 6Z 1K 3D 6G
Q	2X 3F 3Y 3C 5L 5W 5C 6Y 6C 2P 5M 5C 6V 6T 6E 6X
I	1I 1L 4C 6G 6J 10 2J 2F 2B 3U 3R 3M 3A 4A
O	3P 4N 5B 6N 1M 1G 1A 2Q 2M 3B 4J 6U 6L 6B
F	1Z 2N 30 4Q 5P 6S 1R 1D 1C 3N 4F 5T 5S 5H 6H
P	1M 4T 4Z 6W 1H 2A 5K 5B 6K
C	1Q 1W 2F 4I 4L 5Y 5D 6I 60 1F 1U 2T 2S
X	1P 1E 3K 3N 3Q 4U 4E 5T 5H 6X 6F 1P 2D 40 4I 4W 4S 6J
Z	2Q 4A 5N 6R 4Z 6Z
R	1Y 1C 1F 20 2C 3E 2R 3J 3C 5V 6Q
V	1J 2R 5G 6V 6Z 1N 2I 3G 3Q 4N 5E 5R 5Q 6C 6R
L	2V 2B 2D 3B 5A 6L 1J 1T 2K 2C 3X 4D 5J 5U
Y	6E 1Q 2W 5G 6Y 60
W	1S 1R 1H 2K 3L 4R 5R 5U 5V 5M 6H 20 3I 3H 3W 30 4T 4R 4X 6F
U	1A 2A 3G 4V 4D 4K 6U 6K 3T 3K 4C 4K
T	3R 3X 3D 5S 5F 5I 6B 1Z 1Y 2Z 2U 3Y 3V 4H 5X 6N
H	1D 2T 3V 3H 4B 5Z 6T 1S 2H 3Z 3P 4E 5F 6D
G	
D	
K	1T 2H 3A 4J 4M 4T 1I 2Y 3E 5A 5Y
E	1V 2P 2S 3U 4X 4P 6P 1X 1L 1E 3S 3F 4L 5W 5P 5N 5I 6P
S	1X 1G 2I 2M 3I 5X 2L 3L 4Y 4Q 4G 6A 6I 6S 6W
N	1K 10 1N 1U 2L 2W 4F 5J 5K 5Q 1W 4V 4M 50 5D 6M

Underlined type denotes wheels in reversed positions.

TABLE K

B	1L 1P 10 1V 2M 2X 4G 5K 5L 5R 1V 4U 4L 5N 5C 6L
J	2A 2Z 3N 4P 4Z 5P 6R 5K
M	1C 2K 3K 4X 5F 6E 1U 1A 2F 2D 4T 40
A	3T 3U 4I 6N 2W 2U 2M 4A 5Y
Q	2F 2H 2V 3X 3A 4H 6A 1J 3C 6F
I	2Y 3G 3Z 3D 5M 5X 5D 6Z 6D 20 5L 5B 6U 6S 6D 6W
O	1J 1M 4D 6H 6K 1N 2I 2E 2A 3T 3Q 3L 3Z 4Z
F	3Q 40 5C 60 1L 1F 1Z 2P 2L 3A 4I 6T 6K 6A
P	1A 20 3P 4R 5Q 6T 1Q 1C 1B 3M 4E 5S 5R 5G 6G
C	1N 4U 4A 6X 1G 2Z 5J 5A 6J
X	1R 1X 2G 4J 4M 5Z 5E 6J 6P 1E 1T 2S 2R
Z	1Q 1F 3L 30 3R 4V 4F 5U 5I 6Y 6G 10 2C 4N 4H 4V 4R 6I
R	2R 4B 50 6S 4Y 6Y
V	1Z 1D 1G 2P 2D 3F 2Q 3I 3B 5U 6P
L	1K 2S 5H 6W 6A 1M 2H 3F 3P 4M 5D 5Q 5P 6B 6Q
Y	2W 2C 2E 3C 5B 6M 1I 1S 2J 2B 3W 4C 5I 5T
W	6F 1P 2V 5F 6X 6N
U	1T 1S 1I 2L 3M 4S 5S 5V 5W 5N 6I 2N 3H 3G 3V 3N 4S 4Q 4W 6E
T	1B 2B 3H 4W 4E 4L 6V 6L 3S 3J 4B 4J
H	3S 3Y 3E 5T 5G 5J 6C 1Y 1X 2Y 2T 3X 3U 4G 5W 6M
G	1E 2U 3W 3I 4C 5A 6U 1R 2G 3Y 30 4D 5E 6C
D	
K	
E	1U 2I 3B 4K 4N 4U 1H 2X 3D 5Z 5X
S	1W 2Q 2T 3V 4Y 4Q 6Q 1W 1K 1D 3R 3E 4K 5V 50 5M 5H 60
N	1Y 1H 2J 2N 3J 5Y 2K 3K 4X 4P 4F 6Z 6H 6R 6V

Underlined type denotes wheels in reversed positions.

TABLE E

B	1Z	1I	2K	20	3K	5Z	2J	3J	4W	40	4E	6Y	6G	6Q	6U					
J	1M	1Q	1P	1W	2N	2Y	4H	5L	5M	5S	1U	4T	4K	5M	5B	6K				
M	2B	2A	30	4Q	4A	5Q	6S	5J												
A	1D	2L	3L	4Y	5G	6F	1T	1Z	2E	2C	4S	4N								
Q	3U	3V	4J	60	2V	2T	2L	4Z	5X											
I	2G	2I	2W	3Y	3B	4I	6B	1I	3B	6E										
O	2Z	3H	3A	3E	5N	5Y	5E	6A	6E	2N	5K	5A	6T	6R	6C	6V				
F	1K	1N	4E	6I	6L	1M	2H	2D	2Z	3S	3P	3K	3Y	4Y						
P	3R	4P	5D	6P	1K	1E	1Y	20	2K	3Z	4H	6S	6J	6Z						
C	1B	2P	3Q	4S	5R	6U	1P	1B	1A	3L	4D	5R	5Q	5F	6F					
X	10	4V	4B	6Y	1F	2Y	5I	5Z	6I											
Z	1S	1Y	2H	4K	4N	5A	5F	6K	6Q	1D	1S	2R	2Q							
R	1R	1G	3M	3P	3S	4W	4G	5V	5J	6Z	6H	1N	2B	4M	4G	4U	4Q	6H		
V	2S	4C	5P	6T	4X	6X														
L	1A	1E	1H	2Q	2E	3G	2P	3H	3A	5T	60									
Y	1L	2T	5I	6X	6B	1L	2G	3E	30	4L	5C	5P	50	6A	6P					
W	2X	2D	2F	3D	5C	6N	1H	1R	2I	2A	3V	4B	5H	5S						
U	6G	10	2U	5E	6W	6M														
T	1U	1T	1J	2M	3N	4T	5T	5W	5X	50	6J	2M	3G	3F	3U	3M	4R	4P	4V	6D
H	1C	2C	3I	4X	4F	4M	6W	6M	3R	3I	4A	4I								
G	3T	3Z	3F	5U	5H	5K	6D	1X	1W	2X	2S	3W	3T	4F	5V	6L				
D	1F	2V	3X	3J	4D	5B	6V	1Q	2F	3X	3N	4C	5D	6B						
K																				
E																				
S	1V	2J	3C	4L	40	4V	1G	2W	3C	5Y	5W									
N	1X	2R	2U	3W	4Z	4R	6R	1V	1J	1C	3Q	3D	4J	5U	5N	5L	5G	6N		

Underlined type denotes wheels in reversed positions.

TABLE S

B	1Y	2S	2V	3X	4A	4S	6S	1U	1I	1B	3P	3C	4I	5T	5M	5K	5F	6M		
J	1A	1J	2L	2P	3L	5A	2I	3I	4V	4N	4D	6X	6F	6P	6T					
M	1N	1R	1Q	1X	20	2Z	4I	5M	5N	5T	1T	4S	4J	5L	5A	6J				
A	2C	2B	3P	4R	4B	5R	6T	5I												
Q	1E	2M	3M	4Z	5H	6G	1S	1Y	2D	2B	4R	4M								
I	3V	3W	4K	6P	2U	2S	2K	4Y	5W											
O	2H	2J	2X	3Z	3C	4J	6C	1H	3A	6D										
F	2A	3I	3B	3F	50	5Z	5F	6B	6F	2M	5J	5Z	6S	6Q	6B	6U				
P	1L	10	4F	6J	6M	1L	2G	2C	2Y	3R	30	3J	3X	4X						
C	3S	4Q	5E	6Q	1J	1D	1X	2N	2J	3Y	4G	6R	6I	6Y						
X	1C	2Q	3R	4T	5S	6V	10	1A	1Z	3K	4C	5Q	5P	5E	6E					
Z	1P	4W	4C	6Z	1E	2X	5H	5Y	6H											
R	1T	1Z	2I	4L	40	5B	5G	6L	6R	1C	1R	2Q	2P							
V	1S	1H	3N	3Q	3T	4X	4H	5W	5K	6A	6I	1M	2A	4L	4F	4T	4P	6G		
L	2T	4D	5Q	6U	4W	6W														
Y	1B	1F	1I	2R	2F	3H	20	3G	3Z	5S	6N									
W	1M	2U	5J	6Y	6C	1K	2F	3D	3N	4K	5B	50	5N	6Z	60					
U	2Y	2E	2G	3E	5D	60	1G	1Q	2H	2Z	3U	4A	5G	5R						
T	6H	1N	2T	5D	6V	6L														
H	1V	1U	1K	2N	30	4U	5U	5X	5Y	5P	6K	2L	3F	3E	3T	3L	4Q	40	4U	6C
G	1D	2D	3J	4Y	4G	4N	6X	6N	3Q	3H	4Z	4H								
D	3U	3A	3G	5V	5I	5L	6E	1W	1V	2W	2R	3V	3S	4E	5U	6K				
K	1G	2W	3Y	3K	4E	5C	6W	1P	2E	3W	3M	4B	5C	6A						
E																				
S																				
N	1W	2K	3D	4M	4P	4W	1F	2V	3B	5X	5V									

Underlined type denotes wheels in reversed positions.

TABLE N

B	1X	2L	3E	4N	4Q	4X	1E	2U	3A	5W	5U
J	1Z	2T	2W	3Y	4B	4T	6T	1T	1H	1A	30	3B	4H	5S	5L	5J	5E	6L
M	1B	1K	2M	2Q	3M	5B	2H	3H	4U	4M	4C	6W	6E	60	6S			
A	10	1S	1R	1Y	2P	2A	4J	5N	50	5U	1S	4R	4I	5K	5Z	6I		
Q	2D	2C	3Q	4S	4C	5S	6U	5H										
I	1F	2N	3N	4A	5I	6H	1R	1X	2C	2A	4Q	4L						
O	3W	3X	4L	6Q	2T	2R	2J	4X	5V									
F	2I	2K	2Y	3A	3D	4K	6D	1G	3Z	6C								
P	2B	3J	3C	3G	5P	5A	5G	6C	6G	2L	5I	5Y	6R	6P	6A	6T		
C	1M	1P	4G	6K	6N	1K	2F	2B	2X	3Q	3N	3I	3W	4W				
X	3T	4R	5F	6R	1I	1C	1W	2M	2I	3X	4F	6Q	6H	6X				
Z	1D	2R	3S	4U	5T	6W	1N	1Z	1Y	3J	4B	5P	50	5D	6D			
R	1Q	4X	4D	6A	1D	2W	5G	5X	6G									
V	1U	1A	2J	4M	4P	5C	5H	6M	6S	1B	1Q	2P	20					
L	1T	1I	30	3R	3U	4Y	4I	5X	5L	6B	6J	1L	2Z	4K	4E	4S	40	6F
Y	2U	4E	5R	6V	4V	6V												
W	1C	1G	1J	2S	2G	3I	2N	3F	3Y	5R	6M							
U	1N	2V	5K	6Z	6D	1J	2E	3C	3M	4J	5A	5N	5M	6Y	6N			
T	2Z	2F	2H	3F	5E	6P	1F	1P	2G	2Y	3T	4Z	5F	5Q				
H	6I	1M	2S	5C	6U	6K												
G	1W	1V	1L	20	3P	4V	5V	5Y	5Z	5Q	6L	2K	3E	3D	3S	3K	4P	4N	4T	6B
D	1E	2E	3K	4Z	4H	40	6Y	60	3P	3G	4Y	4G						
K	3V	3B	3H	5W	5J	5M	6F	1V	1U	2V	2Q	3U	3R	4D	5T	6J		
E	1H	2X	3Z	3L	4F	5D	6X	10	2D	3V	3L	4A	5B	6Z				
S																		
N																		

Underlined type denotes wheels in reversed positions.

APPENDIX VI

SUMMARY OF RESULTS

By using the values derived from a study of the "V" and "Z" messages it was possible to find messages in which three values of the indicator were known—the first, second, and fifth letters. A little experimentation soon yielded the value of the remaining two indicator letters and also values for the "dog setting" square.

The lines d and r indicate which letters correspond to direct and reversed setting, respectively, of the wheels.

Figure 1 gives the dog setting corresponding to the various combinations of the first two wheels. There are no values entered in row 5 or in column 5 because in the messages submitted wheel 5 was not used.

Figure 2 gives the plain-text equivalents for the enciphered indicators.

Figure 3 gives the complete settings of those cipher messages which were read. No attempt was made to read any further messages since it appeared that a complete solution would be a matter of time only.

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

	1	2	3	4	5	6
1				BCZ		CDV
2	ABY		BDV	BDZ		ACZ
3	BCZ	ADW		BEX		ADW
4		CDV				AEX
5						
6	ACZ		BDV	CEV		

FIGURE 1

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

FIGURE 2

Enciphered Indicator	Deciphered Indicator	Message No.	Enciphered Indicator	Deciphered Indicator	Message No.
ZRZPP	YALPB (61342)	(156)	SCRLT	GOJCK (26314)	(218)
VDLSU	HKXJA (24631)	(162)	DRTUV	FANEH (31624)	(252)
MRLDO	DAXUC (31642)	(179)	NNBQU	NQAIA (46132)	(253)
BSKVF	VVCDZ (34126)	(186)	DDJQP	FKDIH (26143)	(229)
LPDUU	CFTEA (24631)	(189)	QRPCP	JAOMB (31642)	(206)
SSSVJ	GVHDE (36412)	(196)	PSYLV	ZVQCH (64213)	(177)
VGBKL	HIAWQ (23164)	(210)	RNTLE	IQNCO (26314)	(165)

FIGURE 3

O