According to information from Capt. Middleton

This brochure was written by Miss Wilson. It apparently attempts to set forth the principles upon which these codes were solved, as though this had actually been the case. But the fact is that a copy of two Spanish codes was furnished M.I.D. by the British, and the translation and relationship between the various versions of the basic codes was worked out from them. Mendelsohn did not and could not explain why the true facts were suppressed in this brochure.

W.F. Friedman
1/15/22

Note: The brochure also makes the problem look a good deal more complex than it really is.

TABLE OF CONTENTS

TABLE OF CONTENTS

SPANISH CODES

On August 24, 1918, the photostat of a Spanish code book was received from Panama. This code book (called for convenience code "Y") begins with 2921 (A) and follows in alphabetical sequence throughout. The numerical sequence breaks after code group 7040, "nom", and begins over with 0001 as "nombr-ar-amiento-e-s." The final number in the book is 2920 (blank). Numerous blank spaces occur before the beginning of each letter and 2386-2920 inclusive is entirely blank. Each page has two columns of forty numbers each, with the numbers at the right of the meanings. Changes in encipherment have evidently been made by pasting new strips of numbers over the old ones as can be most clearly seen on pages 12, 30, 34 and 52, where the strips are imperfectly pasted and show portions of numbers beneath. The book is marked plainly in ink on the first page as follows:

> "Cifra 74 para la Correspondencia reservada entre
> El Consulado de Espana en Panama y El Ministro de
> Estado y la Legacion en Washington"

The telegrams previously received between Panama and the Spanish Foreign Office in Madrid were decoded successfully from this book with the exception of the following groups which were either beyond 7040 or fell on blanks in the book: 8345, 0827 and 8370. The occurrence in the telegrams of two groups above 7040 seemed to indicate that there was in existence either a supplement or a revision of the book, possibly its enlargement to 10,000 groups. No indication appeared of the method used in transmitting telegrams other than those to and from Panama except the following extract from page 81:

Signos Convencionales

anulacion de la cifra anterior	2310
aumentante de unidad	2311
disminuyente de unidad	2312
inversion de guarismos	2313
supresion del primer numero	2314
supresion del ultimo numero	2315

We had on hand a large amount of unsolved material in the Spanish number code and made the assumption that a part at least of these messages could be read by the new book, especially such codes as were used between various points of secondary importance. This theory was based upon the hypothesis that the Spanish consular system did not employ more than one basic book and seemed more plausible from the fact that our 74 or "Y" book probably had a later edition, enlarging and supplementing it.

It was necessary to test this theory, apparently so well justified, before proceeding to any other basis of investigation. The fact that to do so involved detailed study can be seen from the following circumstances:

(1) The complexity of indicators was confusing as

shown in the following list. (The letters at the left are arbitrary names given to codes in our records; the numbers are indicators which show the code key to be used in deciphering. All messages are between Spain and the places mentioned)

A-B	301	Washington, Berlin, Havana, Mexico, Buenos Aires, Paris, Bogota, Lima, Panama
C	101	Berlin, Bogota, Havana, Washington, Lima, London, Vienna
D	229	Havana, London
E	249	Washington
F	131	Caracas, New York
G-H	(133)	
	(132)	Mexico
	(123)	
I	129	Buenos Aires, Para, Montevideo
J	141	Lima, Quito, Buenos Aires, Mexico
K	143	Havana, London
L	111	Morocco
M	9	San Juan
N	32	Santo Domingo
O	187	Mexico
P	181	Costa Rica, Guatemala, Salvador
Q	303	Berlin
R	155	Bogota, Havana
S	167	Berlin
T	215	Sofia, Vienna
U	209	Salvador, Costa Rica
V	159	Vienna
W	149	Montevidea, Buenos Aires
X	153	Washington
Y	74	Panama
Z	253	Berlin

These indicators fall naturally into groups as follows:

301-303-101
209-229-249-129-149-159
131-132-133-123-153-143-141
187-167-[illegible]
181-141-101

153-155-159
153-253
215
9-32-74

Whether this grouping of indicators has any significance has not yet been determined. The case of code "G-H", in which 133, 132 and 123 are used interchangeably is an exception to the general practice. The fact that only three have less than three numbers seemed significant and later these three only proved to be the consular codes, strictly speaking, with a different system from the others.

(2) The second cause for uncertainty as to the best initial procedure was the possibility that some of these codes might be consular and some diplomatic. We chose code 301, "A-B", for investigation because it was used between several points and contained many short messages which might well be of a consular nature.

(3) In the third place the absence of plain text prevented any assumption of the nature of the messages or any clew to thepossible meaning of groups preceding and following plain text.

(4) Lastly, the complexity of the material and the difficulty of analysis was increased by the occurrence of five-number groups instead of four in various telegrams, although such groups were comparatively rare.

This resume will be divided into the following periods or developments in the process of solving the code;

(Note: All material used during the period of investigation was destroyed and therefore this account must of necessity be incomplete especially because of the lack of many examples and details which influenced us at the time.)

(A) First period, during which an attempt was made to fit the number code or some part of it to the 74 book. This was coincident with the preparation of the material and the sorting and classification of cards of all the codes available.

(B) Intermediate stage, in which it was certain that the 74 book had no relation to the 501 code (A-B). At this time the outstanding characteristics of all the number codes were determined, the order of the numbers ascertained, punctuation identified, and assumptions tested of high frequency groups.

(C) The final phase, consisting of the receiving of circular No. 46 on November 30, 1918 and the consequent reading of the code.

We will first discuss the introductory period, namely, the analysis of 74 or "Y", and the attempt to determine by what re-arrangement, encipherment or supplement it could be fitted to 501 messages. At the same time the clerical work necessary was being done by clerks and typists. As an explanation of the latter is necessary before beginning any kind of code study, we will consider it first although in fact all the clerical work was not finished until well into the final period.

In the first place, all messages must be transcribed upon form sheets (see specimen, page 7.) At the top of this form is written the classification given themessage in the office records, also the person by whom it is signed, its source and destination.

The numbers of the code message are written below in two vertical columns, so that the reference to separate groups can be made conveniently by means of the capitals "A" and "B" at the top of the columns and the small letters at the left of each group. For example the reference to group 6134 on page 7, would be "B-189 Be".

(Note: Later, a capital S was placed before the letters A, B, etc., to distinguish the Spanish code from those of other governments.)

From To Date

Ministro Espana, HAVANA No. B-189 Ministro Estado, MADRID 11/22/18
C.B. 6189 S.D.

	A		B
a	30106	a	0314
b	9978	b	3904
c	1915	c	4570
d	6126	d	0015
e	7328	e	6134
f	7880	f	4079
g	0692	g	4770
h	1283	h	5769
i	9783	i	9079
j	5360	j	0185
k	2092	k	5684
l	9511	l	8613
m	8777	m	0692
n	5397	n	1283
o	2684	o	9783
p	6414	p	4495
q	7468	q	6314
r	0192	r	6684
s	9079	s	8222
t	3070	t	9112
u	8298	u	3000
v	4417	v	5963
w	6960	w	6915
x	0314	x	2313
y	4893	y	Ministro Espana
z	9831	z	

After the groups of a telegram are entered upon the forms as described, cards are made for each number in the message. Messages composed of five-number groups cannot be carded until a study of the code in question has advanced to such a point as to enable the investigator to determine whether the five-number groups are true groups or merely a re-formation of numbers to disguise the code. In the upper left-hand corner of the card is written the group under consideration;

3851 A-B 83 p2 Bh
1038 0483- - - -8062 8613

after it the letter indicating the code series; next, the number of the telegram in this series with the reference to the form page upon which the telegram has been transcribed. If a telegram has more than one page, p2 or p3, etc. is added. Below this are written the two groups which immediately precede the group in the telegram, followed by a dash and the two groups which follow it. It is important to avoid mixing cards of different series confused because of errors in the indicator, omission of indicator or similarity of indicator.

When all the groups of one code series have been typewritten, the cards are verified and filed in numerical order. Frequency tables are then made by counting the number of cards representing each group. Each hundred is entered in ten vertical lines on a single page so that the resulting table is composed of ten pages, and can be readily referred to. As a supplement to the large frequency table, working sheets of frequencies above five are usually made for convenient reference in the large series. The following page shows the high frequency working sheet as originally compiled for Series E (indicator 249).

WORKING FREQUENCY

SERIES E - INDICATOR 249

0001	22	1082	8	2082	11	3073	6	4002	6
0023	10	1165	45	2100	15	3119	42	4006	27
0024	112	1244	5	2130	14	3122	17	4100	5
0294	6	1266	5	2160	9	3168	35	4155	8
0515	18	1385	19	2178	14	3350	21	4238	6
0546	9	1472	44	2179	10	3501	5	4324	73
0564	6	1660	12	2291	9	3506	8	4338	8
0596	6	1739	7	2318	19	3517	9	4403	5
0685	5	1809	12	2417	7	3518	31	4424	68
0709	7	1934	10	2467	22	3570	5	4524	16
0744	10			2644	12	3578	5	4538	15
0825	18			2813	25	3594	7	4563	9
0858	14			2855	12	3637	21	4596	8
0915	5			2913	5	3645	5	4624	15
0921	9			2986	5	3681	18	4741	7
0925	39					3763	6	4779	5
0945	52					3772	13	4879	16
						3821	15	4934	9
						3887	6		
						3900	18		
						3952	7		
						3972	6		

5001	41	6108	7	7023	10	8119	49	9110	5
5124	24	6195	18	7106	5	8317	5	9111	6
5223	9	6207	6	7123	8	8336	5	9215	5
5224	12	6284	7	7185	16	8365	6	9273	18
5228	7	6345	41	7221	6	8372	10	9398	5
5245	6	6385	6	7318	15	8510	8	9424	11
5363	7	6438	8	7350	23	8518	9	9650	6
5468	5	6472	59	7380	11	8596	7	9664	6
5506	5	6538	5	7406	6	8608	7	9815	8
5509	5	6585	20	7481	7	8627	5	9856	8
5546	21	6646	12	7506	5	8637	20	9879	5
5666	5	6677	7	7525	9	8681	5		
5672	5	6680	5	7813	41	8696	10		
5678	6	6889	11	7885	7	8786	17		
5707	5	6919	5	7902	5	8803	9		
5772	5			7919	7	8886	11		
5802	18					8952	6		
5804	5								
5810	24								
5825	9								
5829	22								
5860	7								
5886	7								

We thus have a graphic picture of the comparative number of occurrences of each group and a valuable aid in guessing the identity of groups frequently repeated. In addition, we have all the interrelations of each group and can make classifications based upon groups of similar use and those which tend to fall together in a majority of cases. Also the frequencies of different series can be compared to advantage, similar phenomena noted, and parallel intervals discovered. In short we are able to gather data in regard to the general character of the code, such as;

(1) Whether the system is changed at certain intervals
(2) Whether the vocabulary is limited or differentiated and whether there are distinctly different types of telegrams
(3) W hether regular variants are used
(4) Whether some parts of the book are not used

Since the investigations of the first period were carried on while typists and clerks were engaged in this introductory work, the material at hand was necessarily incomplete. Series 301 was ready first and therefore used exclusively at the beginning. Several methods of investigation and experiment were devised and assigned to different individuals. Although some of these methods overlap in various respects, we will consider each separately under the following points:

(a) Basis
(b) Stage reached
(c) Why abandoned or possibilities remaining

I. The first method was that of simple addition and subtraction.

(a) It was based upon the presence in code book 74 of the pasted strips and upon the assumption that these strips were consecutive and not cut up with the pages as units.

(b) Adding was continued from 1 through 1000, and subtracting from 1 through 100, using the 301 group sequence. 1703-1590-0932-0614-6014. 6014 was also tested with all high frequency words in 74.

(c) This method was found to be incorrect for 301 because all of the resultant groups failed to decode by 74. In addition, a large number of 301 high frequency groups were tested with common words in 74 and failed to show the same differences. Finally, too large a proportion of numbers were brought out of range, and there was no way of determining how to treat numbers higher than 7040 because we were uncertain whether 7040 was the end of the book or whether a supplement had been added, which latter supposition would account for the high numbers between 7040 and 10,000. It was therefore impossible to determine whether we were justified in subtracting 7040 from the groups brought out of range by addition and adding 7040 before subtracting when groups were smaller than the subtractive, or whether 10,000 should be used as a basis.

II. The failure to discover a simple method of encipherment by addition or subtraction led to the supposition that an enciphering table was employed in which the numbers were arranged in some systematic way.

(a) This theory was based on the fact that such a means of changing the code was easier and more natural than pasting on large numbers of strips at frequent intervals.

(b) Numerous experiments were made with high frequency 74 groups in the effort to find a table which would make any one of them equal to a high frequency 301. In one experimental table the outer numbers were arranged alternately and the inner ones obliquely. This looked well because 2302, period in 74, was represented by 6014, the most frequent group in 301.

2302(74) equals 6014(301)

	0	5	1	6	2	7	3	8	4	9
0	0	2	5	9	14	20	27	35	44	54
5	1	4	8	13	19	26	34	43	53	63
1	3	7	12	18	25	33	42	52	62	71
6	6	11	17	24	32	41	51	61	70	78
2	10	16	23	31	40	50	60	69	77	84
7	15	22	30	39	49	59	68	76	83	89
3	21	29	38	48	58	67	75	82	88	93
8	28	37	47	57	66	74	81	87	92	96
4	36	46	56	65	73	80	86	91	95	98
9	45	55	64	72	79	85	90	94	97	99

(c) Although this table fitted exactly the two highest groups in both codes, it was a simple coincidence since none of the other groups tallied and 6014 occurred frequently as an initial group. The observations made at this time of the peculiarity of the use of 6014 were the germ of the idea determined upon at the end of this period, namely that 6014 must be quotation marks because of its unusual interrelations.

III. The next assumption was that 0281 in the 74 book was equivalent to 2921 in the new encipherment.

(a) The basis of this was the fact that in the 74 book the page on which 0301 occurs begins with 0281 and the 0301 has a distinct line underneath as though especially indicated for some reason. Since the indicator number of the A-B series is 301, the possibility presented itself that strips might have been pasted on with the page upon which 0301 occurred as page 1, namely making A equal to 0281 instead of 2921.

(b) Several words in 74 which would naturally have high frequency were tested by subtracting 2640 from group 2641 through group 7040, and adding 7040 and subtracting 2640 from group 0001 through group 2640.

(c) We abandoned this theory because:

(1) It was equivalent to Method I.
(2) By close examination the line under 0301 was attributed to a wrinkle in the strip caused by uneven pasting.
(3) We found that series 133, 123 and 132 were identical thus apparently disproving the theory that indicator numbers have some connection with the method of encipherment.

IV. In the meantime we had been making a series of tests of sequences of high frequency groups from each indicator series by adding and subtracting 60, 160, 260, 360, etc. to discover whether any series could be read by the vocabulary as it stood before the last strips were pasted on, or whether any succeeding strips used the same system.

(a) This hypothesis was based on the fact that on page 34 in the 74 book the strip was pasted on unevenly and showed a difference of 40 between the last two numbers.

(b) 560, 460, 360, 260, 160 and 60 were added and subtracted from high frequency sequences taken from all indicator series, including the unclassified.

(c) This theory was abandoned;

(1) Because the numbers became largely out of range without subtracting 7040.

(2) Most of the possibilities has been covered by Method I.

(3) The fact that the 61 occurring at the right of 5601 in the 74 book, page 34, and belonging to the preceding strip pasted underneath was identical with the final digits of 5561 directly opposite 5601, suggested that the strips might not have been in continuous numerical succession but might have been divided on each page and the columns reversed.

V. The study of multiples of 40 was made although coincident with Methods I and IX.

(a) This investigation was carried on independently of I and IX because the columns were of 40 groups each and the strips were not divided in the middle.

(b) Tests in the A-B series in the normal order were unsatisfactory.

(c) We therefore abandoned the theory with the reservation that some transposition method or encipherment might have been used.

(Note: On September 26th we noticed that the digit before 61 on the strip underneath 5601 on page 34 must be a 3 or an 8. As there are no numbers ending in 861 in this position on any page, the possibilities were reduced to the differences between 5601 and 0361, 1361, 2361, 3361, 4361, 5361, 6361. Trials were again made supplementing Method IX by taking high frequency groups from all series, transposing in all orders, adding and subtracting 5240, 4240, 3240, 2240, 1240, 0240, 0760 and decoding according to 74; also by taking common 74 groups, adding and subtracting 5240, etc., transposing in all orders and testing results to see if they occurred as high frequency groups in any series. The failure of this method offered almost conclusive proof that the 74 book was not used, but the impression was so strong that this must have been the basis of at least some of the codes on hand that the theory was not set aside.)

VI. The so-called circular method involved Method I but was confined to multiples by tens, hundreds and thousands.

(a) This was based upon the observation of various beginnings of 301 telegrams as seen in the charts following:

Chart A

1.	7468	5623	2327	0603	2936	0314	A53
2.	7368	0192	5665	8997	5477	0614	A56
3.	7368	0909	9370	0258	7095	7448	A57½
4.	7368	2799	0592	9674	3196	6137	A58
5.	7461	0462	4971	0698	6915	0939	A77
6.	7468	9079	0278	2912	3070	3469	A5½
7.	7368	2799	9079	6687	7912	3070	A7
8.	7468	0194	1915	1218	2662	4971	A10
9.	7468	0194	1218	2662	8613	0683	A11
10.	7468	8992	0162	2812	7447	4584	A12
11.	7468	0192	4841	3852	2367	7147	A15
12.	7368	3676	9079	0592	6444	1126	A16
13.	7468	6915	1218	2662	4971	0692	A20
14.	1218	2662	7368	6815	0294	4971	A21

Chart B

1.	1495	6014	1978	1816	6915	A9
2.	1978	1915	7369	3326	8196	B42
3.	8581	6014	2078	1915	2732	A23½
4.	1125	6915	2078	1915	9640	B217
5.	8671	4732	2076	6915	4378	A-B45
6.	0379	0619	2078	1915	4365	A-B102
7.	3070	2532	1978	2016	6720	A18
8.	2215	2832	1978	1915	1955	A-B105
9.	1955	7132	1976	6715	7868	A-B125
10.	1915	1590	1976	6915	6702	A43
11.	5797	9939	1978	1915	0683	B55
12.	7277	1126	1978	1915	0683	A59½
13.	8363	3360	1978	1915	0683	A61
14.	0571	6390	1978	1915	0939	A61
15.	30159	3004	1978	6815	5502 3026	B4

By comparison of frequent initial groups we saw that certain numbers varying by only one digit were used similarly, notably 7368 and 7468 (Chart A) and 1978 and 2078 (Chart B). Since these groups were 100 apart we believed first that two words of synonymous meaning must happen to come 100 apart. When we observed, however, that the same phenomenon occurred with other groups of two and that similar numbers often followed the so-called twin groups, we knew that the last two digits must be the page numbers. For example, in Chart A, lines 6 and 7, 7368 and 7468 are both followed by 9079, in the second case with 2799 intervening. In the first case 2912 is the second group after 9079 and 7912 in a similar relation to the second 9079. Also in Chart A, lines 2 and 12, 0192 and 0592 are associated with 7468 and 7368 respectively. In Chart A, lines 9 and 14, 7468 and 7368 (This time not initial) have an affinity for 1218 and 2662 which can occur before or after 7368 or 7468; in lines 13 and 14, 6815 and 6915 occur respectively after 7368 and 7468. Numerous interrelations of this nature can be followed by reading the charts. For instance, in Chart B the occurrence of 1915, 2015, 6815 and 6915, almost without exception after 1978 and 2078, points at once to the fact that the groups in question stand for the different forms of a verb occurring on page 78, the endings of which are to be found on page 15. Anotherkind of twin group is also evident here, 5000 apart instead of 100, in phrases such as 1978,-6915, 1978-1915, ls. 10 and 12, Chart B; 7468-9079-0278-2912-3070 and 7368-2799-9079-6687-7912-3070, ls. 6 and 7, Chart A. We were at a loss to account for this at the time until the continued recurrence of this phenomenon, notably in our initial study of Z-0069-6069 page 36, and the corresponding groups in other indicator series forced us to the theory that variants were used 50 apart in the inverted order.

(b) A number of charts of the different series were constructed which showed that two or more groups in each series unfailingly behaved in the same manner, but nothing was definitely proved as to their identity because the theory of the 74 book was still influencing investigations and we believed that groups could be identified by some numerical method.

(c) We concluded that some method of transposition of numbers was utilized in an enciphering system based upon the 74 book.

VII. The study of vocabulary sequences at intervals of 10, 100 and 1000 was being made simultaneously.

(a) This was based on the same observation that high frequency groups were often 10, 100 or 1000 apart and was really a continuation of Method VI., approaching the point in the reverse order.

(b) A sequence vocabulary was constructed of possible words in the Y book occurring at the regular intervals mentioned above.

(c) No method of fitting in any of these sequences of meanings to code groups of the same character could be devised. The only satisfactory feature was the occurrence of the period and comma next each other.

VIII. The study of the sequence 5296-6014-4556-6014-7470-7508-~~2927~~-0683-8580-3959, taken from 501, was next undertaken

(a) In this study we assumed that an encipherment was made of only the first two numbers, in view of the fact that the last two numbers were the same on the strips underneath the present ones in the 74 book as seen on pages 12, 30, 34 and 52, where the strips had been imperfectly pasted.

(b) All frequent groups ending or beginning (to account for inversion) in 96, 56, 14, 70, 08, 37, 83, 60 and 59, were taken from the 74 book and an attempt made to fit in words to make a connected meaning. Cards were made of all spelling group possibilities and classified by the final figures.

(c) Every attempt to form a sequence of connected words was without success. This method was only another evidence of the now almost certain fact that the 74 book was impracticable. The time was not wasted, however, for from this came the idea of a possible re-arrangement of the initial digits or word numbers with the page as a unit.

IX. We then experimented with changing the order of all the digits instead of only the first two.

(a) The different transposition orders possible are as follows:

a	1234	i	2314	q	3412
b	1243	j	2341	r	3421
c	1324	k	2413	s	4123
d	1342	l	2431	t	4132
e	1423	m	3124	u	4213
f	1432	n	3142	v	4231
g	2134	o	3214	w	4312
h	2143	p	3241	x	4321

Several high frequency words of the 301 series were transposed in all these ways and decoded according to the 74 book; additives and subtractives through 100 were used with the 301 groups and the results transposed in all orders; the 301 groups were next transposed in all orders and addition and subtraction tried with these transposed forms.

(b) The above processes were carried out exhaustively up to the point that the resulting groups ran out of range of the book.

(c) The failure of every kind of transposition with or without addition and subtraction, and with the addition and subtraction both before and after the transposition of the digits proved beyond a doubt that the only way to obtain results was to analyse code groups instead of searching for a numerical method of transference.

(Note: 1. Additional evidence to the same effect was found by considering the group 1111 whose meaning is requerir in the 74 book. No matter what the transposition order used, 1111 must be the same in all encipherments in any method without adding or subtracting. Theone passage in which 1111 occurred in 301 was inverted in all orders and translated by 74 with no result except the usual one of disconnected words).

(Note: II. The possibility of a mononnumeral additive as suggested in Slater's Telegraphic Code, page 7, etc., had previously been considered. With any transposition order all possible monomumeral additives or subtractives must be determined by the following words taken from the 74 book, all possible meanings for a group occurring once;

1111.....requerir	5555.....guante
2222.....sanjar	6666.....mag
3333.....aprobacion	7777.....x
4444.....dedique	

These additives and subtractives thus determined were tried without success in Method I.)

X. The transitional period between the search for numerical correspondence and the enclusive use of analysis was the study of vacant places in frequencies to determine whether correspondence could be found in the rise and fall of the frequency line. We also hoped to add further proof of the lack of correlation between the two codes and gain a more definite knowledge of the interrelation of all of the codes.

(a) As indicated in the description of the 74 book, the numbers from 2386 to 2921 are blank. Upon thetheery that a similar blank or low frequency part of the book might occur in new encipherments or codes, graphs were drawn of several indicator series showing the high and low points of the frequency line in the various series. In addition, all telegrams received in the 74 code were carded, filed, and the frequencies taken. From this data a graph was drawn of the 74 book and compared with those of the various series. Two series were also plotted in the simple inversion order (See Method VIII.)

(b) When themethods previously enumerated were abandoned as unsatisfactory, these groups also were supposed to be useless.

(c) The graphs made in the simple inversion order "r", however, clearly indicated the identity of method of the two series because of the approximate correspondence of the high and low points and the general similarity of the lines. (All graphs were destroyed upon removal from Washington).

We now come to the intermediate stage in which the theory of the 74 book was definitely abandoned. As a result of the preceding investigations and of familiarity with the numbers, the following points were accepted and taken as a basis for further work.

(a) The last two digits are the page number, and the first two the number of the word on the page.

(b) Punctuation is on page 14 in the 301 series, on page 14 also is 253, on page 24 in 249, on page 38 in 229, on page 25 in 129 and on page 70 in 101. This was evident by the frequent recurrences and peculiar position of 0314, 0414, 5314, 5414 and 6014 in the 301 series; of 0214, 0314, 5214, 5314 and 5914 in the 253 series; of 4224, 4344, 9524, 9424 and 0024 in the 249 series, etc.

(c) Several variants are used as proved by the similarity of groups 50 apart in the inverted order such as 1915 and 6915 in Chart B, page 18, lines 5, 6, 10, 11, etc.

The clerical work had now reached a point where the large series were typed on forms, carded and filed, and the smaller series begun. Unfortunately, however, owing to the fact that the real order of the numbers was unknown at the time the filing began, all groups were filed according to the first two numbers, for which reason a recompilation was necessary because the real frequencies were available only by finding each number in its numerical order according to the first two digits. We therefore made a tentative working tabulation of groups with frequency above 5 of the chief indicator series for immediate use while the cards were being resorted.

This isolation of important groups led to the discovery of a striking similarity of intervals between certain ones in the various series. For example, we noticed that 57 was the common difference between 0338 and 6058 in the 129 series, 0314 and 6014 in the 301 series, and also between 0024 and 5324 in the 249 series, if 10,000 was first added to 0024. A table showing other intervals follows:

301	249	255	229	101	129
0314	4324	0214	0338	7070	1125
0414	4424	0314	0438	7170	1225
0514	4524	....	....	....	....
1114	5124	1014	....	7870	....
1214	5224	1114	1238	7970	2025
5314	9324	5214	5338	2070	6125
5414	9424	5314	5438	2170	6225
6014	0024	5914	6038	2770	6825
9314	3324	9214	....	....	....

In the hope of finding more such intervals and thus determining identical pages and the system of page arrangement, we made on strips a tabulation in the inverted order of numbers occurring three or more times. Since each strip showed all the frequent words on a page and the intervals between them, by comparing strips of the different series we expected to fit together the various encipherments. A careful search for more common differences resulted in the discovery of a very limited number on pages other than those of punctuation. We could not account at the time for the fact that so many correspondences stood out on one page and that so few other groups behaved in the same way. Our failure was due to the fact that we compared 129 with 301 instead of 301 with 249 or 255. Since the 129 series is between Madrid and Buenos Aires and is chiefly of a commercial nature, the vocabulary is so different that similarities of intervals were less likely to be found. A nother reason that other intervals were not seen is the alphabetical twisting on the pages, namely the continuation of the alphabetical sequence in the first column when the second is full, (see page 59) thus disguising the equal intervals by necessitating the addition of 100.

Although the strips were apparently unsatisfactory they at least showed us the most efficient way to make a recompilation of frequencies. Therefore, new frequency tables in the correct order were compiled from the original sheets in the following manner: Ten sheets were ruled, one for each thousand, for the tabulation of ten vertical columns of code groups with their frequencies. Cross-section paper is best for this purpose. As the code groups from the first frequency tables were read off, they were entered on the proper page and column. A group ending in 00 thus falls in the first column of the first page; in 01 in the second column of the first page; in 10 in the first column of the second page; in 11 in the second column of the second page, etc. The resulting tabulation shows the groups on each page of the code book tabulated in separate columns and the numbers of the words on the page following in consecutive order so that high frequency pages and pages containing variants can be picked out at a glance. The example given on page 28 shows the frequencies of pages 20-29 inclusive in Series S, indicator 167, between Madrid and Berlin.

Series S - 167

20		21		22		23		24		25		26		27		28		29	
0420	2	0221	2	0322	1	0023	3	0524	1	0025	1	1126	165	1127	2	1028	1	1629	1
0520	1	0321	1	0622	5	0223	1	1224	1	1225	2	1226	124	1227	1	1128	4	2529	1
0620	1	0521	1	1222	1	1023	1	1424	1	1825	2	1326	6	1527	1	2128	1	3629	6
0820	5	1221	1	1522	2	1123	1	2124	3	2025	1	1426	5	2027	29	2528	1	3729	1
1220	1	2221	6	2322	1	1423	1	2724	2	2525	11	1726	14	2127	78	2628	2	4129	5
1620	1	2321	1	2522	1	2823	1	2824	3	2825	114	1826	7	2227	2	2728	1	4329	3
2420	1	2821	1	2522	2	3123	4	5824	3	3525	1	1926	15	2327	1	4128	1	5129	1
2620	3	3521	9	2622	23	4123	10	6124	2	3725	3	2026	11	2427	9	4528	1	5429	4
2920	1	4621	1	2722	9	4723	1	6424	1	4725	1	2126	1	2527	4	4628	1	6129	1
3020	1	5521	1	2822	1	5123	1	7224	1	7125	1	2226	1	2627	6	5928	1	6329	1
3220	1	5721	5	3222	2	6623	2	7324	3	7825	4	4126	1	2827	2	6028	1	6629	1
3320	1	6621	1	4222	10	6723	1	7424	2	7925	7	6126	7	3127	2	6228	1	7529	2
3720	3	6721	1	6622	1	7423	1	7524	6	8325	2	6226	14	3227	14	6428	1		
5720	1	6821	10	6922	3	7523	4	7624	1	8525	1	6626	14	4127	6	6528	1		
6220	1	7821	1	7022	1	8123	7	7824	3	9225	4	6726	6	4327	3	7028	1		
6320	3	8721	1	7722	2			8524	2			6826	19	4827	1	8028	6		
6520	3							9724	1			7026	1	5427	5	8428	1		
6720	3											7126	12	5527	2				
7420	1											7226	1	7027	10				
7720	1											7326	7	7127	28				
8220	1											7426	5	7627	1				
												7826	20	8627	1				
												9126	1	8727	1				
														8827	1				
														9727	3				

While waiting for the completion of the corrected frequency tabulations, we made experiments from charts composed of the initial and final groups of telegrams in consecutive order according to date. The first page of the chart for the C or 101 series follows:

Series C, (101)

	Date														
C 1	11/28/17	8893	4209	7970	4289	4104	4444	8696	2045	----	4998	4456	5362	6746	4637
C 2	" 29 "	4897	7996	0567	4139	7669	6283	4104	5924			2971	7874	8224	7259
C 3	" 30 "	9085	8678	5362	7996	4337	0346	7669	7996	----	3404	7996	0767	0465	0008
C 4	" " "	5227	5362	7889	7996	4337	7060	7170	2044	----	9857	7970	3331	9283	8309
C 5	12/ 1/17	4046	6153	8678	3944	0060	3331	0751	7874	----	6242	6103	7669	4583	7530
C 6	" " "	2044	7977	7669	5472	5362	7996	0767	0346						
C 7	" " "	4170	7996	0767	4139										
C 8	" 3 "	4104	5924	2971	8474	8224	7259	5362	7870					7996	2665
C 9	" " "	5227	5362	7996	0767	7060	7170	3331	7959	----	0295	2717	8553	4397	7871
C10	" 4 "	5227	5362	7996	2665	4139	7170	0427	2845	----	6253	0456	2956	4534	2770
C11	" " "	5227	5362	7996	0767	7947	7170	3833	0383	----	6661	5818	4989	3272	5751
C12	" " "	0741	1540	0656	8698	9572	3331	0395	4678	----	9246	0656	1224	7802	0881
C13	" " "	2044	6664	2971	9477	4605	9047	5362	1932	----	2466	7970	6867	9761	2770
C14	" 5 "	5227	5362	7996	2665	1016	7170	5394	9983	----	3331	6351	7871	7669	8762
C15	" " "	4305	4104	9581	4959	5924	5362	7870	7996					2665	2230
C16	" " "	0527	7259	0956	2144	7871	6764	9047	5362	----	7946	4499	2981	1666	2770
C17	" " "	5227	5362	7996	2665	0346	7170	1360	4007	----	3237	9285	0021	9996	8666
C18	" 6 "	2044	6024	8224	8696	7070	8166	2770	4276	----	9745	2637	1013	3331	7259
C19	" 5 "	7793	0785	2904	2232	9266	8198	3331	7752	----	7685	3573	4989	6724	9252
C20	" " "	0741	6073	2971	4456	5362	6746	2665	2230	----	5651	7070	3077	3331	1522
C21	" 7 "	9085	8678	5362	7996	2665	7060	7669	7996	----	1540	7996	1730	1016	0008
C22	" " "	5227	5362	7996	1730	1106	7170	5394	4647	----	4833	0547	0761	7752	9329
C23	" "	7871	3091	3331	8204	1253	6864	7375	0527	----	4046	7798	9960	1564	0159
C24	" 8 "	5227	5362	7996	1720	0346	7170	9646	6126	----	5982	4072	9985	7970	0958
C25	" " "	4989	4456	4102	9675	3581	7370	8857	0955	----	3684	3331	3476	0741	0215
C26	" " "	6126	3833	0383	0956	3237	8696	0741	2589	----	7870	0404	3987	7970	2195
C27	" 9 "	0527	7259	0956	4862	7370	2770	4086	7704	----	7970	7170	9383	8455	2770
C28	" 11 "	7356	7888	0618	7070	8892	7941	3331	9248	----	4826	7871	9248	0607	0340
C30	2/24/18	8932	4456	5362	2170	2044	4009	4006	7970	----	6224	3553	2380	6431	4176
C29	" 27 "	7593	7017	6056	5982	0955	1944	7871	6664	----	0954	6967	0538	5982	2770

The most noticeable thing in reading this chart is the recurrense of groups ending in 70 at suitable intervals for punctuation. Five of the telegrams out of the first thirty end in 2770, so we assume that 2770 is period and that 2670 should therefore be comma (see page 20, VIII. (c)). A search for 2670 is unsuccessful but we come upon 7070 and 7170 which look better for period and comma. 2770 must then be the AB 6014, or quotation marks, the only other thing connected with punctuation which comes to mind as a possible ending. Another 2770 should precede in each case if this is true. It is true in C-27 in the table and a search in original telegrams C-10, C-13, C-14 and C-27 brings a similar result, proving that our sign for opening and closing quotation is correct. Then 7370 occurring before 2770 must be colon. We look at the beginning and find that 4170 begins C-7, a four group telegram. All the set phrases that occur to us which could begin a telegram are "Urgent", "Confidential", "Congratulations", or a request to repeat. However, since we have nothing to help us we leave that consideration for the time being and return to the punctuation groups, 7870 and 7970, which also appear as good candidates for period and comma. We soon reject them, however, in favor of the original 7070 and 7170 because 7170 occurs in the same vertical line in the chart seven times at about the right distance to end an introductory clause. Then 2971 and 7871, C-2, C-14 etc. must be a's, one accented and one not, or one capital and one not, if we follow the arrangement of single letters in the 74 book and if the punctuation page comes first or last as is natural to suppose. No more 71's or 72's are in evidence, therefore we turn to the next peculiar phenomenon, namely 5227 and 7996 which not only have an attraction for each other individually, but both together occur continually near punctuation groups. Copying the occurrences of 5227 and 7996 we find:

C 2	11/29/18	4897	7996	0567	4139			
C 3	11/30/18	----5362	7996	4337	0346	7669	7996	
C 4	"	5227	5362	7669	7996	4337	7060	7170
C 6	12/1/18	----5362	7996	0767	0346 End			
C 7	"	4170	7996	0767	4139 End			
C 9	12/3/18	5227	5362	7996	0767	7060	7170	
C10	12/4/18	5227	5362	7996	2665	4139	7170	
C11	"	5227	5362	7996	0767	7947	7170	
C14	12/5/18	5227	5362	7996	2665	11016	7170	
C17	"	5227	5362	7996	2665	0346	7170	
C21	12/7/18	9885	8678	5362	7996	2665	7060	7669
C22	"	5227	5362	7996	1730	1106	7996	7170
C24	12/8/18	5227	5362	7996	1720	0346	7170	

5227 does not occur near the end but 7996 does several times at good intervals for da or para. These two groups must be parts of an initial phrase such as:

(1) "From __________ to __________." or
"To ______________ from ________"
(2) "In reply to your telegram - - - - "
(3) "Received your telegram of - - - - "
(4) Date
(5) Number of telegram

No recurring groups are evident for "November" and "December", so we eliminate point 4. In C-7, 4170 is probably not "Confidential" or "Urgent" with *de* or *para* following, and if 4170 is "Congratulations", 7996 must be *a*. 2971 and 7871 are already called a's, therefore the 4170 is probably "Please repeat" and 7996 either *numero* or *telegrama*. Whichever one 7996 is, *numero* or *telegrama*, the groups following must be numbers. We write them out for clearness:

C 2	11/29/18	7996	0567	4139		
C 3	11/30/18	7996	4337	0346	7669	7996
C 4	"	7996	4337	7060	7170	
C 6	12/1/18	7996	0767	0346 End		
C 7	"	7996	0767	4139		
C 9	12/3/18	7996	0767	7060	7170	
C10	12/4/18	7996	2665	4139	7170	
C11	"	7996	0767	7947	7170	
C14	12/5/18	7996	2665	1016	7170	
C17	12/5/18	7996	2665	0346	7170	
C21	12/7/18	7996	2665	7060	7669	7996
C22	"	7996	1730	1106	7170	
C24	12/8/18	7996	1730	0346	7170	

It is safer to begin with numbers next the punctuation for these must be uno, dos, tres, cuatro, cinco, seis, siete, ocho, nueve, diez. Unfortunately we have no one group occurring in each of the last two columns to call diez, nor have we anything near 71, our only tentative alphabetical guide. We put the numbers and code groups out in order, however, just to see how they lie, and are pleased by the fact that they fall into approximate groups:

Frequency	Tens	Units
2	1730	
2	4337	
2		4139
4		0346
1		7947
3		7060
4	2665	
4	0767	
2	7669	

(cinco
(cincuenta
(cuatro
(cuarenta
(diez
(dos

(noventa
(nueve
(ocho
(ochenta

(seis
(sesenta
(setenta
(siete

(treinta
(uno
(veinte

1730 is later in date than the others in both occurrences (C-22, C-24) and must be a higher number than the rest. Either cincuenta or cuarenta fits in the larger group, but 1730 and 4337 look too far apart (7 pages) for cincuenta and cuarenta (see note, page 34). So we may say that perhaps 1730 is cuarenta and 4337 diez. If so, 2665 following 7996 in telegrams of preceding date must be treinta and 0767 veinte, especially in view of the fact that pages 65 and 67 are a good interval apart for tr and v. The telegrams now read:

C 2	11/29/18	7996	0767	4139		
C 3	11/30/18	7996	4337 diez	0346	7669	7996
C 4	"	7996	4337 diez	7060	7170 period	
C 6	12/1/18	7996	0767 veinte	0346 End		
C 7	"	7996	0767 veinte	4139		
C 9	12/3/16	7996	0767 veinte	7060	7170 period	
C10	12/4/18	7996	2665 treinta	4139	7170 period	
C11	"	7996	0767 veinte	7947	7170 period	
C14	12/5/18	7996	2665 treinta	1016	7170 period	
C17	"	7996	2665 treinta	0346	7170 period	
C21	12/7/18	7996	2665 treinta	7060	7669	7996
C22	"	7996	1730 cuarenta	1106	7170 period	
C24	12/8/18	7996	1730 cuarenta	0346	7170 period	

(Note: In this connection the comparative size of the letters of the alphabet was calculated as follows:)

A	12.56	N	1.72
B	4.73	Ñ	.06
C	11.99	O	1.90
CH	1.08	P	6.46
D	5.68	Q	.53
E	6.84	R	4.76
F	3.01	S	5.27
G	3.30	T	5.52
H	2.63	U	.60
I	2.67	V	3.65
J	1.22	W	.28
K	.19	X	.11
L	2.91	Y	.30
LL	.20	Z	.83
M	6.53		

7669 is now evident in C-3 and C-21 as y connecting two 7996's and the proper distance after 0767. It would be unnecessary to say;

"Please repeat (telegram) and (telegram)------",
(number) (number)

therefore 7996 is probably one of the hundreds not included in our tabulation. 4139 nearest to 4337 must be dos. 7060 cannot be uno, tres, cuatro or cinco, because those connections are already determined; it might be seis or siete coming before 2665, treinta, or again nueve or ocho and start a new alphabetical sequence. Looking at C-9 and C-10, we adopt nueve as the most probable choice because of the treintidos on the following day. 0346 and 7947, the only two remaining numbers, are near each other and therefore are seis and siete.

In this way very plausible suppositions were ready to supplement the frequencies when they were finished. In this particular case of the 101 series, the above material was utilised in connection with the compiling of the encipherment rather than in the initial breaking both because 301 contained more material and because our failure to discover a numerical system for transference from encipherment to encipherment caused us to abandon work on secondary codes.

After the completion of the new frequency tables, the main effort of the intermediate stage was spent upon the study and analysis of code groups by means of comparisons of their interrelations and of the preferences which they showed in their associations with certain other numbers also interrelated. To do this we first took from the files high frequency groups landing themselves easily to analysis, and sorted.

the cards as nearly as possible with reference to the associated members. We next made so-called investigation sheets from the cards by copying in sequence the striking similarities, entering the reference to the telegram in the middle where the dash is on the card. Like groups were then marked with one color wherever they occurred so that the nature of their connections would be easily followed. For example, the following is the first part of the tabulation made for 0069, one of the largest frequencies in the Z or 253 series:

Investigation Sheet Z-0069

	Groups Preceding		Reference			Groups Following	
1.	8228	1704	Z-16	p6	Ab	0868	2074
2.	5623	4668	Z-16		Be	0868	2074
3.	9908	9307	Z-163		Am	0868	8204
4.	4224	2096	Z-164		Bl	0868	5568
5.	4800	0693	Z-102	p4	Al	0868	7311
6.	3522	6348	Z-164	p3	Bd	0868	0978
7.	4105	3122	Z-81	p2	Ak	5606	0868
8.	8643	6643	Z-1		Bu	0887	0818
9.	0868	5605	Z-66	p2	Bl	2428	3278
10.	9522	0693	Z-84	p2	Ac	8873	1366
11.	0693	5664	Z-22		Bc	0406	1411
12.	0693	5227	Z-62		Bm	1081	6337
13.	1081	9029	Z-164		Ab	0692	2428
14.	5399	8153	Z-85		Ag	5062	0693
15.	2287	9401	Z-58		Au	7684	0693
16.	5222	0474	Z-232		Bo	9080	0693
17.	4105	3522	Z-75		Aw	5606	0420
18.	3522	8373	Z-56	p2	Bz	0---	
19.	3522	7486	Z-164		Be	7982	4224
20.	1081	3085	Z-1604		Ab	1584	5738
21.	1081	5770	Z-199		Ax	0289	9106
22.	1081	7176	Z-69		Bt	2428	1081
23.	7861	4668	Z-90	p2	Bd	2428	8197
24.	5889	0183	Z-86		Bp	2428	7943
25.	8873	1366	Z-84	p2	Af	2428	7176
26.	8104	6411	Z-160		At	2428	0214
27.	0788	5828	Z-62		Bf	2428	9257
28.	9157	7207	Z-81	p2	Bx	2428	9346
29.	8873	9346	Z-72		Ag	7207	2428
30.	1385	2428	Z-202	p2	An	0887	1366

31.	7243	2428	Z-168		Be	3821	2246
32.	2428	9699	Z-90	p2	Ar	8392	5461
33.	2428	9882	Z-32		Af	8117	4206
34.	3028	6458	Z-202		Ai	9157	5825
35.	2504	0682	Z-1026	p2	Bf	9157	9166
36.	8378	6345	Z-76	p2	Aa	9157	9655
37.	1715	5889	Z-81	p2	Ax	9157	7207
38.	9307	3278	Z-160	p2	Ba	9157	5627
39.	1207	0314	Z-76	p2	Am	4636	9157
40.	0758	9157	Z-62	p2	Al	3186	9486
41.	4899	2772	Z-72		As	0756	4794
42.	5964	2772	Z-24		Au	1562	3255
43.	0437	2772	Z-214		Bi	8048	0314
44.	0437	4324	Z-201	p3	Ag	8200	0207
45.	9394	7517	Z-161	p2	Ah	9627	0437
46.	1973	3969	Z-169		Br	4286	0437
47.	9346	0910	Z-13		Bx	7207	0437
48.	1014	8799	Z-90	p2	Ap	2629	0107
49.	1014	0218	Z-70	p2	An	2629	0107
50.	5461	8799	Z-86	p2	Af	2629	1014
51.	7342	0314	Z-3		Af	1322	2629
52.	2469	1593	Z-157		Av	3384	2629
53.	1715	1014	Z-132		Ag	8104	2629
54.	6224	1014	Z-199		Bo	3384	2629
55.	0437	6720	Z-76		As	6102	0214
56.	2883	6720	Z-72		Bo	7657	6618
57.	4332	6720	Z-1031	p3	Ak	7981	0693
58.	0574	4668	Z-232		Bw	6720	0---
59.	3011	9698	Z-1031	p2	Ad	3470	0069

The rest of the tabulation consists of a large number of small connections in which0069 occurs two or three times with the same number which is usually in the same position, occasionally one removed. From the presence of such numerous relations so closely linked together we conclude that 0069 stands for some word or syllable which is used in a great variety of connections, of which a good proportion are very frequent phrases. Since it has also a very marked tendency to appear both before and after certain frequent groups and either next to or one removed from them, we assume that 0069 is some syllable which can be either a single word or an ending, such as a, an, e, en or o. We will eliminate an, e and o for the time being because they are not likely to be as frequent as theothers. Then if our theory in regard to the nature of syllable groups is correct and if the punctuation page is either at the beginning or end of the original book, it is natural to suppose that 0069 is en and that the letter a with similar high frequency and parallel use will appear on page 15, immediately following the z punctuation, page 14. Looking in the frequency table we find that two high groups do appear on that page, namely 1715 and 6715. We next make investigation sheets of these groups as follows (partial tables only are given):

Investigation Sheet Z-1715-a

6711	2708	Z-808	Ak	1014	7428
6711	2808	Z-811	Ak	1014	1428
2428	7580	Z-831	Bf	1014	0603
4241	2656	Z-831	Ay	2772	1096
5229	1874	Z-886	Bf	2772	4583
1802	8648	Z-839	Bd	4372	0417
2208	0214	Z-809	Am	9928	1593
0214	3728	Z-928	Be	1593	3099
8761	4668	Z-970	Br	8873	9546
0069	9405	Z-922	Bn	8873	9346
6575	1081	Z-924	3Aw	9157	5875

Investigation Sheet Z-6715-a

5057	1769	Z-805	Bs	1014	2408
3628	1302	Z-826	Bt	2772	7671
2461	[illegible]	Z-860	Ag	2772	0437
0901	7211	Z-904	2 Bl	4332	8784
9649	7871	Z-936	2 Aw	4332	8784
1204	4664	Z-880	Al	9928	7737
3323	4768	Z-973	Ak	1593	0888
6715	8988	Z-811	2 Ak	8384	9346
3304	6983	Z-951	Bn	9257	6002
9215	5581	Z-973	7 Ae	9157	0354

An examination of these two groups not only satisfies us that their general character is the same as that of 0069 previously considered, but also confirms our former impression that variants 50 apart are used in the code book (see page 34). The recurrence could scarcely be accidental of such parallel phrases as 1061-1715-9157 (Z-914) and 6983-6715-9157 (Z-951); 5581-6715-9157 (Z-975); 1715-1593-3099 (Z-928) and 4768-6715-1593 (Z-973); 1715-8873-9346 (Z-970) and 6715-8384-9346 (Z-811); 1715-2772-1096 (Z-851), 1715-2772-4583 (Z-886) and 6715-2772-7671 (Z-826), 6715-2772-0437 (Z-860). Therefore, we are fairly confident in calling 1715 and 6715 a and 0069 en and proceed to enter the equivalents in the telegrams together with the punctuation as far as known. We also begin our file of tentative vocabulary cards (see page 41).

The next step with the cards is to look for a variant for 0069. The group 5069, although small, works out very favorably as follows:

2074	2407	Z-16	Bi	0868	0930
6509	0214	Z-1026 p3	Bv	0868	2396
0868	4699	Z -73	As	8281	0693
2428	9098	Z-1026 p2	Av	3200	3701
2428	3995	Z-1026	Az	1096	8200
3283	3371	Z-9½	Bd	9401	5037

Since we see here the same attraction for 0868, 0693 and 2428 which 0069 has we add 5069 to our tentative identifications and proceed to study in a similar way all the recurring groups found in connection with 0069, 5069, 1715 and 6715, branching out from group to group and phrase to phrase. In this way a feeling for the relative values and probable meanings is developed which is invaluable to the code worker.

The process of studying and analyzing groups is too intricate to follow in detail in this account except to show striking characteristics of certain classes of words such as the preposition **an** just described. It may benoted in this connection that it is preferable for one person to make detailed study of one series at a time in order to be able to keep the groups in mind more definitely and build up a structure of suppositions. Persons working on separate series may then compare notes to advantage or one person may work on different codes during alternate weeks.

As soon as a number of investigation sheets had been completed and filed it was found difficult for anyone not working continuously on one code indicator to keep in mind all the interrelations necessary without referring constantly to the sheets and reading a mass of irrelevant material. Accordingly when investigations sheets were of such a nature as to lead to fairly definite conclusions, analysis cards were made showing the chief interrelations, with written statements of the conclusions reached and any data or guesses justified by the evidence. In many cases it was possible to determine the probably part of speech. The analysis card of 1715 follows;

1715 301

1715 1014, 3 times, twice with 7428 following.

Note-

6715	1014	2428
1715	2772	twice-6715 same
1715	4332	once-6715 same twice
1715	9928	once-6715 same
1715	8873	9346-twice

Note-

6715	8384	9346
1715	1593	once-6715 same
1715	9157	once-6715 same twice

Syllable with variant _a_ because follows page 14

When the analysis cards were definite enough to lead to a positive identification, the tentative vocabulary file was started which later became the identified file. These tentative cards had absolutely no foundation in actual fact but were often pure supposition based upon impressions. Far from considering them as final we welcomed any opportunity to approach from another angle and prove or disprove the theory. Many groups would thus be candidates for several possible meanings. The tentative cards were a device to narrow down the possibilities and furnish a basis for elimination.

At this point the comparison of the various series was seriously begun in order to find the method of correlation of the different encipherments and thus make available for use all data obtained. A knowledge of the system would also, we thought, enable us to construct the original book and give us the alphabetical placing of all groups in all codes. The following tabulation of D-8885, series 229, shows considerable similarity to Z-0049 in that it is large and varied and never after punctuation, although the fact that D is a smaller series brings out a larger number of smaller connections in the same space. The fact that a variant 3885 is also found, adds further evidence to the identification. The definite breaks between two or three large connections and subsequent large number of small connections are not so good here, however, as to make theidentity sure.

Investigation Sheet D-8886

1.	8181	0126	D-62		Bd	1736	6363
2.	1729	1738	D-12	p2	Bl	2796	5677
3.	0737	6492	D-4		As	2796	5756
4.	3648	5256	D-62		Bu	2796	4426
5.	5548	8809	D-34		Ap	2796	0538
6.	4326	2796	D-66		Bi	8104	0438
7.	2059	2796	D-77		Bg	6784	1823
8.	6219	3368	D-79		Bx	6981	2894
9.	6219	5737	D-35	p2	AJ	0756	8942
10.	5737	9684	D-4		An	3256	4326
11.	7314	1138	D-80		BJ	5259	1219
12.	7885	3310	D-37½		Bn	5259	2987
13.	3310	0005	D-58	p2	Ay	4836	2892
14.	5924	5241	D-58		Ay	7039	7022
15.	6580	7587	D-60		As	2307	2059
16.	9642	7587	D-58	p2	As	7744	0756
17.	2868	8362	D-12	p3	As	4564	8679
18.	2868	0024	D-62	p2	At	3885	1125
19.	2868	5532	D-20		Bm	0737	6925
20.	2868	3861	D-85		Bg	4768	8216
21.	2263	5431	D-84	p3	Bl	2868	9575
22.	9651	0737	D-79		Am	8736	6109
23.	2616	5738	D-58	p2	Af	8736	6109
24.	0548	5438	D-40½		Bg	8736	1509
25.	0436	0338	D-84		Ag	6560	1509
26.	1509	5707	D-62		Ap	1785	1706
27.	1158	3783	D-80	p2	Af	3768	0651

28.	1331	3198	D-34	p3	As	4768	8148
29.	7301	6725	D-75		Af	5720	3761
30.	3924	6311	D-64	p2	Bg	3661	5436
31.	1928	1342	D-71		Ag	3661	0638
32.	1928	1342	D-64		Ag	3661	0638
33.	6928	1342	D-60		Al	3661	0638
34.	6051	8145	D-85	p2	Av	5608	5338
35.	9630	1176	D-68		Ae	5608	6161
36.	3457	0638	D-13		Ah	5608	5925
37.	1125	5608	D-66		Bs	8519	1593
38;	5548	1359	D-62		Bo	1125	0741
39.	0024	8885	D-62	p2	Au	1125	2087
40.	2087	3685	D-72		Bl	6038	7044
41.	0658	6038	D-43		Af	7044	4883
42.	2087	3685	D-61		Ak	2307	8328
43.	7087	0260	D-59		Ao	6038	2307
44.	7087	9636	D-58		Bx	8216	0418
45.	5747	0172	D-84	p2	Br	9404	7087
46.	3685	6948	D-82		Bm	7481	2734
47.	1823	2734	D-77		Bk	1928	9946
48.	22903	2920	D-80		Ac	2734	5913
49.		22979	D-42		Ab	2834	6038
50.		23956	D-22		Ab	2834	3571
51.	5465	9512	D-84	p3	As	1928	0130
52.	3163	2322	D-48		Av	0130	1725
53.	5574	8605	D-9		Ah	6580	1725
54.	9807	1387	D-67		Ae	6580	4000

The definite alignment of the frequencies intotwo or three large connections combined with a very large number of small but often interlocked relationships is more or less vaguely discernible but not distinct enough to justify a final decision. Nevertheless we are able to deduce various positive and negative concdusions, of a doubly hypothetical nature however, because they are probable only with the proviso that D-8885-3885 is an . Among other things we notice:

(1) 2796 follows directly four times, precedes directly twice, and follows one removed once. Theonly similar cases in Z-0069 are (a) 2428 which follows directly eight times, precedes directly twice, follows one removed once and precedes one removed twice; (b) 9157 which follows directly five times, precedes directly once, and follows one removed twice. Consulting the frequencies we see that D-2796 occurs nine times, while Z-2428 occurs one hundred sixty-four times and Z-9157 sixty times. Comparing the punctuation groups already known to be identical we find D-6038 with frequency of thirty-one and Z-6914 of thirty-six, which circumstance renders extremely improbable any connection between 2796 and either 2428 or 9157.

(2) The following combination offers possibilities although Z has no parallel in the 0069 sheets;

2087	3485	D-61		Ak	2807	8528
7087	0260	D-59		Ao	6038	2807
7087	9636	D-58		Bx	8216	0418
5747	0172	D-54	p2	Br	9404	7087
3485	6948	D-82		Bm	7481	2734

The frequency of 2087, 18 and of 7087, 15, shows that we have another important variant. Looking through the Z's for a similar one we find that the largest variant besides 0069 and the a's is Z-8011-5011; therefore we compare the two:

Investigation Sheet D-7087-2087

1.	4674	6038	D-41		Ar	6556	1750
2.	3230	6038	D-12½	pl	Ap	9135	8932
3.	0638	6038	D-61		Ai	3685	8885
4.	4674	6038	D-44		Ay	1125	End
5.	8885	9804	D-34	p2	Bt	1861	0782
6.	3885	1125	D-62	p2	Aw	7972	6219
7.	8679	3685	D-59		Am	0260	3885
8.	2584	7643	D-72		Bj	3685	8885
9.	8344	2584	D-12½	p2	An	9135	0757
10.	9007	1939	D-58		Bv	9636	8885
11.	3783	0338	D-47		Bm	8734	2498
12.	3134	0338	D-84		Bm	4490	1771
13.	5684	0338	D-83		An	1771	4282
14.	2087	0338	D-85		Bg	4490	5067
15.	9924	6939	D-84	p2	An	5067	8784
16.	0338	1601	D-82		Be	0260	2210
17.	9135	0438	D-80	p2	Ap	0756	2673
18.	7883	0438	D-38		Ag	9642	7087
19.	7087	9662	D-38		Ai	0260	7039
20.	2894	4599	D-14		As	7548	0438
21.	1509	8852	D-57½		Ad	1928	1342
22.	1509	8852	D-66		Ad	1928	1342
23.	1509	8852	D-72		Ad	1928	1342
24.	1509	2702	D-73		Ad	1928	1342
25.	1509	2702	D-12½	pl	Ad	1928	1342
26.	1509	2702	D-62		Ad	1928	1342
27.	1509	2702	D-69		Ad	6928	1342
28.	1509	2702	D-61		Ad	6928	1342
29.	6109	2702	D-82		Ad	6928	1342
30.	22978		D-42		Ab	2702	0638
31.		22994	D-71		Ab	2702	1509
32.		22990	D-64		Ab	2702	6109
33.	1568	2442	D-40		Av	6556	1509

(30 unrelated cards)

Investigation Sheet Z-8011-3011

1.	4660	0814	Z-80		Bm	4080	0603
2.	4660	0814	Z-59		Bp	4080	0603
3.	9905	1114	Z-66		Ae	9655	2428
4.	9822	1114	Z-85		Br	7209	7859
5.	1114	4482	Z-66		Ay	3788	0190
6.	1472	9446	Z-67		Ax	2428	5914
7.	7685	9006	Z-86		Bi	1984	0214
8.	1096	5846	Z-64	p2	Ab	2772	0314
9.	3384	3781	Z-11		At	1293	9549
10.	2048	3781	Z-23		Ai	1261	7332
11.	6648	3781	Z-62		An	1261	1732
12.	0437	0806	Z-81		Bn	3374	0603

13.	0437	1577	Z-40		Ap	6560	2879
14.	5675	4379	Z-4		As	6340	8010
15.	0815	9652	Z-16	p2	Bg	6360	1419
16.	9516	5951	Z-16	p4	Bh	0868	0482
17.	4088	3522	Z-200	p2	An	0848	0468
18.	3681	4668	Z-2		Be	6785	0368
19.	3681	4668	Z-10		Bn	6785	0868
20.	9157	7907	Z-16	p5	Bg	9157	3775
21.	0282	4551	Z-168		Bj	9157	8406
22.	5010	8767	Z-23		Bn	4695	0069
23.	5214	3283	Z-103	p2	Ab	9698	0069

(15 unrelated cards)

Although the correspondence is not especially good in detail, we are reassured by several considerations:

(1) There is an identical proportion of large and small connections and of related and unrelated cards.

(2) The wide variety of use is itself an argument in favor of the identity of the groups in case they represent de, para, por, or con.

(3) The use of 0814 in the Z chart, lines 1 and 2 is parallel to that of the D punctuation groups 0538 and 9438, lines 11, 12, 13, 14, 17 and 18 in the D-7087-2087 table. Also Z-5214, line 23, has the same relation to Z-8011 as D-0538 has to D-7087 in line 16. Finally Z-1114 occurs immediately before and one removed before Z-8011 in lines 4 and 5, an arrangement identical to that of D-0358, lines 14 and 16.

(4) The D passages containing 1509, 8832, 7087, 1928 and 1342, lines 21-29 inclusive, although they have no good parallel in

Z are suggestive of set phrases containing one of the prepositions of our hypothesis, especially in view of the fact that the D indicator number is less widely used than the Z and therefore must have a more highly specialized vocabulary.

With these outstanding characteristics of Z-0069-5069, D-8885-3885, D-2087-7087 and Z-8011-3011 in mind, we try the C's (101) just ready at this point, in which series we have already made tentative alphabetical identifications by working with introductory phrases. The variants of C (101) appear as follows;

Code Groups	Frequency	Code Groups	Frequency
1224	9	6224	5
2045	15	7045	13
0751	19	5751	6
2070	2	7070	61
2170	5	7170	32
2871	2	7871	33
2971	25	7991	3
0741	23	5741	13
4989	27	9989	2
3892	1	8892	14

We have already accounted for 2070-7070, 2170-7170, 2871-7871, and 2971-7971, and therefore choose the pair next largest as a tentative on. The space between 4139, dog, and 0741-5741 as a possible on appears abnormally large in the dictionary for an interval of only two pages, and so we examine the sheets to try to add strength to the theory.

Investigation Sheet C-0741-5741 (Condensed)

1	2076	2070	CC-27	p3	Ax	4212	6127
2	7070	6729	CC-27	p3	Bl	7981	7463
3	7375	0527	C-23		Aj	7259	7070
4	7170	6897	C-5	p3	As	1522	7912
5	2380	7170	CC-21	p3	Ag	1894	8753
6	7870	5924	C-26	p2	Bg	6362	7996
7	9176	8743	CC-3		Am	9248	9610
8	9266	6476	CC-23	p3	Bn	9248	3705
9	2386	8696	CC-24		Bs	9248	0797
10	6325	8696	CC-18		Bx	1520	6582
11	7669	8696	C-26		Bb	1530	2045
12	7170	5717	C-12		Be	8696	8926
13	7802	6025	CC-27	p3	Ab	8696	0562
14	6832	0915	CC-21		Ao	8696	6664
15	7375	2989	CC-27		Bp	8696	7045
16	0141	4648	C-4		An	9223	8696
17	3331	4648	C-28		An	9223	4160
18	7229	9239	CC-13		Bs	9223	7176
19	6293	7170	CC-21	p6	Aa	1530	3553
20	6293	7170	CC-20	p6	Bb	1530	3553
21	7971	4341	CC-28	p2	Bv	5751	2662
22	3796	1525	CC-15		Ao	5751	6540
23	0104	6253	CC-20	p5	Ah	5751	4183
24	2604	1096	C-30		Bx	5751	0153
25	7631	8104	C-23½		Aw	0751	0153
26	0675	6890	C-12	p3	An	0751	6103
27	0783	0932	C-12	p3	Bm	0751	6103
28	2851	7669	C-12	p2	Bw	0751	7889
29	2283	9527	C-0		An	0751	0057
30	0301	7045	C-12	p2	Aa	0751	2851
31	8696	8969	CC-20	p5	Bt	7349	7676
32	6832	1376	CC-24	p2	Am	7349	3023
33	8696	7070	C-20		Ar	6559	1462
34		10140	C-10½		Ab	6559	1462
35	7669	8696	C-26		Bb	1530	2045
36	0301	7045	C-12	p2	Aa	0751	2851
37	2045	0607	C-19		Aq	0741	2283
38	2045	7649	C-1		Ak	7752	9985
39	7375	2989	CC-27		Bp	8696	7045
40	9256	8696	CC-15	p2	Ab	9541	7045
41	0607	5741	C-19		Ar	2283	5388
42	9672	9481	CC-22		Ao	2283	7658
43	2869	2293	CC-8½		Ag	2283	7658

(30 unrelated cards)

Examing this for en, we notice among other things:

(1) The relative percentage of unrelated cards is approximately the same as that of Z-0069 and D-8885.

(2) The way in which the punctuation falls in the vicinity of all three is analagous:

Z-0069

0314	4109	Z-1026	p2	Aq	5901	1005
7343	0314	Z-26		Af	6434	7311
6720	0314	Z-56		Bw	8873	2085
0362	4555	Z-1204	p2	Ad	6720	0314
0214	1377	Z-1029	p4	Bb	5958	4328
0693	0214	Z-1201		Ba	3384	3392
0457	9080	Z-29		Ba	7701	0214
7793	5102	Z-1243		Aw	6643	5914

D-8885

3657	0638	D-13		Ah	5608	5925
1928	1342	D-71		Ag	3661	0638
0436	0338	D-84		Aa	6560	1509
5548	8809	D-34		Ap	2796	0338
2087	3685	D-72		Bl	6038	7044
	22979	D-42		Ab	2834	6038
0638	6038	D-43		Af	7044	4283

C-0741-5741

7070	6729	CC-27	p3	Bi	7981	7463
8696	7070	C-20		Ar	6569	1462
7170	6897	C-	p3	As	1522	7912
2360	1170	CC-21	p3	Ag	1894	8763
7229	9289	CC-13		Bs	9223	7170

The most important fact here is the failure of punctuation groups to fall immediately after the prospective en, except 6038 and 5914, which were called quotation marks identical with AB-4014 in the study of intervals (see page 25).

(3) C-8696 is used in the same way with C-0741-5741 as Z-2428 is with Z-0069 in that:

(a) It has the same relative position in each cases as:

Z-69		Bf-0069	2428	1081
C-12		Be-5741	8696	8926
Z-72		Ag-0069	7207	2428
C-4		An-5741	9223	8696
Z-202	p2	An-2428	0069	0887
C-26		Bb-8696	0741	1530
Z-90	p2	Ak-2428	9699	0069
CC-20	p5	Bt-9696	8969	5741

(b) It follows C-0741-5741 directly five out of eight times. Z-2428 follows Z-0069 directly eight out of thirteen times.

(c) It acts as a common center, from which branch out new series of interlocking group formations. For example, in lines 15 and 36 it leads into C-7045 which with its variant, C-2045, occurs in both positions before C-0741-5741 and one removed after, but never immediately after. With this is frequently associated 1530 (lines 10, 11, 19, 20) which also often follows the original C-0741-5741. Similarly Z-2428 allies itself in several distinctly differentiated relationships, notably with 1081 (whose variant, 5081, exists but does not appear in this tabulation) which falls one removed after and one removed before, but never immediately after the central group. 1081 is itself the center of other alliances starting with 9029, 5770, etc., lines 13 and 21, page 36.

(4) Certain other high frequency groups besides C-8696 follow the central group almost exclusively in common with others in D and Z which exhibit the same tendency in relation to D-8885 and Z-0069. A few instances are: C-0751-5751 follows C-0741-5741 directly twelve times and does not occur elsewhere in the tabulation; D-2796 follows D-8885 directly four times out of seven, D-3661 follows directly in every occurrence and does not occur elsewhere. Still better examples are Z-9157 which follows Z-0069 five times out of seven, and Z-0868 six times out of eight.

As a result of the foregoing processes and others growing out of them, we conclude that the correspondence is good. Consequently in view of the fact that the alphabetical sequence is possible, C-0741-5741 rises sufficiently in the scale of probability to warrant a tentative vocabulary card. We should next work backward on the basis of C-4139, C-4337 and C-1730 (see pages 34 and 35) to find *dos*, *dies* and *quarenta* in the 255 and 229 series. (These branch operations cannot be followed chronologically because they were simultaneous and closely interwoven).

Continuing our direct line of thought, the two next largest variants, 4989-9989 and 2045-7045, of almost equal frequencies, are candidates for *de*, *por*, *para*, *con*. 89 has no alphabetical guide and 45 is near 0346, *seis*, so we are without guidance except for the fact that if 4989-9989 is *para*, 3892-8892 is at a good distance for *por*. That leaves the large 2045-7045 for *de* which is evidently impossible, but lines 35-40 inclusive of the C-0741-5741 sheet containing 2045-7045 show remarkable similarity to lines 42-45 inclusive of D-8885-3885, in which 8087-7087 gave rise to the whole search for de, para, por or con, again leading us to suppose that we are dealing with some common preposition. With the issue thus confused we have recourse to the sheets. C-4989-9989 offers nothing of value except the closely related sequence following:

8622	3476	C-20		bf	7771	1167
8622	3476	C-8		As	0161	2888
7070	9816	C-9	p2	Ak	0161	6121
7070	9816	C-9	p2	Bg	9405	7970
7669	9816	C-9		Bl	8497	6121
9816	1216	C-9		Ba	9651	6121
1216	8662	C-9	p2	Aa	9651	3844

The only other connections are four cases with 7070 and one small relation of three. The number of unrelated cards is more than double the number of related. The only element to strengthen our position is the fact that the closely related sequence above calls to mind that on the sheets of D-2087-7087 there is only one interlocking series of relations of any consequence, i.e., lines 21-32 inclusive, page 45.

We go on to the second candidate, C-2045-7045, which is at once disqualified for a preposition by the following references from the investigation sheet:

1	8331	3272	C-16		Ba	0893	7871
2	3892	6196	CC-22		Bd	9911	7871
3	9829	9779	CC-8	p2	Bl	3175	7871
4	0751	0930	C-24		As	1704	7871
5	0707	0788	C-22		Al	5279	7071
6	8132	9073	C-12	p2	Bm	4624	7871
7	9761	0159	C-4		Al	9911	7871
8	6103	7070	CC-24	p2	Bb	8253	7971
9	6056	7070	CO-21	p5	Ay	7881	7971
10	8096	9654	C-12		Bo	2971	0761

11	7871	7070	C-26		Ba	0992	8597
12	2971	6460	C-4		Bt	6146	2994
13	6381	7870	CC-13	p2	Ae	5955	3821

Here the predominant occurrence of two of the a's on page 71 of our previous tentative identifications (page 30) in the second place to the right of 2045-7045 indicates that the preceding groups 0893, 9911, 3175, etc., must be verbs. (This isone method of determining parts of speech, see page 40). 2045-7045 must therefore be a pronoun, evidently se to fit in before siete, 7947. This is confirmed by the construction "la - verb - se" in line 12 and by the occurrence in line 11 of a verb of the first conjugation in the third person singular present followed by a comma, and another verb with the reflexive pronoun. The elimination of 2045-7045 also lends more probability to 4989-9989 as para.

As a result then of this comparison of C, we have entered 0741-5741 and 2045-7045 as en and se in the tentative vocabulary and accept 4989-9989 and 3892-3892 as probable for para and por, thus opening a new alphabetical sequence.

We carried out this process (which it is unnecessary to follow in all its ramifications) in a variety of connections without being able to accomplish our object of discovering enough identical pages to establish the system of interlocking blocks. As a result of these fruitless efforts we abandoned all treatment of the small series in favor of the large indicators, chiefly 301, in which there was a larger field and less wasted effort in tracing scattered words.

With work thus concentrated on 301 we continued the consideration of the characteristics of the different parts of speech begun by the study of the characteristics of prepositions, page 38. The conjunction y was an object of early speculation. A casual observance of 1899 and 6899 in the 301 series, and 2813 and 7813 in the 249 suggest that they were variants similar to 0059-Z and 1715-Z, perhaps e or de, the latter of which was giving us especial trouble. An examination of the table, however, proved that these two were of an entirely different character from the prepositions and probably identical:

Investigation Sheet AB-1899-6899 (Condensed)

6521	0555	AB-89		B1	0214	0732
3195	0314	AB-94		Aj	7048	9600
4348	0314	AB-43½		Ax	5239	6915
9754	2886	B-10		Aw	2562	0514
5049	0314	B-31	p2	Ar	8684	4456
0683	7460	B-37		Au	6014	1126
7232	0213	AB-134	p3	Av	4666	5133
3959	5149	AB-136	p2	Ab	1093	2043
8344	0802	AB-40		At	3443	4321
2355	7182	AB-44		Al	6924	5820
5822	9003	AB-45		At	7432	1899

Investigation Sheet E-2813-7813 (Condensed)

7106	0024	E-624		Bb	0024	8500
7318	0024	E-511		Ay	6269	6345
2266	0624	E-550		Bc	0024	3460
0526	4524	E-612	p5	Ar	1165	0596
0563	4524	E-612	p2	Ay	9815	1472
4324	0360	E-549	p4	At	9664	8382
2809	1837	E-22½		Ab	4324	3896
2558	3637	E-519		Bj	8608	2813
1165	8596	E-510		Az	8623	----
1866	0679	E-595	p2	Bw	3896	1999

In this case there are almost no interconnections. Ab-1899-6899 has no associations except with the punctuation groups ending in 14. E-2813-7813 manifests the same tendency but occurs twice with 1165 in varying positions; It is also one removed from itself in E-519 Bj. It is reasonable to suppose that these groups may be y since that conjunction is naturally the most common word used in a variety of ways and not in groups of recurring combinations as observed previously. Their occurrence immediately after punctuation groups, assumed to be commas, is also exceedingly good, as "_____, y _____ _____". The position "_____ _____ y _____" is also good. If E-0024 and Ab-6014 are quotation marks, the theory also holds in cases such as "0024 _____ _____ 0034 y 0024 _______ 0024", in which y connects two names quoted.

In this connection, we made investigation sheets of the groups inside the quotation marks in the effort to identify spelling groups. The groups Z-0290 and AB-3195 or 3296 were very frequent with punctuation groups especially Z-5914 and AB-6014. Therefore we again made sheets to see to what extent this was true.

Investigation Sheet AB-3196-32960

	301	A-28-1/16 (3296)		Ab	6014	4556
	30192	B-97 (3296)		Ab	6014	6720
	301	A-6 (3196)		Ab	6886	0414
30141	8613	B-26 (3296)		Ac	6720	5411
30154	8613	B-2 (3296)		Ac	2501	1126
5950	3613	A-27 (3196)		Ap	6014	8020
6303	1093	B-17 (3296)		Ao	2987	6741
1703	6741	A-17 (3196)		Ax	8032	1978
3070	3469	A-5½ (3196)		Ah	6886	5414
7640	3026	A-7 (3196)		Ak	9640	1715
6126	3070	A-9 (3196)		Aj	6014	1715
2426	7408	A-10 (3196)		Au	6014	8020
8236	1150	AB-163 (3196)		Bo	6014	9056
1214	5241	B-44 (3296)	p2	Bu	6014	4556
8287	6314	A-13 (3196)		At	6014	5881

Investigation Sheet Z-0290

8327	7116	Z-221	Ae	5914	6258
8327	7116	Z-223	Ao	5914	6258
8327	7116	Z-222	Ao	5914	2692
0214	0868	Z-209	As	5914	6258
2788	5037	Z-174	Aq	5914	1261
0599	5650	Z-40	Ak	5914	9194
8392	4660	Z-64	Ax	5914	5728
6930	4660	Z-303	Bg	6446	1081
0942	9738	Z-204	Bw	2772	5914
1283	8788	Z-77	Ak	1114	2772
7551	1419	Z-99	Bo	6240	6224
4882	5314	Z-187	Ai	7126	5364

The fact that the AB groups, 3196 and 3296, were predisposed to appear as initial and that many of the telegrams in which they were thus used were short, together with the frequency of the quotation marks directly after both AB-3196-3296 and Z-0290 gave ground for the belief that we were dealing with the word vapor. The code groups inside the quotation marks would then be syllables spelling the names of steamers or, in the case of single groups, the names themselves. The plausibility of the theory is evident from the table below, in which the groups quoted follow AB-3196-3296 in each case:

SERIES E 2813-7813-Y

		0024	6895	0024	E-401	p6	Aq	0024	7173	0024	
0024	2262	6309	8336	0024	E-445		Bo	0024	0239	0815••••	0024
	0024	3102	3350	0024	E-107	p2	Ag	0024	7481	7885	0024
0024	3637••••	5825	0993	0024	E-175-1/8	p4	Ag	0024	3102	3350	0024
	0024	6280	0659	0024	E-472	p3	Ae	0024	3162	1872	0024
	0024	3162	6816	0024	E-266	p2	Aj	0024	7123	0024	
	0024	0533	1136	0024	E-485		Au	0024	6058	0024	
	0024	3483••••	7106	0024	E-624		Bb	0024	8500	3821••••	0024
0024	0550	3518••••	2266	0024	E-550		Bo	0024	3460	3978••••	0024

The identity of the spelling groups was determined early in the third amd final stage by utilizing lists of Spanish ships and their dates of sailing obtained by going through the Shipping Board files (see page 108).

A group which presented especial difficulties was AB-1703, of strikingly high frequency and of somewhat the same tendencies as Z-0069 and D-8885. Following the precedent of these and other groups it should have another variant, but the other high group on the page was 6303. The most surprising feature developed, however, from an examination of the investigation sheets of these two:

AB-1703

4112	3013	AB-162	p2	Bg	6990	8613
1126	9112	AB-163		Am	6990	6161
1388	1111	AB-157	p3	Bl	1590	6612
0277	9272	AB-178		By	1590	9471
1126	5665	AB-165		Ai	9640	8613
1126	5665	AB-186		Ag	9640	8613
5993	8874	AB-157	p2	Bt	8230	9671
----	----	--------------			----	----
4770	7423	AB-183		Ap	9633	9112
0675	1497	AB-154		Aq	6741	3282
----	----	--------------			----	----

AB-6303

5487	3737	AB-19	p2	Bj	6990	9112
----	----	--------------			----	----
0485	1111	AB-196	p2	Bw	1590	5070
9112	5665	AB-178	p3	Ar	9640	1126
----	----	--------------			----	----
5716	9636	AB-171		Bo	8330	5714
----	8174	AB-181		Ab	8330	7987
7927	4510	AB-141		Ar	9633	0314
0314	4110	AB-141		Bn	6741	0314
3741	6444	AB-176		Ah	6741	8305

Such parallel uses as those indicated by the underlined groups in
t
the partial tabulation above occurred repeatedly and forced us to conclude that a difference of 46 was used for variants as well as 50. A search in the 249 (E) series for a similar phenomenon revealed a parallel case in E 0945-6345:

E-0945

0330	3119	E-944	p2	Bf	3122	----
1100	7206	E-946		Bk	3122	0945
0921	0024	E-928		Ai	6585	1165
6910	2882	E-925		Bo	1667	5758
5245	3778	E-906	p2	Ba	9111	6785
0001	7508	E-910	p2	Bk	7010	1087
3637	6384	E-948	p2	Av	2712	1665
0925	4516	E-949	p2	Ai	0515	0858

E-6345

5829	4394	E-891	p3	Bd	3122	9724
9307	2762	E-911	p2	Bo	3122	0945
3485	0024	E-908		Ai	6585	1165
8962	2882	E-925	p3	Bv	1667	1694
1042	9091	E-925		At	9111	6785
0024	0947	E-921		Bo	7010	8902
4569	7350	E-911	p2	Ag	2712	7179
8549	0390	E-960		Bo	0515	3778

This identity was practically certain because of the very good parallels but the difference had now changed to 54. In the 253 (Z) cards still another pair of the same kind appeared, this time with the difference again 46:

Z-5037							Z-0437						
0069	9612	Z-815		Ai	5611	0314	0437	4975	Z-61		Bh	8019	0314
5037	4586	Z-331	p7	As	4586	5037	0069	7207	Z-876	p2	Ao	4583	5037
9104	2088	Z-860		Al	6282	0437	8201	1112	Z-61		Bf	4975	0437
4157	5461	Z-860		Bw	8788	0437	9157	6711	Z-201	p3	Ao	4332	0437
0437	4583	Z-876	p2	Al	5257	0437	0437	4332	Z-201	p3	Ae	4324	0069

Although these three identities were undoubtedly good and one was found in each of the three important series, an exhaustive search failed to reveal any more such pairs. In the smaller encipherments also, one such variant unfailingly appeared in the frequencies always with a difference either of 46 or of 54.

We could not understand these isolated pairs in a general system of variants 50 apart. Still the persistence of 46 and 54 as the only differences could not be accidental. Later experiments with arrangements of numbers on a hypothetical page showed that these differences are caused by the alternation of columns and that the interval is really the same. This is clear by writing in the word numbers of a hypothetical page:

0	50
1	51
2	52
3	53
4	54
5	55
6	56
7	57
8	58
9	59
10	60
11	61
12	62
13	63
14	64
15	65
16	66
17	67

If we place 17 in the left-hand column as in this case, 67 must fall directly opposite. The variant, 63, is thus four above 17 in the right-hand column and the interval is 46. Suppose, however, that 63 in the right-hand column is the original one of the pair; its variant must now be four above in the opposite column, namely 09, and the interval is 54, as is the case in the 249-E series. (Here we thought we had discovered an interlocking system of variants, because in 301 the variant is 1703-6303, in 249, 6345-0945, and that 09 would therefore appear as the first one of a pair in some other encipherment. No such correlations exist, however, and the case of A-B and E is probably accidental). In other words the apparent differences obtained by subtraction were false because when the original word occurs in the right-hand column, it is necessary to add 100 to the left-hand number and subtract the right-hand one in order to get the true difference. The actual number of code groups between AB-1703 and AB-6303 is evidently identical, namely, 45. This corroborated the idea first suggested in Method V111. (page 21) by the fact that the last two encipherments of 74 were identical and that the first two digits must be the ones re-arranged on the page. It has never been explained why such an isolated case should occur among the variants. If introduced to prevent detection of the code, other variations would naturally have been used also in place of a large number of easily distinguishable ones 50 apart. The following are the variants as they finally appear on 24 different pages.

301 VARIANTS

1703-6303	de	0662-5662	con
2004-7004	del	0769-5769	se
2912-7912	e	3070-8070	si
4112-9112	el	0675-5675	la
3613-8613	en	2276-7276	las
0314-5314	comma	3676-8676	la
0414-5414	period	2577-7577	los
1715-6715	A	4079-9079	me
1815-6815	a	2987-7987	para
1915-6915	a	1388-6388	pero
3222-8222	por	1590-6590	su
1126-6126	que	1091-6091	sus
2532-7532	ha	1899-6899	y
0839-5839	es		
3041-8841	esta		
1861-6861	como		

It is unnecessary to follow further the investigation made of every comparatively high group in the principal indicator series. Although we were able to establish identities between pages in several instances, we could not establish links enough to see any system. In addition, the task of comparison was so monumental that it delayed the development of the vocabulary. Consequently we decided to confine ourselves to 301 as the sole basis of investigation, and hoped by first getting a large foothold in 301 to find the system of transference not only from one encipherment to another but also from the original book.

The possibilities of such study can be seen from the following illustration similar to the experiments with 101, page 29, a part of the large chart of beginnings of A-B telegrams (received later) which alone would have been sufficient to break the code. The selection of cases from the chart was made on the usual basis of recurring groups, especially the period group, 0414, three or four removed from the beginning:

AB-46	5/22/18	566	301	5397	5876	8579	
AB-49	5/24/18	570	301	5587	4495	8579	
AB-98	8/5/18	762	301	5360	2119	0414	
AB-101	8/10/18	769	301	7014	0883	2119	0414
AB-102	8/13/18	774	301	5411	1703	2119	0414
AB-105	8/18/18	799	301	8709	3871	2119	0414
AB-107	8/21/18	803	301	8709	0883	2119	0414
AB-108	8/21/18	801	301	8709	0883	2119	0414
AB-112	8/28/18	820	301	5897	5470	2119	0414
AB-113	8/28/18	821	301	5597	5470	2119	0414
AB-115	8/29/18	826	301	5397	3871	2119	0414
AB-119	8/30/18	830	301	5597	3871	2119	0414
AB-121	8/30/18	831	301	5397	2684	2119	1213
AB-122	9/1/18	833	301	5397	0883	2119	0414
AB-131	9/6/18	843	301	9011	9870	0414	----
AB-144	9/20/18	901	301	8709	2674	9870	----
AB-153	10/18/18	1001	301	8709	3871	1384	0414

Here it is apparent that 2119 is the only group common to the August telegrams and therefore equals agosto since we already know that 15 is the first a page. I f such is the case, 1703 in AB-102, occurring before 2119, is fixed as de and the long uncertainty ended in regard to 1703-6303. We are now in doubt whether 5411 preceding 1703 is doce or trece. The actual date of the telegram is the thirteenth but doce is better in the alphabetical sequence after 1703 - de. The decision is made in favor of doce, however, by the fact that 8709 must be dies since it begins to appear as soon as the dates go above the twelfth of August. Accordingly we shift our attention to 8709 and make sheets as follows:

Investigation Sheet AB-8709

1283	4160	AB-142		Ao	3871	0414
3669	4112	B-17		Bp	3871	5714
5901	9112	A-26		Al	3871	----
8615	8980	AB-196		Bf	3871	----
4443	9112	B-221		Bp	3871	8579
9112	5725	B-102	p2	Ab	3871	1899
0683	9112	B-102		Bi	3871	0314
8727	0426	AB-32		Ae	3871	0192
2684	1899	AB-23		Bd	3871	8615
0499	0448	B-2	p1	Ah	3871	5110
6576	8980	AB-81		Ao	3871	1602
0465	1827	AB-48		Ad	3871	4417
1001	301	AB-154		Ac	3871	1384
799	301	AB-105		Ae	3871	2119
1448	7009	A-62	p5	Bw	5470	7577
6214	8980	B-1	p1	Be	5470	0033
5360	9680	B-85¼		Av	5470	8880
5891	1703	B-85½		Ao	5470	8889
0362	6303	AB-147		At	5470	2004
1283	8683	B-205		Af	5470	0414
1283	8683	B-207		Af	5470	0414
7969	4732	B-31	p2	Bn	5470	5049
7305	1915	B-82		Aw	5470	1130
7305	6915	B-82	p2	As	5470	1130
9112	7009	A-62	p7	Bh	5470	0414
5414	9112	A-40		Bj	5470	6575
4177	5707	B-106		Aw	5470	6775
0692	6570	AB-59		Bh	5470	----
301	9112	AB-43		Ad	2684	9222
901	301	AB-144		Ac	2674	9807
8327	9633	B-131		Am	2684	0314
9112	7009	AB-146	p2	Aw	2694	4417
7043	1088	B-2	p1	Aq	2684	9640
3469	5975	A-6		Aj	2684	----
6824	8613	AB-52		Aw	2684	6279
6369	8029	AB-23		Bs	2684	6899
1899	3784	AB-54		Bi	3684	1703
0692	1703	B-114		Ax	2684	2004
801	301	AB-108		Ao	0883	2119
803	301	AB-107		Ao	0883	2119
1703	9640	A-28-1/32		Aw	0883	8615
3469	9363	B-102		An	0883	1703

Four groups only follow 8709, namely 3871, 5470, 2684 and 0883, and must represent numbers below ten. The first ten Spanish numerals fall into the following alphabetical sequence:

cinco	dos	nueve	seis	tres	uno
cuatro		ocho	siete		

Therefore, if the numerical sequence corresponds, 5470-3871 and 0883-2684 probably mean cinco-cuatro, nueve-ocho or seis-siete. Examining the first chart again, we see that 2119 is replaced by 9870 for setiembre when the September telegrams begin. In that case 5470-3871 are seis-siete. Again 1384 follows 9870 as Octubre, placing 0883-2684 as nueve-ocho. 9011 in AB-131 must be dos if 8709 is diez because doce, the only other possibility is already accounted for. By following out these new hypotheses an endless chain of assumptions is possible, and we already have a rough idea of the block system:

09	-	d	70	-	s
10	-	d	71	-	s
11	-	d	83	-	n
19	-	a	84	-	o

All these lines of investigation were interrupted by the reception of the telegram leading to the solution of the code in a much quicker way.

In addition to the study of the numbers themselves made during the intermediate period, we searched the files at the State Department to obtain information concerning possible subject matter. In order to facilitate the utilization of this material, we made for all telegrams date cards indicating the source, destination and classification in office files:

12/13/17 - (1413) 253 From Polo to Madrid 24 s

The letters l, m, or s indicate long, medium or short. These date cards were compared with the data obtained and any promising telegrams carefully analysed in the effort to determine their character. All groups in these telegrams singled out for analysis were studied to see their connections in other telegrams, whether they were used generally or only in asspecial group of telegrams between certain places. Spelling groups were noted most especially and their presence in other connections traced.

The following notes of coincidences found later proved that every outside source should be utilized to the utmost in connection with the analysis of codes. In the State Department files, 763.7219/2710 #7102, is a letter dated November 14,1918 from the Spanish Ambassador in Washington regarding orders received from the Spanish Government to communicate the policy of the new Spanish Cabinet. On November 13,1918, a long cablegram SA70, 500 8SD, with many unusual words and new spelling groups was received by the Spanish Embassy from the Spanish Foreign Office. The value of this discovery is evident from the following parallel:

763.7219/2710
#7102 From Riano
to State Department
November 14, 1918.

"Por order de mi Gobierno communico que al presentarse en el Congreso de los Diputados el nuevo Gobierno Espanol presidido por el Sr.Marques de Alhucemas, sin la asistencia del Ministro de Estado, Sr. Conde de Romanones que no pudo encontrarse presente en el acto por estar enfermo con fiebre, el Presidente del Consejo de Ministros expuso que la politica exterior del Gobierno que presidia esta orientada en intima inteligencia con las potencias occidentales de Europa y con los Estados Unidos. Se presentaron dos proposiciones incidentales de redaccion distinta pero de finalidad identica, felicitandose por el termino de las hostilidades y por ver alborear la luz de la justicia sobre la fuerza, base de la libertad y de la fraternidad entre los pueblos. Fue aprobada la segunda de las referidas proposiciones que apoyo el Sr. Hontoria, obteniendo solamente dos votos en contra. El Gobierno de Su Majestad al encargarme ponga lo que antecede an conocimiento de los Estados Unidos me dice tambien que su deseo es que llegue a conocimiento de las Camaras Americanas el casi unanime sentimiento del Congreso Espanol que ha evidenciado con su voto la fervorosa simpatia que siente hasia los pueblos y Gobiernos aliados"

Cable from Madrid to
Washington, November 13, 1918
SA70, 5008SD.

"301. En el Congreso al presentarse el nuevo Gobierno (sin mi presencia por encontrarme en cama con fiebre) Presidente de Consejo expuesto que politica exterior nuevo Gobierno esta orientada en intima inteligencia con potencias occidentales y Estados Unidos. Se presentan des proposiciones incidentales de distinta redaccion pero de finalidad identica, felicitandose del tormino de las hostilidades y de ver alborear el reino de la justicia sobre la fuersa base de la libertad y fraternidad entre los pueblos. Fue aprobada la segunda de las referidas proposiciones que apoyo Senor Hontoria, obteniendo solamente dos votos en cont quedo evidenciado que el casi unanime sentimiento del Congreso Espanol es de fervorosa simpatia hacia los pueblos y Gobiernos aliados. Tengalo asi presente y hagalo saber a ese Gobierno para que llegue a conocimiento de esa Camara."

Romanones

An even more marked case of the failure of the Spanish Ambassador to make any attempt to safeguard his Government's diplomatic code was found in the case of a letter written by him to the State Department on November 15, 1918 (763.72119/2702 #7130) in regard to a speech made in the Spanish Cortes by Sr. Gimeno, former Minister of State, speaking in favor of the Allies. The parallels follow:

Letter from Riano to
State Department,
November 15, 1918
763.72119/2702 #7130

"Por ordem de mi Gobierno y rogandole tenga a bien ponerlo en conocimiento de las Camaras Americanas, tengo la honra de comunicarle que en la sesion del Senado Espanol el Sr. Gimeno, Ministro que fue de Estado, pronuncio un brillante discurso encomiando a la pas y dedicando palabras efusivas a todos y cada uno de los paises aliados. Despues de breve discusion el Senado acordo por unanimidad conste en acta que se felicite por la pas y el triunfo de la justicia sobre la fuersa."

Cablegram from Madrid to
Washington, November 14, 1918
SA 71, 5009SD.

"43 301. En la sesion del Senado Senor Gimeno Ministro que fue de Estado pronuncio brillante discurso encomiando la pas y dedicando palabras efusivas a todos y cada uno de los paises aliados. Despues breve discusion el Senado acordo por unanimidad conste el el, acta se felicite por la pas y el triunfe de la justicia sobre la fuersa. Sirvase ponerle en conocimiento de ese Gobierno para que llegue al de esa Camara."

Romanones

On November 16, 1918 Riano wrote to the State Department (85500/48 #7149) in regard to the serious situation in Belgium, and incorporated in his letter the following text of a cablegram received from his Government on the same day (SB-127, 5178SD.)

"****** la situacion alli es desesperada. Soldados Bolchevistas procedentes del frente y otros llegados de Berlin con objeto de hacer revolucion han desposeido Principe Ruperto de Baviera al Gobernador y a todo su Gobierno, constituyendose como tal y pretendiendo dar el poder a los mas extremos anarquistas Belgica. Ministro de Espana Bruselas ha despachado un emisario para que atravesando las lineas informe al Ministro Belgica y Estados Unidos de que lo unico que puede salvar situacion antes de que el pueblo fraternice con Bolchevistas es que marchen immediatamente Aliados sobre Bruselas pues de lo contrario considera seguro gravisimos desordenes. Principe Ruperto de Baviera abandonado por sus soldados y Duque Alberto de Baviera se han refugiado en Legacion de Su Majestad pidiendo proteccion del Gobierno hasta que puedan pasar a Habana o lleguen a Bruselas los Belgas."

Again on November 18, 1918 Riano wrote to the State Department (763.7214/4179 #7172):

> (Translation) "I have just received a telegram from the Minister of Foreign Affairs of Spain informing me that the "Union for Relief of Prisoners of War" of Vienna has telegraphed to His Majesty that hundreds of thousands of relatives of prisoners of war in Siberia and Turkestan appeal to him for the salvation of these prisoners who are in a serious situation in consequence of the armistice and who are urgently in need of clothes, food, medicine and fuel etc. He begs the President to cooperate in relief."

Cablegram SB-129 5177-SD from Madrid to W ashington, dated November 17, 1918, reads:

> "La Union de Socorro a Prisioneros de Guerra de Viena ha telegrafiado a nuestro Soberano, exponiendole que cientos de miles de amigos de los prisioneros de guerra que estan en Rusia, Siberia y Turkestan le ruegan la salvacion de los mismos en grave situacion por consecuencia del armisticio y solicitan apoye Su Majestad para que obtengan ropa, alimento, medicamentos y cumbustibles que sus familias no pueden enviarles. Sirvase participarlo a ese Gobierno expresando el vivo interes de Su Majestad porque se tome en cuenta en la medida de lo posible la situacion de dichos prisioneros de guerra en los trabajos de organizaciones de socorro que se estan autorizando."
>
> Romanones

On November 22, 1918, the Spanish Embassy wrote to the State Department (340.521 #7211) regarding the protection of the interests of Spanish subjects in occupied regions. Cablegram SB134, 5184SD, November 21, 1918, from Madrid to Washington, describes the situation and expresses the gratitude of the Spanish Government in precisely the same terms, i.e.,

"for any and all facilities which it does not doubt that the American troops of occupation will furnish the persons and property of Spaniards settled in the territories which the troops in question will occupy", etc.

A letter dated September 13, 1918, from the Spanish Embassy to the State Department says:

"The Minister of Foreign Affairs has telegraphed me extract of financial agreement signed in Spain August 29,1918 by Mr. Norman Davis, special financial delegate of the United States, and the Bank of Urquijo and Bank of Barcelona, Article V. of this agreement" etc.

Compare E-283, 5607SD, San Sebastian to Washington, Sept. 10, 1918:

"Reservado. El veintinueve de agosto se firmo entre Mr. Davis, como delegado especial financiero de Estados Unidos y el Banco de Urquijo y el de Barcelona, un acuerdo," etc.

On October 14, 1918, the Spanish Ambassador transmitted to the American Government (763.72119/2552) Turkey's request for an armistice contained in E-411, 5793SD, Madrid to Washington, October 13, 1918:

(Translation) "I have just received a note from the Charge d'Affaires of Turkey, dated yesterday the eleventh, a translation of which follows: 'The undersigned, Charge d'Affaires of Turkey, has the honor in accordance with orders received from his Government to request the Royal Government to communicate by telegraph with the Secretary of State of the United States to the effect that the Imperial Government begs the President of the United States of America to take upon himself the task of re-establishing peace, that he inform all the belligerent states" etc.

The Ambassador says on September 3, 1918:

"I submitted by cable to the Minister of Foreign Affairs your suggestion of August 21st, that any representations as to special circumstances invoked with the view that licenses which have been refused be reconsidered, be made to the representative of the War Trade Board in Spain, rather than direct to the War Trade Board in Washington through the intermediation of this Embassy and that I have received a cablegram from the Minister of Foreign Affairs informing me that your proposal is acceptable to the Spanish Government."

E-225½, 5856SD, Washington to Madrid, August 23, 1918, begins:

(Translation) "I have received today a note from the Secretary of State proposing to me that ***** licenses refused by the War Trade Board be reconsidered ***** the request be made not through the intermediation of this Embassy, but through the representative of the War Trade Board in Madrid *****" etc.

A communication of July 7, 1918 (852,001 A12/55 Confidential) treats of the plot to assassinate Alphonse XIII, giving details as described in SB-31,5051SD, Madrid to Washington, July 7, 1918;

(Translation) "Very urgent. The Chief of Police of Madrid has received a cable message apparently sent by the Chief of Police of Chicago on June 23rd, stating that secret correspondence found at the headquarters of a band of anarchists in Chicago shows that there exists a plot? to assassinate the King of Spain" etc.

On July 8, 1918, Mr. Willard sent to the State Department from Madrid (763.72114/3869) a copy of the note verbale from the German Foreign Office to the Spanish Embassy in Berlin, sent by pouch to the Spanish Minister of State by the Spanish Ambassador in Berlin;

"En reponse a la note verbale du 27 mai, le Department des Affaires Etrangeres a l'honneur de faire savoir a l'Ambassade Royale d'Espagne que le Gouvernement Allemand prend, avec satisfaction, acte de la proposition du Gouvernement des Etats-Unis d'Amerique en vue d'une conference, a reunir a Berne, ayant pour objet des questions concernant les prisonniers de guerre, et qu il est dispose a designer des delegues pour asister a cette entrevue" etc.

The same substance is contained in AB-72, 8049WD, Berlin to Madrid, June 28, 1918;

"****** the Minister of Foreign Affairs of the German Government receives with satisfaction the proposal of the Secretary of State of the United States in regard to a conference in Berne concerning prisoners of war and is disposed to appoint delegates" etc.

Lastly, on July 25, 1918, Riano transmitted to the State Department a message received from Polo, the Spanish Ambassador in Berlin, quoting information from the Berlin press regarding the death of Quentin Roosevelt (012/20982). This quotation is contained in SAB-89, 5714 WD, Berlin to Madrid, July 23, 1918;

(Translation) "The press publishes an official account of the death in an aerial battle of the aviator, Captain Quentin Roosevelt, who fell near Chambray mortally wounded by two bullet wounds in the head. He was buried with military honors in the same town. I am urgently requesting confirmation"etc.

The same with small changes came out in SE-119, 5385SD, Madrid to Washington, July 25, 1918.

The two phases of the work of the second period were then (a) the analysis of groups and group sequences; (b) the comparison of certain telegrams with data concerning the probable nature of their content. Through these means, the meanings of code groups and combinations were gradually crystallising.

This slow process was rendered unnecessary because the Spanish Foreign Office on November 24, and 25, 1918, sent out circular telegram No. 46 to Washington, Costa Rica, Panama, Santo Domingo and Lima. This message was encoded in four different ways, namely: to Washington and Costa Rica in 301, to Lima in 141, to Santo Domingo in 32, and to Panama in 74. The latter message was read by the 74 code book received from Panama.

By comparing 74 with 301, five words were identified definitely, namely gobierno, Alemania, contra, propiedad and solicitar. The identity of the other groups was obscured by sligh paraphrasing and the fact that the method of encoding varied, but by experimenting we were able to determine the parallels as follows:

CIRCULAR MESSAGE 46

		SY-15		SB-196	SA-72	SJ-9	SH-11
Series:		74		301-36	301	141	32
Date:		11/24/18		11/24/18	11/25/18	11/24/18	11/24/18
FROM MADRID TO:		PANAMA		COSTA RICA	WASHINGTON	LIMA	SANTO DOMINGO
	Gobierno	5602	Gobierno	8250	8250	5466	3297
	Aleman	3165	Aleman	5820	5820	2696	3906
	solicita	1500	(solicit-	3071	3071	7118	8048
	....		(a	6815	6815	2491	6211
	....	....	....	....	....	....	(ha-3435
	haga	5717	haga	5532	5532	1268	(ga-3201
	cuanto	4312	cuanto	5802	5802	1776	5989
	posible	0537	posible	0522	0522	6084	6856
	para	0289	para	7987	7987	4265	6512
	evitar	5172	evitar	1941	1941	7343	2658
	que	0827	que	1126	1926	7068	7203
	firm-	5387	firmado	5745	5745	1047	2986
	ado	3041	....	....	....	....	....
	armisticio	3377	armisticio	1550	1550	7724	4326
	se	1351	se	0769	0769	6711	7859
	(ad-	3041	(adopt-	2918	2818	9394	3688
	(op-	0151	(en	8613	3613	4105	2265
	(ten	1699	....	....	....	....	....
	....		en	3613	....	....	....
	....		Costa Rica	6701	....	....	....
	....		Nicaragua	3683	....	....	....
	....		Guatemala	8931	....	....	....
	....		o	5684	....	....	....
	....		Honduras	6433	....	....	....
	....		,	0614	....	....	....
	(au	3488	....		aun 5852	7327	4529
	(n	6976	....	....	....	....	....
	ahi	5129	....		7519	4096	3826
	medidas	6760	(medida-	0279	0279	6557	9405
	....		(s	1214	....	....	....
	(hostigacion-	5804	(hostil-	9153	....	4569	3591
	(es	5062	(es	1214	....	....	....
	contra	4203	contra	1365	1365	5630	5745
	Alemania	3165	Alemania	5820	5820	2696	3906
	o	0077	o	5684	1595	1062	9822
	contra	4203	contra	1365	1365	....	5745
	propiedad	0780	propiedad	5525	5525	0087	7086
	Alemania	3165	Alemania	5820	5820	2696	3906

By studying this analysis we saw that the 74 book had no interrelation with the other codes used, and that apparently 32 was alse independant. 6701, 3683, 8930 and 6433 occurred only in SB-196 to Costa Rica and the context ~~of~~ of the telegram pointed to the assumption of Costa Rica, Nicaragua, Guatemala and Honduras respectively for these groups. Arranging the identified words in numerical order, the alphabetical sequences fell into eight blocks with a probable ninth for 88 through 99:

AB-301

6701	Costa Rica
5802	cuanto
3613)	en
8613)	
0614	comma
1214	s
6815	a
2918	adopt-
7519	ahi
5820	Alemania
0522	posible
5525	propiedad
1125	que
8230	Gobierno
8931	Guatemala
5532	haga
6433	Honduras
9133	hostil
1941	evitar
5745	firmado
1550	armisticio
5852	aun
1365	contra
0769	se
3071	solicit-
0279	medidas
3683	Nicaragua
5684	o
7987	para

An arrangement of J-141 in a similar way revealed the name system although the size of the blocks did not correspond in any way. Here also there were eight divisions with a possible ninth.

J-141

4105......en	5466......Gobierno
	1268......haga
6711......se	4369......hostil
7113......solicit-	
	1776......cuanto
7724......armisticio	
7327......aun	6084......posible
5630......contra	0087......propiedad
7343......evitar	7088......que
1047......firmado	
	2491......a
6757......medida	9394......adopt-
1062......o	4095......ahi
4265......para	2696......Alemania

When we tabulated N-32 in the same way, however, we were unable to find blocks:

N-32

3201......ga	8048......solicit-
7203......que	6856......posible
9405......medida	2658......evitar
3906......Alemania	7889......se
6211......a	2265......en
6512......para	2986......firmado
9822......o	7086......propiedad
3826......ahi	5688......adopt-
4326......armisticio	5989......cuanto
4529......aun	3591......hostigacion
3435......ha	3297......Gobierno
5745......contra	

Here our system failed to work out and the occurrence of firmado and propiedad on one page precluded any possibility of experimenting further in this direction. Only two groups of words fell into possible blocks, namely:

3826......ahi	2265......en
4326......armisticio	2986......firmado
4529......aun	

Even here, only the second case is at all probable because ahi and armisticio would hardly appear on the same page, nor would aun be apt to be three pages away from armisticio. The first two figures of these groups, however, fit the case much better. Hostigacion and Gobierno, of which the initial numbers are 35 and 32 respectively, make the hypothesis more tenable. This led us to notice that ga would then be on the same page as Gobierno, contra, two pages before cuanto etc. A tabulation showed that in the N-32 encipherment, the normal order of figures is used. Seven blocks appear with a probable eighth between 00 and 22:

N-32

2265	en	6211	a
2658	evitar		
2986	firmado	6512	para
3201	ga	6856	posible
3297	Gobierno	7086	propiedad
3425	ha	7203	que
3591	hostigacion		
		7859	se
3688	adopt-	8048	solicit-
3826	ahi		
3906	Alemania	9405	medida
4326	armisticio	9822	o
4529	aun		
5745	contra		
5989	cuanto		

Before proceeding to a complete tabulation of all the blocks determined by Circular 46, we added data obtained from certain other identical telegrams. The first of these found were received on November 30, i.e. A-64, Madrid to Washington, Indicator 301; F-19, Madrid to Caracas, Indicator 131; and R-8, Madrid to Bogota, Indicator 151. Aside from the fact that they were of approximately the same length, each one contained a high frequency group (A-6303, F-5684 and R-7469) two apart in relatively the same place in the telegram. Allowing for punctuation which is used in A-64 and not in the others, we established the following identities between 301, 131 and 155:

A-64	F-19	R-8
5001SD	8990SD	9182SD
10/29/18	10/29/18	10/29/18
MADRID TO WASHINGTON	MADRID TO CARACAS	MADRID TO BOGOTA
Circular 33	Circular 32	Circular 33
301	131	155
1015	2819	3125
8222	8432	8780
4727	4837	7685
6303	5684	7469
3741	2990	3927
6444	6193	7130
6303	5684	7469
6741	5990	6927
8304	8186	9871
0314	——	——
2512	3518	3422
5338	6320	8024
2004	2485	3570
9170	8557	7836
1403	0784	2569
5314	——	——
4669	8542	1304
6915	4556	4855
2799		

Tabulating the seventeen identical pages,we made the following parallels showing part of the interlocking of blocks:

A-B	F	R
03	84	69
04	85	70
05	86	71
12	18	22
13	19	23
22	32	80
23	33	81
24	34	82
25	35	83
26	36	84
27	37	85
38	20	24
41	90	27
42	91	28
43	92	29
44	93	30
70	67	36

A search for further parallels led to the discovery of R-9 and F-21½, the former sent from Madrid to Bogota on November 13, 1918, the latter to Caracas on November 12:

R-9	F-21½	R-9(Cont'd)	F-21½(Cont'd)
11/13/18	11/12/18	11/13/18	11/12/18
MADRID-BOGOTA	MADRID-CARACAS	MADRID-BOGOTA	MADRID-CARACAS
2917	0974	9904	7342
3042	2263	7469	5684
0680	0332	3639	1560
0908	0646	2212	(Punctuation)
2212	0169	3188	1340
9818	7714	2450	1377
4535	4526 ?	2947	2368
1304	8742	2952	1879
1168	9783	8166	5881
4623	4119	2984	1036
8822	8918	2741	2062
7200 ?	3899	1660	8299 ?
1304	8742	3784	1836
0581	0533	2312	0269
1107	9546	7937	8358
6485	4835	8600	9027
8185	5257	5935	0656
6780	6432	0723	0219
5829	4492	3225	0721
7469	5684	1975	0651
9601	7928	2947	2368
1666	9381	7260	3899
1296	1410	2505	5245
2180	1832	0234	9355
0674	9350	0723	0219
0827	9890	2239	0160
2212	0169	7466	9181
5427	4490	1296	1410
2947	2368	0226	6789
1241	0562		

Adding this series of parallels to those obtained from F-19 and R-8, we have a skeleton of the page interrelation of the two series. In the table below, the numbers underlined are the original ones obtained from the parallel and from filling in consecutive numbers:

R-F	R-F	R-F	R-F
00-27	25-21	50-77	75-51
01-28	26-89	51-78	76-52
02-29	27-90	52-79	77-53
03-30	28-91	53-80	78-54
04-42	29-92	54-00	79-31
05-43	30-93	55-01	80-32
06-44	31-94	56-02	81-33
07-45	32-95	57-03	82-34
08-46	33-96	58-97	83-35
09-47	34-55	59-98	84-36
10-48	35-56	60-99	85-37
11-49	36-57	61-22	86-38
12-69	37-58	62-23	87-39
13-70	38-59	63-24	88-40
14-71	39-60	64-25	89-41
15-72	40-61	65-26	90-04
16-73	41-62	66-81	91-05
17-74	42-63	67-82	92-06
18-14	43-64	68-83	93-07
19-15	44-65	69-84	94-08
20-16	45-66	70-85	95-09
21-17	46-67	71-86	96-10
22-18	47-68	72-87	97-11
23-19	48-75	73-88	98-12
24-20	49-76	74-50	99-13

Starting with the underlined numbers only, we can fill in F-11, 12, 13, after R-97, 98, 99 because F-14, 15, 16, etc. begins elsewhere after R-19. Similarly we may enter F-47, 48, 49, 75, 76, 80, 87, 88. 29 must fall on 02 because 40 is sure, and 30 on 03, because although 03 could be 30 or 41, if the latter were chosen, 30 would be left unattached unless it were after 78. It is probably not after 78 because of the shortness of the F sequences 27-29, 50-51, and the length of F, 32-40. Then 52, 53 and 54 no doubt equal 76,77 and 78 because 55 is already placed and 31 is thus taken care of opposite 79. Now, 94, 95, 96 fall in place unless a very short series has been used. Taking stock of the remaining numbers we find 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 97, 98, 22, 23, 24, 25, 26 still unplaced with three spaces to put them in, one of five places, the other two of six. 22-26 naturally fall in the five place space, and 97, 98 precede 99. All that remains is to fill in 00-09 backwards from 10.

This complete correspondence of page numbers between two encipherments and partial correspondence for a third finally disproved the theory so long entertained that there must be a regular system for mixing blocks and that a page in 301 could be numerically transferred to a new encipherment or to the original book (see appendix). We also gave up the probability of discovering the significance of the indicator numbers. The preceding tabulations showed at least the general method of page placing and block arrangement, and were a guide in the compilation of new encipherments.

The final result of our block system as obtained from circular 46 and the two following parallels appear in the table on the following page. Meanings of the groups are entered when known.

301	131	155	141
5802) cuanto)			1776
14)03 63)	07)84 56)	25)69 74)	
2004	2485	3670	
8305	8186	9871	
2512	3618	3422	
1013	2619	3125	
3613) en)			4145
53)14 03) comma)			
6815 a)			2941
2818) adopt-)			9594
7519) ahi)			 4095
5820) Alemania			2696
0522) posible)			6084
8222	8432	8780	
5525) propiedad)			 0087
1125) que)			7088
4727	4837	7685	

801	131	155	141
8250)			5486
Cobierno)	....		
5552)			1268
haga)	....		
9133)			4569
hostigacion)	....		
5338	6320	8024	
1941)			7343
evitar)	....		
37)41	29)90	39)27	
67)	59)	69)	
6444	6193	7130	
5745)			1047
firmado)	....		1047
1550)			7724
armisticio)	....		
5852)			7327
aun)	....		
1365)			5630
contra)	....		
0769)			6711
se)	....		
3071)			7113
solicitar)	....		
0279)			6557
medida)	....		6557
7987)			4265
para)	....		
1595)			1062
o)	....		

It is plain that the complete solution of the code is now merely a process of filling in words. This phase consisted of (1) writing in the telegrams all known meanings with the cards as references; (2) guessing the intervening words with the guidance of the block system, the frequencies, the investigation sheets and the analysis cards.

A few examples of some of the first words obtained by guessing intervals may not be superfluous. A very noticeable spelling group was the following from SA-48 and SA-40;

SA-48	SA-40
3778	8778
8613 en	8613 en
3613 en	3613 en
6303 de	1703 de
8999	8999

We had already called 8613-3613 en and considered 6303-1703 successful candidates for de. The natural inference of supplying M and z for Menendez was upheld by the fact that in the block system 0279 was medida and 1899-6899 was previously called y (page 55). Then we looked up 8999 in the cards to find more spelling groups containing z. The following combinations appeared in four different connections;

<u>A</u>

	1126	6014	6179	9468	8615	A-39		Bq	6014	3841	
3196	1214	6014	6179	9468	8613	A-39		Am	6014	1899	6014
	3196	6014	6179	9468	8615	A-43		Ao	6014	2678	
			4379	9468	3615	B-5	p2	An	6899	2562	0614
		4379	9268	1815	8613	B-10	p2	Bg	1899	2562	

<u>B</u>

3778	6150	6126	A-12½		Bb	0932	1214	
3778	6150	1126	A-29		Ag	0932	0265	
3778	6150	6126	B-53		Ak	6796	2972	

<u>C</u>

1126	5662	0511	B-64		Ae	7456	7358	1915
	2156	0624	B-47	p2	Aa	7456	1620	

<u>D</u>

1899	0475	2912	7447	B-44	p3	As	6896	2654	6014

In case "A" 3196 had been placed as <u>vapor</u> since it was followed so frequently by 6014******6014. Accordingly, we looked through our list of Spanish ships obtained from the Shipping Board for a name ending in the letter <u>z</u> and found that the "Martin Saenz" left Havana August 26, and arrived at New Orleans September 2. The reference to the third example was telegram A-43 which was received on September 3, and most probably concerned the return cargo or route of the "Martin Saenz". This was confirmed by the fact that since 0769 was <u>se</u> in the block system, 9468 could be <u>sa</u>. In the fifth line a different method of encoding <u>Saenz</u> appeared and 9268, two before 9468, was naturally <u>S</u> followed by 1815-a. This fondness of encoders for using different ways of spelling a word in syllables in order to avoid duplication, led to many new identifications. Finally, 6179 was left for Martin. This gave us two words on page 79, 0279, medida and 6179, Martin, with the first one according to alphabetical sequence occurring last numerically, another instance of the method or re-arrangement on the page. The examples under case "A" now read:

A

que "Martin Sa-en-z" 3841
vapor 1214 "Martin Sa-en-z" y "
vapor "Martin Sa-en-z" 2678
4379 Sa-en-z y 2562 0514
4379 S-a-en-z y 2562

Since neither vapor nor quotation marks appeared in the last two lines and since 1365 is contra, we could assume with a fair degree of certainty that 2562 was compania.

In case "B" the Spanish name "Marques" was evident from M-ques, especially as armisticio was 1550. 0932 was on the same page as haga and therefore might well be hermanos.

In "C" 7456 followed a twice with different beginnings, pointing to a verb ending. -sca is more common than -sco and ca was therefore entered for 7456, a fair interval before 1365, contra. We then tried for verbs with subjunctive in sc which would fit in the meaning, and for a governing verb to precede the 1126, que.

Another ship with a z came out in case "D" namely, the "Legazpi". 6986 on the page before para was p, and 2634 two pages after haga was good for i. 7447 had to be ga because it could not be the a (already 1815) and could not be a syllable of more than two letters. That left 0475 for L and 2912 for e on the page preceding en-3613.

It is impossible here to follow up even one of the many paths in the labyrinth of ways leading to new words. The investigator has only to try to overlook no possibilities in guessing from the context made by identified groups, and in analysing the high frequency words of which the alphabetical placing is known.

The most essential thing in this period of vocabulary building is speed with accuracy. A system of procedure must be adopted when several people are working, calculated to unify their efforts and make all work together to one end without duplication. To accomplish this end, (1) all workers should be assigned to a special part and their conclusions promptly reported for the benefit of the rest; (2) every individual's work should be made available to everyone else so that each can make use of the latest data; (3) one person should inspect all results so that a standard requirement of entrance into the vocabulary is maintained and the danger lessened of admitting words from hastily drawn conclusions.

In order to bring about these results, those engaged in solving the Spanish code adhered to the following system: A, B and C guessed meanings from examination of a certain group of words or pages, entered them on slips of paper called "supposition slips" with references justifying assumptions, attached slips to the investigation sheet or sheets and put them in basket for D. D also studied the telegrams but first kept up to date with the work of the others and so was familiar with every phase. D, upon receiving a supposition slip, if the case were an acceptable one, marked it "O.K.", filed the investigation sheets among those kept for reference in case of error, and gave slip to typist. The latter would then make five cards as follows: The first one was in red and gave the meaning of the group in the series under consideration.

3196 B Vapor

This card was merely a guide to indicate that the group was placed and was inserted in the original or unidentified file, then the reference cards for that number placed in an identified file. A vocabulary card for the identified file was then made in duplicate exactly like the red card except in black. One of these was placed in the identified file with the reference cards belonging to it, and the other in a separate small file for more convenient use by the investigators. The remaining two cards, also duplicates, showed the Spanish meaning first and the code group following. These were for the two vocabulary files, constantly used by the code clerks to place alphabetical sequences more exactly than was possible in the block form:

Vapor 3196 B

The typist after making and filing the cards as

d

described would then hand the original supposition slip to a clerk whose duty it was to fill in words. The latter took all the reference cards and entered the new meanings in every occurrence in the telegrams, finally destroying the slip.

In case D did not accept the meaning on the supposition slip he entered his reason for refusal with references justifying that refusal, date, and his own initials and filed the investigation sheets, with supposition slip or slips attached, in the file of unidentified investigation sheets for further consideration when data should be available. If he considered the meaning a possible one, although not sufficiently so to warrant a vocabulary card, he inserted it in the tentative vocabulary for later transference to the identified file. In this way the result of all work was available for comparison and the latest history of every group could be readily ascertained.

After all the pages were known and the words filled in as far as possible, we proceeded to the compilation of the other encipherments. Let us follow this process in an imaginary case typical of an encipherment with a fair amount of material available.

We first take out of the file of the new encipherment to be considered, (1) groups of highest frequency, (2) long sequences of groups on one page, (3) variants. These are analysed and suppositions made as previously described. The punctuation page (an even number except in I-129 and F-131) is easily detected and the a page usually follows. The following is a copy of two pages of frequencies in series 169, from Vienna to Madrid, with suppositions made for punctuation and a groups:

Series 169

Group	Frequency	Supposition	Group	Frequency	Supposition
2230	2		(2931	(5)	
2630	1		([illegible]031	1	
2830	1		(7831	1	A
3130	1		(7931	4	a
3530	1		(8031	(11)	a
(7130	(18)	comma			
(7230	(8)	stop			
(7430	2	colon			
(7530	1				
7730	1				
(7930	4				
(8030	1				

When an identification has been made, a sheet numbered in two columns from)) through 99 is given a number corresponding to the last two figures of the identified group. The word is entered in its proper place according to the first two figures and the equivalent page of the 301 series copied in the new order. On the following page is the new page 31 of the 159 series, taken from page 15 of the 301 series after the supposition of *a* had been made and the order of columns determined (see page 92).

00	abdicar-acion	50	abrogar
01	abdicado	51	abrogado
02	abdicando	52	abrogando
03	a las	53	abrumado
04		54	abru-
05		55	abru-
06	abi	56	absoluto-amente
07	abierto	57	(absolver)
08	abismo	58	
09	(abjurar)	59	absolver
10		60	absolv-
11		61	abstiner
12	abl	62	abstengo
13	a los	63	
14	able	64	
15	abnegasion	65	abstraer
16	abo	66	abstraido
17	(abocar)	67	abstracto
18		68	(abstruso)
19	abocado	69	absolvido
20	abolicion	70	absurdo
21	abol-	71	
22	abominable	72	(abuelo)
23	abon-	73	
24	abon-ar	74	abund-
25	abono	75	abundamiento
26	abord-ar	76	abund-
27	abord-	77	
28	A	78	A
29	a	79	a
30	a	80	a
31	(aborrecer)	81	a bordo
32		82	a fin
33		83	a pesar
34	(abrasar)	84	a que
35		85	a que se refiere
36		86	ab
37	abre	87	aba
38	abras-	88	
39	abras-ar	89	
40	abras-	90	aban
41	abreviar	91	a la
42	abreviado	92	a esta
43	abreviando	93	abandonar-o
44	abrigar	94	abandonado
45	abrigado	95	abandonando
46	abrigando	96	Abastecimientos, Ministro de
47	abril	97	abast-
48	abrir	98	abast-
49	abriendo	99	abd

After one page other than punctuation has been filled in from the 301 vocabulary, we have another element to guide us in further identifications because the alphabetical break always falls in the same column throughout a complete encipherment. Thus from the position of the break on the *a* page, we know whether the columns of the new vocabulary are to be in the same or the reverse order of series 301. In the case of series 159, however, there are no other cards except *a* for page 31, so we have to find either a non-variant page or a variant page with another sure word in addition to the groups 50 apart to know where the break comes. The *de* page is a particularly good one for this purpose because we know that if the difference between the two high frequency words is 46, the order of the columns is the same as in 301, but that if the difference is 54 the order is reversed.

When we have made every supposition possible from the frequency sheets, we enter the identified words on the typewritten forms and proceed as if solving a new code except that every time we find a new word, we now have a new page. As we proceed, we fill in the key word to each new page on an index sheet to act as a guide in the alphabetical sequence by indicating the placing of the blocks. The index page of series 159 follows:

Column A - Corresponding pages of series 301
" B - Pages of new encipherment, series 159
" C - Suppositions of words from frequencies
" D - Suppositions of words according to alphabetical blocking.

	A	B	C	D
	90	00	su.	
	91	01		
	92	02		telegrama
	93	03		teniente
Block	94	04		
1X	95	05		tres
	96	06		un
	97	07		veinte
	98	08		veto
	99	09	Y.	
	02	10		cuando
	03	11	de.	
	04	12	del.	
Block	05	13		
111	06	14		disagradable
	07	15		
	08	16		
	09	17		
	56	18		c
	57	19		
	58	20		capitan
Block	59	21		certificar
11	60	22		ci
	61	23	como.	
	62	24	con.	
	63	25		conde
	64	26		cri
	65	27		contestar
	00	28		coronel
	01	29		
	14	30	puntuation.	
	15	31	A.	
	16	32		
	17	33		ada
	18	34		aficionado
	19	35	al.	
	20	36		
Block	21	37		
1	48	38		amos
	49	39		
	50	40		
	51	41		as
	52	42		asunto
	53	43		B
	54	44		
	55	45		
	34	46		I
Block	35	47		
V1	36	48		incidente
	37	49		ingles

	A	B	C	D
	72	50		
	73	41		
	74	52		
	75	53	ea.	
	46	54		Francia
Block	47	55		ga
V	50	56		gestion
	31	57		
	32	58	ha.	
	33	59		
	10	60		dia
	11	61		
	12	62	el.	
Block	13	63	en.	
1V	38	64		enterar
	39	65	es.	
	40	66		Espana
	41	67		esta
	42	68		exigencia
	43	69		F
	44	70		familia
	45	71		
	86	72		
	87	73	para.	
	88	74		permanecer
Block	89	75		
V111	22	76	por	
	23	77		
	24	78		prisionero
	25	79		pu
	26	80	que	
	27	81		recomendacion
	28	82		referente
	29	83		
	66	84		
	67	85		
	68	86		ruega
	69	87	se.	
	70	88		senor
	71	89		sirvase
	76	90	le.	
	77	91	le.	
	78	92		m
	79	93	ma.	
	80	94		
	81	95		
	82	96		muy urgente
Block	83	97		nos
V11	84	98		ochenta
	85	99		oponer

In making suppositions, errors often occur due to garbled groups especially in those series in which only a limited number of telegrams are available. It is therefore not advisable to be too persistent in one line of attack but to approach from another angle when an obstacle presents itself. The compilation of new encipherments is also facilitated by knowing the approximate order of frequency of the words and syllables used in Spanish code messages. The following are the highest groups in series S-167 and C-101, the largest encipherments except 301, 253 and 249, the frequency tables of which have been destroyed:

S-167		C-101	
de	189	de	67
comma	185	comma	65
que	155	y	40
en	135	period	37
period	124	que	36
y	114	en	36
el	106	a	35
a	106	para	29
la	97	a	28
se	78	quotation	28
por	58	la	25
no	57	plural	25
Alemania	52	telegrama	23
del	45	quinientos	23
Espana	39	me	18
a	39	por	17
con	34	no	15
las	30	del	13
de la	30	Estados Unidos	13
a	29	Gobierno Espanol	12
para	29	con	12
su	27	e	12
al	27	el	12

In the encipherments in which we have received only a limited number of telegrams, there is of course much greater variation in the order of frequencies. Compare V-159 between Madrid and Vienna, in which the content is so varied that all groups except grammatical particles are driven out of the frequencies;

V-159

comma	18	comma	5
de	15	del	4
que	15	se	4
a	12	la	4
su	11	lo	4
period	10	me	4
y	10	ha	4
a	9	no	3
el	9	0	3
en	8	o	3
por	6	para	3
con	5	e	3

We thought that a new system had been introduced when series Q, indicator 303, began to come in on April 5, 1929. In these telegrams five-number groups were of rather frequent occurrence but they all ended with 100, 101, 102 and 103. The new system therefore was only the addition of four pages to the book. We found by following the usual process of compiling a new encipherment that the four pages left blank by the extra ones were 49, 66, 71 and 88, and had been taken from the middle of blocks without interrupting the continuity of the alphabetical sequence. The only evidence of any system in choosing these pages was the common difference of 17 between the first two and the last two. Yet, in spite of the fact that they were skipped, a considerable number of groups from those pages appeared in the frequencies. Some of these extra groups were used as punctuation in the same way as the real punctuation, page 16, and others were inserted as nuls as follows:

5565	6036	3350	4059	4449	5915	4734
Consejo	Obreros	y	Solidades	nul	en	Munich

2832	6871	2605	0227
Ministro	nul	de la	Justicia

6235	5877	4784	2246	7064	2388	3705	0369
no	puede	firmar	una	condicion	nul	de	paz

The way the nuls and new punctuation fall can be seen in the following copy of page 88 of the Q encipherment:

(Page 88)

00		50	
01		51	
02		52	
03		53	opening quotation
04		54	
05		55	nul
06	comma	56	punto
07	comma nul	57	
08		58	
09	period	59	
10	semicolon	60	
11		61	
12	colon	62	
13		63	
14		64	
15		65	
16		66	
17		67	
18		68	
19		69	
20		70	
21		71	
22		72	
23	nul	73	
24	nul	74	
25		75	
26		76	
27		77	
28		78	
29		79	
30		80	
31		81	
32		82	
33		83	
34		84	
35		85	nul
36		86	
37		87	
38		88	
39		89	
40		90	
41		91	
42		92	
43	comma	93	nul
44	comma nul	94	
45		95	
46	period	96	
47		97	
48	nul	98	
49		99	

[illegible]ed, each new telegram furnishes new

data in regard to the use of groups ending in 49, 66, 71 and 88

The nuls and punctuation occurring in Q-303 with

which may later enable us to draw more definite conclusions.

their frequencies are as follows, with the exception of those in

telegrams r[illegible]: have not been

included i[illegible] consideration of enci[illegible] serial

1249	1	nul	5571	1	period
2849	4	nul, comma	6871	5	nul
3049	11	period	9571	1	comma
3349	1	nul	9671	1	period
4449	2	nul punto	0688	1	comma
5049	3	nul	0788	6	nul, comma
6949	2	nul, comma	0988	3	punto
7149	1	comma	2388	1	nul
0666	3	comma	4488	1	nul, comma
0866	2	period	5388	1	opening quotation
2266	2	nul, comma	9388	1	null
3966	1	comma			
4166	1	period			

The frequencies of these groups according to uses are:

nul	17
nul or comma	13
period	9
comma	7
nul or period	2
opening quotation	1
closing quotation	1
semicolon	1
colon	1

Although the Q vocabulary is as complete as the others as far as vocabulary is concerned, each new telegram furnishes new data in regard to the use of groups ending in 49, 66, 71 and 88 which may later enable us to draw more definite conclusions.

The two indicator series, N-32 and M-9, have not been included in the consideration of encipherments. These serial numbers are not variations of the diplomatic code nor are they based upon the 74 book as far as can be determined up to the present time. It is difficult to make much progress with these codes because of the small amount of material available - 27 short telegrams in M-9 and 12 in N-32.

The N's have been analysed as far as possible upon the basis of circular 46. As noted on page 75, the page numbers in this case are the first two. Although the groups go up to 10,000, there are a considerable number of pages upon which we have no occurrences up to date, namely pages 05, 08, 10, 11, 12, 13, 15, 33, 40, 41, 46, 53, 58, 66, 74, 81, 85. The following is the tentative index page of N-32 as far as it is possible to determine the alphabetical sequence before obtaining more material:

		00			58	50	
		01			59	51	
		02			60	52	
		03			61	53	No occurrence
		04			62	54	Compania Transatlantica
		05	No occurrence		63	55	
		06			64	56	
		07	punctuation		65	57	contra
		08	No occurrence	00?	01?	58	No occurrence
		09			02	59	cuanto
		10	No occurrence			60	
		11	No occurrence		03	61	de
		12	No occurrence		15	62	a
		13	No occurrence		16	63	
		14			17	64	
		15	No occurrence		87	65	para
		16			88	66	No occurrence
		17			89	67	
		18			22	68	posible
		19			23?	69	
	11	20		24?	25	70	propiedad
	12	21	E			71	
	15	22	en		26	72	que
	38	23			27	73	
	39	24			28	74	No occurrence
	40	25	ese		29	75	
	41	26	evitar		66?	76	
	42?	27		68?	67?	77	
44?	43?	28			69	78	se
	45	29	firmando		70	79	si
	46	30			71	80	su
	47	31			90	81	No occurrence
	30	32	Gobierno		91,	82	sus
	31	33	No occurrence	92or	34	83	
	32	34	ha	93or	35	84	
	33	35	hostigacion	94or	36	85	
	18	36	adoptar	95or	37	86	
		37			72	87	
	19	38	ahi		73	88	
	20	39	aleman		74	89	
	21	40	No occurrence		75	90	la
	48	41	No occurrence		76	91	
	49	42			77	92	
52?	50	43	armisticio		78	93	
	51?	44			79	94	medida
	53	45	aun		80?	95	
	54	46	No occurrence		81?	96	
	55	47		83?	82?	97	
	56	48			84	98	o
	57	49			85	99	

(Numbers on left indicate
equivalent pages in 301)

After all encipherments had been completed as far as possible from the material received, it was necessary to revise the vocabulary. This was a tedious process and consisted of (1) putting all new words in all the series, and (2) reading the dictionary through and inserting in parenthesis common words which must occur between identified groups. Finally, new copies of the vocabularies of each indicator number were typewritten. Since that time all new words or corrections have been entered in the vocabularies in the correct place in each encipherment. In case apparent contradictions are caused by garbled groups, both possibilities are entered with the references for use when new evidence is found. This is necessary because new telegrams received in the encipherments which have been finished are not carded.

The following points may be mentioned with reference to decoding telegrams and detecting the errors due to garbling and other causes. The clerks who encode the telegrams often make mistakes of which some of the most usual are as follows:

(1) Interchanging two figures i.e., writing 4565 instead of 4556.

(2) Copying the meaning of the group in the opposite column i.e., encoding 1707-neutral for 6707 - noruega, or 2111 - pedir for 7111 - participar.

(3) The confusion of high frequency groups which the encoder thinks he remembers, such as calling 8999 y instead of 5899.

(4) A similar confusion of high frequency groups of

two encipherments when two series are used between the same places.

(5) The addition of a wrong ending to a verb, such as adding ira to temer for the future form; also the substitution of endo for iendo.

(6) Incorrect encoding of unusual names or foreign words through failure to read the writing of the original text correctly for example, making N's for U's etc.

(7) The incorrect encipherment of one word used several times in a message, and the copying of this same group to indicate that word in its other occurrences.

In addition to these errors common to encoders, different senders have different styles of encipherment and their methods are markedly different. In the J series, between Madrid and Lima, the ar of the infinitive is added to the group standing for the infinitive in the code book:

J-3	2965 participar	2324 ar	1711 se
J-4	8905 enbarcar	2324 ar	3154 las
J-8	1753 justificar	2324 ar	
J-12	0818 trabajar	2324 ar	

"America"and "Americano" are usually indicated by one group but the encoder in Lima says in J-6, (4297-7761. Again in the L
(America no
series used with Morocco, numbers are encoded with y instead of the usual vienticinco etc.:

L-1	6513 veinte	3415 y	6150 cinco
L-1	6513 veinte	3415 y	5211 tres

Some Military Attaches also have a fondness for high-flown language which makes the reading of the telegrams more difficult.

In addition to detecting these errors on the part of the encoder, the decoder must guard against them on his own part for he is liable to make the same mistakes as he looks up the numbers in the code book or writes down the ones he imagines he remembers.

The methods of correcting errors and determining the correct form of garbled groups are, (1) guessing the word according to the context and looking up the goup to see if it is similar; (2) making permutations by filling in on a card all possible variations of the group in question. The permutation card of the 301 group 4341 follows:

Bn AB-3

4341	establecido
4314	emersion
4431	gratuito
4143	expuesto
0341	en
1	evasion
2	ex
3	(esposa-o)
5	Pres. de los Est. Un.
6	estan
7	estim-ar
8	estrategico
9	estudiado

4041	-----
1	estable
2	establec-er
4	estableciendo
5	estacion
6	estadia
7	estadistica
8	estado
9	"

(Reverse side)

4301	corrosion
1	diviso
2	(altura alto)
3	gratitud
5	arrest-ar
6	cola
7	signific-ar
8	moderad-a-o
9	sufrido

4340	Escocia
2	exasperacion
3	expulsion
4	farol
5	(final)
6	fosforo
7	funcionario
8	ana
9	(anad)

If the permutation fails, the error must be in more than one figure, and must be found by guessing. Frequent errors are 4469 for 5569; 2370 for 3470; 8608 for 0668, and similar confusions. 3, 5 and 8 are often interchanged, also 6, 9 and 0, and 1, 4 and 7. The percentage of garbling varies greatly, especially in wireless messages, the correctness of which is dependent upon atmospheric conditions. Some very radical changes of code groups are justifiable in doubtful messages. In Z-641, page 3, Aj, 2026 should be 6226 and there is apparently no reason for the error. In Z-640, Bm, 8887 is <u>nete</u> and should have been encoded 7207 <u>neta</u>. When there are two identical digits in a code group, both are often increased or diminished by one i.e., 2528 becomes 3538. Other errors are due to repeating the last figures from the preceding number. Fon instance, in Z-1046:

```
3673              3673
8673 should be 6730
0758              0758
```

Other frequent types of garbled groups are (Z-676): 7820 for 0682; 7086 for 7057; 8218 for 8157; 4201 for 4268; 1181 for 2922. In S-21, At, 7936 should be 7326.

In conclusion it may be well to add that every supplementary aid possible must be utilized in solving codes or reading telegrams because of the wide range of subjects and the references made to persons and places concerning which very little information can be obtained from American sources. Therefore, in the case of the Spanish code, three files are kept: (1) subject cards; (2) personnel cards; (3) current events cards. On the subject cards are entered any person, place or subject mentioned in the telegrams read up to date with reference to the telegram, and a short statement of the connection. When the subject appears again in a new telegram, all the available material previously translated is easily referred to:

(1)

Fürstenberg, Prince
SH-48 9047 SD November 5, 1918
From MEXICO To MADRID

Austro-Hungarian Minister in Mexico
requests ----------
to communicate name of new Foreign Minister
and instructions -

The personnel cards contain names of persons prominent in Spain and names of commercial firms with international connections. This list is obtained from the Spanish newspapers, the "Pan-American Bulletin" and miscellaneous sources:

(2)

Comillas, Marquis of

President of the

Cia Transatlantica

See 9/12/18 Spain

The current events cards are clippings of the chief political events, filed according to date: Changes in cabinets, revolutions, location of diplomatic missions, and transfers of diplomatic agents can thus be followed day by day:

(3)

December 1, 1919 Spain

Spanish Cabinet is Out

MADRID, Dec. 1. The Spanish Ministry resigned today.

The fall of the Ministry has been predicted for ten days unless the Government could induce the Deputies to proceed with the budget measure, which has been under constant fire in the Cortes.

In addition we have a small file of Spanish boats:

(4)

"Axteri Mendi"

Called the "Elantsobe" before
requisitioned by Spanish Government

"La Epoca" September 2, 1918

B

The filing system of telegrams consists of (1) the original copies of all telegrams received in the office, marked with the letter of the indicator series and the number of the telegram received in that series i.e., "SAB-102" means Spanish official telegram number 102 sent in the 501 code. These originals are marked "Solved" as soon as the translations are sent in: (2) all the form sheets upon which the code groups are copied for decoding, with carbon copy of translation and memorandum a attached as soon as completed.

Finally, in order to make accessible any telegram received in any series, with date, source, destination and number given by the Spanish sender, we enter these points in a record book as soon as each telegram is received.