CAUTION: THESE RECORDS WILL BE USED FOR OFFICIAL PURPOSES ONLY, DO NOT REMOVE PAPERS NOR REVEAL CONTENTS TO UNAUTHORIZED PERSON(S)

RECORDS CHARGE-OUT

9641

DATE OF REQUEST	SUSPENSE DATE
25 Jan 61	10 Feb 61

FILE OR SERIAL NUMBER AND SUBJECT	From File of Special Consultant (Friedman) Studies in German Diplomatic Codes Employed during the World War Register No. 191 ~~Confidential~~		
TO	NAME AND EXTENSION OF PERSON REQUESTING FILE Mr. William Friedman LI 6-8520	ORGANIZATION, BUILDING, AND ROOM NUMBER 310 - 2nd Str., S. E., Wash., D. C.	
RETURN TO	Mrs. Christian, AG-24, Ft. Geo. G. Meade, Md.	DATE RET'ND.	INITIAL HERE
INSTRUCTIONS	WHEN TRANSFERRING FILE TO ANOTHER PERSON, COMPLETE SELF-ADDRESSED TRANSFER COUPON BELOW, DETACH, STITCH TO BLANK LETTER-SIZE PAPER AND PLACE IN OUT-GOING MAIL SERVICE.		

9641

2ND TRANSFER COUPON

TO:

FILE (serial number and subject)

TRANSFERRED TO: (name and extension)

ORGANIZATION, BUILDING, AND ROOM NUMBER

DATE	(sig)	(ext.)

~~*Confidential*~~ **Register No. 191**

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

STUDIES IN GERMAN DIPLOMATIC CODES EMPLOYED DURING THE WORLD WAR

30 April 1959

This document is re-graded "CONFIDENTIAL" UP of DOD Directive 5200.1 dated 8 July 1957, and by authority of the Director, National Security Agency.

Paul S. Willard
Colonel, AGC
Adjutant General

NO ACCOUNTING NECESSARY

REGISTRATION CANCELED
by
Authority Hqs, ASA ltr dated 27 Feb 46
2d Ind 11 Mar 46, signed:
HAROLD G. HAYES, Col., Signal Corps
Acting Chief, Army Security Agency

~~Confidential~~

Register No. 191

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

STUDIES IN GERMAN DIPLOMATIC CODES EMPLOYED DURING THE WORLD WAR:

I. CODE 18470 AND ITS DERIVATIVES

II. THE "FUENFBUCHSTABENHEFT"

III. GERMAN METHODS OF CODE ENCIPHERMENT

BY

CHARLES J. MENDELSOHN, PH. D.

FORMERLY CAPTAIN, M. I. D., G. S.

UNITED STATES

GOVERNMENT PRINTING OFFICE

WASHINGTON : 1937

FOREWORD

The work underlying these studies was done in 1918–19 in Washington, where the writer was a captain in the Military Intelligence Division of the General Staff, United States Army, in charge of work on German codes. The pages on German methods of code encipherment were written at that time, and the first draft of the study of 18470 immediately after the writer was demobilized in 1919. The account of The "Fuenfbuchstabenheft" of 1921 was written in that year, and the matter on additional codes of the 18470 family several years later.

When the suggestion was made that the studies be printed, the material was subjected to a thorough revision. During this revision small additions were made at various points, and in the account of Code 18470, sections 22, 23, 24, 25 and 26, and note 23 were written. The specimen messages given in section 27 were studied afresh and a considerable number of garbled code groups were restored; the discussions accompanying the messages were also added. The general plan, however, was not changed.

The writer recalls with pleasure and gratitude the constant aid and encouragement given by Maj. H. O. Yardley and Capt. J. M. Manly (who were at different times at the head of the Code and Cipher Section) during his pursuit of the investigations set forth, and the cooperation of his associates, among whom he would mention Misses E. N. Rickert and D. Jachens and Messrs. Rice and V. Weiskopf. He likewise wishes to thank his old friend, Lt. Col. William F. Friedman, Signal Reserve, Chief of the Signal Intelligence Section, War Plans and Training Division in the Office of the Chief Signal Officer, for his kindness in obtaining authority for the writer to examine certain of the records preserved from the days when the studies herein discussed were actually pursued.

DECEMBER 1936.

CONTENTS

STUDIES IN GERMAN DIPLOMATIC CODES EMPLOYED DURING THE WORLD WAR

I. CODE 18470 AND ITS DERIVATIVES

(1) Introduction

From December 1917 until several months after the signing of the armistice with Germany the American Expeditionary Forces in France constantly intercepted wireless messages of German origin in numeral code. Some of these messages originated in Germany and were transmitted mainly from Berlin—a few from Nauen. With a few exceptions, these were intended for German representatives in Spain, and were addressed, in clear, Ministro Negocios Extranjeros Madrid Fuente. Other messages, originating in Spain, were directed to Berlin. The telegrams originating in Germany usually bore a signature in clear—Auswaertig, Kuehlmann. etc.; those sent from Madrid were usually signed by Ratibor (German Ambassador to Spain), or Bassewitz (Counsellor of the German Legation at Madrid).

The signatures appended to the messages made it clear that they were diplomatic despatches. They were accordingly labeled "German Diplomatic Code", and under that designation were sent to Washington. There they were referred for study to section 8 (the Code and Cipher Section) of the Military Intelligence Division of the General Staff—commonly called M. I. 8. A copy of specimens of these messages, as received in Washington, is given here, following this page.

After months of effort success was attained in the reading of certain of these messages, and the labor expended upon them widened our knowledge of German code methods, and increased our means of attacking the problem of deciphering German codes. For this reason, and for any further value that the work done in this field may have for cryptographic research, the process of deciphering these messages is here described in detail.

COPY OF PAGE 76 OF THE MESSAGES INTERCEPTED AND SENT TO WASHINGTON BY THE A. E. F

(It so happens that this page contains one message in each of the codes—18470, 12444, and 1777—that form the chief subject of the present study)

* * * * * * * * * * * * *

GENERAL HEADQUARTERS, AMERICAN EXPEDITIONARY FORCES,
GENERAL STAFF, SECOND SECTION (G. 2, A–6)

(DISTRIBUTION "C") GERMAN DIPLOMATIC CODE

A. Jan. 28, 1918. 10.17 p. m.
LP de Eaa #231–W23

Minister De Negocs Extra Genoues Madrid Fuente. This should read Ministro de Negocios Extranjeros (i. e., Minister of Foreign Affairs). Often abbreviated as "M N E."

21 792 1777 15798 27361 8491 18540 11478 20679 20524 29713 25461 16770
27064 19802 69622 22139 20951 22582 9616 20678 4130 16265 18747 17546
BUSSCHE

B. Jan. 29, 1918. 01. 41 a. m.
De EGC #383–W92—28/1/18—22r30 M N E

027 485 728 557 18470 3020 13376 11090 7671 15317 3020 26377 27306 39477
16507 15826 30825 26176 1617 29103 10212 18055 27289 21250 3133 20393
28800 19852 ..... 22654 17536 13048 30182 7459 20037 19922 17152 29272
27165 6849 21932 28964 13616 17230 4406 28475 2422 11867 12539 25981
24330 25471 17949 20027 25004 14360 18138 19558 3611 39584 3612 7860
23373 26868 19242 11002 30840 27572 29646 15472 17087 13401 1650 3611
8786 3617 28818 29235 3618 8102 10286 14538 12270 11848 18156 82 .. ..
22682

C. Jan. 29, 1918. 01.52 a. m.
Lp EGC #385–W56—28/1/18—22r30 M N E

12444 389 485 19640 14324 67444 20102 10405 23806 15596 3461 5208 12689
14433 28085 26611 22061 19994 7303 25573 14595 13704 21304 11920 1462
19177 10843 25282 26896 29233 14324 17814 17654 16058 30351 6298 19524
1500 15999 19649 27882 27483 7986 22273 27823 20942 153?1 6365 18090
22022 27656 67444 RATIBOR

Here follow a few sample messages from other codes than those represented in the sample page of A. E. F. messages.

FROM PAGE 75

D. Jan. 28, 1918. 10.13 p. m.
LP de Eaa #230 27
Ministro de Nego Extranegeous Madrid Fuente

27 792 511 171 255 1357 6031 70595 009616 2305 6933 2675 9336 0200 7399
9975 2301 5279 1299 1599 BUSSCHE

FROM PAGE 755

D) Aug. 21, 1918. 1.12 p. m.
EGC de LP #294–W39 20/8 M. N. E. M. F.

1236 4565 78427 4565 59407 70688 26868 24249 68840 09584 64876 85793 98161
11431 14088 02876 88601 66370 90245 75559 95803 08242 76551 83239 03528
04369 19626 38193 57122 28576 64784 5717 20818 29509

FROM PAGE 756

C) Aug. 22, 1918. 01.58 a. m.
LP de EGC #404–W28 M N E

5717 88819 5717 85831 84009 48556 32486 00876 82609 92086 73299 74788
32246 71666 14111 68941 58269 93190 58425 41907 51685 16166 4565 20818
3029

FROM PAGE 757

D) Aug. 22, 1918. 02.46 a. m.
LP de EGC #405–W30 M N E

1111 36021 1111 88378 63199 96378 67320 80054 64640 18181 48997 32996
36105 53786 43377 91695 44505 77181 72954 22261 12849 78861 33277 04491
4565 19818 3011

FROM PAGE 758

B) Aug. 22, 1918. 03.19 a. m.
LP de EGC #409–W120 M N E

98989 7111 77989 07183 1333 9674 0512 68866 66612 3224 76441 7715 37212
66581 3378 43673 89973 62289 0335 32600 0845 8669 52752 30430 248– 44602
4958 35086 etc.

(2) CODES IN GENERAL

A code, for the purposes of this study, may be defined as a collection of words, syllables, letters, and expressions, each provided with a symbol which is used in communications to represent the word or expressions to which it belongs. The most common symbols are letters and numerals. The former do not here concern us.

The basis of the usual numerical code is a dictionary, an alphabetical vocabulary, the words of which are numbered consecutively. An ordinary dictionary may be, and often is, employed in this manner,[1] but it is more usual to construct a special vocabulary suited to the uses to which the code is to be put. For convenience in handling, it is common to arrange the vocabulary with a hundred words or expressions to the page, numbered from 00 to 99.

[1] For a time the Germans used an ordinary dictionary between Germany and Mexico.

This basic arrangement affords a poor degree of secrecy; given a fair number of messages or a very long single message, a few words will be identified by analysis, and the coincidence of numerical and alphabetical sequence will suffice, with care and patience, to work out the rest.[2] Accordingly, in codes intended for secret communications, the basic arrangement is usually more or less distorted. The fundamental problem for the cryptographer who is "attacking" a code is to reduce it to the original alphabetical arrangement. (See pp. 5; 34 *ff.*)

(3) The German Code 13040

At the time of America's entrance into the war, German codes were an unexplored field in the United States. About a year later we received from the British a copy of a partial reconstruction of the German Code 13040 (about half of the vocabulary of 19,200 words and 800 of the possibly 7,600 proper names). This code and its variations or encipherments (see p. 8) had been in use between the German Foreign Office and the German Embassy in Washington up to the time of the rupture in relations, and our files contained a considerable number of messages, some of them of historical interest, which were now read with the aid of the code book. (For specimen messages in 13040 and its encipherments, see p. 10 *ff.*) The work of reading these messages, with the light that it shed on German methods of code structure, paved the way for the work on the unknown codes that had been used in the messages intercepted by the American Expeditionary Forces; and while some of the preliminary work on the new German codes was done simultaneously with the work of decoding messages in 13040 and its encipherments, progress in the new work was very greatly furthered by knowledge acquired from work on the older code.

The code 13040 consists of five parts:

1. A trinumeral code.
2. A set of miscellaneous common phrases.
3. The vocabulary proper.
4. An onomasticon.
5. Grammatical directions.

1. The trinumeral code (Dreinummerheft) was used for numbering and dating messages, and for such remarks as "Antwort auf Telegramm", "Im Anschluss an Telegramm", etc. These three-number groups are found at the beginnings of messages, and were used without change to introduce telegrams in most of the various Foreign Office codes. Even at the time of the Peace Conference at Versailles, the German delegates to the Conference, while employing what was probably a brand new code, numbered and dated their messages with the aid of the old trinumeral code. A copy of part of a page of the Dreinummerheft is here appended.[3]

[2] The Germans used a code not belonging to those discussed in this study for messages going from Berlin via Madrid to the Colonial Administration in Africa. The following passage on pp. 90–91 of the work sheets of intercepts in this code led to the solution of the code: 97953 97960 97972 97960 97861 97960 97709 97960 97738 97960 97575 97530 97544 97530 97453 81870 97280 96719 96983. It was reasoned, because of the repeated occurrence of groups from the same page and from neighboring pages separated in no less than five instances by the same group (97960), that the passage constituted a series of numbers separated by stops. Now numbers are usually given in an ascending series, while these page numbers, with but two exceptions, form a descending series. It seemed possible, on this basis, that the code was arranged in inverse alphabetical order. The attempt was then made to find frequent code groups at numerical positions in the code corresponding to the alphabetical position of words that were certain to occur frequently in the messages. Telegramm was the first one tried out, and a very frequent code group was found close enough to the required alphabetical position to be provisionally identified with the word. The same process was repeated with other very common words. The attempt was then made to identify other code groups in the neighborhood of those already tentatively identified, and by continuing this process the code was "broken" with no great difficulty.

[3] A discussion of the new Nummerheft, which came into use in 1921, will be found on p. 96.

PART OF THE DREINUMMERHEFT

050	060	070	080	090
vom 5 Sept	vom 8 Febr	vom 8 Mai	vom 8 Aug	vom 4 Nov
1 Nr. 150	1 Nr. 260	1 Nr. 370	1 Nr. 480	1 Nr. 90
2 vom 14 Dez	2 vom 18 Mai	2 vom 24 Nov	2 76	2 85
3 Nr. 250	3 Nr. 360	3 Nr. 470	3 Nr. 80	3 Nr. 190
4 48	4 vom 4 Dez	4 vom 16 Aug	4 vom 19 Jan	4 vom 18 Apr
5 Nr. 350	5 Nr. 460	5 Nr. 70	5 Nr. 180	5 Nr. 290
6 vom 18 Febr	6 vom 26 Aug	6 66	6 vom 28 Apr	6 97
7 Nr. 450	7 Nr. 60	7 Nr. 170	7 Nr. 280	7 Nr. 390
8 vom 28 Mai	8 57	8 vom 29 Jan	8 vom 14 Nov	8 vom 27 Juli
9 Nr. 50	9 Nr. 160	9 Nr. 270	9 Nr. 380	9 Nr. 490

This arrangement is for decoding. The German Code Bureau must have had another arrangement in which numbers and dates, etc., appeared in regular order.

It seems reasonable to suppose that encoders were instructed to use these groups only in the introductions to messages, and not for similar expressions in the body of messages. These instructions, however, if issued, were not always observed. (See p. 18 and note 12).

2. Eight pages of miscellaneous common phrases, largely prepositional, and alphabetically arranged. Examples are: aus welchem, gegen das, ein fuer allemal, etc. Some of the encoders employ these phrases freely, others hardly use them at all; in general as time went on, the tendency was to use them less and less. No evidence of their use in connection with other codes than 13040 has been found. It seems probable, however, from the fact that the vocabulary of 18470 begins with page 10, just as the vocabulary proper of 13040 does, that the phrases were designed to be used, like the Dreinummerheft, with different codes.

3. The vocabulary proper (see p. 7), covering 189 pages, 100 groups to a page. Two groups on each page are numerals and two are stops; the others comprise the vocabulary. This vocabulary was originally strictly alphabetical. The two numerals to a page were inserted in this alphabetical arrangement in consecutive order and at definite positions in the page. The odd (lesser) numerals are put in the block of 10 words which is *alphabetically* fifth; the even (greater) numerals in the block of 10 words which is alphabetically tenth. Furthermore, the final digit of the numeral and the final digit of the number marking its position on the page always total 10 or 0. (Numbers from 000 to 09 are arranged in a slightly different scheme.) The two stops are placed in the 10-word blocks that are alphabetically first and sixth. Their position in the block is also governed by rule:

The number of the page in the *original alphabetical arrangement* of the code is divided by four; the position of the stops is then determined by the remainder thus:

Remainder	First stop at	Second stop at
0	0	1
1	2	3
2	4	5
3	6	7

The vocabulary of each page was divided into 10 blocks of 10 words each, and the position of these blocks was then changed, apparently at random, although it is with reluctance that one accepts the conclusion that the Code Section of the German Foreign Office left anything to chance. The alphabetical sequence was further disarranged by changing the order of the

pages among themselves: the first four pages were given four new consecutive numbers (10–13 for example became 228–231); the next four were similarly renumbered and removed from the first four in the process, etc. Apparently this renumbering, like the rearrangement of the 10-word blocks, was left to chance.

Certain pages containing frequent words such as und, die, etc., are given a double number, the object being to lower the number of repetitions in messages with the attendant danger of identification of very common groups.

4. An onomasticon, comprising both geographical and personal names. These names are represented by code groups running from 24,000 to 99,999. Of the 76,000 possible code groups, however, which might be covered by these numbers, only one-tenth are used; page numbers and penultimate (block-of-ten) numbers are used as in the vocabulary proper, but each penultimate number has only one terminal digit associated with it, the other nine not being used. Thus, if 25179 is used, 25170–25178 will not occur at all. The alphabetical arrangement shows evidence of several smaller collections of names. Some are obviously supplements to the list.[4]

5. Four pages of grammatical directions, etc. These comprise such instructions as "Past tense", "Gen. Pl.", etc. They contain directions for the tenses of verbs, the cases of nouns, degree of an adjective, etc., also code groups that indicate that a certain number of letters are to be removed from the end of the word that they modify. The last-mentioned are used for spelling purposes. (See p. 57.) These pages contain also a large additional number of stops. It was felt that they had been compiled separately from the vocabulary, since the two regular stops and numbers per page are absent. This feeling was fully confirmed later, when it was found that the German Colonial Code (see p. 4, note 2) had used the same set of grammatical directions as 13040.

On page 130, which contains a hodge-podge of supplementary words and phrases, the groups 40 to 49 are given the meaning "Chiffre Nr." Thus the code, while known as 13040, is indicated by any number from 13040 to 13049. In the messages, this indicator number is placed sometimes before and sometimes after the trinumeral groups. In the case of this particular code it is sometimes omitted entirely, the provenience of the message evidently being regarded as a sufficient indication of the code employed.

[4] Such, substantially, is the British description of the onomasticon. A more detailed study of this name list will be found on p. 59, in connection with a survey of the personal names of 18470.

00	einmal	50	
01	einmarsch	51	eingestehen
02		52	eingetroffen
03		53	
04	einnahme	54	eingezogen
05		55	eingreifen
06		56	
07		57	einhalb
08	eingenommen	58	einhalten
09		59	
10		60	80
11	einkommen	61	
12		62	
13	eingeladen	63	eingeraeumt
14	einladung	64	einreichen
15		65	eingereicht
16	einlage	66	
17	einlassen	67	
18	einlaufen	68	einrichten
19	eingelaufen	69	eingerichtet
20	einfluss	70	
21		71	einigen
22	einflussreich	72	einigermassen
23		73	eingeleitet
24	einfordern	74	einigung
25		75	
26	einfuhr	76	einkauf
27	einfuehren	77	stop
28	einfuehrung	78	
29		79	einklang
30	eines	80	
31	einfach	81	eingabe
32		82	eingang
33		83	
34	einfall	84	
35		85	eingeborene
36	stop	86	
37		87	eingegangen
38		88	eingehen-t
39		89	eingehend
40		90	
41	79	91	einlegen
42	einheimisch	92	einleiten
43	einheitlich	93	
44		94	einlenken
45	einholen	95	
46	eingeholt	96	
47		97	
48		98	einloes/ung-en
49	einiger	99	

(4) Encipherments of 13040: 5950 and 26040

Two methods of varying or enciphering 13040 were encountered in M. I. 8, both of which had been described by the British when they turned over to American authorities the skeleton copy of the code. These encipherments were known as 5950 and 26040.

Just as a renumbering of the pages of the original alphabetical vocabulary had produced 13040, so a second renumbering of these pages was resorted to to make 5950. In this renumbering, as in the other, the four-page blocks were kept intact—for what purpose cannot be divined, since a page-by-page renumbering is a far better procedure.[5] For the proper names a separate table was employed. The Germans seem to have believed that this change in pagination made a new code book. As a matter of fact, as we shall see later (see p. 18 *ff*), it does nothing of the kind.

In addition to the change in pagination, the arrangement of the blocks of words on each page was altered. The fifth block (penultimate figure 4) became the first (penultimate figure 0), and the first, second, third, and fourth blocks were moved down one place. The other five blocks were rearranged in the same manner, the tenth block (penultimate figure 9) becoming the sixth (penultimate figure 5), and the others dropping down one place. (See the next paragraph.) The whole procedure is similar to the change in arrangement of the blocks-of-ten in going from the original alphabetical code to 13040, except that in making 5950 from 13040 a single formula is used for all the pages.

For *en*coding in 5950 either of two procedures may have been used. The new page numbers may have been written in the book page by page; the encoder would then simply take these numbers instead of the 13040 numbers. Or the change may have been made by a table, 13040 to 5950. The change in the penultimate figure of each code group was made by a table, as follows:

13040	5950
0	1
1	2
2	3
3	4
4	0
5	6
6	7
7	8
8	9
9	5

This table, however, is memorized after a little practice and the change becomes automatic. *De*coding was done by means of tables—5950 to 13040— for both pages and word blocks.

The other encipherment of 13040 is known as 26040, and is indicated by any of the numbers 26040 to 26049. It consists of 5950 with an additive or subtractive. The message is written in 5950; then a certain number (always one between 100 and 999) is added to or subtracted from each group. Thus, if the message in 5950 is, say, 17406 18965 10531 10669 etc., and a subtractive of 200 is used, the message will read 17206 18765 10331 10469 etc., and the recipient will add 200 to each group before decoding. If an additive is used, the recipient subtracts before decoding. Specimen messages in 26040 will be found on pages 12*f*.

[5] Two tables for changing 13040 to 5950—one for the vocabulary, and one for the proper names—will be found following this page.

Conversion table; 13040 to 5950

(13 in the column headings signifies 13040 and 59, 5950)

13	59	13	59	13	59	13	59
10	114	69	154	126/127	56/57	187	188
11	115	70	155	128	58	188	189
12/13	116/117	71	156	129	59	189	190
14	118	72/73	157/158	130	60	190	191
15	65	74	184	131	141	191	216
16	66	75	185	132/133	142/143	192	217
17	67	76	186	134	144	193	218
18	68	77	187	135	145	194	219
19	192	78	61	136	73	195	180
20	193	79	62	137	74	196	181
21	194	80	63	138	75	197	182
22	195	81	64	139	76	198	183
23	137	82	38	140/141	27/28	199	50
24	138	83	39	142/143	29/30	200/201	51/52
25	139	84	40	144	31	202	53
26	140	85	41	145	32	203/204	54/55
27	105	86	123	146/147	14/15	205	196
28	106	87	124	148	16	206	197
29	107	88	125	149	17	207	198
30	108	89	126	150	18	208	199
31	146	90	171	151	204	209	208
32	147	91	172	152	205	210	209
33	148	92	173	153	206	211	210
34	149	93	174	154	207	212	211
35/36	19/20	94	77	155	175	213	220
37/38	21/22	95/96	78/79	156	176	214/215	221/222
39/40	23/24	97/98	80/81	157	177	216	223
41/42	25/26	99/100	82/83	158/159	178/179	217/218	224/225
43	88	101	101	160	109	219/220	235/236
44	89	102	102	161	110	221	237
45	90	103	103	162/163	111/112	222	238
46	91	104	104	164	113	223	239
47	127	105	96	165	132	224	10
48	128	106/107	97/98	166	133	225	11
49	129	108	99	167/168	134/135	226	12
50/51	130/131	109	100	169	136	227	13
52	167	110	84	170	163	228	159
53	168	111	85	171	164	229	160
54	169	112	86	172	165	230	161
55	170	113	87	173	166	231	162
56	119	114	200	174	226	232	212
57	120	115	201	175/176	227/228	233	213
58	121	116	202	177	229	234	214
59	122	117	203	178	230	235	215
60	33	118	231	179	46	236	150
61	34	119	232	180	47	237	151
62/63	35/36	120	233	181	48	238	152
64	37	121	234	182	49	239	153
65	92	122	69	183	42		
66	93	123	70	184	43		
67	94	124	71	185	44		
68	95	125	72	186	45		

Proper names, 13040 to 5950

(13 in the column headings signifies 13040, and 59, 5950)

First two figures

13	59	13	59	13	59	13	59
24	50	44	86	62	82	82	78
25	51	45	87	63	83	83	79
26	52	46	88	64	84	84	80
27	53	47	89	65	85	85	81
28	*36	48	54	66	28	86	40
29	*37	49	55	67	29	87	41
30	*38	50	56	68	30	88	42
31	*39	51	57	69	31	89	43
32	58	52	94	70	*62	90	*90
33	59	53	95	71	*63	91	*91
34	60	54	96	72	*64	92	*92
35	61	55	97	73	*65	93	*93
36	24	56	*48	74	44	94	70
37	25	57	*49	75	45	95	71
38	26			76	46	96	72
39	27			77	47	97	73
40	66	58	32	78	74	98	*98
41	67	59	33	79	75	99	*99
42	68	60	34	80	76		
43	69	61	35	81	77		

Third figure

*In groups marked by an asterisk, the third figure remains unchanged. In other groups the third figure changes as follows:

13	59	13	59
0	1	5	6
1	2	6	7
2	3	7	8
3	4	8	9
4	0	9	5

The table for changing the *third* figure of the proper name groups is the same as that used for changing the *penultimate* figure in the groups of the vocabulary proper.

The following telegram, which will illustrate the use of 13040, was sent by Ambassador Bernstorff in Washington, under instructions from the German Foreign Office, to the German Minister in Mexico, and has become famous under the name of the "Zimmermann Note." It was deciphered by the British, and a copy of the code text with the decipherment was given by them to the United States Government.

130 Nr. 3
13042
13401 Auswaertiges Amt
8501 telegraphiert
115 vom 16ten Januar
3528 colon
416 Nr. 1
17214 Ganz geheim
6491 Selbst
11310 zu
18147 entziffern
18222 stop
21560 Wir
10247 beabsichtigen
11518 am
23677 ersten
13605 Februar
3494 un
14963 eingeschraenkten
98092 U-boot
5905 krieg
11311 zu
10392 beginnen
10371 stop
0302 Es wird
21290 versucht
5161 werden
39695 Vereinigte Staaten von Amerika
23571 trotzdem
17504 neutral
11269 zu
18276 erhalten
18101 stop
0317 Fuer den Fall
0228 dass dies
17694 nicht
4473 gelingen
22284 sollte
22200 stop
19452 schlagen
21589 wir
67893 Mexiko
5569 auf
13918 folgender
8598 Grundlage
12137 Buendnis
1333 vor
4725 stop
4458 Gemeinsame
5905 Kriegs
17166 fuehrung
13851 stop
4458 gemeinsamen
17149 Friedensschluss
14471 stop
6706 reichliche
13850 finanzielle
12224 Unterstuetzung
6929 und
14991 Einverstaendnis
7382 unsererseits
1587
(15857) dass
67893 Mexiko
14218 in
36477 Texas
5870 comma
17553 Neu
67893 Mexiko
5870 comma
5454 Ar
16102 iz
15217 on
22801 a
17138 frueher
21001 verlorenes
17388 Gebiet
7446 zurueck
23638 erobert
18222 stop
6719 Regelung
14331 im
15021 einzelnen
23845 Euer Hochwohlgeboren
3156 ueberlassen
23552 stop
22096 Sie
21604 wollen
4797 Vorstehendes
9479 dem
22464 Praesidenten
20855 streng
4377 geheim
23160 eroeffnen
18140 comma
22260 sobald
5905 Kriegs
13347 ausbruch
20420 mit
39689 Vereinigten Staaten
13732 fest
20667 steht
6929 und
5275 Anregung
18507 hinzufuegen
52262 Japan
1340 von
22049 sich
13339 aus
11265 zu
22295 sofortiger
10439 Beitretung
14814 einladen
4178 infinitive with zu
6992 und
8784 gleichzeitig
7632 zwischen
7357 uns
6926 und
52262 Japan
11267 zu
21100 vermitteln
21272 stop
9346 Bitte
9559 den
22464 Praesidenten
15874 darauf
18502 hinweisen
18500 comma
15857 dass
2188 ruecksichtslose
5376 Anwendung
7381 unserer
98092 U-boote
16127 jetzt
13486 Aussicht
9350 bietet
9220 comma
76036 England
14219 in
5144 wenigen
2831 Monat
17920 en
11347 zum
17142 Frieden
11264 zu
7667 zwingen
7762 stop
15099 Empfang
9110 bestaetigen
10482 stop
97556 Zimmermann
3569 stop
3670 Schluss der Depesche

90481—37——2

Since all 26040 messages must be transposed into 5950 before they can be read, it will not be necessary to quote any encoded in 5950. The following short message in 26040, sent by Bernstorff to Zitelmann at Manila, on January 17, 1917, is of interest because of its reference to the code to be employed in future communications. As reproduced here, the first column of figures gives the code groups as they were sent; the second column gives the 5950 code groups obtained by adding 212 to each group in the first column; and the third column gives the 13040 code groups.

416			Nr. 1
26046			
22493	22705	17545	Neues
20600	20812	20902	Verfahren
17639	17851	15891	59
18068	18280	19770	50
5337	5549	20339	mit
14199	14411	13401	Auswaertigem Amt
11414	11626	1216	vom
14875	15087	23677	ersten
7103	7315	13605	Februar
15770	15982	22872	ab
16674	16886	5376	anwenden
29172	Add 212 to each code group.		

(Signed) BERNSTORFF

It is a bit puzzling that Manila should be instructed in a message written in 26040 (which is 5950 with an additive or subtractive) to correspond with the Foreign Office in plain 5950.

On January 21, 1917, 10 days before the announcement by Germany of the unrestricted submarine warfare which led to the American rupture in diplomatic relations, and ultimately to America's entrance into the war, Bernstorff sent the telegram below to Zitelmann at Manila. The message is interesting historically as showing how Germany was preparing to meet the inevitable crisis. Especially interesting in this connection is the word "wieder", showing that the machinery of the German ships in American waters had already been taken apart at some previous time in preparation for making the ships unfit for use.

547			Nr. 4	11306	11738	1228	Vorbereitung
16092	16524	17214	Ganz geheim	4202	4634	17924	en
3319	3751	6491	selbst	16129	16561	17251	fuer
7342	7774	9464	dechiffrieren	14987	15419	6909	Unbrauchbar
17460	17892	15882	Dargelegt	5913	6345	8035	machung
2514	2946	14236	im Amschluss an	4584	5016	19906	Maschine
3659	4091	8481	Telegramm	10317	10749	2939	n
19935	20367	11757	3	11377	11809	1449	vornehmen
19900	20332	11722	stop	11269	11701	1241	stop
6962	7394	13684	Falls	4625	5057	19997	Massnahme
21414	21846	19336	Schiffs	10352	10784	2974	muss
4584	5016	19906	maschine	14552	14984	3474	unbedingt
10317	10749	2939	n	8455	8887	4377	geheim
22421	22853	17593	nicht	22714	23146	11836	bleiben
21668	22100	21440	wieder	9947	10379	10369	Bei
13832	14264	13254	auseinander	4907	5339	20229	minder
8657	9089	4579	genommen	10995	11427	1017	vertrauens
10910	11342	16432	Kapitaen	22124	22556	21796	wuerdigen
18675	19107	19047	e	10910	11342	16432	Kapitaen
16450	16882	5372	anweisen	4202	4634	17924	en
23422	23854	22294	sofort	19934	20366	11756	anheimgeben
1848	2280	3770	underline following word	16940	17372	9262	bevorstehende

19951	20383	11773	Ankunft
1167	1599	14689	eines
18778	19210	1900	Revisors
20074	20506	15246	oder
23527	23959	22399	sonst
13597	14029	2619	plausible
12256	12688	8978	Gruende
12297	12729	4719	vorschuetzen
11400	11832	1422	stop
9947	10379	10369	Bei
12750	13182	5072	welchen
21386	21818	19308	Schiffen
10567	10999	16089	ist
16756	17188	9078	bereits
2597	3029	14219	in
10604	11036	16126	jetziger
10610	11042	16132	Jahreszeit
11306	11738	1228	Vorbereitung
18040	18472	7462	zur
18987			
(14987	15419	6909)	Unbrauchbar
5913	6345	8035	machung
13945	14377	13367	ausgeschlossen
15007	15439	6929	und
11710	12142	5832	kommt
22599	23031	17821	nur
14851	15283	23873	eventuell
20760	21192	21282	Versenkung
2597	3029	14219	in
15956	16388	17078	Frage
7129	7561	13851	stop
18474	18906	18846	Drahtantwort
47392			Add 432

(Signed) BERNSTORFF

To the foregoing telegram of Ambassador Bernstorff, Zitelmann replied as follows (again the word "wieder" is to be noted):

723	Nr. 2		
728	Antwort auf Telegramm		
547	Nr. 4		
11207	11738	1228	Vorbereitung
11782	12313	8603	getroffen
11970	12501	8841	stop
13733	14264	13254	Auseinander
22149	22680	17470	nehmen
4485	5016	19906	Maschine
10218	10749	2939	n
21571	22102	21442	wieder
19808	20339	11729	angeordnet
23418	23949	22339	soweit
8358	8889	4379	Geheimhaltung
11813	12344	8634	gewaehrleistet
8560	9091	4581	stop
16546	17077	5567	Auf
7337	7868	9558	den
4579	5110	20000	meisten
21287	21818	19308	Schiffen
8358	8889	4379	Geheimhaltung
12423	12954	4994	wegen
5873	6404	8144	Mannschaft
16110	16641	17331	gefaehrdet
16020	16551	17291	stop
10811	11342	16432	Kapitaene
21783	22314	21604	wollen
21399	21930	19420	schleunig
14888	15419	6909	Unbrauchbar
5814	6345	8035	machung
20068	20599	15289	ohne
13733	14264	13254	Auseinander
22149	22680	17470	nehmen
18524	19055	18995	durch
8052	8583	11173	Zerstueckelung(?)
17217	17748	15738	Cylinder
14903	15434	6924	und
11657	12188	5878	Kolben
14618	15149	23739	erwirken
23278	23809	22249	so dass
11441	11972	5662	keine
20661	21192	21282	Versenkungen
4327	4858	18198	erforderlich
52381			Add 531

(Signed) ZITELMANN

Usually the number added or subtracted was indicated to the recipient at some point in the message previously agreed upon. Probably there was no agreement as to whether addition or subtraction was to be used; the recipient would try one, and if that did not work, would try the other. Five different methods of employing this encipherment were encountered: (1) A number composed of the first, third, and fifth digits of the last code group of the message is subtracted—the recipient then adding this number; (2) the first, fourth, and fifth digits of the fourth code-group from the end of the message are similarly used as a subtractive; (3) the second, fourth, and fifth digits of the code group just described are used to form a subtractive; (4) the fifth, third, and first digits (in that order) of the last code group of the message are

Several methods were used in M. I. 8 for finding what number had been added or subtracted. In general these methods consisted in attempting to guess a word of the message, and obtaining the additive or subtractive from that. In one case a message which had not been read contained a name group, 77146. Another message from the same source, which could be read, contained the group 77244, and it was assumed that the two name groups might be identical. The decoded message required an addition of 202. Since 77244 is 98 greater than 77146, it followed, if the two name groups were really identical, that the number to be added in the unread message was 98 greater than that in the message that had been read. 300 was accordingly added to the code groups of the message, and was found to be correct. It was then noticed that the fourth group from the end of the message, 32100, which would not give a reading, provided the key number in its first, fourth, and fifth figures. In another case a message sent for forwarding, and preceded by an introduction in another and indecipherable code, was read by assuming that it might begin with the word "Nummer." Still another message was read by assuming that a German message, however short, was likely to contain und, der, or die. Now no message had ever used any but a three-figure additive or subtractive. Accordingly all the values of und, der, and die in the code book were arranged in a table; another table was made of all the code groups in the message that differed from the und, der, and die values by 999 or less, and the form of encipherment necessary in each case was noted. The intention then was to try out each in turn. Before that was done, however, it was noted that one of the differences—763—was made up of the fifth, third, and first digits of the last group of the message. 763 was accordingly tried first and proved to be correct. In 1919 the Germans were sending 26040 messages to Mexico in which they used a constant subtractive. This was guessed by trying for the word Nummer at the very beginning of the message and for the words "Deutsche Botschaft Mexiko" near the beginning. Incidentally it was stupid code writing that left these openings; the address should have been in clear—later it was so written—and the "Nummer" should have been given in the trinumeral code. At the best, however, the method is unsafe.[6]

(5) Various Codes in the Messages Intercepted by the A. E. F.

We now return to the messages intercepted by the American Expeditionary Forces in France. (See the specimen messages pp. 2, 3.) A careful inspection of the messages brings out the fact that we are not dealing with a single code but with a whole series of codes. We note the occurrence of various indicator numbers in the messages—12444, 1357, 18470, 1777, 2815, 4565, 5717, 44499, 58585, 2310, 98989, 1111, 80574, and traces of some others. Usually (but not always, as we shall see; cf. p. 20) a different indicator number meant a different code. The following description of the material was written after a preliminary survey of the sheets of messages:

> Outside of some odds and ends, these messages consist of matter in codes indicated by the following numbers: 12444, 1357, 18470–9, 4565, 1111, 5717, 58585, 98989, 1777. Among messages that cannot be assigned to any of these codes a six-figure code is striking because of the fact that the messages almost invariably consist of six groups of six figures each, with 000,000 at the end. The indicator is 297075.
>
> The codes whose indicator numbers are given above are used in no regular sequence so far as can be noticed. At some periods one code will be used more, at others another. So, too, it cannot be told whether the various codes are used for different kinds of subject matter.
>
> Certain peculiarities, however, are noted in different codes.
>
> *12444.*—The encipherment of this code is almost certainly constant. The vocabulary consists probably of 31,000 code groups, with proper names in addition as in Code 13040.
>
> *1357.*—This code consists mainly of four-figure groups; these predominate to such an extent that a message in this code strikes the eye and stands out from messages in other codes.

[6] A further discussion of German methods of code encipherment will be found on pp. 97 *ff.*

4565, 1111, and 5717.—These codes seem to be connected, although peculiarities in the enumeration of messages written in them are noted below. It seems a fair presumption that this is a code—if it is one code—with an encipherment that changes in the midst of a message. A message will begin with the indicator number—one of the three numbers given. This is followed by another number, and the indicator number is then repeated, thus: 4565, 27730, 4565. The last two figures of the second group—30 in this case—represent the number of code groups that follow up to the occurrence of another indicator number, when the same process is repeated or the message ends. An examination of any of the messages in this code will make this clear. It is a reasonable supposition that the other figures of the second group indicate the encipherment employed.

Certain peculiarities are noted in the *numbering* of the messages. 12444, 1357, 1777, and 18470 use the regular German three-figure system for numbering and dating (Nummerheft), and the messages in these three codes form one continuous series. (See 311A, C; 312A; message no. 480 is in 12444, no. 482 in 1357, and no. 483 in 18470.) It is to be noted that 1357 messages going *from* Madrid *to* Berlin form a separate series.

58585 and 4565 have their own enumeration in clear and preceded by the word "Nr." at the beginning of the message. (But see end of 2B, C, D; 5A, 6D.) The messages in these codes form a continuous numerical series, as do those written in 12444, 1357, 18470, and 1777. Possibly there is some connection between the codes that form a series, or possibly they are used for a particular kind of subject matter.

98989, 5717, and 1111 are numbered at the end of the messages. It is remarkable that in spite of the very intimate connection noted above among 1111, 5717, and 4565, the messages written with these indicator numbers do not form a numerical series: 1111 and 5717 are numbered in sequence with 98989, while 4565 forms a numerical series with 58585.

We may further emphasize the difference in general appearance between messages in one code and those in another—e. g., the low range in the 1357 messages as compared with the higher range in 12444 and the much higher numbers of 4565.

The first step in "attacking" the messages was necessarily to separate those written in the various codes. The messages with the index number 12444 were, more or less at random, picked out to be worked at first.

Entrance into a code is most commonly gained by associating a piece of code with its corresponding clear text. In the present case, we were in possession of no clear text whatever—it was not until after the code had been "broken" that a piece of clear—an advertisement of German warbonds—was matched up with its code original. (See p. 51.) Entrance into the code had accordingly to be sought by a process of analysis.[7]

(6) Arrangement of the 12444 Messages for Study

The 12444 messages, once having been picked out for attack, were prepared in the manner regularly followed in M. I. 8. They were assembled and copied on index sheets or work sheets, which were numbered consecutively. A specimen sheet of 18470 will make the method clear, and follows below. The two columns are designated by the capital letters A and B; the small letters at the sides indicate the position of the individual code groups in the columns. The term C. B. No. refers to the numbers of the messages on the A. E. F. sheets of intercepted messages. The place from which the message was sent, with the signature if there was one, and the place to which it was going were also noted. On the specimen sheet here given (18470 messages, p. 15) Am would refer to 21419; Bg would refer to 24981. When work was begun, the 12444 messages filled some 800 of these sheets.

[7] The writer here wishes to make a slight digression. It is the custom, in writing on cryptography, to introduce results obtained with such phrases as "it was noticed that", "it was obvious that", "it appeared at once", etc. No more discouraging practice could be imagined. To take a specimen problem from any of the more common books on the subject, put hours and hours of work upon it with no visible results, and finally see the light of day, only to find from the book that the author saw the weak spot at a mere casual glance, takes all the joy out of the student's work. The writer is in no position to question the veracity of cryptographers who make such statements; he rather supposes that they do not intend to mislead, but merely scorn the base degrees of young ambition's ladder. But, be that as it may, and be the confession never so stultifying, few things were found obvious in the study of these German codes. The results obtained, and especially the initial results, were reached only after months of work with often absolutely nothing to show for the labor expended, save mental wear and tear.

18470

From Bussche | C. B. NO. 20B | to EGC | Date 8/12/17

A		B	
a	555	a	23555
b	651	b	29222
c	801	c	3612
d	728	d	22224
e	563	e	24050
f	689	f	29465
g	400	g	24981
h	387	h	24811
i	076	i	24735
j	18475	j	20262
k	11059	k	15780
l	16297	l	29647
m	21419	m	20910
n	7565	n	15542
o	3375	o	20712
p	13404	p	3250
q	15572	q	1927
r	27754	r	7573
s	36808	s	8467
t	24735	t	30208
u	20262	u	18654
v	10056	v	27733
w	10413	w	29614
x	11190	x	23401
y	24019	y	24922
z	11797	z	10365

15 (message book page number)

A card index was next made for the sheets, so that any occurrence of any code group, with its context, could be instantly referred to. A copy of a specimen index card of 18470 is given here. At the top is the code group with the reference to the index or work sheets; below appears the context—the two code groups immediately preceding and the two immediately following in the message.

8467 18470, 15 Bs

1927 7573 30208 18654

This card index, showing a large number of occurrences for various groups as well as repetitions of several groups in succession, showed that we had to do with a constant code—i. e., one like 13040—not one that, like 26040, changed by some process of encipherment from message to message.

In order to have the various occurrences of the groups in compact form, the cards were copied, number by number, into a "Frequency Book." Groups that occurred less than three times in the messages were disregarded in this process, since it was thought that such infrequent groups would not justify the labor involved in copying the cards.[8]

Certain general conclusions were drawn from the frequencies. Numbers below 1000 did not occur, so that the book was seen to begin at page 10. Frequently occurring groups were found between 1000 and 30999, where there was a sharp tapering off in the frequency and a great increase in the number of code groups that did not occur at all. This led to the conclusion that the vocabulary proper was comprised between 1000 and 30999—i. e., covered 300 pages, unless, as in the case of 13040, some pages should be found to have double numbers. (See p. 6.) Reasoning on the analogy of 13040, the groups above 30999 were assumed to represent the proper names.

(7) First Attempts at Identification of Code Groups

First efforts at identification were directed toward finding the meaning of common groups and toward discovering the code equivalents of the commonest words in the language. Kaeding in his "Haeufigkeitswoerterbuch" points out that die, der, and und constitute 15 percent of the German language. It was to be expected, on the analogy of 13040, that each of these words would have several code groups assigned to it, but that the code groups for each word would occur successively in the book and would constitute a solid block. Thus vom in 13040 is represented by five variants—1214–1218. Even at that, however, no groups could be found which seemed likely candidates for the meanings in question. One reason in the case of die and der was suspected from the start—it was thought that the telegraphic nature of the language had greatly reduced the frequency of these two words. This reasoning, however, would not account for the absence of a block of words for und, since und is not nearly so readily omitted. This mystery was not solved until later. (See p. 38.)

The frequently occurring code groups gradually became familiar in the process of constantly reading and rereading the messages much as one listens to a foreign tongue and gradually absorbs some words. In the latter case, however, these words are usually learned with their

[8] This was a mistake. Often a group that occurs only once will have its meaning fixed beyond doubt by the context (e. g., a spelling group in the middle of a word). The card index is bulky and the Frequency Book is compact; if the latter is complete, the former can be discarded and the cards used over again for other purposes. Finally, the time involved in consulting the card-index for the rare groups more than offsets the labor saved by omitting these from the Frequency Book.

meanings, whereas, in the study of the code messages, numbers tantalizingly remained numbers. A striking example was 13788,[9] found so frequently at the beginning of messages. This was first supposed to be a preposition—probably fuer; this meaning, however, offered difficulties and had to be abandoned (see p. 39), and there were other guesses that met a similar fate.

The introduction to the message in 12444, page 676 Ag—744 533 572 25993 755 875 (Im Anschluss an Telegramm Nr. 294 vom 5ten Maerz 25993 Nr. 432 vom ersten April)—attracted attention because of the presence of the five-figure group in the midst of the three-figure groups. The context made it perfectly clear that 25993 was und. Incidentally the encoder had blundered in inserting this five-figure group in the midst of his trinumeral groups, since trinumeral groups were provided for und to avoid this very occurrence. His blunder, however, led to no further results; 25993 proved to occur but 25 times in all the 12444 messages, and code groups numerically on either side of it occurred most infrequently in the messages and could not be variants. Nor would any other code group on the same page work satisfactorily when a meaning alphabetically in the neighborhood of und was assigned to it. It was feared for a while that our code was thoroughly cross-referenced, i. e., entirely unalphabetical. The real facts in this case were discovered later. (See p. 38.)

Following this identification of the lonely und, a study was made of all instances in 12444 in which three-figure groups and five-figure groups occurred side-by-side. No further meanings were found; in fact, no other groups were positively identified for some time, although the blocks 27160–9 and 18130–9 and certain others were seen to behave like prepositions.

(8) The Encipherment: 18470 the Basic Code for 12444, 1777, and 2310

At this stage the work on the code was turned by outside circumstances into a new direction. M. I. 8 had come into the sudden and temporary possession of a large corps of typists, and it was considered wise to prepare as many codes as possible for study while this force was available. 18470, which looked like a constant (i. e., unenciphered) code, was the first one chosen.

In the course of making the index sheets for 18470 it was noticed that the general appearance and range of the code were similar to those of 12444. This relationship once suspected, it was than assumed that its nature might well be similar to that already known to exist between 13040 and 5950, and an effort was made to obtain a starting point for tentative page identifications. The number 1900 is a common "end of the message" indicator in 12444 and the group 2440 was seen to be even more frequently used for the same purpose in 18470. Accordingly it was assumed that page 19 of 12444 might be the equivalent of page 24 of 18470. If this supposition was correct, it was apparent that the 0-block of 10 code groups on a page of 12444 corresponded to the 4-block in 18470. Since this was the identical relationship between the blocks of 5950 and 13040 (see the table, p. 8), it seemed possible that the block transposition table used in that case might have been used again. To test out this possibility, examination was made of the most frequently occurring groups in 12444 and 18470. One of the most frequent groups in 12444 is 63*64*. If the assumed relationship was correct, it was fair to suppose that a group ending in *54* was similarly common in 18470. A search revealed the very frequent occurrence of 18*654*, and this meant, if the theory was correct, that page 63 of 12444 might well be equivalent to page 186 of 18470. In a similar manner 25*876* of 12444 was tentatively identified with 27*166* of 18470, which would make page 258 of 12444 equivalent to page 271 of 18470. A few more common groups were similarly associated.

[9] In this study isolated code groups of 12444 and 1777 are for convenience' sake regularly reduced to their 18470 equivalent. (See sec. 8.) At this stage of the study, the relationship of these three codes had, of course, not been suspected.

Systematic work was then begun to establish further identifications. The effort was made to identify frequently recurring *series* of code groups in the 12444 messages with recurring series in the 18470 messages, the constant variation in the penultimate figure together with the identity of the final figure in each case being the key to the identification. Enough such series were soon found to establish beyond doubt the correctness of the theory, and to identify several additional pages. The following are examples:

18470:	19155	5959	17136		18470:	19103	28115	29845
12444:	1765	4969	3746		12444:	1713	12125	13805

In most cases the series was short. Frequently the correspondence in the penultimate figures of code-groups following groups already identified would give rise to the suspicion that the pages of the second groups were equivalent, and further comparison of the code groups of the pages in question would substantiate the supposition. (This led to the development of the systematic method described below.) Many suppositions turned out to be untenable and had to be discarded after considerable labor. In two cases entire messages in the two codes were found to be almost identical. (See p. 85 *ff*, where one of these messages in two codes is reproduced.) Many tentative identifications were thus confirmed and many new ones made.

The work was gradually systematized as it progressed. When the 1777 messages were examined and seemed, from their general appearance, to represent another encipherment of 18470, a few tentative page identifications were made, mainly from frequently repeated beginnings of messages. When about a dozen such identifications had been made, a set of instructions, based on previous experience, was drawn up, and the work was given over to a clerical force.

It will be remembered that all the occurrences of all the code groups found in the messages in our possession had been put on cards after the fashion generally followed in code study in M. I. 8. (See p. 17.) Each card contained a code group, reference to the message from which that occurrence was taken, the two code groups which preceded and the two which followed it in the message in question. These are the cards referred to in the set of instructions which follows:

The following correspondence in pages has been found:

1777	18470	12444
12	24	19
14	108	188
36	191	17
54	250	285
56	59	49
88	267	254
97	255	294
122	81	110
182	19	224
198	11	155
204	117	114
213	271	258
226	268	26

The method for finding further correspondence is as follows:

1777 AND 12444

Take the cards for a page of 1777 and for a corresponding page of 12444, e. g., 14 and 188. Put together cards with the *same two terminal* digits, e. g., 1421 and 18821. If a code group immediately preceding or

following the group under examination on the card of one code has the *same two terminals* as a group in the same position on the card of the other code, the two pages containing these groups may be regarded provisionally as equivalent. Thus, suppose we find (1777) 1421 30900 and (12444) 18821 2200; we should then regard page 309 of 1777 and page 22 of 12444, provisionally, as equivalent. A record is kept of all such instances with the references to the pages of the messages. Often the same pages will turn up together more than once in examining the same sets of cards and the provisional identification will be substantiated. In any case, after the examination of the cards as described is concluded, the list of probable and possible identifications that have been made is taken, and the cards for these pages are then compared in the same manner as the original set. In the course of this comparison note is made of all (1) confirmations, (2) possible contradictions, and (3) new possibilities.

1777 AND 18470

The original set of 1777 cards can now be passed on to another who can make the comparison with the corresponding cards of 18470. In the example chosen, 14 of 1777 would be compared with 108 of 18470. This work proceeds in the same manner as before with one important modification: 1777 code groups are compared with 18470 groups containing the *same terminal* digit *and* a *penultimate* digit differing from that of 1777 according to the following table. (It is desirable to practice this table for a few minutes so that it can be worked by heart in either direction.) [The table has been given on p. 8.]

Sometimes the provisional identification will extend to several code groups; if the correspondence reaches the end of the groups recorded on the cards in either direction, the messages from which the cards were made should be consulted to see how far the correspondence actually extends.

The labor of working out an encipherment of this kind would, of course, be vastly less in a case in which the messages in the base code could be read; the context would then give many cases of page equivalence.

A few of the intercepted messages were in a code designated as 2310, and our files contained some further messages in this code. 2310 was now seen to be another encipherment of 18470. One peculiar feature of this encipherment is that the Germans gave three designations—2310, 2815, and 80574—to one and the same thing. This appears from the following introductions to messages (the references are to the sheets of the intercepts):

(31 G)	(31 C)	(38 B)
2310	2815	80574
28774	28774	28771
3390	3390	3390
23146	23146	

It is evident that we have here the same text with three different code indicators. 28771 is, of course, a variant for 28774.

In the following two messages we have the same introduction in 2310 and in 2815, followed by messages in 2815 and in 2310, respectively:

(23 E)	(28 C)
2310	2815
28771	28777
22826	22826
3390	3391
954	(22691)
115	692
2815	923
etc.	2310
	etc.

This encipherment is further discussed elsewhere; see note 10; also pages 90 and 96.

The tables of page equivalence among 18470, 12444, and 1777 still contain eight or nine isolated blanks; some of the pages occur so seldom as to provide insufficient material for determining their equivalents. For practical purposes, however, precisely because it is the infrequent pages that are lacking, the tables are just as serviceable as if they contained no blanks. A copy of the tables follows this page. In the case of the high number name groups, 31,000–99,999, the table of parallel numbers remained fragmentary. In some cases the groups are alike in all three encipherments—e. g., 79804, Wilson. In 12444 and 1777 they are always alike. Where a change is made from 18470 in these encipherments it is confined to the first two figures of the group; thus, 38176 in 18470 becomes 78176 in 12444 and 1777. (On this point see p. 61.)

The first result of the proof that these various codes are so closely related to one another was that the frequency of occurrence of individual code groups was greatly increased and opportunities for analysis were thereby extended. The 18470 messages comprised, at the time, about 1,000 sheets, the 12444 material about 800, and the 1777 messages about 400. The material on hand in 18470 and 12444 was already very large, so that this gain was not so great as might at first appear.

The fact that the same transposition table was employed for the word blocks in going from 18470 to 12444 and 1777 as had been used in changing 13040 to 5950 was of psychological value in strengthening the belief that the new code (18470) would prove to have been composed on lines similar to the old one (13040). Up to this point this had really been more of a hope than a belief, and a hope rather shaken by the unpleasant experience with the group 25993 (und) recounted above (p. 18).

It was felt to be reasonably certain that the basic code of the three in question was 18470. The transposition table for the word blocks went in the same direction in going from 18470 to 12444 and 1777 as in going from 13040 to 5950. (See pp. 8; 95 *f.*) Moreover, 18470 was designated in the messages by any of the code groups 18470–9 just as 13040 was designated by 13040–9, while the code indicator number for 12444 and 1777, like that of 5950, was a constant, so that the conclusion seemed quite safe. It will be recalled that in changing the page numbers of 13040 to make 5950, the four-page blocks had been kept intact. (See p. 8.) It was supposed that a similar phenomenon would appear here, and it was a bitter disappointment when the pages proved to have been rearranged one by one instead of by larger blocks.[10]

Later, when the relationship between 18470 and its alphabetical original was being worked out (see p. 34), the advantage derived from the knowledge that 18470 was the base of 12444 and 1777 was very great indeed; the change in going from the alphabetical original to 18470 had been made with true German method, that in transforming 18470 to 12444 and 1777 with an alien carelessness, and the result was that the former had an inherent weakness which was absent from the latter.

[10] In making 2310–2815–80574 the page numbers were changed four pages at a time. This encipherment was not much used at the time of the A. E. F. interceptions, and it seemed fair to conclude that it was older than 1777 and 12444. After the decipherment of the messages this inference was proven, and further light was cast on the dates of the various encipherments, by the telegram (12444 messages, p. 33 *ff.*) reproduced on p. 84.

12444 to 18470

12		18	12		18	12		18	12		18	12		18	12		18
126	10	152	180	60	69	81	110	81	290	160	145	219	210	291	148	260	12
155	11	225	197	61		2	111	303	198	161	196	96	211	240	204	261	177
260	12	94	21	62	137	256	112	115	115	162	227	185	212	270	52	262	144
302	13	44		63	186	163	113	230	242	163	113	173	213	301	220	263	229
106	14	159		64	251	31	114	117	245	164	224	232	214	195	184	264	127
93	15	95		65	199	112	115	162	236	165	27	201	215		77	265	279
150	16	118	216	66	124	288	116	222	154	166	236	277	216	66	289	266	140
234	17	191	139	67	46	114	117	194	42	167	34	95	217	47	254	267	243
307	18	158	171	68	237	16	118	248	34	168	293	239	218	203	26	268	259
224	19	24	60	69	83	91	119	305	207	169	39	140	219	210	98	269	201
99	20		73	70	79	105	120	128	51	170	190	190	220	263	212	270	57
152	21	62	183	71	236	273	121	281	37	171	68	252	221	89	258	271	130
44	22	143	177	72	38	303	122	256	156	172	54	116	222	198	87	272	150
193	23	238	146	73	70	92	123	244	306	173	213	299	223	254	252	273	121
19	24	252	205	74	257	66	124	155	128	174	105	164	224	19	248	274	233
178	25	302	90	75	185	255	125	175	125	175	98	11	225	104	59	275	
226	26	268	179	76	249	296	126	10	89	176	134	103	226	26	142	276	43
165	27	149	100	77	265	264	127	180	261	177	72	162	227	90	38	277	216
149	28	141	304	78	209	120	128	174	199	178	25	286	228	289	240	278	295
	29	235	70	79	200	55	129	30	97	179	76	263	229	193	265	279	205
129	30	146	144	80	85	271	130	107	167	180	60	113	230	298	131	280	100
133	31	114	110	81	110	107	131	280	196	181	50	158	231	45	121	281	306
237	32		203	82	106	157	132	239	291	182	285	298	232	214	235	282	197
191	33	53	69	83	99	249	133	31		183	71	274	233	88	300	283	287
167	34	168	195	84	138	176	134	42		184	264	250	234	17	136	284	187
66	35	204	80	85	41	251	135	282	75	185	212	29	235	253	182	285	250
45	36	297	151	86	35	297	136	284	63	186	55	71	236	165	166	286	228
189	37	171	209	87	272	62	137	102	284	187		68	237	32	283	287	153
72	38	277	233	88	288	84	138	208	143	188	108	23	238	300	88	288	116
169	39	56	221	89	176	259	139	67	200	189	37	132	239	218	228	289	266
102	40	207	227	90	75	266	140	219	170	190	220	211	240	278	101	290	160
85	41	148	246	91	119	28	141	299	17	191	33	56	241	258	210	291	182
134	42	167	202	92	123	206	142	276	243	192	111	292	242	163	58	292	242
276	43	304	194	93	15	22	143	188	229	193	23	267	243	192	168	293	246
13	44	22	12	94	97	262	144	80	117	194	93	123	244	52	53	294	255
231	45	36	15	95	217	160	145	96	214	195	84	257	245	164	278	295	307
67	46	202	145	96	211	30	146	73	161	196	181	293	246	91	104	296	126
217	47	154	94	97	179	57	147	156	282	197	61	50	247	308	36	297	136
208	48	109	175	98	269	41	148	260	222	198	161	118	248	274	230	298	232
	49	59	83	99	20	27	149	28	65	199	178	76	249	133	141	299	223
181	50	247	280	100	77	272	150	16	79	200	189	285	250	234	238	300	283
	51	170	108	101	290	54	151	86	269	201	215	64	251	135	213	301	206
244	52	262	137	102	40	10	152	21	46	202	92	24	252	273	25	302	13
33	53	294	159	103	226	287	153	221	218	203	82	235	253	309	111	303	122
172	54	151	225	104	296	47	154	166	35	204	261	223	254	267	43	304	78
186	55	129	174	105	120	124	155	11	279	205	74	294	255	123	119	305	58
39	56	241	82	106	14	147	156	172	301	206	142	122	256	112	281	306	173
270	57	147	130	107	131	309	157	132	40	207	169	74	257	245	295	307	18
305	58	292	188	108	101	18	158	231	138	208	48	241	258	271	247	308	
49	59	275	48	109		14	159	103	78	209	87	268	259	139	253	309	157

12 in the column headings signifies 12444, and 18, 18470.
To convert *12444 into 18470* take 12444 page number from central column; the corresponding page of 18470 is then at the *right*.
To convert 18470 into 12444 take 18470 page number from central column; the corresponding page of 12444 is then at the *left*.
The page number of the code *from* which the change is to be made is always taken from the central column.

1777 to 18470

17		18	17		18	17		18	17		18	17		18	17		18
232	10	94	17	60	211	197	110	53	292	160	120	151	210	287	91	260	122
198	11	71	245	61	107	118	111	283	67	161	270	60	211	290	81	261	126
28	12	24	90	62	104	217	112	93	252	162	193	193	212		238	262	196
144	13	15		63	145	223	113	223	294	163	173	216	213	271	275	263	98
106	14	108		64	171	152	114	96	83	164	174	138	214	181	77	264	125
13	15	79	200	65	259	174	115	133	253	165	151	191	215	40	127	265	123
29	16	135	55	66	294	37	116	204	176	166	292	126	216	213	288	266	199
129	17	60	21	67	161	204	117	30	281	167	304	178	217	112	88	267	129
136	18	177	185	68	154	52	118	111	257	168	205	155	218	232	226	268	101
182	19	238	237	69	240	175	119	80	71	169	252	272	219	235	101	269	95
45	20	227	103	70	37	160	120	102	290	170	134	309	220	54	161	270	186
189	21	67	11	71	169	235	121	152	64	171	139	256	221	141	213	271	282
	22	149	284	72	187	260	122	81	276	172		274	222	224	27	272	219
40	23	249	196	73	92	265	123	39	163	173		113	223	113	57	273	159
12	24	150	308	74	244	285	124	147	164	174	115	222	224	233	149	274	222
51	25	131	181	75	148	264	125	201	146	175	119	283	225	246	302	275	263
137	26	241	148	76	236	261	126	216	141	176	166	187	226	268	202	276	172
134	27	272	201	77	264	108	127	265	18	177	90	20	227	299	201	277	42
186	28	12	50	78	143	230	128	285	280	178	217	59	228	266	58	278	300
	29	16	15	79	258	267	129	17	254	179	209	33	229	242	80	279	231
117	30	58	119	80	279	207	130	47	96	180	284	205	230	128	305	280	178
143	31	106	122	81	261	25	131	307	214	181	75	279	231	251	36	281	167
203	32	83	288	82	91	34	132	289	249	182	19	218	232	10	271	282	245
133	33	229	32	83	164	115	133	33		183	253	224	233	138	111	283	225
250	34	132	85	84	55	170	134	27		184	103	236	234	207	180	284	72
107	35	202	102	85	84	16	135	97	258	185	68	219	235	121	128	285	124
246	36	191	87	86	50	42	136	18	270	186	28	76	236	234	142	286	198
70	37	116	94	87	86	157	137	26	72	187	226	98	237	69	210	287	303
	38	281	296	88	267	233	138	214	306	188		19	238	262	158	288	82
123	39	46	248	89	57	171	139	142	156	189	21	100	239	43	132	289	100
215	40	23	177	90	144	293	140	52	243	190	62	69	240		211	290	170
46	41	309	82	91	260	221	141	176	36	191	215	26	241	296	154	291	105
277	42	136	73	92	297	139	142	286	303	192		229	242	200	166	292	160
239	43	254	112	93	206	78	143	31	162	193	212	194	243	190	159	293	140
304	44	153	10	94	87	90	144	13	95	194	243	74	244	298	66	294	163
307	45	20	49	95	194	63	145	305	269	195	208	282	245	61	259	295	155
39	46	41	114	96	180	206	146	175	262	196	73	225	246	36	241	296	88
130	47	306	135	97	255	124	147	257	299	197	110	298	247	156	92	297	56
300	48	109	263	98	237	75	148	76	286	198	11	109	248	89	244	298	247
	49	95	255	99	203	22	149	274	266	199	256	23	249	182	227	299	197
86	50	78	289	100	239	24	150		242	200	65	54	250	34	278	300	48
	51	25	268	101	269	165	151	210	125	201	77	231	251	157	104	301	277
140	52	118	120	102	85	121	152	114	35	202	276	169	252	162	209	302	275
110	53	308	184	103	70	44	153		99	203	32	183	253	165	287	303	192
220	54	250	62	104	301	68	154	291	116	204	117	43	254	179	167	304	44
84	55	66	291	105	158	295	155	218	168	205	230	97	255	99	145	305	280
297	56	59	31	106	14	247	156	189	93	206	146	199	256	221	47	306	188
89	57	273	61	107	35	251	157	137	234	207	130	147	257	168	131	307	45
30	58	278	14	108	127	105	158	288	195	208		79	258	185	53	308	74
56	59	228	78	109	248	273	159	293	179	209	302	65	259	295	41	309	220

17 in the column headings signifies 1777, and 18, 18470.

To convert either code into the other, follow the directions given on the preceding table for converting 12444 into 18470 and 18470 into 12444.

2310, 2815, and 80574 (see p. 20) to 18470)

(Parentheses indicate that the equivalence is assumed on the basis of the correspondence of other pages in the same 4-page block)

23		18	23		18	23		18	23		18	23		18	23		18
58	10	46	48	60	12	258	110	98	192	160	232	130	210	150	188	260	112
59	11	47	49	61	13	259	111	99	193	161	233	131	211	151	189	261	113
60	12	48				260	112	100				132	212	152			
61	13	49	26	62	70	261	113	101	90	162	202	133	213	153	(306)	262	102
			(27)	63	71				91	163	203				307	263	103
42	14	18	(28)	64	72	206	114	194	92	164	(204)	134	214	106	308	264	104
43	15	19	(29)	65	73	207	115	195	93	165	205	135	215	107	309	265	105
(44)	16	(20)				208	116	196				136	216	108			
45	17	21	38	66	54	209	117	197	86	166	(286)	137	217	109	178	266	174
			39	67	55				87	167	287				179	267	175
14	18	26	40	68	56	274	118	(198)	88	168	288	222	218	250	180	268	(176)
15	19	(27)	41	69	57	275	119	199	89	169	289	223	219	251	181	269	177
(16)	20	(28)				276	120	200				224	220	252			
17	21	(29)	62	70	34	277	121	201	230	170	290	225	221	253	286	270	234
			63	71	(35)				231	171	291				287	271	235
30	22	50	64	72	36	126	122	126	(232)	172	292	174	222	218	(288)	272	236
(31)	23	51	65	73	37	127	123	127	233	173	293	175	223	219	289	273	237
32	24	52				128	124	128				176	224	220			
33	25	53	238	74	86	129	125	129	266	174	222	177	225	221	242	274	118
			239	75	87				267	175	223				243	275	119
18	26	62	240	76	88	122	126	122	(268)	176	224	146	226	186	244	276	120
(19)	27	(63)	241	77	89	123	127	123	269	177	225	147	227	187	245	277	121
(20)	28	(64)				124	128	124				148	228	188			
(21)	29	(65)	202	78	282	125	129	125	(98)	178	266	149	229	189	154	278	242
			203	79	283				99	179	267				155	279	(243)
34	30	22	204	80	284	282	130	210	100	180	268	158	230	170	156	280	244
35	31	(23)	205	81	285	283	131	211	101	181	269	159	231	171	157	281	245
36	32	24				284	132	212				160	232	(172)			
37	33	25	234	82	154	285	133	213	94	182	298	161	233	173	78	282	130
			235	83	155				95	183	(299)				79	283	131
70	34	30	236	84	156	(294)	134	214	96	184	300	270	234	82	80	284	132
(71)	35	31	(237)	85	157	295	135	215	97	185	301	271	235	83	81	285	133
72	36	32				296	136	216				272	236	84			
73	37	33	74	86	166	297	137	217	226	186	258	273	237	(85)	(166)	286	270
			75	87	167				227	187	259				167	287	271
54	38	66	76	88	168	142	138	142	228	188	260	150	238	74	168	288	(272)
55	39	67	77	89	169	143	139	143	229	189	261	151	239	75	169	289	273
56	40	68				(144)	140	144				152	240	76			
57	41	69	246	90	162	145	141	(145)	102	190	158	153	241	77	170	290	306
			247	91	163				103	191	159				171	291	307
50	42	14	248	92	164	138	142	138	104	192	160	278	242	274	172	292	308
51	43	15	249	93	165	139	143	139	105	193	161	(279)	243	275	173	293	309
52	44	(16)				140	144	(140)				280	244	276			
53	45	17	250	94	182	(141)	145	141	114	194	206	281	245	277	106	294	(134)
			251	95	183				115	195	207				107	295	135
10	46	58	252	96	184	302	146	226	116	196	208	198	246	90	108	296	136
11	47	59	(253)	97	185	303	147	227	117	197	209	199	247	91	109	297	137
12	48	60				304	148	228				200	248	92			
13	49	61	110	98	(178)	305	149	229	(118)	198	246	201	249	93	182	298	254
			111	99	179				119	199	247				(183)	299	255
22	50	42	112	100	180	210	150	238	120	200	248	218	250	94	184	300	256
23	51	43	113	101	181	211	151	239	121	201	249	219	251	95	185	301	257
24	52	44				212	152	240				220	252	96			
25	53	45	262	102	190	213	153	241	162	202	78	221	253	(97)	254	302	146
			263	103	191				163	203	79				255	303	147
66	54	38	264	104	192	82	154	278	(164)	204	80	298	254	302	256	304	148
67	55	39	265	105	193	83	155	279	165	205	81	299	255	303	257	305	149
68	56	40				84	156	280				300	256	304			
69	57	41	214	106	294	85	157	281	194	206	114	301	257	305	290	306	(262)
			215	107	295				195	207	115				291	307	263
46	58	10	216	108	296	190	158	230	196	208	116	186	258	110	292	308	264
47	59	11	217	109	297	191	159	231	197	209	117	187	259	111	293	309	265

23 in the column headings signifies 2310 (2815, 80574), and 18, 18470.

To convert either code into the other, follow the directions given in the table above for converting 12444 into 18470 and 18470 into 12444.

12444 to 1777

12		17	12		17	12		17	12		17	12		17	12		17
12	10	121	96	60	237	33	110	122	105	160	63	283	210	154	303	260	28
183	11	283	130	61		300	111	287	212	161	262	101	211	69	296	261	18
19	12	10	225	62	157	194	112	174	229	162	20		212	161	161	262	90
93	13	304	160	63	270	299	113	205	306	163	223	258	213	104	175	263	33
188	14	273	37	64	231	145	114	204	128	164	222	196	214	269	255	264	108
70	15	49	268	65	266	249	115	252	54	165	134	102	215	188	92	265	80
251	16	52	53	66	285	35	116	274	58	166	142	173	216	55	65	266	293
180	17	36	198	67	39	129	117	95	43	167	250	256	217	130	55	267	94
24	18	105	47	68	98	192	118	109	279	168	159	298	218	99	108	268	65
23	19	12	211	69	32	144	119	145	24	169	123	29	219	151	214	269	125
162	20		189	70	15	137	120	230	176	170	243	172	220	275	63	270	89
139	21	190	207	71	76	10	121	38	259	171	185	28	221	248	135	271	207
27	22	78	284	72		110	122	199		172	220	164	222	286	140	272	24
76	23	19	202	73	103	169	123	74		173	216	163	223	43	14	273	235
272	24	169	123	74	147	57	124	295	112	174	291	274	224	182	116	274	224
107	25	209	41	75	258	269	125	146	91	175	263	293	225	62	220	275	
56	26	226	71	76	23	277	126	232	154	176	170	26	226	137	156	276	239
87	27	22	184	77	127	77	127	96	227	177	284	141	227	177	134	277	126
260	28	221	22	78	179	182	128	164	95	178	51	289	228	132	238	278	259
150	29	219	241	79	242	234	129	117	78	179	148	292	229	162	158	279	168
305	30	206	265	80	102	217	130	61	136	180	17	120	230	244	199	280	289
82	31	152	204	81	197	295	131	305	90	181	86	64	231	307	42	281	47
69	32		246	82	31	228	132	100	224	182	128	126	232	138	257	282	299
263	33	110	245	83	255	191	133	143	235	183	11	84	233	296	11	283	210
157	34	257	186	84	233	165	134	277	159	184	77	40	234	129	177	284	72
46	35	116	195	85	46	94	135	271	171	185	193	273	235	183	66	285	54
17	36	92	181	86	107	307	136	180	149	186	84	250	236	253	222	286	59
288	37	64	151	87	27	226	137	120	103	187		60	237	203	111	287	44
121	38	301	254	88	158	232	138	195	215	188	14	52	238	278	203	288	37
67	39	297	270	89	141	206	139	21	152	189	70	276	239	155	280	289	228
193	40	234	262	90	181	244	140	272	21	190	309		240	58	51	290	292
253	41	75	148	91	175	89	141	227	201	191	133	104	241	79	174	291	249
297	42	281	36	92	265	166	142	202		192	118	79	242	294	290	292	229
223	43	167	301	93	13	133	143	306	185	193	40	170	243	303	266	293	225
287	44		209	94	135	302	144	119	267	194	112	230	244	140	242	294	97
99	45	246	117	95	178	119	145	114	138	195	85	197	245	83	124	295	131
85	46	35	127	96	60	125	146	196	146	196	214	45	246	82	233	296	261
281	47	68	294	97	254	74	147	247	81	197	245	147	247	53	39	297	42
48	48	48	68	98	101	179	148	91	155	198	67	221	248	149	50	298	218
15	49	56	218	99	45	248	149	186	122	199	280	291	249	115	282	299	113
304	50	298	132	100	201		150	29		200	156	167	250	236	208	300	111
178	51	280	98	101	211	219	151	87	100	201	191	309	251	16	38	301	93
16	52	238	80	102	215	31	152	189	142	202	73	115	252	57	59	302	144
247	53	66	73	103	187		153	256	237	203	288	236	253	41	243	303	260
285	54	165	213	104	241	210	154	176	114	204	81	97	254	88	13	304	50
216	55	267	18	105	160	239	155	198	113	205	308	83	255	264	131	305	30
49	56	26	106	106	106	200	156	276	30	206	139	153	256	217	143	306	163
252	57	124	86	107	25	62	157	34	271	207	71	34	257	282	231	307	136
240	58	166	264	108	268	88	158	279		208	300	75	258	213	205	308	
286	59	302	118	109		168	159	184	25	209	94	278	259	171	190	309	251

12 in the column headings signifies 12444, and 17, 1777.

To convert either code into the other, follow the directions given in the table above for converting 12444 into 18470 and 18470 into 12444.

(9) Identifications of Code Groups by Analysis; Introductions to Forwarded Messages

A few words, almost uniformly prepositions, were now identified by analysis with reasonable certainty. The Germans were forced, in communicating with South America, because of the British cable control, to relay messages at Madrid. Berlin would wireless to Madrid, and Madrid would then get the messages to South America in any way that presented itself. In the course of examining the 12444 messages, the occurrence of the code group 26040 near the beginning was noticed in some of the telegrams. The group was not in the usual position of the code indicator, but, on the contrary, was preceded by several groups that were undoubtedly in 12444. Accordingly the identity of this group with the indicator number of another German code (see p. 8) was at first thought to be a coincidence. On trial, however, the messages, from the point where the group 26040 occurred, were found to afford a reading in 26040. Moreover, one of the messages (A. E. F. messages, p. 12C) was found to be identical with a code message taken from the mails by the New York censor on its way to Barranquilla, Colombia. The conclusion was accordingly drawn that the 12444 code groups preceding the 26040 messages comprised forwarding directions addressed to Madrid.

These forwarding directions uniformly contained, at or near the beginning, the group 27160, and this group with its variants, 27161, etc., was taken to mean fuer. A study of other occurrences of this group revealed the fact that when it stood at the beginning of a message a message in another code often followed. Further investigation showed that in the 12444 messages, page 815, there was a message going from Berlin beginning 25875 14326 (in 18470, 27165, 18816), while on page 723 was another going from Madrid to Berlin beginning 19648 14326 (in 18470, 18138, 18816). It was considered at least probable that 18138 was von. A number of messages began with 28524 25469 18860 22430 11012 2651 15065 1138 (e. g., 12444 messages, p. 687), while others began 11012 2651 15065 1138 22430 28524 25469 18860. (In 18470 the two beginnings read, respectively, 25014 26759 10850 1920 8102 26891 1655 22528 and 8102 26891 1655 22528 1920 25014 26759 10850.) The conclusion was drawn that that part of the message preceding 1920 in each case denoted the sender of the message; that the part following 1920 was the recipient, and that 1920 meant an. 18654 was found in such phrases as 18134 (first read as von, later found to be vom, see p. 29) 19155 18654 5959, while in the phrase 27165 (fuer) 19155 5959 (18470 messages, p. 453 A, etc.) 18654 was absent. This led to the identification of 18654 as in and to the supposition that the group following it was a place name. Similarly, other prepositions—auf, nach, aus, durch—were identified.

As identifications were made they were entered first on cards and then in a tentative code book. In each case a reference to the passage or passages in the messages which had led to the identification was inserted after the meaning assigned to the code group. The practice of recording these references was continued until some 3,500 code groups had been identified.

The telegram on page 191 of the 12444 messages was thought, from the 26040 message that it contained, to be intended for Buenos Aires, and a study of the group 18816 which appeared before 5581 (Buenos Aires) led to the conclusion that it might well be Gesandtschaft. The constant occurrence of the group 11604 in the introductions to the messages to be forwarded led to its interpretation as weitergeben, and a thorough study of all its occurrences

greatly strengthened this supposition. Weeks later this was discovered to be an error: 11604 is regularly preceded by a number, and this number was found to coincide with the number of code groups in the message to be forwarded; accordingly 11604 means Gruppen, but, since it is used so frequently in the circumstances described, results obtained from taking it as weitergeben were not invalidated.

The 26040 message found in 12444 messages, page 189, is forwarded without an indicator number, and was tried out and read as 26040 from its general appearance. Since there was no code indicator, the exact point at which the forwarded message began was not known, and the four groups 22331 19563 16277 22331 were at first assumed to be part of the forwarding directions, and were not deciphered with the rest of the message.[11] They were striking because of the repetition of the group 22331. Later it was found that the four groups were really part of the forwarded message and read: "Nummer 3 auf Nummer ____." This discovery had a most important bearing on the study of 18470. The group 17136 is very common in that code, and especially so at or near the beginning of *forwarded* messages. It appeared possible that this group might signify Nummer, and might be used to give a special serial number to the forwarded message that followed, distinct from the main serial number given in the trinumeral code as the opening group of the message. A search was made to see whether 17136 could be found in circumstances similar to those in which 22331 had been found in the 26040 message, and the following cases, among others, were found in the 18470 messages:

Page 94	Page 453	Page 466
17136	17136	17136
26326	13668	23596
8499	15317	8498
17136	17136	17136

It was further found that certain forwarded messages had their numbers expressed in the trinumeral code, and that when this was the case the group 17136 *never* appeared at the beginning of the message. The forwarded message would begin *either* in the trinumeral code *or* with 17136, etc. This made the identification of 17136 as Nummer a practical certainty, and meant that almost without exception the following group in the message would be a number.[12]

[11] It may be that the greater resemblance of numbers to one another had some influence on the German Foreign Office in its choice of numeral codes in preference to letter codes. From the standpoint of the possibility of mutilations these figure codes with their one-figure difference are far inferior to five-letter codes with a two-letter difference. If one figure is mutilated, in a code of 30,000 code groups, there may be 37 or 38 possibilities to be considered in attempting to restore the garbled text of a five-figure code group, while in the case of five-letter codes with a two-letter difference these possibilities are limited to five.

[12] The generosity of the Foreign Office in its use of the word Nummer is acknowledged by the writer with gratitude. In the case of one 26040 message it was guessed as the first word and furnished the key to the additive of that message as well as of a whole series of messages in which the additive had been similarly employed. (See p. 14.) In the case of 18470 this word was of very great assistance in the actual breaking of the code.

It would seem that the encoder in the Foreign Office, when he came to the word Nummer introducing a message within a message, found himself in a dilemma. On the one hand he had almost certainly been told to use the trinumeral code at the beginning of a message, and to use it at the beginning of a message only. Now in the case of a message within a message the encoder was confronted by a beginning that was not a beginning, so that his instructions told him both to use the trinumeral code and not to use it. Accordingly, sometimes he used it and sometimes he did not. Even so, the actual use of the word Nummer in cases where the trinumeral code is not employed, instead of beginning with the number itself and omitting the word Nummer, is a useless waste, and achieves no result except the weakening of the carefully planned code structure.

90481—37——3

At the same time, and by a similar analysis (see the messages quoted on p. 29), the very common group 30020 was identified as Telegramm or Telegramm Nr., and as in the case of 17136, code groups following this in messages were almost certain to represent numerals.[13]

Introductions to messages to be forwarded gave the first line on the punctuation system. 3670 and 3672 coming at the end of such introductions were taken to be colons, and further study made it clear that page 36 was devoted largely if not exclusively to punctuation. With the aid of the introducing groups 27160 (fuer) and 18136 (von), a collection was made of introductions to messages sent for forwarding on the theory that the last group of the introduction was certain, in the majority of cases, to be a stop of some kind. Where the forwarded message was in the same code as the introduction, the dividing line between the two was not clear unless the forwarded message began with the trinumeral code. Many forwarded messages, however, were in codes other than the introduction, and in many of these cases the general appearance of the codes differed so markedly that the end of the introduction was quite clear.

An examination of the final groups of the introductions revealed that the terminal figure was predominantly 1 or 2. It had been assumed that stops would be freely sprinkled through the book as in 13040. It now seemed fairly certain that the stops would be found to end in the digits 1 and 2. Detailed study afterward showed that this conclusion required modification and amplification. (See pages 58 *f.*)

Introductions to messages going to South America likewise paved the way for the hypothesis, later confirmed, that the composition of 18470 differed in one important respect from that of 13040. It will be remembered that in the latter code all proper names were found in the high number groups 24,000–99,999. (See p. 6.) In the message introductions of 12444 it appeared reasonably sure from the accompanying 26040 messages that 5581 was Buenos Aires and that 4211 was Santiago. At first this was interpreted to mean that some proper names—probably mainly, if not entirely, geographical—had been inserted in the body of the vocabulary. The identification of 18654 as in, however, led to the formation of the theory that these pages contained names only. The preposition in, occurring as it does so frequently with place names, led to the identification of many groups as names of places, even though it was not known which places they represented. These place names appeared on low numbered pages—none of the pages bore a higher number than 80—and pages containing one place name were found to be furnishing others. A study was accordingly made of all pages up to page 80 from this point of view.

While some were found to be clearly vocabulary pages and others grammatical pages, the bulk of these pages, mainly on the basis of the test with in, were felt to contain place names and place names only. The comparatively small number of groups from these pages that were found in actual use in the messages helped to confirm this view; and later the absence of numerals on these pages (see p. 30) showed conclusively that they did not belong to the vocabulary proper. How further names on these pages were identified will be shown later. (See p. 55.)

[13] The following is a copy of the first memorandum showing signs of a break in the code (14213 was wrongly identified and turned out to mean Wiederholung. 4847, instead of hundert, was found to mean zehn).

"17136—Nummer.—It begins messages forwarded for and from 3415 and 5959, and 'Nummer' is a favorite word for beginning such forwarded messages. Moreover it is *never* used when one of these messages contains its number in the Dreinummerheft, as on pp. 25, 84, 478, 533, 952, 6, etc., [of the 18470 messages].

"30020—Telegramm (nr.). See Frequency Book, and note connection with 15317.

"14213—Empfang, empfangen, Empfangsschein (?). To be tested. [See p. 39.]

"4847—A frequently occurring number (?) which may be hundert.

"8498—Auf. See, e. g., 466k.

"15317—Im Anschluss an. See especially pp. 435, 464, and 817. [The essential parts of these messages are quoted on p. 29.] Note that the introduction of the forwarded message tallies with the wording of the three-figure introduction above. With 17136 it gives the phrase Nummer ------ im Anschluss an Nummer -------."

A comparison of the three messages in 18470, pages 453, 464, and 817 led to the identification of the group 15317. The beginnings of these messages are as follows:

	Page 453			Page 464			Page 817	
a	285	Nr 8	a	692	Nr 9	a	555	Nr. 14
b	937	80	b	169	33	b	851	82
c	961	Vom 2 Juli	c	362	Vom 11 Juli	c	744	Im Auschluss an
d	728	Antwort Auf Tel.	d	744	Im Auschluss an Tel.	d	692	Nr 9
e	878	Nr 7	e	285	Nr 8	e	169	33
f	316	53	f	937	80	f	18475	Code indicator
g	18478	Code Indicator	g	18470	Code Indicator	g	27167	Fuer
h	27165	Fuer	h	27164	Fuer	h	19107	
i	19155		i	19155		i	8967	
j	5959	(a place)	j	5959	(a place)	j	5959	(a place)
k	17136	Nummer	k	17136	Nummer	k	17136	Nummer
l	13668	A Number	l	13249	a number	l	23489	(a number)
			m	15317		m	15317	
			n	30020	Tel. Nr.	n	17136	Nummer
			o	13668	a number	o	13249	(a number)

The trinumeral introductions showed the interrelation of these messages. A comparison of 464 m–o with 453 k–l and of 817 m–o with 464 k–l showed that this relationship was again referred to in the messages proper, and fixed 15317 as Im Auschluss an. Later, when 19155 had been identified as Generalkonsulat (see p. 39) it was seen that 817 h–i had written this word in two groups— 19107 (General) 8967 (Konsulat).

(10) The "Breaking" of the Code

All the identifications of words up to this point were independent of one another so far as the structure of the book was concerned. True, one group had helped in identifying another, but purely as the result of analysis. The feeling that the code would turn out to be an alphabetical code rearranged on lines similar to those of 13040 was still merely a feeling. The actual break in the code—the point at which new identifications would begin to be made not purely by analysis, but by analysis assisted by a knowledge of the method of the composition of the book—had not yet arrived. But it was now at hand.

A study of the groups following Telegramm Nr. showed the very frequent presence of one of the series 18130–9 at a distance of two or three groups from 30020. This series had been identified as von. In the endeavor to find an alphabetical arrangement, search had been made to find vo*m* in the neighborhood of vo*n*, but without success. The occurrence of these supposed von groups in the circumstances described provided the answer to this puzzle: Occurring after Telegramm Nr. the groups could be nothing but the beginning of a date, and must signify vo*m* and not vo*n*. Examination showed that only the groups 18130–5 were used for this purpose, 18136–9 not being found in the position in question. Accordingly, 18130–5 was seen to be vom and 18136–9 von, and the first sign of the alphabetical structure of the code was apparent.

It will be remembered that von had been identified from its use in the introduction to forwarded messages, and that the whole block 18130–9 had been found to be used in this way. (See p. 26.) Later it was found that where such a message was introduced by 18130–5 the next group was never a name (which would be preceded by von) but was uniformly a masculine or neuter noun, such as Konsul or Konsulat (which would be preceded by vom).

Vom proved of further value still. If there was no flaw in the reasoning, such a phrase as 30020____ 18130____ ____ would mean Telegramm Nr. ____ vom (a number) (a month). This meant that a new supply of numerals was opened up, and that the 12 months of the year should

be found with no great difficulty, even though the identification of the individual months would require further labor.

A very frequent numeral group was 4847. Such phrases as 30020 (Tel. Nr.) 4847 6705 18130 26478 15433 were quite common at a certain point in the messages. This point was in the midst of messages numbered between 1000 and 1100, and dated—all this in the trinumeral code—in the months of July and August. The conclusion was drawn that these references were to telegrams of recent date, that the group 4847 was 10, and that the month two groups removed from vom (15433) was Juli. True, there was no way of telling whether the reference was to other telegrams of the sender or to telegrams of his correspondent at the other end. This, however, was not a serious difficulty. A list had been made of all telegrams in our collection going from Berlin to Madrid and a similar list of messages going from Madrid to Berlin. This list recorded the numbers of the messages, their dates, and any references to other messages that were found in the trinumeral introductions. Now it chanced that Berlin and Madrid kept very closely abreast in their sending of messages, so that, say, number 1024 of Berlin and number 1024 of Madrid would be sent at about the same time, and, for the present, it was not necessary to worry as to whose telegrams were referred to.

The whole theory concerning vom, 10, and Juli was presently confirmed in an unexpected manner. The introduction to the 26040 message to South America referred to above (p. 26) contained, in 12444, the phrase 19642 20808 4743 (transposed into 18470: 18132, 4848, 15433). The group 4848, higher by one than 4847, might very well be the corresponding ordinal, 10ten, and the phrase would then read vom zehnten Juli. Now the 12444 message was dated December 22, but the 26040 message began with the words Nummer 2 vom 10ten Juli, and it was perfectly clear that the December message was a repetition of an old telegram, and that the 12444 introduction referred to this fact. The presence of this message in the files, while it furnished no new words, converted what had previously been merely reasonable supposition into absolute certainty.[14]

(11) The Numerals

With the aid of the phrase Telegramm Nr ____ vom ____ ____ the list of the 12 months was now made up, since it was known that in every occurrence of this phrase the last word must be a month, and the last word but one must be an ordinal numeral not greater than 31.

The occurrences of all the months in the 18470, 12444, and 1777 messages were assembled, and a list was made of all code groups occurring between vom and the name of a month. 10 had already been identified. It was seen that another dating number, and one other only, occurred on the same page as 10. Further investigation disclosed the fact that there were uniformly two numbers to a page of the code book, as in the case of 13040.

[14] The introduction to this message as deciphered later reads as follows:

In 12444	In 18470	
20623	14213	Wiederholung
8720	27210	des
13071	10761	Post-chiffres
25874	27164	fuer
18090	6080	Bogota
19642	18132	vom
20808	4848	10ten
4743	15433	Juli
25329	30919	dieses Jahres
24986	13376	48
28814	11604	Gruppen
25362	30952	stop

It will be remembered that in the case of 13040 the numerals were so inserted that the terminal digit of the numeral and the terminal digit of the corresponding code group, when added together, gave a total of 10. No similar procedure was followed in 18470—the work of identification would of course have been easier if it had been. Instead, it was found that the code groups for these ordinal numbers ended in 9, 8, 7, and 6, and that the two ordinals on a page ended either in 9 and 8 or in 7 and 6. 10ten ended in 8, the other ordinal in 9. This other number was, in all probability, either 9ten or 11ten, with the chances all in favor of the former, since the system probably began with 1 rather than with 0.

The group 10326 was found to occur frequently *after* the names of months, while 10327 was found between vom and the name of a month. Occurring after a month, 10326 was regularly followed by another number group. An example is the phrase 18130 8449 2709 10326 8448. These circumstances led to the conclusion that 10326 (10327 was assumed to be the corresponding ordinal) denoted the century—19—and that of the numbers that followed it the most frequent were 14, 15, 16, and 17, to make 1914, 1915, 1916, and 1917, the 4 years immediately preceding the year in which the messages were sent.

5, 6, 7, and 8 were obtained from the telegram numbers as 10 had been. (See p. 30.) This gave a sequence of numbers from 5 to 10, as follows (the *cardinals* are given):

6808	5
6877	6
4766	7
4725	8
4888	9
4847	10

and showed that the scheme of arrangement of the numbers was—

Code group terminal	Number
8	a odd
7	b even (=a+1)
6	c odd (=b+1)
5	d even (=c+1)
8	e odd (=d+1)
7	f even (=e+1)

It was now possible to say of any numeral group whether it represented an odd or an even number. Moreover, it was known in what digit the code group representing each number would end; to continue the table above, the code equivalent for 11 would end in 6, while the code groups for 12, 13, 14, and 15 would terminate respectively in 5, 8, 7, and 6, etc. The peculiar sequence of the pages, which was to be of vital significance in the further recovery of the book, now began to be apparent. It was assumed that here, as in the case of 13040, the numerals had been inserted in the original straight alphabetical book, and that the arrangement of the pages, in the order of the numerals they contained, would give the alphabetical sequence of the pages. When pages began appearing in pairs, as, for example, pages 47 and 48 in the table above, this assumption was very greatly strengthened.[15]

It was at first supposed that one pair of consecutive pages would be followed by another pair, and so forth. When the gradual identification of further numeral groups proved that this supposition was wrong, it was thought that the arrangement might prove to be pair, single page, pair, single page, etc. This latter arrangement, indeed, proved very enticing. It was upset, and the true system found, largely by the peculiarity in the numbering of a single message.

[15] As it is, the numerals are in sequence, paralleling the alphabetical vocabulary; if this parallelism had been destroyed by scattering them through the book, the encoder would have had difficulty in finding the numerals desired.

On September 11 Ratibor sent a long message to Berlin, numbered 1222, which related to the German-Spanish controversy about submarine warfare. Three messages were found in close proximity to this one which were peculiar in the complete absence of trinumeral groups at the beginning. These also went from Ratibor to Berlin, and had similar beginnings. These messages are given in full on page 72*ff*. The beginnings of the three messages are as follows:

18470 messages, page 707---- 3239 27206 6705 22417
18470 messages, page 714---- 3258 27206 6705 22417
18470 messages, page 726---- 9496 18138 30020 6705 22417

It seemed likely that the message number of these telegrams was given in 18470 instead of the Dreinummerheft, and 6705 was known to be a number from its occurrence in dates. The three telegrams were accordingly conjectured to be continuations of no. 1422, and 6705 was taken to be 14, and 22417 to be 22. 6705 for 14 fitted very well because it was elsewhere found following 10326 (see p. 31) to make what would then be the combination 19–14. Moreover, ending in 5, it had the proper termination. 22417, however, while it terminated properly for 22, would not fit into the supposed scheme of arrangement of the pages.

The numbers were tried out in the various possibilities allowed by their terminals and more and more of them were gradually fixed by other evidence. Thus, the references to telegrams in the body of messages helped fix many of them. 31 was fixed by the fact that the other number of the page was absent from the list of days of the month. The true arrangement of the pages gradually became apparent, and the recalcitrant 22417 then settled into the position for which it had all along been contending. The table of pages with numbers from 1 to 31 as it now appeared was as follows:

3238	1		4725	8		8356	15		22417	22		26418	29
3257	2		4888	9		8315	16		20366	23	August	26477	30
1926	3	an	4847	10		8448	17	auf	20325	24		23596	31
1995	4		6796	11		8467	18		20438	25			
6808	5		6705	12		10326	19		20477	26			
6877	6		10418	13	April	10395	20		22386	27			
4766	7		10487	14		22458	21		22315	28			

The most gratifying part of the arrangement was that when the few words beginning with A, which had been identified and which are here inserted, an, auf, April, August (the identification of the months will be described presently), were inserted opposite their respective pages they were seen to run in alphabetical sequence, proving that the sequence of the numerals and the alphabetical sequence of the code pages were identical.

In addition to the numerical sequence of two numbers to a page beginning with no. 1, 13040 has, on pages alphabetically preceding this sequence, a series of numbers, two to a page, running 0, 00; 000, 01; 02, 03, etc., to 09. By analogy it was thought that 08 and 09 would be found in 18470 on page 31, and nos. 33 and 34 on page 236. Both these expectations were fulfilled, though the finding of 33 showed that a change was made at that point in the correspondence of the number with the terminal digit of its code group.[16] (See p. 34.)

(12) The Months

In the meantime, however, the 12 months of the year had all been identified. It will be remembered that Juli was the first to be found. (See p. 30.) Juni was identified in a similar

[16] The number of code groups apparently used for days of the month seemed at first too large, since there were 33 different groups instead of the expected 31. The difficulty was solved by assuming that two of these would turn out to be *words* for numbers instead of numeral groups. This assumption was confirmed, 24343 and 18585 being identified as erster and zweiter, respectively. 24343 had the wrong terminal digit for a numeral group, but 18585, by a coincidence, ended in a 5, and might, accordingly, have been a numeral.

manner to Juli. It should have been found at once because of its occurrence on the same page as Juli; instead, this proximity was not noticed until after the identification, and furnished a pleasant surprise, since it confirmed the alphabetical arrangement.

The main criteria for locating the other months were two: The month most referred to in a collection of messages covering a period of about a month is most apt to be a recent one—the current month, the month preceding it, or the month before that; it would be strange if the messages, say, for August, contained references mainly to January. This served to arrange the months roughly as to the time of year to which they referred. The use of the table of telegrams referred to above (p. 30) led to more definite results. If a telegram contained mention of Telegramm Nr 1032 vom 19ten—, it was merely necessary to consult the list, if it contained the telegram in question, and see on the 19th of which month telegram no. 1032 had been sent. Other little points were also of assistance: The months were divided into long and short months, according to the mention or nonmention of the 31st; and February was fixed by the absence of the 29th, 30th, and 31st. By a combination of all these methods the whole calendar was finally determined.

(13) The Numerals Continued

At this point two lines of investigation were begun which resulted in the finding of very many additional numbers which, in time, shed new light on the composition of the book. The first of these was the result of work in three different directions.

(1) The very frequent group 30007, occurring on the same page as Telegramm, and now found to be used in constant association with numbers, was identified as tausend.

(2) The group 7177 had attracted attention before the breaking of the code because of its frequent occurrence in combination with itself. In fact 7177 7177 occurred in the 18470 messages no less than 15 times. The group could not well be a syllable, since no syllable is subject to such frequent doubling in different contexts, and the only thing in langugage that seemed possible as the equivalent of the group was 000. The group was now seen to occur regularly in combination with numbers, and the meaning 000 was rendered highly probable.

(3) The groups 1500–1509 had aroused curiosity because of the peculiar fact that they were frequently followed by the same group or groups as preceded them. The suggestion had been made that they might turn out to signify "ich wiederhole" or an equivalent expression. Many expressions, too, were found of the following type:

10418	2069	1501	30007	27491	11740	22985	1508
13	06		tausend				

It was now seen that what followed 1500, etc., was, in these expressions, a repetition of what preceded it, but a repetition in different form—the rewriting of a numeral to insure against garbling. Thus the decipherment of the phrase just given was completed to read

1306 dash tausend drei hundert sechs dash

The rewriting of the phrase was sometimes followed by a second occurrence of 1500, etc., and sometimes not, which fitted in well with the signification "dash."

Very many numeral expressions were thus found written in two different ways. Sometimes the number would be found expressed in figures and in words as in the example just given. Elsewhere the figures were rewritten in a different form, e. g.,

8356	26557	1501	18707	4888	1509 (18470 messages, p. 97 Ay, *ff.*)
15	59	dash	155	9	dash

The large supply of new numbers which was thus assured was further increased by the discovery that the groups 3610 *ff.* were also dashes (see above) and were used in the same manner as 1500,

etc. Still more numerals were added when the group 13925, on the same page as Mai, and commonly found after numerals, e. g.,

4847 7177 13925 (18470 messages, p. 570 A)
10 000

was identified as Mark, and its associate 10800 as Pfennig, e. g.,

18555 13925 13068 10800 (18470 messages, p. 464 B)
zwei Mark 50 Pfennig

while in similar phrases 10844, on the same page as 10800, was taken to mean Peseta, and its companion 22298 to be centimo.

The other source of numerals was found in a simpler manner. 17136—Nummer—occurs frequently as the last group but one or the last group but two of a message. Examples are the following: 17136 18977 (18470 messages, p. 104, A m); 17136 29068 1926 (ibid., p. 477, A m). In these cases the encoder, to guard against garbling, has repeated the number of the message which had been given at the beginning in the trinumeral code. This is another example of kind-heartedness in the use of the word Nummer. (See p. 27, note 12.) True, the message number was sometimes repeated at the end without the use of the word Nummer. In such cases it was impossible to tell off-hand whether the final groups of the message repeated its number or were merely the last words of the telegram. All concluding groups of messages the terminal digits of which indicated that they might represent numbers were studied from this point of view.

It will be remembered that the code groups for the cardinal numerals from 1 to 31 terminated in the digits 8, 7, 6, and 5 in regular sequence, and that in each case a code group higher by one than that for the cardinal number was used for the corresponding ordinal. (See p. 31.) When 23669 was found to be apparently 33 it was thought that there must be some mistake, since the group for 33 was expected to end in 8. (See table, p. 32.) Further investigation showed, however, that there is a change in the composition of the book at this point and that from here on cardinal number groups terminate in 9, 8, 7, and 6 instead of 8, 7, 6, and 5. The reason for this variation probably is that in the case of the numbers 1–31 it was necessary to provide for ordinals for dates, and it was convenient to have these ordinals immediately following the cardinals. If the cardinals of these numbers terminated in 9, 8, 7, and 6, the ordinal of the number terminating in 9 would terminate in 0 and would be shoved into another 10-word block. Beginning, however, with 33 the ordinals are dropped. It will be noticed that while in the case of the numbers 1–32 an odd cardinal number has an even terminal digit, and an even cardinal an odd terminal digit, the arrangement is reversed beginning with no. 33.

The precise position of the blocks-of-ten containing the numerals could not be determined until words had been identified in quantity. It was supposed that the practice would follow that of 13040, and that was later found to be the case; the numerals are entered in the blocks that are alphabetically fifth and tenth. (Cf. p. 5.)

(14) Structure of the Code Book. The Alphabetical Arrangement. Code XX

Attention has been directed (see p. 31) to the symmetrical order into which the pages of the code book fall when arranged in the order of the numerals. The discovery of this arrangement was of prime importance in further reconstructing the code book, since it changed the code from one in which pages followed one another at haphazard to one in which they were arranged in alphabetical order.

In order to reap the full benefit of this knowledge, an archetype of 18470 was postulated—an original alphabetical code, called, for convenience, XX, whose pages had been renumbered to make 18470 just as the pages of 18470 were renumbered to make 12444, 1777, and 2310.

This code, like 18470, was assumed to begin with page 10, and a table was gradually worked out showing its relationship to 18470, similar in all respects to the tables showing the relationship of 18470 to 12444, etc. The only difference in the new table was the fact that the composer of the code had used a system here, the discovery of which facilitated and checked the work of reconstruction. (See table on p. 41 *ff*.)

Numerals are not found on the name pages or on the pages of grammatical directions; they are inserted only in the pages of the vocabulary proper. The pages of vocabulary containing numerals consequently form a code book complete in itself, and undoubtedly originally compiled as a unit.

A table is here given of pages 10–37 of XX in their relationship to 18470. Since we are still primarily concerned with numerals, the numerals on each page are added at the right.[17]

XX	18470	Numerals
10	44	0–00
11	71	000–01
12	72	02–03
13	43	04–05
14	20	06–07
15	31	08–09
16	32	1– 2
17	19	3– 4
18	68	5– 6
19	47	7– 8
20	48	9–10
21	67	11–12
22	104	13–14
23	88	15–16
24		
25	103	19–20
26		
27		
28	204	25–26
29	223	27–28
30	264	29–30
31	235	31–32
32	236	33–34
33		
34	136	37–38
35		
36		
37	135	43–44

[17] The blanks in the table are left for demonstration purposes; all these numbers were later identified.

Examination of this table shows that when the 18470 pages are arranged in the order of the corresponding pages of XX, they fall into blocks of four, each block conforming to the following scheme in which the letters denote page numbers:

a
b
b+1
a−1

c
d
d+1
c−1

etc.

It is furthermore true that an even page number in XX is always represented by an even page number in 18470, and the odd-numbered pages, of course, correspond similarly.

These facts, in connection with what was already known concerning the terminal digits of the code groups representing numerals (see pp. 31, 32, 34), made possible the prediction of several things concerning the numeral groups in advance of their identification, and consequently helped to check tentative identifications.

Thus, in the table just given we know that the 18470 page corresponding to XX page 33 is to be 263 (i. e. 264 minus 1), and that it will contain the numerals 35 and 36, the code groups for which will terminate respectively in 7 and 6. Similarly we know that, since XX, 23=18470, 83, XX, 24 will correspond to 18470, 84, and the numerals on this page, when they are found, will be 17 and 18, with code equivalents terminating in the digits 8 and 7 respectively; and we know further that XX, 26 will be represented by 18470, 224, which will contain the numerals 21 and 22, with code groups ending in 8 and 7. With XX, 35 and XX, 36 the case is different. These two pages constitute a pair, being the means of a block of four, and the 18470 equivalent is not known for either. We are certain, however, that the equivalent of 35 will be an odd numbered page, and that the numerals on that page (39 and 40) will have code groups ending in 7 and 6, while the equivalent of 36 will be an even numbered page with numerals (41 and 42) represented by code groups ending in 9 and 8. If we find a code group ending in 9, which, from its context, we are tempted to identify as 41, we can be certain that our supposition is wrong if the page number of the group is odd; thus, the odd numbered 18470 page 201, for example, cannot be the equivalent of the even numbered XX page 36.

The arrangement of 18470 pages given in the table on page 35 can, in the nature of things, hold for only half of the book. If we take the page numbers beginning with 10, and arrange them in blocks of four, we shall find that each pair of 18470 pages in the table just given consists of the two consecutive pages taken from the center of a four-page block. Thus, from the block 66–69 we have 68 and 67, and from the block 234–237 we have 235 and 236. This leaves the extremes of each block-of-four unused. Thus, from the blocks just mentioned we have not used 66 and 69, or 234 and 237. Accordingly for each block of 18470 pages arranged as on page 35 we find a corresponding block in which pairs of extremes are employed. The formula for the

arrangement of the 18470 blocks composed of means has already been given (p. 36). In the blocks composed of extremes the arrangement is as follows, e, f, g, and h being page numbers:

e
f
f−3
e+3

g
h
h−3
g+3

A sample will illustrate:

XX	18470	Numerals
130	74	229–230
131	113	231–232
132	110	233–234
133	77	235–236

It was at first not known, of course, in what manner series of blocks of means and of extremes would follow one another. It was perceived that several blocks of one kind occurred together, as, for example, the blocks of means at the beginning of the book. After the parallel table for XX and 18470 had progressed further (see p. 41 *ff.*), it was seen that the compiler had started with seven blocks composed of two pairs of means each. The sequence then is: Eight blocks of extremes, eight of means; eight of extremes, eight of means; eight of extremes, eight of means. We should then expect, at the end, a block of seven extremes corresponding to the block of seven means at the beginning.

Complete symmetry, however, was unattainable, since pages assigned to names and to punctuation were allowed to cut, to a slight extent, into the four-page blocks assigned to the alphabetical vocabulary. As a rule complete four-page blocks were used for names and punctuation (pp. 10–13, 14–17, 22–25, 26–29, 34–37, 38–41, 50–53, 54–57, 58–61, and 62–65). In seven cases, however, the four-page blocks assigned to the alphabetical vocabulary were invaded (pp. 18 and 21, 30 and 33, 42 and 45, 46 and 49, 66 and 69, 70 and 73, and the two nondescript pp. 183 and 184), and in this process six pairs of extremes and one pair of means were employed. Moreover, the vocabulary consists of 246 pages (not 248) so that one four-page block remained incomplete.

The net result of these circumstances was to present an excess of five pairs of means for use in the vocabulary over the number of pairs of extremes. The compiler, as a consequence, found himself unable to make a collection of seven blocks of extremes at the end to correspond to the seven blocks of means at the beginning, and we find him introducing one block of means just before the end. Why he put this block among the extremes and not after them does not appear; nor is it clear why the usual chiastic arrangement was discarded in this block and the one that precedes it. The irregularities in these blocks are further discussed on page 47, note 19.

As the skeleton gradually filled, the scheme of arrangement of blocks of means and blocks of extremes became more and more apparent and facilitated the work of checking groups supposed to represent certain numbers, and, as will presently appear, words as well.

Attention has thus far been confined to the arrangement in blocks and series of blocks of the 18470 pages. The symmetry of arrangement of the XX pages was, however, not allowed

to go neglected. When the 18470 pages were arranged in numerical order, beginning with page 10, and divided into blocks of four, it was found that the corresponding blocks of four XX pages presented the same pattern as the 18470 blocks—they contained either two pairs of means each or two pairs of extremes. This was not the result of accident, nor did it happen automatically as the result of the arrangement of the 18470 pages. The experiment of composing a table was tried in M. I. 8, and it was found that the 18470 pages can be arranged in apple-pie order while the XX blocks will go all askew unless due care is exercised. The law to be observed in order that the arrangement may come out correctly is this: If the extremes of a four-page block of 18470 have been associated with the extremes of a XX block, then the means of this 18470 block must likewise be associated with the extremes of a XX block, and, by the same token, if the extremes of the 18470 block have been associated with the means of a XX block, the means of the 18470 block must likewise be associated with the means of a XX block. (See table on p. 41 *ff.*) On the other hand, if the 18470 pages are arranged in numerical order, the symmetry in the series of blocks, the alternation of a series of blocks of means with a series of blocks of extremes, is not found in the XX pages.[18]

Trouble was rarely encountered so far as numerals were concerned. The group 15958 was found in a context that made its meaning almost certainly 194. This meant that 18470 page 159 would have to correspond with XX page 112—an odd page with an even one—and that the respective mates of these pages would also violate the odd and even rule. Weeks later it was found that the group 15958 was a garbled form of 15858, and the trouble was cured. It was, of course, in the case of tentative word identifications that the knowledge of the systematic arrangement was of greatest value.

(15) Further Identifications

With the gradual arrangement of the pages in alphabetical order the search for new word identifications entered upon a new phase. Certain old teasers were teasers no longer. Thus, the mystery concerning und was cleared up. (See p. 18.) It was found that unds had been scattered through the book in a fashion similar to that in which the stops had been entered—that any (possibly every) page was apt to furnish an und, and that the terminal digit for the corresponding code group was uniformly 3, just as the code groups for stops regularly end in 1 and 2. Later, it was found that und was not the only word so treated (see p. 51): des, nicht, and eine are similarly scattered through the book with code equivalents ending in 0, and the same statement holds true for der with code groups ending in 1, for die, eine, and den with code groups ending in 2, and for zu, des, and eines with code groups ending, like those for und,

[18] The compiler of the code was concerned primarily with the arrangement of the 18470 pages. He could have extended the symmetry to the XX page series, had he been so inclined. The procedure would be as follows: Divide the 246 pages of XX and the 246 pages of 18470 each into blocks of four (the last block, of course, containing only two). Mark off seven blocks-of-four at the beginning and seven at the end, and divide the rest into series of eight blocks-of-four each. Take any two series of XX blocks and any two of 18470 (of course a seven-block series cannot be associated with an eight-block series). Call these series XXa, XXb, 18470a, and 18470b. Then match the pages thus until all have been used:

XXa any pair of extremes with 18470a any pair of means;
XXa any pair of means with 18470b any pair of means;
XXb any pair of extremes with 18470a any pair of extremes;
XXb any pair of means with 18470b any pair of extremes.

Repeat this process with the remaining series. If now the XX pages are arranged in numerical order, the 18470 pages will follow the typical block-of-four extremes-and-means arrangement; and if the 18470 pages are arranged in numerical order, the XX pages will conform to the typical pattern. In the actual making of the code, series a and b have not been kept distinct.

in 3. A detailed study of the system followed by the compiler of the code in entering these stops and particles will be found below (p. 58 *f.*).

The group 3249 was on the page alphabetically preceding an and was constantly used with dates; it was accordingly identified as am. 1405, on the very first page of the book alphabetically, was likewise found before dates, and was recognized as ab. 13788 (see p. 18), when its alphabetical position in the B's was once known, turned out to be nothing more startling than bitte.

Some groups required bolder guessing and more roundabout methods of approach. On page 17 of the 18470 messages was a telegram reading 19103 2441 51096. That was the entire message—merely the one significant group 19103, followed by Schluss der Depesche (2441) and the signature (51096). This lone group was on the page preceding Gesandtschaft. The telegram was *from* Berlin, and genehmigt suggested itself as a likely meaning for the group. Several messages began with the phrase 27160 19155 5959 (e. g., 18470 messages, p. 817). The group 19155 was on the same page as genehmigt, and 5959, from other evidence, was quite certainly the name of a place. Generalkonsulat seemed reasonable for 19155, if the identification for genehmigt was correct. A search through the Almanac de Gotha showed that the only German consulate-general in Spain was at Barcelona, so that, if no mistake had been made, 5959 was Barcelona. One message, and one only, had the phrase 27160 19107 8967. This message was one of the series already mentioned as yielding the phrase Im Anschluss an Telegramm. (See p. 29.) Now, from the connection between messages, it was certain that the phrase in question was the equivalent of 27160 19155 5959, and the two groups 19107 and 8967 were put down as general and Konsulat, respectively. Needless to say, no identification was accepted until *all* the occurrences of the group in question had been investigated.

These and similar identifications were due to the finding of the alphabetical position of the pages containing the groups in question. Investigation by analysis, however, went on as before, and some examples may be given here. The identification of new groups was, of course, greatly facilitated by the growth in vocabulary even in cases where the alphabetical position of the group was not known. Take, for example, the very frequent group 14213. This is found constantly in messages of which the following two are typical:

18470 messages, page 507:	14213	18136	30020	4888	*	*	*	24443
		von	Tel. Nr.	9				
18470 messages, page 638:	14213	18136	30020	6796	*	*	*	24443
		von	Tel. Nr.	11				

(Asterisks indicate an omission of code groups not pertinent to the present discussion)

It was quite evident that we had to do here with a form message, and it was thought at first that the message was a request to acknowledge receipt of some other telegram, and that 14213 was Empfangsschein, Empfangsbestaetigung, or some equivalent expression. (See p. 28, note 13.) A study of the occurrences of the group, however, showed that it was followed at times by the words *von* Telegramm Nr., which would allow the meaning supposed, and at times by *aus* Telegramm Nr., which would not allow it. The problem now was to find a word that would go with either von or aus, and Wiederholung suggested itself as the solution. (According to the German system, the same code group would be used to denote the verb,

wiederholen.) Confirmation of the new supposition was found in the 18470 message on page 770. This message is in a slightly different form from the two just cited above. It reads:

13788 30046 18131 8449 17136 6705 13376 22593 17947 14213
Tel. vom 17ten Nr. 12

(Blanks indicate words not identified at the time.)

It was conjectured that this was a request for repetition; and the repetition itself was found on page 780 in a message marked in the "Dreinummerheft" as an answer to the one just quoted:

14213 18139 30020 6705 13376
von Tel. Nr. 12

(The complete text of the telegram requesting the repetition is as follows: Bitte Tel. vom 17ten Nr. 12–48 da verstuemmelt wiederholen. Incidentally, this was the first complete message in this code to be deciphered.)

9496 was identified as Schluss from its use in the introduction to the last installment of Ratibor's long message Nr. 1222 (see p. 32)—9496 18138 30020 6705 22417. From its association with Schluss, 14179 was guessed to be Krieg, and when the combination 14179 25722 was found the alphabetical position of 25722 in the E's led to the identification of that group as Ende, and fixed more firmly the meaning Krieg for 14179.

(16) The Parallel Table XX–18470

As a result of a process of gradual change, and as a simplification of more cumbersome plans, the table reproduced here was evolved as the best means of presenting an easily accessible conspectus of what was known of the alphabetical arrangement of the book. This table differs from the 18470, 12444, etc., parallel tables in only one respect—one word was written opposite a 18470 page whenever a word on the page was known. This obviated constant reference to the bulky and scantily filled volume containing the tentative code book and provided an excellent summary of the book, which could constantly be kept up to date with a minimum of labor and which was as handy for consultation as a map. It was unnecessary to insert the numerals in the table: pages 1–9 of XX do not exist, and pages 10–15 contain the numerals 0–09; page 16 contains 1 and 2, and every page thereafter two numerals. The numeral that will be found on any given XX page can thus be determined mentally by simply applying the formula (XX page number−15) 2=numeral. Thus, page 230 of XX, for example, will contain the numeral (230−15) 2=430 (and, of course, 429 also). With a little practice the terminal digit of the code group for any given numeral is also easily found mentally. (See p. 31 *f.*)

Parallel table, XX—18470

XX		18		XX		18	
England	10	44	Ab	Tanger	50	102	Dampfer
Deutsch	11	71	Abgelaufen		51	85	Dass
Canada	12	72	Absatz	Washington	52	82	Dein
Griechenland	13	43	Achtzehn	Valencia	53	105	Derselbe
Mexico	14	20	Ag	Hamburg	54	270	Dezember
Punct.	15	31	Alle	Buenos Aires	55	309	Dieses Monats
Gram. Dir.	16	32	Am	Azoren	56	306	Dir
Marokko	17	19	An	Kanarien	57	273	Dortig
Portugal	18	68	Angehoerig	Iberien	58	274	Drei
17	19	47	Anleihe	Belgrad	59	305	Durch
14	20	48	Annonce	Berlin	60	302	E
Santa Cruz	21	67	Antwort	Holland	61	277	Ei
Kap Verd	22	104	April	Tuerkei	62	286	Ein
Amerika	23	83	Artikel	Zaragoza	63	293	Eingegangen
Gram. Dir.	24	84	Auf	Zuerich	64	290	Einsenden
London	25	103	Auflage	Sindora	65	289	Einzahlung
Las Palmas	26	224	Aufnahme	Niederlande	66	242	Elf
Gram. Dir.	27	203	August	21	67	257	Ende
Algeciras	28	204	Auslage	18	68	254	Enthaelt
Aarhuss	29	223	Auswaertiges Amt	Paris	69	245	Er
Russisch	30	264	Bad	Spanien	70	244	Erbitte
15	31	235	Bank	11	71	255	Erhalten
16	32	236	Baumwolle	12	72	256	Erliegen
Preussen	33	263	Beginnt	Schweiz	73	243	Erst
Madrid	34	136	Bei	130	74	288	Erwuenscht
Gram. Dir.	35	131	Belohnung	137	75	291	Exemplar
Punct.	36	132	Bericht	134	76	292	Fabrik
Muenchen	37	135	Besetzt	133	77	287	Faellig
Gijon	38	134	Besonders	168	78	276	Februar
Colon	39	133	Bewaffnet	163	79	303	Ferner
Dakar	40	130	Bis	164	80	304	Flagge
Frankreich	41	137	Bitte	167	81	275	Folgend
Santiago	42	262	Boerse	52	82	272	Fortsetzung
13	43	237	Bras	23	83	307	Frieden
10	44	234	Buchstaben	24	84	308	Fuenf
Stuttgart	45	265	Cap	51	85	271	Fuer
Palma	46	222	Centimo	122	86	192	Gaenzlich
19	47	205	Chiffre	145	87	155	Geeignet
20	48	202	Com	142	88	156	Gegner
Nymwegen	49	225	Da	125	89	191	General

XX in the column headings signifies the Original Alphabetical Code, and 18, 18470.
To convert *XX into 18470* take XX page number from central column; the corresponding page of 18470 is then at the *right*.
To convert *18470 into XX* take 18470 page number from central column; the corresponding page of XX is then at the *left*.
The page number *from* which the change is to be made is always taken from the central column.
Directions for finding the alphabetical position of any 18470 page will be found on p. 44.

XX	18
170	266
161	267
158	268
173	269
54	270
85	271
82	272
57	273
58	274
81	275
78	276
61	277
190	278
205	279
202	280
193	281
118	282
149	283
146	284
121	285
62	286
77	287
74	288
65	289
64	290
75	291
76	292
63	293
120	294
147	295
148	296
119	297
192	298
203	299
204	300
191	301
60	302
79	303
80	304
59	305
56	306
83	307
84	308
85	309

Pages of 18470 that were devoted to proper names (see p. 55) were separately compiled and were not part of the original XX structure. Accordingly the table provides no XX equivalents for these pages. Instead of XX pages at the left of these 18470 pages, one proper name from each 18470 page is given—e. g., Amerika at the left of page 23. Similarly pages 183 and 184 of 18470 were provided for miscellaneous supplementary matter and had no XX equivalents (compare the case of p. 130 of 13040, discussed above p. 6).

Given the XX number of any page, its position in the alphabet could always be determined within certain limits by finding the XX number in the central column and noting its alphabetical position as fixed by words entered at the right. Thus, if, to take an arbitrary example, XX page 190 was known to contain September, and XX page 204 to contain Telegramm, it was certain that XX pages 191–203, even though no word had been identified on any of them, would contain words alphabetically between September and Telegramm. As given here, the table is complete. It started, of course, as a mere skeleton, and grew by slow degrees. It was kept constantly in sight while work on 18470 progressed, and was the most valuable tool in the workshop.

Code XX comprised 246 pages running from 10 to 255. This explains why no 18470 equivalents are given for numbers in the central column above 255.

The identification of the group 24496 will serve to illustrate the actual use of the table. A frequently recurring type of message was—

24496	14213	18136	30020	* * *
	Wiederholung	von	Tel. Nr.	* * *

We look at 244 in the central column of the table and see from the number at the left that it corresponds to XX page 70. We then look at page 70 in the central column and see from the words at the right opposite pages above and below 70 that the page comes in the E's. This is one of those pleasant cases in which the alphabetical position soon settles the meaning of the

group, since erbitte fills the bill exactly. Further illustration of the use of the table may be found by taking any of the examples of 18470 messages, and using the table to find the alphabetical position of code groups.

Even when many numerals had been found and the alphabetical position of a large number of pages established, the alphabetical contents of a page were known only within broad limits. Thus, if, say, XX pages 210–240 were paralleled with their 18470 equivalents, it might well be that in this number of 18470 pages only one, say 231, was represented by an identified word. All that could be said of page 210 then, was that it contained words that were alphabetically 21 pages before vier, and of 240 that it contained words that were alphabetically 9 pages beyond vier.

Two tables were constructed that it was hoped would be of service in the further identification of words. The first, the value of which proved to be far less than that of the second, was a frequency table of common German words, and was based on some 50 messages, mainly in 13040, that had been decoded in M. I. 8. Some of these messages were lengthy diplomatic reports in epistolary form; some were telegrams. The stops in these messages were likewise counted. The table compares the frequencies of common German words in the messages with the frequencies of the same words, as given in Mauborgne's "Data." The same words are then given again, arranged in the order of their frequency in the messages.

Mauborgne's "Data"		Same words in messages (5,859 words)	In order of frequency in messages	
Die	3,298	77	Und	101
Der	3,250	88	Der	88
Und	2,853	101	In	77
Ein, etc.	2,028	18	Die	77
In	1,757	77	Von	69
Zu	1,472	49	Zu	49
Den	1,239	43	Den	43
Das	1,149	15	Mit	38
Nicht	1,035	33	Nicht	33
Ich	1,004	29	Ich	29
Von	991	69	Dass	27
Ist	927	23	Dem	27
Des	909	25	Des	25
Sie	901	14	Ist	23
Dass	880	27	Ein, etc.	18
Sein	876	17	Sein	17
Es	843	6	Das	15
Dem	826	27	Sie	14
Sich	822	12	Sich	12
Mit	792	38	Es	6

The following words were counted in the messages because the reading of the messages had left the feeling that they were common. It will be noticed that they break into the order of words already given:

An_____	42	between den and mit
Fuer____	38	the same as mit
Bei_____	33	the same as nicht
Er_____	21	between ist and ein
Zur_____	15	the same as das
Hat_____	12	the same as sich

A count of the stops in the same messages showed one stop to every 10 to 12 words. Telegraphic messages were examined separately from those in epistolary form, but the results were not essentially different in the two classes. Only three messages were sent *from* Berlin, and the longest of these comprised only 78 code words. These, counting the additive indicator at the end as a stop, contained one stop, on the average, to each 16 words; the number of messages seems too small, however, to draw any conclusions from this fact. The total number of code words in the messages examined was 5859, the total number of stops (including 21 additive indicators and 13 "Schluss der Depesche" groups) 559. It is worth noting that of these 559 stops, or 525 if we exclude additive indicators and "Schluss" signs, 25 percent or more were taken from the same page of the code book as the code group preceding the stop, or from an adjoining page.

To determine more closely the alphabetical position of code words which, at first, were fixed in such comparatively broad limits, another table was constructed, to show how many pages the words assigned to each letter of the alphabet might be expected to cover. For this purpose Heath's German Dictionary, the von Igel code (then in possession of M. I. 8), and 13040 were employed. The first and last were reduced to a basis of 100 pages, but the von Igel code, which comprised 109 pages, was left as it was, the error being small. This table follows:

Distribution of pages among letters of alphabet in German alphabetic code of 100 pages

According to Heath's Dictionary		On basis of von Igel code		On basis of 13040		Average of preceding	
Letter	Pages	Letter	Pages	Letter	Pages	Letter	Pages
A	1–9	A	1– 8	A	1– 8	A	1– 8
B	10–16	B	9– 15	B	9–14	B	9– 14
C		C	16	C	15–17	C	15
D	17–19	D	17– 21	D	18–21	D	16– 19
E	20–24	E	22– 28	E	22–27	E	20– 25
F	25–28	F	29– 34	F	28–30	F	26– 29
G	29–34	G	35– 40	G	31–35	G	30– 34
H	35–39	H	41– 44	H	36–39	H	35– 39
I		I	45– 46	I	40–42	I	40– 41
J		J		J		J	
K	40–45	K	47– 51	K	43–45	K	42– 46
L	46–49	L	52– 55	L	46–48	L	47– 50
M	50–53	M	56– 60	M	49–52	M	51– 55
N	54–55	N	61– 63	N	53–55	N	56– 58
O	56	O	64– 65	O	56	O	59
P	57–59	P	66– 69	P	57–62	P	60– 63
Q		Q		Q		Q	
R	60–62	R	70– 74	R	63–67	R	64– 67
S	63–74	S	75– 86	S	68–75	S	68– 78
T	75–77	T	87– 89	T	76–78	T	79– 81
U	78–82	U	90– 94	U	79–83	U	82– 86
V	83–89	V	95–100	V	84–88	V	87– 92
W	90–94	W	101–105	W	89–91	W	93– 96
X		X		X		X	
Y		Y		Y		Y	
Z	95–98	Z	106–109	Z	92–97	Z	97–100
(Error about 2 pages)		(Error 9 pages)		(Error about 3 pages)			

The code book 13040 was an invaluable aid, since it constitutes a special kind of dictionary prepared for the same uses and under the same general auspices as the book on which we were at work. Now the vocabulary proper of 13040 contains 189 pages. Because of the unknown size of the onomasticon, the exact number of pages in the vocabulary proper of 18470 was at first not known. When a few words had been identified, a count was made of the pages that separated them, and this count was then compared with the number of pages separating the same words in 13040. Absolute accuracy was not to be expected in this comparison, since the two books could not be supposed to differ in the same proportion at all points; and, as a matter of fact, there is considerable variation. The first table made for this study is here reproduced.

The number of pages separating certain words in 13040 and in 18470 is as follows (13 indicates 13040, 18, 18470):

Ab–Wiederholung
13—182
18—242 Ratio 4/3

April–December [on the spelling—December or Dezember—see p. 48]
13—27
18—33 Ratio about 5/4

Ab–Januar
13—86
18—106 Ratio 5/4

Bis–Von
13—152
18—184 Ratio somewhat less than 5/4

The following words occupy the pages mentioned, taken in alphabetical order:

October
13—114
18—137 Ratio somewhat less than 5/4

Fortsetzung
13—61
18—82 Ratio 4/3

Fuer
13—63
18—82 Ratio 4/3

Sieben
13—141
18—191 Ratio somewhat more than 4/3

Vorigen Jahres
13—176
18—234 Ratio 4/3

Wiederholung to end of book
13—11
18—say, 14 or 15

This would make 18470 contain about 256 pages, and its ratio to 13040 would then be 4/3. In general this ratio seemed to be approximately correct. Originally, before discovery of the name pages, the ratio had been assumed to be 3/2.

This proportion was further confirmed by the finding of the number 483 written as 1995 27387—that is, by means of two code groups—since this was an almost certain indication that the code groups for numerals did not reach as high as 483, and that the vocabulary pages consequently did not extend as high as 257. The matter was finally settled when the *word* (not the numeral) zwoelf and the numeral 480 were found on the same page (p. 185 of the code), since zwoelf is alphabetically almost the last word in the language.[19] This meant that 18470 contained 246 pages, and that the ratio of its vocabulary to that of 13040 was very close to 4/3.

[19] The irregular arrangement at the end caused a great deal of trouble, for it was not known at first that the final alphabetical block would consist of only two pages instead of four (see p. 37), and it was not suspected that two pairs of means would be found intruding among the extremes. P. 182 of 18470 contains the word zehn, and p. 185 the word zwoelf. According to the general scheme these pages should have been separated by another pair of extremes, and it was impossible to imagine two pages of words between zehn and zwoelf. So, too, the 18470 block of means immediately preceding p. 182, and corresponding to XX pp. 250–253, did not fit into the general arrangement. Parallel with these peculiarities and directly connected with them are the two irregular XX blocks corresponding to 18470 pp. 198–201 and 162–165. With the rest of the code arranged as it is, it was impossible to arrange these pages at the end according to the rules given above (p. 34 *ff.*), and the compiler evidently was unwilling to do his work over. As it is, we have XX p. 246, an extreme, as the partner, in a block, of 247, a mean, and the same holds true for 252 and 253, 248 and 249, and 250 and 251. There are other irregularities also in these blocks, as a consultation of the rules will show.

Such difficulties as these were gradually removed as the word identifications increased in number. They serve to emphasize the fact that the decipherment of a code is facilitated by systematic construction, while, on the other hand, it is made more difficult as system in code structure is abandoned.

This ratio was applied as a check and served to place pages in all cases when a word was identified on a page on which no words were already known. A few examples will make this clear. In each case the new word is italicized. 13 in each case indicates 13040 and 18, 18470.

Gruppen (11604)—Haelfte (25225).—In 13 the words are separated by 12 10-word blocks; in 18 the distance to be expected would be, say, 16 blocks=1 or 2 pages. Now 18 page 252=XX, page 98; and 18 page 116, being an even page, must go with an even page of XX, and is put two pages before 252 at XX page 96. This gives the grouping—

XX	18
94	
95	115
96	116
97	
98	252

18470 page 115 being placed next to its mate, page 116.

Reichskolonialamt (26914)—*Rubel* (25882).—In 13, 37 blocks; in 18 say 49 blocks=4–5 pages. 18 page 269=XX page 173, and 18 page 258 must go with an even numbered page of XX. 173+5=178, and we have XX page 178=18 page 258. As a further check on Rubel it was linked up to Satz (26184), thus:

Rubel—Satz, in 13=24 blocks; in 18, say 32 blocks=3 pages. Now Satz (18 page 261) is at XX page 181, and 181−3=178, thus checking the position of Rubel.

The following examples are interesting because the solution of the difficulties involved gave additional information concerning the composition of the code book. The chain of words Chiffre, December, dieses Monats, and drei showed the following relationship in 13040 and 18470, respectively:

	Actual distance in		Expected in 18 from 4/3 ratio
	13	18	
	Blocks	*Pages*	*Pages*
Chiffre–December	63	7	8
December–drei	51	4	6–7
December–dieses Monats	31	1	4
dieses Monats–Drei	20	3	2–3

Thus Chiffre and December, December and drei, and December and dieses Monats seemed too close to one another in 18470; the only one of the four pairs that acted according to expectations was dieses Monats–drei. The first attempt to solve the difficulty was the assumption that our code spelt the 12th month Dezember instead of December as in 13040. This adjusted the trouble for the last three pairs of words, but increased the difficulty in the case of Chiffre–Dezember, for if Chiffre was too close to December it was much too close to Dezember. To solve the new difficulty it was assumed that a number of words spelt in 13040 with *C*o, might, in 18470, be spelt with *K*o, thus bringing Chiffre and Dezember closer together. Januar and Konsulat were separated in 13040 by 51 blocks, which suggested a separation of 68 blocks

(6–7 pages) in 18470. Januar (15799) was at XX page 115. This would put Konsulat (8967) at XX, page 116+6=121 giving the arrangement—

XX	18
118	86
119	297
120	294
121	89

or at page 123, giving

XX	18
122	
123	89
124	86
125	

Now XX 118 was already paralleled by 18, 282 so that the first arrangement was inadmissible; and the association of 89 and 86 with XX 123 and 124 gave a bad XX block at that point since XX extremes were wanted there. (See p. 34 *ff.*) Allowance for the Co words removed to Ko, and a consequent increase of the pages between Januar and Konsul to 10, gave—

XX	18
122	86
123	
124	
125	89

which removed the difficulties.

A similar test, in addition to others, was applied where new words were identified by analysis without knowledge of the alphabetical position of their pages, and the position of a number of pages was fixed by these means.

(17) More Examples of Identifications

As new groups were identified, the identifications and the evidence were put on cards and the identifications were entered in the code book. With the aid of the card index of code groups and frequency books, each occurrence of each identified code group then had its meaning entered in the indexed message sheets. (See p. 15 *ff.*) These last were then studied over and over again, and more new identifications were gradually added, the process constituting an endless chain.

With the gradual growth in the vocabulary, however, another means of identifying code groups became increasingly available. Instead of taking a code group in a message and endeavoring to identify it from its context and code book position, it became possible to reverse the process—to start with an identified code group, ascertain from a dictionary and 13040 what is likely to precede or follow it in the code book, and then, with the aid of the frequencies, to search for this neighboring group. The two processes in combination are illustrated by the

identification of the group 28935. In the 18470 messages, page 54, in the midst of an account of the Brest Litowsk peace negotiations, we come upon the phrase—

28935	
10552	der
13541	besetzten
19237	Gebiete

A glance at the table shows us that page 289 comes alphabetically immediately before page 242, and that the latter contains the word elf. Einwohner suggests itself as a likely identification for the group. Other occurrences of 28935 are looked for. In the 18470 messages, page 805, But we find—

30510	durch
28935	
1682	Acc Pl.
11566	gross
30092	Teil
1669	Gen. Pl.
18180	Von
1033	Elsass
18654	in
4132	Frankreich

Einwohner does not fit well here. Further reflection suggests Einverleibung as suitable to both passages. The two groups 28936 and 28937 immediately following 28935 are then looked up. The former is found to occur (18470 messages, p. 270, A p) in this connection—

15372	Im
28936	
10054	mit

The latter is found frequently as follows (18470 messages, p. 2, A j, *ff*):

10055	mit
—	
—	
—	
—	
28937	—

The two groups 28936 and 28937 are identified as Einvernehmen and einverstanden, and Einverleibung is confirmed.

The group 20738 had been identified as the syllable vat. The group after vat in the code book can hardly be anything but Vater. This group, 20739, is found to occur several times followed by a high number name group. In the 12444 messages, page 83, we find—

12444=in 18470		
4049	20739	
29420	25510	erhielt
10030	7720	letzte
30072	28362	Nachricht
15936	10326	19
6966	8356	15

Evidently someone is missing and "his *father* last heard from him, etc."

Sometimes help can be secured from outside. One message was found, long after the code had been broken, in both code and clear, and furnished a number of new words in addition to gratifying confirmation of identifications already made. An account of this message follows, and other cases where external evidence was of service are added. Incidentally these examples will show how entry was obtained into the onomasticon.

(18) The Clear-Text War-Bond Message

The message in 1777, page 62, was in the shape indicated by the words on the *right* of the code groups when the group 4774 was identified as Anleihe. A clear-text message taken by the United States naval authorities from the messenger who was carrying it to South America, a copy of which had been sent to Military Intelligence, was then matched up with the code message and gave the additional identifications that appear on the *left* of the code groups. The clear-text message and the code message follow:

CLEAR-TEXT OF BOND MESSAGE

Kaiserliche Deutsche Botschaft in Spanien — Madrid den 26 Maerz 1918.

No. 3. Hier ist nachstehendes Radiogramm vom Auswaertigen Amt eingegangen.

Als 8 Kriegsanleihe werden ausgegeben 5 prozentige fruehestens 1 Oktober 1924 kundbare Schuldverschreibungen und 4½% Schatzanweisungen, beide zu 98. Anlosung, Einloesung der Schatzanweisungen und Stueckelungen fuer beide Papiere wie bei der 6 und 7 Anleihe. Erster Zinsschein fuer beide Papiere Januar 1919 faellig. Zeichnungsfrist vom 18 Maerz bis 1 Juli. Einzahlung beginnt 28 Maerz. Eine Werbung unter Angehoerigen auch neutraler Staaten ist erwuenscht. Vermittlungsstellen, fuer die besonders kleinere Banken geeignet scheinen, erhalten 30 Pfennig fuer je 100 Mark und voraussichtlich Zuschuss zu Werbungskosten. Auslagen fuer Zeitungsannonce (?) die Kriegsanleihe propagiert werden erstattet

(Signed) Ratibor

An die Kaiserliche Gesandtschaft
Caracas.

CODE TEXT OF BOND MESSAGE

The words at the *right* had been identified when the code text was matched up with the message in clear. The 18470 equivalents have here been added, and one or two garbled groups have been restored in parentheses.

It will be noticed that the code message contains more than the clear text; the latter lacks the directions that follow "werden erstattet." This difference in length had prevented the matching up of the code and the clear text when an attempt had been made before the breaking of the code to locate the code mate of the bond message among our telegrams. The words on the left enclosed in parentheses were for some time thought to be garbled, since they do not fit into the alphabetical order. The independent discovery, however, of nonalphabetical groups for zu and for forms of the article, in addition to those early found for und, cleared the matter up. (See p. 38.) The code text not paralleled by the clear text—the translation is here enclosed in brackets—could not be read at the time the two messages were matched up, but was later deciphered with the exception of two words. It will be seen that the clear text did not contradict any of the identifications that had been previously made.

	333		Nr. 376	Schuldver-	11227	9317	
	889		vom 22ten Maerz	schreibungen			
	1777	[18470]			7109	16949	vier
Als	20325	3215			14263	28653	einhalb
	13036	4726	8te	prozentige	5034	7824	
	22189	14179	Kriegs	Schatz	17799	9089	
anleihe	13084	4774		anweisungen	2119	6709	
werden	5209	11849		beide	4229	13619	
	11208			(zu)	2533	13123	
ausgegeben	(11608)	20448			21178	29068	98
	5364	30854	fuenf		20551	23091	stop
prozentige	5034	7824		Aus	9901	20341	
fruehestens	5316	30806		losung	21733	11223	
	20349	3239	1sten		19720	11010	comma
	14673	17563	Oktober	Einloesung	21149	29039	
	18436	10326	19	(der)	3581	20271	
	9935	20325	24	Schatz	17799	9089	
kundbare	26769	12959					

anweisungen	2119	6709	
Stuecke	12662	21652	
lungen	21781	11271	
	21377	27167	fuer
beide	4229	13619	
Papiere	21855	23295	
wie	2227	14917	
bei	4269	13659	
	18588	6878	6ter
	9953	20393	und
	13077	4767	7ter
Anleihe	13084	4774	
	30071	4861	stop
Erster	19403	24343	
Zins	25304	16544	
schein	17736	9026	
	21373	27163	fuer
beide	4229	13619	
Papiere	21855	23295	
	25159	15799	Januar
	18436	10326	19
	6906	24046	neunzehn
faellig	21003	28743	
comma	16600	29240	
Zeichnungs	12518	20108	
frist	5305	30845	
	21440	18130	vom
	8578	8468	18ten
	17101	13941	Maerz
	20770	13060	bis
	20349	3239	1sten
	6843	15433	Juli
comma	26350	9890	
Einzahlung	13262	28952	
beginnt	27531	26321	
	11326	22316	28sten
	17108		
	(17101)	13941	Maerz
stop	29311	14001	
Werbung	5225	11815	
unter	16009	12049	
Angehoerigen	18523	6813	
auch	8523	8413	
neutraler	6993	24083	
Staaten	13860	21450	
erwuenscht	15842	28832	
stop	16661	29251	
Vermittlungs	28165	16755	
stellen	19375	21265	
fuer die	21321	27111	
besonders	17052	13492	
kleinere	12871	28561	
Banken	21950	23590	
geeignet	29567	15557	
scheinen	17738	9028	
	9758	25598	erhalten
	7787	26477	30
	1410	10800	Pfennige
	21376	27166	fuer

je	6824	15414	
	13216	28906	100
	17135	13925	Mark
	17193	13983	und
voraussichtlich	21466	18156	
Zuschuss	24976	18266	
(zu)	26473	12563	
Werbungs	5225	11815	
kosten	26174	12664	
comma	26350	9890	
Auslagen	11694	20484	
	21377	27167	fuer
Zeitungs	12538	20128	
annoncen	30017	4807	
(die)	27592	26382	
	22189	14179	Kriegs
anleihe	13084	4774	
propaganda	12279	8169	
deletion group	2912	1602	
ieren	15205	11445	
	1350	1590	dash
propagieren	12285	8175	
werden	5209	11849	
erstattet	19400	24340	
stop	6831	15421	
[Material	17128	13918	
	21374	27164	fuer
Propaganda	12279	8169	
wird	26449	12539	
	14522	30512	durch
Funken	5385	30875	
uebermittelt	11478	9668	
werden	5209	11849	
stop	9351	20691	
Bisheriges	20776	13066	
Zeichnungs	12518	20108	
ergebnis	9744	25534	
viel	7101	16941	
versprechend	25485	17975	
stop	25781	16871	
Bitte um	15733	13723	
briefliche	9855	23795	
Benachrichtigung	3456	13296	
	21447	18137	von
	8491	5581	Buenos Aires
zur	24238	20028	
gleichzeitigen	7203	18743	
Verstaendigung	25466	17956	
	21448	18138	von
	27721	4211	Santiago
Mexico	10677	1467	
(?)	5613	5903	
Bogota	1790	6080	
und	15413	29103	
Caracas	2898	1288	
(?)]	21278	?	
	(Signed)	BUSSCHE	

(19) The Barred-Zone Message and Its Paraphrase

In the 18470 message, page 46, quoted below, the identifications recorded in the right-hand column of words indicated that the message dealt with an announcement of the extension of the German barred zone. The date was found to coincide with such an extension, and the official announcement of the widening of the zone was obtained from the Norddeutsche Allgemeine Zeitung of January 8, 1918. The announcement and code message read as follows:

Nord. Allg. Ztg., Jan. 8, 1918.

Erweiterung des Sperrgebiets

Die nachstehende Ergaenzung der Sperrgebietserklaerung vom 31 Januar 1917 wird bekanntgegeben:

Um die feindlichen Stuetzpunkte auf den Kap Verdischen Inseln und den Stuetzpunkt Dakar mit dem anschliessenden Kuestengebiet wird vom 11 Januar 1918 ab ein neues Sperrgebiet mit folgendem Grenzenverlauf erklaert:

Von Kap Palmas Leuchtturm

nach 10° 0′ N 29° 30′ W
" 17° 0′ N 29° 30′ W
" 20° 30′ N 25° 30′ W

auf dem Breittenparallel 20° 30′ N in oestlicher Richtung bis zum Schnittpunkt dieses Parallels mit der Strand-Linie der westafrikanischen Kueste.

Mit dem gleichen Datum wird das Sperrgebiet um die Azoren nach Osten bis ueber die unseren Gegnern als Stuetzpunkt dienende Insel Madeira ausgedehnt, so dass dieses Gebiet folgende neue Grenze erhaelt:

Von 44° 0′ N 27° 45′ W
nach 44° 0′ N 34° 0′ W
nach 42° 30′ N 37° 0′ W
nach 37° 0′ N 37° 0′ W
nach 30° 0′ N 26° 0′ W
nach 30° 0′ N 17° 0′ W
nach 34° 45′ N 12° 0′ W
nach 36° 45′ N 12° 0′ W

nach dem Anfangspunkt zurueck.

Neutrale Schiffe, die zur Zeit der Veroeffentlichung dieser Erklaerung in Haefen innerhalb des oben angefuehrten Sperrgebiets liegen, koennen dieses Gebiet noch verlassen, ohne dass das fuer das Sperrgebiet angeordnete militaerische Verfahren Anwendung findet, wenn sie bis 18 Januar 1918 auslaufen und den kuerzesten Weg in freies Gebiet nehmen. Fuer neutrale Schiffe die in das neu erklaerte Sperrgebiet geraten, ohne dass sie von seiner Erklaerung Kenntnis haben oder haben erhalten koennen, sind ausreichende Schutzfristen festgesetzt.

Es wird dringend geraten die neutrale Schiffahrt zu warnen und umzuleiten. Berlin, den 5 Januar 1918.

	033	Nr. 30	Osten	26899	
	716	V 8 Jan (1918)		13060	bis
	135	Antw. auf Tel.	ueber	9528	
	547	Nr. 4	Madeira	3413	
	18475		stop	24450	
	27594	Folgende	Errichtung	25611	
	21723	Sperr		23971	neuen
	19236	gebiets	hiervon?	24950	
erweiterungen	28871			22840	getrennten
	30197	sind		21723	Sperr
heute	24973			19236	gebiets
veroeffentlicht	16843		umfassend	14418	
worden	12295		Kap Verdische Inseln	2285	
stop	25502			11723	und
Ausdehnung	20386		Dakar	4090	
Azoren	5636		mit dem	10012	
	21723	Sperr	anschliessenden	4854	
	19236	gebiet	Kuesten	12978	
	29645	nach		19236	gebiet

	27162	stop	die	17702	
	24083	Neutrale		17508	ohne
	9728	Schiffe	Kenntnis	29432	
in	18654		neuen	23971	
betreffendem	13479			21723	Sperr
Kriegsschauplatz	14181			19236	gebiets
haben	15116			18654	in
Frei	30734		*dieses*	30918	
geleit	19127		*geraten*	18867	
wenn (sie)	11812			30198	sind
	13060	bis	voellig	16623	
	8468	18 ten	ausreichende	20414	
	15799	Januar	Schonungs	9373	
auslaufen	20430			30845	fristen
und	20393		festgesetzt	30306	
	21723	Sperr	stop	28722	
	19236	gebiet	Naehere	26092	
auf dem	8405		Einzelheiten	28957	
kuerzesten	12949		werden	11848	
Weg	14606		durch	30510	
verlassen	16738		hiesigen	24938	
stop	16811		spanischen Botschafter	7047	
	27165	fuer	dortiger Regierung	27377	
	24083	neutrale	mitgeteilt	10029	
	9728	Schiffe			BUSSCHE

A comparison of this proclamation with the text of our telegram made it clear that we had to do, in this case, with a *paraphrase*, and the telegram was reconstructed by the addition of the words in the left-hand column. Words in this column that are italicized had been previously provisionally but not finally identified. The group 9373 was first taken as Schutz, as in the clear text, but when this meaning was about to be entered in the code-book it was found to stand too near to Schon (9371). It was then feared that the identification of Schon might be wrong, but the change from Schutz to Schonung served to right things all around.

(20) The Word "Dampfer"

The identification of the group 10275 led to the fixing of a large number of additional code groups. 10275 was found frequently preceded by the words Waren aus, at other times by spanisch or another word from a name page. These facts and the alphabetical position of the word on a page containing words in the early part of the D's led to a provisional identification of the group as Dampfer (Waren being, of course, the noun, i. e., merchandise, not the verb). If the identification was correct, the group was certain to be followed in many cases by the name of a steamer. It was felt that the German steamers that had taken refuge for the war in Spanish harbors would be the ones most frequently referred to. A list of these was procured, and the groups immediately following 10275 in the messages were then examined to see whether or not

they spelled the names of vessels. Here follow a few examples of spelled names that came to light in the 18470 messages:

Page 531, A f.....	10275	Dampfer
	27976	Tet
	9539	ua
	29611	n
Page 609, A r.....	10275	Dampfer
	1542	quote
	40132	Anna [Note the high number name group]
	21689	Stro
	14233	wig
Page 652, A j.....	10275	Dampfer
	10646	Prinzregent
	2196	Santa Cruz
	8583	de
	5092	Tenerife

The fact that the Anna Strowig was known to be in Barcelona, and the phrase 18654 5959 (in Barcelona) in connection with the steamer's name in the 18470 messages, page 559, A p, served to confirm 5959 as Barcelona, and to place beyond question the identification of genehmigt, Generalkonsulat, general, and Konsulat with which 5959 was so closely bound up. (See p. 39.) The syllable groups that were identified were valuable in aiding to identify other groups in their alphabetical neighborhood.

The identifications were not confined to German vessels. The group 4137 had been tentatively identified as meaning franzoesisch. In the 18470 messages, page 785 A r, occurs the phrase 4137 10275 1540 4421 9963 3196 8583 29410 23872 17650 1543, which, with the aid of Lloyd's Register, was read as franzoesischer Dampfer quote A mir al de Ker sai nt quote. When the message was afterward read, it proved to be concerned with the submarine question, and to give an account of an encounter between a U-boat and the French steamer mentioned.

(21) Certain Proper Names

Several place names were identified comparatively early. 5581 was found, from the introductions to messages sent from Berlin to Madrid for forwarding to Buenos Aires, to signify Buenos Aires (see p. 26), and 4211 was identified with a fair degree of certainty as Santiago. 1186 was taken to be deutsch from its general behavior rather than from any particular passage, and 1142 in like manner seemed to be Deutschland. The following phrase in 18470 messages from Berlin to Madrid—

Page 639, A g			Page 745, A l	
6231			6232	
6024			6024	
27166	fuer	compared with	27160	fuer
6234			27376	dortig
3415			6231	

served, on the assumption that 6234 and 6231 were either variants or at least closely related to each other, to fix 3415 as Madrid. It served also to arouse the suspicion that 6024 might be Berlin—a suspicion which proved to be correct. The names of steamers served to fix some additional place names. (See above.) The number of place names was, however, considerably

increased by the series of messages beginning in 18470, pages 170 and 669. These messages contained what were evidently lists of names in a context of which the following examples are typical:

18470 messages, page 670, A b		Ibid., page 171, B e	
6878	6tens	30751	
30785		21294	
27935		15645	
7454		9829	
55300		18097	
13376	48	29487	
9829		19342	stop
6365			

18097 and 29487 were especially frequent before a stop. At other times, however, the stop would be preceded by such groups as 3257 (meaning 2) 29486, or 1926 (meaning 3) 29486. In other passages 18097 was absent, and 11000 (practically confined to these messages) occurred in its place. It was believed that the whole constituted a series of names, and that the numerals might have to do with the addresses of the people involved, but no progress could be made on the address theory by assuming "street", "avenue", or any other form of address that could be thought of in either German or Spanish to accompany the numbers. The solution was reached through 18470 messages, page 171, A h:

19155	Generalkonsulat
5959	Barcelona
3239	Erstens
64639	
19154	
18097	
29487	

64639 appeared in the signature in messages sent from the consulate general in Barcelona to Berlin via Madrid, and had already been identified as Ostman von Leye, German consul general at Barcelona. The presence of "erstens" before the name of the consul general made it appear that what followed was a list of the personnel of the consulate, and that the whole message consisted of the names of German consular officials in Spain. The groups 18097 and 29487—the latter never preceded by a numeral, while 29486 always was—were then identified from their alphabetical position as verheiratet and kinderlos, and 29486 and 29485 as Kinder and and Kind, while 11000 was seen to mean ledig. The higher numerals at first supposed to be part of an address undoubtedly give the ages of the respective persons.

The Almanac de Gotha served to decipher the consuls' names precisely as the list of German steamers and Lloyd's Register had helped in the case of the ships. Also, as in the case of the ships, one name would yield several code groups, since Jaenicke, for example, was encoded—

18470 messages, page 670, A g	
15734	Ja
25748	en
11717	ic
29403	ke

Since each consul's name was preceded by the name of the city where he was stationed, these cities were identified at the same time as the consuls. The list yielded a total of several cities, and their alphabetical position helped to confirm other suppositions for names. The names in the gazetteer have been rearranged in blocks-of-ten just as the words in the vocabulary proper of 13040 and 18470. This was first indicated by the finding, in widely separated blocks, of the groups 1186 (Deutschland) and 1142 (deutsch), and was later substantiated by other

identifications. The arrangement of the pages conforms to that of the blocks of means and extremes in the ordering of the pages of the vocabulary proper.

(22) Grammatical Directions

It remains to say a word or two about the parts of the code book that have hitherto been mentioned only incidentally—the grammatical directions and the high number names. The first grammatical sign to be found was "Schluss der Depesche", 2440–2444. (See p. 18.) On the analogy of 13040, it was concluded that the whole of page 24 would be devoted to grammatical indications. The same conclusion was reached for page 36 after the finding of the colon 3670 (see p. 28), and for page 15 (see p. 33). Groups on page 16 were likewise found occurring in such positions that they seemed to be grammatical signs of one kind or another.

Page 36 proved to contain only colons, dashes or hyphens, and stops or commas—at least nothing else was found. Similarly page 15 contains dashes and quotation marks. Pages 24 and 16 are more varied in their contents.

The group 2490–4 occurred several times, uniformly under such conditions as these (18470 messages, p. 829, A w): 2493 12444. Each time it occurs the group is followed by a code indicator; it was accordingly identified as a signal for a change of code.[20]

The groups 1650, etc., had attracted attention because they were very frequently found following proper names. Now, in addition to spelling by syllables, as described in the case of names of steamers and consuls (see pp. 55, 56), the Germans employ another method of spelling, especially to represent the proper names that have not been included in the book. They take from the code book a name that coincides for several letters with the name to be spelled, indicate by a code group that the remaining letters are to be deleted, and then, if necessary, add code groups to finish spelling the name they are writing. This had been done repeatedly in the 13040 messages.

It seemed likely, accordingly, that the groups mentioned on page 16, were deletion groups. This was finally proved by the name of a ship. The steamer Brasilia had been found spelt Brasili-a. In the 18470 messages, page 144, A l, occurred the phrase 5599 1654 4422. 5599 is on the same page as 5581 (Buenos Aires), and the phrase was read, in connection with a further study of 5581, as Brasilien, delete two letters, a. Similarly (18470 messages, p. 337, A w) 5593 1605 was read as Brasilianer, delete three letters (or last syllable). These deletion groups, to some extent, no doubt, on account of garbling, seem not to be used with entire uniformity of meaning; this difficulty, however, is more academic than practical.[21]

2465 was identified as Present Participle from such passages as this (18470 messages, p. 819, B m):

29645	nach
6666	(a place, later identified as Norwegen)
28797	fahren
2465	
9728	Schiffe

2420 was found to be Past Participle, 2470 Past Tense, etc. In each case several successive code groups are assigned to the one meaning.

[20] It would not suffice, in the German system, to indicate a change of code merely by the use of the indicator number of the new code, since that number, like any other within the range of the code, has a meaning in the code that is being used. Thus 1777 in a 18470 message would mean the seventy-seventh word on page 17, 12444 the forty-fourth word on page 124, etc. The code indicator, when the code is changed in the midst of a message, is regularly not enciphered. Thus, a change from 12444 to 18470 is indicated by 1950 18470.

[21] The spaces between brasilianisch and Brasilien were filled with the phrases brasilianischer Botschafter, etc. This system is followed regularly with similar name groups, such as spanisch, deutsch, etc.

(23) Stops, Und, Die, Etc.

A detailed study served to amplify the theory concerning the insertion of stops throughout the vocabulary and the assigning of code groups to und, der, die, nicht, etc., throughout the code book regardless of alphabetical order (cf. pp. 18, 28, 38). This study showed that the plan, not without merit in itself, has been executed by a code compiler to whom system was a god and regularity a religious rite.

The stops and the particles referred to have been inserted in those blocks-of-ten which are alphabetically first and sixth on the page. This had a definite purpose: We may suppose that the page of 100 code groups was divided into two columns each containing 50 code groups. The encoder, with the book in straight alphabetical order, could then look at the top block-of-ten in each column for his stops, und, etc., and at the bottom block of each column for his numerals.

The stops and particles, however, like the numerals (cf. pp. 31, 34), were not inserted at random within their blocks, nor were they even assigned to pages in a haphazard manner. What follows is based on a study of every identified stop, etc., in the code book, and contradictions, where they are found, occur in such small numbers that they can safely be assigned to garbling or to mistakes in identification. Some apparent contradictions can, in fact, be shown to be due to telegraphic errors. After the underlying plan had been worked out, and before the occurrences had been completely studied, the occurrence of a stop, und, or die, etc., was predicted in advance with such regularity that the sport finally began to pall.

Occasionally there is doubt as to the precise meaning of a particle. There may, for example, be uncertainty as to whether the definite or indefinite article was used. In the tabulation that follows such cases are indicated by question marks or suggested alternatives. The stops occurring at code groups terminating in 0 are almost certainly all commas. This was not recognized until comparatively late, and in the deciphered messages in the files of M. I. 8 many of these commas are decoded merely as stops. The point is of no great practical importance. The word "query" denotes the presence, in the code, of a mark of interrogation.

The stops and particles form a series. They are inserted on *even* numbered pages (it will be remembered that the book begins with an even numbered page), opposite a terminal 0 in the block that is alphabetically first and opposite a terminal 1 in the block that is alphabetically sixth, and on *odd* numbered pages opposite a terminal 2 in the first block alphabetically, and opposite a terminal 3 in the sixth block alphabetically. This gives us four series—even page at 0, even page at 1, odd page at 2, odd page at 3—and these series are kept distinct. If we take the even numbered pages in alphabetical sequence we find the entries opposite 0 in the first block—always alphabetically speaking—running in the following sequence and then repeating, right through the book: der(einer?), comma, comma, zu, des, comma, comma, nicht. At 1 in the sixth block on the even pages we find the repeating series dem, stop, stop, der. At 2 in the first block on the odd pages the series is einen, stop, stop, die, den, stop, stop, eine. Finally, at 3 in the sixth block on the odd pages we have und, die(?), query, das, zu, stop (?), query, eines (?). The last is the least well-defined series, and die, stop, and eines are not absolutely certain.

This gives us, in the 246 pages of vocabulary:

stops	139	einen	16
commas	62	die	31
der	46	den	15
zu	30	eine	16
des	15	und	16
das	15	query	31
nicht	15	eines	15
dem	31		

Entries on the pages of the code will run in cycles of 16. Thus, beginning, say, at XX page 42 (=18470, p. 262), we have, filling in blanks where they occur—

XX	18470			XX	18470		
42	262	1st block at 0	der	50	102	1st block at 0	des
		6th block at 1	dem			6th block at 1	dem
43	237	1st block at 2	einen	51	85	1st block at 2	den
		6th block at 3	und			6th block at 3	zu
44	234	1st block at 0	comma	52	82	1st block at 0	comma
		6th block at 1	stop			6th block at 1	stop
45	265	1st block at 2	stop	53	105	1st block at 2	stop
		6th block at 3	die(?)			6th block at 3	stop(?)
46	222	1st block at 0	comma	54	270	1st block at 0	comma
		6th block at 1	stop			6th block at 1	stop
47	205	1st block at 2	stop	55	309	1st block at 2	stop
		6th block at 3	query			6th block at 3	query
48	202	1st block at 0	zu	56	306	1st block at 0	nicht
		6th block at 1	der			6th block at 1	der
49	225	1st block at 2	die	57	273	1st block at 2	eine
		6th block at 3	das			6th block at 3	eines(?)

This complete cycle of 16 pages with 32 entries occurs 15 times in the book, with a 6-page fraction of a cycle at the end of the vocabulary. It is never necessary to search through more than four pages to find a stop, or more than six pages to find a comma.

(24) Code Groups 31,000–99,999

Of the high numbers 31,000–99,999 only one-tenth are used, as in 13040. (See p. 6.) The finding of the series of pages of geographical names rendered it probable that these high-number groups were devoted exclusively to names of persons. A list of places is a constant and may well be incorporated in the body of the book, but people rise and fall and die, and personal names are well cared for in an appendix. Failing any indications of alphabetical order, these personal names had to be identified entirely from their context, and comparatively few were found—somewhat over 100. The identification of 64639 as Ostman von Leye has been mentioned above (p. 56). 79804 was found (18470 messages, p. 804, A n) in a message containing the word Note and two occurrences of the number 14. These associations, together with the date of the message (Oct. 16, 1918), served to identify the group as Wilson. This identification proved correct, even though one of the "14's" refers to Louis the fourteenth! The finding of the word "Punkt" in the message fixed the identification even before much of the message was read. In the case of the list of consuls mentioned above (p. 56), the spelling of the name is uniformly followed by a high-number group, obviously the first name of the official; unfortunately the Almanac de Gotha gives only initials of first names, and other sources for identifying these names were not available.

Preliminary to an attempt to discover the structure of this list of personal names a detailed study of the proper names of 13040 was undertaken. The results of this study will here be summarized.

The original list of names can be definitely separated from the later additions. If we disregard all but the first two digits of the code-group numbers, we find that the names beginning with the same two digits constitute an alphabetical unit, e. g., 24 Rescht–Rotterdamm, 78 Kuhn–La Plata, etc. Furthermore, they regularly fall into larger units each containing four

90481—37——5

of the smaller ones and each comprising an alphabetical section. The following two collections of four will illustrate:

44	Hans–Helby	78	Kuhn–La Plata
45	Henry–Hirsch	79	Lehmann–Limburg
46	Hohenlohe–Iberisch	80	Lincoln–Luebeck
47	Ida–Jaffa	81	Luise–Malacca

Overlappings and irregularities within these units are so very rare as to be entirely negligible. On the other hand, where supplementary matter has been introduced, the old and the new units will, of course, overlap. The new material is recognizable by the fact that a unit is spread over a larger part of the alphabet than a unit of the original matter.

The entire contents of the onomasticon can be divided as follows:

ORIGINAL

(The numerals are the initial two digits of the code group numbers)

82–85	Aachen–Barranquilla	66–69	Malaie–Nagasaki
32–35	Bayerisch–Callao	62–65	Napoleon–Niederlaendisch
40–43	Canada–Deutsche Bank	48–51	Pera–Reimer
74–77	Deutsch–Fort	24–27	Rescht–Schoen
86–89	Frankfurt–Hamburger Nachrichten	58–61	Schottland–Syra
44–47	Hans–Jaffa	36–39	Tabora–Vereinigte Staaten
52–55	Jagow–Krupp	94–97	Victor–Zuerich
78–81	Kuhn–Malacca		

FIRST SUPPLEMENT

28–31	Amer–Geier	70–73	Michelet–Snatow
90–93	Hapag–Mondschu	56–57	Tsingtau–Wiegand (two blocks)

The other supplementary matter, in blocks 98 and 99, covers a larger alphabetical field.

Further examination of these larger units shows that they are built up precisely on the lines of the pages of the 13040 vocabulary. Each two-digit number goes with a possible 100 names, and these hundred names are divided into 10 blocks of 10 each, which are then shuffled among themselves exactly as the blocks-of-ten on the vocabulary pages. Thus, to take an example:

35

00		20		40		60		804	Brown
01		21		41		61		81	
027	Bruessel	22		42		62		82	
03		23		43		63		83	
045	Bryan	24		44		649	Caldera	84	
05		25		45		653	Calcutta	85	
06		26		461	Burian	66		86	
07		27		47		672	California	87	
08		28		48		68		88	
09		290	Bristol	49		691	Callao	89	
10		30		50		703	Brest	90	
115	britisch	31		51		71		91	
12		322	v. d. Bussche	52		72		929	Bulgarien
13		33		53		73		936	bulgarisch
14		34		54		74		94	
15		35		55		75		95	
16		36		562	Buenos Aires	76		96	
17		37		57		77		97	
18		38		58		78		98	
19		394	Cadiz	59		79		99	

The analogy of the onomasticon to the vocabulary pages of 13040 is now complete; we have units of 100 entries in 10 blocks-of-ten, and we have 4 of these units at a time in alphabetical succession, precisely as the alphabetical original of the 13040 vocabulary was disarranged 4 pages at a time.

It remains to explain how the five-figure code groups of the onomasticon were built up. Let us first picture each hundred names as fitted with numerals from 00 to 99, but without page numbers. If we now assign page numbers we shall obtain four-figure code groups conflicting with the four-figure groups of the 13040 vocabulary proper. In order to avoid such conflict, it is necessary to have five-figure code groups above 23999. Accordingly, the pages receive numbers from 24 upward, and to complete the group to five figures an arbitrary digit is added at the end of each code group. Thus, to 9755 a 6 is added, making 97556; 3968 receives a 9, becoming 39689; and 6789 becomes 67893. To make these terminal additions the 10 digits are distributed arbitrarily in each block-of-ten: if 6789 receives a 3 no other word between 6780 and 6789 will terminate in 3. Any block-of-ten among those just given will serve as an example.

It may be noted in passing that the desired result might have been achieved by using three-figure page numbers from 240 upward and assigning 100 names to each page—in other words by continuing the process employed in the vocabulary proper. The code with its present quota of 7600 names would then have ended at 31599. The device adopted has the effect of raising the apparent range of the code to 99,999. It also facilitates the correction of certain cases of garbling.

The structure of the list of personal names in 18470 was found to conform closely to that of the onomasticon of 13040 as it has just been described. We find again 100 entries to the page divided into 10 blocks-of-ten shuffled among themselves. The pages are numbered from 32 up, all code groups being then converted into five-figure numbers above 31999, the end of the vocabulary proper, by the addition of an arbitrary digit at the end. The pages, like those of the vocabulary proper, have been alphabetically disarranged page by page—not four at a time as in 13040. Thus, von Erckert, Erhardt, and Ernst were originally respectively 5771, 5772, and 5776 (note the alphabetical sequence within the 10-word block) but by the addition of the arbitraries at the end became 57713, 57724, and 57768. (The numerical sequence of the arbitraries in this case is accidental, or at least not typical.) Emil was originally 5788 (on the same page but in a different block from the three names just mentioned), and became 57889.

A table showing the changes in these groups in going from 12444 and 1777 to 18470 follows insofar as it can be reconstructed:

High-number name table, 12444 and 1777 to 18470

(The first 2 figures change as follows; the last three remain unchanged; the names are alike in 12444 and 1777)

12444 and 1777	18470	12444 and 1777	18470	12444 and 1777	18470	12444 and 1777	18470	12444 and 1777	18470	12444 and 1777	18470	12444 and 1777	18470
32		40		50		60		70		80		90	
33		41	49	51	43	61	53	71		81		91	
34	42	42	44	52		62	62	72		82		92	
35	31	43		53	45	63		73	57	83		93	
36		44		54		64	64	74		84		94	
37		45	73	55		65		75		85		95	
38		46	74	56	60	66	66	76	36	86		96	
39		47		57		67	67	77		87		97	
		48		58		68		78	38	88		98	
		49	77	59	51	69		79	79	89		99	

A few other correspondences may be conjectured from the table, e. g. 47–75, 60–52. On this basis, however, we should parallel 52 by 44, which belongs to 42.

(25) Survey of the Construction of the Code

It may now be worth while to make a final survey of the book that we have gradually rebuilt, and to follow, as far as we are able, the workers in the German Foreign Office in their work of assembling the code.

In putting together 18470 we see the German compilers making use of the following parts:

1. The Dreinummerheft.—This little dating and numbering code (see p. 3*f.*) is left as it is. In fact, since it has been designed to be used with various German codes, it cannot properly be called a part of any one of them.

2. Six pages of Grammatical Directions, 100 to the page.

3. Two pages to contain the Code Designator ("Chiffre Nummer") and any supplementary matter for which need may later arise.

4. A gazetteer, consisting of 50 pages, with 100 entries to the page.—These pages contain no numerals or stops—merely geographical terms. Whether or not they are intended ever to be used with any other Foreign Office codes than 18470 and its relatives we do not know. The matter is in strict alphabetical order.

5. The vocabulary proper.—This, with its 246 pages containing 100 entries per page, is by far the largest part of the code. It is in strict alphabetical order, broken only on each page to allow for the insertion of—

(*a*) Numerals.—Two numerals are inserted on each page, in the blocks of 10 words that are alphabetically fifth and tenth. They appear in regular order throughout the alphabetical vocabulary. Their position within the blocks in which they appear has been explained at length above (pp. 30*ff*; 33*f.*).

(*b*) Stops and commas.—Stops and commas have been inserted systematically in those blocks of words which are alphabetically first and sixth, as described above, page 58*f.*

(*c*) Certain common words.—Some very frequent words have been inserted on page after page without regard to their alphabetical order. (See p. 38, also p. 58*f.*)

6. An onomasticon containing personal names only. This is as nearly in alphabetical order as is possible for a constantly changing list.

With these parts before him the compiler now sets to work to combine them into a code that shall be capable of keeping the secrets of the office. We are unable to see in precisely what order he is arranging the elements, but we can make a fairly accurate guess. To begin with, he puts the two supplementary pages (part 3) at the end of the vocabulary proper (part 5). He then puts the pages of grammatical directions (part 2) either immediately after the supplementary pages (part 3) or before the vocabulary proper (part 5); in the former case the gazetteer (part 4) will form the beginning of the book, in the latter it will follow the two pages of supplementary matter (part 3). We can say this with a high degree of certainty, since no other arrangement will approach these two in convenience of use. At the very end he puts the onomasticon (part 6), where it can be conveniently consulted and can be added to from time to time. The parts of the book, then, will be in one of the following orders: (*a*) Gazetteer, vocabulary proper, two supplementary pages, grammatical directions, onomasticon; or (*b*) grammatical directions, vocabulary proper, two supplementary pages, gazetteer, onomasticon.

This arrangement has provided a book convenient for encoding purposes. In using it the code clerk will merely have to keep in mind which section he wishes to consult—a thoroughly easy procedure.

The compiler is now ready to provide his code matter with the numerals which are to be used to represent the various words and phrases—in other words, to enter into the book the

code equivalents. So far he has arranged everything for convenience of use; but now he begins to employ guile to put the would-be decipherer off the track. We can picture him as using either of two procedures to attain his end. One entails a double printing of the book, without, however, setting the type anew; for the other a single impression will suffice.

(*a*) Double printing.—The compiler now attaches the code group numerals to the words, etc., on each page. He does not do this in strict alphabetical sequence. He divides the hundred on each page into 10 blocks of 10 each. He then arbitrarily applies a different set of 10 consecutive numbers running from 00 to 09, from 10 to 19, etc., to each block-of-ten. The first 10, which, in an alphabetical arrangement, would have received numbers from 00 to 09, receive, say, 60 to 69, and so for the other blocks.[22] Each page is treated separately. The treatment is applied to all the pages of the gazetteer and of the vocabulary proper. The onomasticon is broken up in a similar way.

[22] While this paper was being revised before going to print, Mr. W. F. Friedman suggested, on the basis of some observations of his own, that further investigation might show that the blocks of 10 in the alphabetical code XX had been transposed systematically and not at random to produce 18470, and that further study might show that 18470 and its whole family had been produced from XX by transposition tables for both pages and blocks-of-ten. He suggested further that a similar condition might be found to exist in the case of 13040 and 5950 and their alphabetical original.

The writer proceeded to make this investigation—to arrange the blocks-of-ten on all the pages of 13040 and 18470 in alphabetical order, and to tabulate the results.

The blocks-of-ten were, in each case, tabulated in four different ways:

(1) With the pages in alphabetical order, the blocks on each page, designated by their penultimate figure, were arranged in alphabetical order.

(2) With the pages once more in alphabetical order the present block numbers were replaced in order by the figure that shows the alphabetical position of each block.

(3) With the pages in the order of 13040 and 18470, respectively, the blocks were arranged as in (1).

(4) With the pages in the order of 13040 and 18470 the blocks were arranged as in (2).

While it is true that any systematic rearrangement of the blocks as in (1) would necessarily make itself evident under a rearrangement as in (2), it was felt, none the less, that one or the other scheme might yield results that might be more readily perceptible.

An illustration follows of a page of 18470 arranged according to each of the above methods. One word is here taken from each block on the page so that the alphabetical order may be followed.

18470, PAGE 256

The page at present runs—

01	erlaubt
17	ersatz
24	ermaechtigen
31	erlass
40	ermordung
54	ernst
64	erregen
71	ermaessigen
80	ero
90	erleichtern

Arranged as in method (1)—

31	erlass
01	erlaubt
90	erleichtern
24	ermaechtigen
71	ermaessigen
40	ermordung
54	ernst
80	ero
64	erregen
17	ersatz

giving the order 3 0 9 2 7 4 5 8 6 1

Arranged as in method (2)—

01	erlaubt comes alphabetically at	1
17	ersatz comes alphabetically at	9
24	ermaechtigen comes alphabetically at	3
31	erlass comes alphabetically at	0
40	ermordung comes alphabetically at	5
54	ernst comes alphabetically at	6
64	erregen comes alphabetically at	8
71	ermaessigen comes alphabetically at	4
80	ero comes alphabetically at	7
90	erleichtern comes alphabetically at	2

giving the order 1 9 3 0 5 6 8 4 7 2

One step more—but a most important one—is still to be taken. This is the final effort to guard against the prying eye. The compiler now assigns numbers to his pages, not in regular order, nor yet at random, but in the manner that has been described in detail above (p. 34 *ff.*). In this process the two pages of supplementary matter and the grammatical directions are all provided for. When the page-numbering is completed the pages bear the appearance of page 134 with its words in alphabetical order as given on p. 66.

The compiler has now finished his encoding book. The user will find a straight alphabetical arrangement for each part of the book. All he will need to do is to find his word or phrase and write down to represent it the page number that he will find at the top or bottom (perhaps both) of the page, adding to it the number of the word or phrase within the block-of-ten in which it appears.

Undeniable signs of systematic change were found, especially apparent when the blocks were rearranged according to method (1); but the results, in the writer's opinion, preclude the conclusion that the changes may have been effected by means of tables.

The following may be offered as the most striking examples of systematic change found in 13040 and 18470, respectively.

13040

Alphabetical p. no.	13040 p. no.	Order of blocks as in method (1)									
11	54	7	?	?	?	0	9	4	2	1	8
12	55	7	5	2	1	9	0	6	3	8	4
13	131	2	0	9	7	6	4	5	8	1	3
14	132/3	9	3	7	4	5	2	8	6	1	0
15	134	4	9	2	5	6	8	3	1	7	0
16	135	1	6	4	7	8	5	0	9	2	3
17	101	2	7	0	8	9	6	1	4	5	3
18	102	5	4	8	0	1	3	0	7	2	6
19	103	3	8	1	9	5	7	2	0	6	4
20	104	8	2	4	3	6	1	7	5	9	0

We note how the 8 travels. On alphabetical pp. 36–45 we have a similar tour, the 8 starting this time at the left end. Many of the pages in that series exhibit an order almost—but never quite—the reverse of that in the pages given here. There is one other similar, but incomplete, tour of the 8 in the first 10 alphabetical pages, which show other peculiarities also.

18470

Alphabetical p. no.	18470 p. no.	Order of blocks as in method (1)									
70	244	5	7	1	9	4	6	2	0	3	8
71	255	0	6	5	3	9	1	7	4	8	2
72	256	3	0	9	2	7	4	5	8	6	1
73	243	1	2	6	4	0	7	9	8	3	5
74	288	7	3	2	1	5	8	9	6	0	4
75	291	9	5	4	0	2	3	?	?	?	1
76	292	4	1	0	8	3	5	6	9	2	7
77	287	2	9	8	1	6	3	4	7	5	0
78	276	6	8	7	0	5	2	3	1	9	4
79	303	8	4	3	6	7	9	0	2	5	1

The encoding book is now given to the printer, and we perceive why the alphabetical arrangement has not been further disturbed. No money is to be wasted. The printer is carefully instructed not to disturb his forms after the printing is finished, for he will have further use for them. When the encoding book is finished he is told to arrange the forms in the order of the page numbers, and to arrange the matter on each page in the order of the numerals opposite the individual words and phrases. When he has done this, he is told to go to press again, and to print just as many copies as before. These new books will serve for decoding; the recipient of a message will look up the code groups which he has received and will write out the clear text accordingly. The pages now present the appearance of page 134 with the code groups in numerical order as given on p. 67.

(*b*) If the book is to have only one printing, the compiler will proceed somewhat differently. He arranges the matter on each page in straight alphabetical order, and attaches code group numerals running from 00 to 99 in straight numerical sequence. In the margin, to the left and to the right (see the specimen page of 18470 as arranged for a single printing, p. 68), he has an extra column with the heading "For encoding change penultimate figure to", and in this column one of the digits from 0 to 9, in disarranged order, is inserted opposite each block-of-ten—a different digit for each block. Each page bears its own arrangement. At the bottom each page will have a table showing how the penultimate figures as received in messages must be changed for decoding. (See the specimen page.) The alphabetical order of the pages is now changed in the manner already described for the double-printing method, and each page is provided with its 18470 page number at the bottom and its XX (alphabetical) page number at the top. Finally, and separately from the book, a page table is provided for the conversion of 18470 page numbers (as received in messages) into XX (alphabetical) page numbers (as appearing at the top of each page). (The page table may be dispensed with if a certain number of books are arranged in the order of the XX pages—alphabetically—for encoding, and an equal number in the order of the 18470 pages for decoding.)

18470 is now ready for use.

Other peculiarities occur, such as sporadic cases of pages exactly the reverse in order of other pages at other points in the book.

The phenomena noticed, however, do not, so far as could be seen, recur at fixed intervals or show any evidence of a general cyclic order. Even if they did, it would be essential, if the change from the alphabetical original of the code book were to be made by tables, to have a small number of different arrangements of the pages. Instead we find the number of repetitions, although larger than a chance arrangement would be likely to produce, to be very small indeed. In 13040, even if we disregard some minor differences on certain pages as possibly due to error of one kind or another, we find only 11 cases of recurring arrangements, and no arrangement appearing more than twice. In other words, on 189 pages we have at least 178 different arrangements. In 18470 only 10 actual repetitions occur, and again no arrangement occurs more than twice. Even if we make allowance for error and go so far as to double the 10, we shall still have 226 different arrangements on 246 pages.

There would, moreover, be no actual gain in printing an alphabetical code and then obtaining its derivatives by tables. The only conceivable gain would be the avoidance of printing the code in a two-part (cross-referenced) arrangement, and it is explained above how the first nonalphabetical derivative (13040 or 18470, respectively) could, if desired, have been produced in a form available for both encoding and decoding without the trouble and expense of a double printing and without any use of transposition tables. All the other derivatives are obtained from the first by a page table and the *extremely simple* block-of-ten table given on page 8.

Why then the use of system, the clear evidences of which have just been pointed out? Simply because it was second nature for the compilers of these codes. Similar phenomena, serving no useful purpose whatever, confront us on every hand. The "Dreinummerheft" is a mass of them. The systematic disarrangement of pages by which XX is transformed into 18470 is another. The insertion of the numerals and stops opposite certain digits of the code groups is still another. And the periodic arrangement for inserting stops, und, die, nicht, etc., in 18470 (see p. 58 *f.*) is an extreme case. At the best these devices achieve no good end. They save no expense; and far from rendering an attempt at decipherment more difficult, they actually facilitate it. The only excuse that can be offered for the employment of such methods is the supposition that the compilers were making an attempt at what, in quite a different connection, has been called "the orderly avoidance of order."

Page 134 of 18470 so far as identified

(In this form, with the *words in alphabetical* order, the page is in the form used for *encoding*)

40		80	bestellt
41	besitz – en	81	stop
42	besitzer	82	
43		83	
44		84	
45		85	bestimmen – t – ung
46		86	
47		87	bestimmungen
48	besitzung	88	
49		89	bestimmt
90	besolden – t – ung	30	
91	besondere – n	31	
92	besonders	32	bestrafen – t – ung
93		33	
94	besorgen – t – ung	34	
95		35	
96		36	bestreiten – t – ung
97		37	
98		38	
99		39	
20	besprechen – ung	10	
21		11	besuch
22		12	
23		13	besucher
24		14	
25		15	
26	besser	16	
27	gebessert	17	betaetigen – t – ung
28	gebessert	18	beteiligen – ung
29		19	beteiligt
60	besserung	50	beteiligung
61		51	
62	bestand	52	
63	bestand	53	betonen – ung
64		54	betont
65		55	
66		56	betrachten – t – ung
67	bestaetigen – t – ung	57	
68		58	
69		59	betrag
00		70	betraege
01	best – en	71	betragen
02		72	betraegt
03		73	
04	bestehen – ung	74	
05	besteht	75	
06	bestehen – d	76	betreffs
07		77	
08	bestellen – t – ung	78	46
09	45	79	betreffend

Page 134 of 18470 so far as identified

(In this form, with the *numbers* in order, the page is in the form used for *decoding*)

00		50	beteiligung
01	best – en	51	
02		52	
03		53	betonen – ung
04	bestehen – ung	54	betont
05	besteht	55	
06	bestehen – d	56	betrachten – t – ung
07		57	
08	bestellen – t – ung	58	
09	45	59	betrag
10		60	besserung
11	besuch	61	
12		62	bestand
13	besucher	63	bestand
14		64	
15		65	
16		66	
17	betaetigen – t – ung	67	bestaetigen – t – ung
18	beteiligen – ung	68	
19	beteiligt	69	
20	besprechen – ung	70	betraege
21		71	betragen
22		72	betraegt
23		73	
24		74	
25		75	
26	besser	76	betreffs
27	gebessert	77	
28	gebessert	78	46
29		79	betreffend
30		80	bestellt
31		81	stop
32	bestrafen – t – ung	82	
33		83	
34		84	
35		85	bestimmen – t – ung
36	bestreiten – t – ung	86	
37		87	bestimmungen
38		88	
39		89	bestimmt
40		90	besolden – t – ung
41	besitz – en	91	besondere – n
42	besitzer	92	besonders
43		93	
44		94	besorgen – t – ung
45		95	
46		96	
47		97	
48	besitzung	98	
49		99	

Page 134 of 18470 (38 of XX) so far as identified

(In this form the page, with a single printing, could serve for both encoding and decoding)

38 (alphabetical or XX page number)

In encoding change penultimate figure to					In encoding change penultimate figure to
	00		50	bestellt	
	01	besitz – en	51	stop	
	02	besitzer	52		
	03		53		
	04		54		
4	05		55	bestimmen – t – ung	8
	06		56		
	07		57	bestimmungen	
	08	besitzung	58		
	09		59	bestimmt	
	10	besolden – t – ung	60		
	11	besondere – n	61		
	12	besonders	62	bestrafen – t – ung	
	13		63		
	14	besorgen – t – ung	64		
9	15		65		3
	16		66	bestreiten – t – ung	
	17		67		
	18		68		
	19		69		
	20	besprechen – ung	70		
	21		71	besuch	
	22		72		
	23		73	besucher	
	24		74		
2	25		75		1
	26	besser	76		
	27	gebessert	77	betaetigen – t – ung	
	28	gebessert	78	beteiligen – ung	
	29		79	beteiligt	
	30	besserung	80	beteiligung	
	31		81		
	32	bestand	82		
	33	bestand	83	betonen – ung	
	34		84	betont	
6	35		85		5
	36		86	betrachten – t – ung	
	37	bestaetigen – t – ung	87		
	38		88		
	39		89	betrag	
	40		90	betraege	
	41	best – en	91	betragen	
	42		92	betraegt	
	43		93		
	44	bestehen – ung	94		
0	45	besteht	95		7
	46	bestehen – d	96	betreffs	
	47		97		
	48	bestellen – t – ung	98	46	
	49	45	99	betreffend	

In decoding change penultimate	0	1	2	3	4	5	6	7	8	9
To	4	7	2	6	0	8	3	9	5	1

134 (18470 page number)

(26) General Critique of the Weaknesses of 13040 and 18470

The preceding pages show how faults in the construction and use of 18470 and its encipherments led to the reading of messages in those codes. The steps in the process of decipherment are there described chronologically. We shall now retrace our steps and summarize the weak spots that were uncovered in the 13040 and 18470 systems and their use.

It would be easy to expand this list theoretically. Moreover, weaknesses undoubtedly exist in these codes that were never discovered in M. I. 8. We shall, however, confine this survey to shortcomings that were brought to light and put to use for purposes of decipherment. 13040, of course, was not deciphered in M. I. 8. Its method of construction is, however, so similar to that of 18470 that we shall consider the two systems together.

We shall first take up faults in construction or compilation, and under this head we shall include everything that enters into the production of the code book—the choice of the vocabulary, its arrangement, and the code groups.

The matter of choice of words for entry into the vocabulary may be disposed of very briefly. In general, the vocabularies appear to be adequate, and in any case such shortcomings as may exist did not essentially facilitate the work of decipherment.

With the code groups the case is only slightly different, if at all. Numeral code groups with a one-figure difference—the type employed in these codes—are in one way of assistance to the decipherer, since he is aware of all the code groups that are to be employed. In the case of five-letter code words with a two-letter difference, or even with a one-letter difference, words which would be called for by the construction table are occasionally skipped, and this adds somewhat to the cryptographer's troubles. The numeral code groups of these German codes could have been made more annoying if the compilers had skipped numbers here and there, and thus apparently increased the size of the code. In that case they would have had to change the system of assigning code groups to the onomasticon, but that would have entailed no great difficulty.

It is in the arrangement of the vocabulary that the compilers have sinned most grievously. As soon as the vocabulary is allowed to remain even partly in alphabetical order—that is to say, as soon as the numerical sequence of the code groups is allowed by the compiler even to some extent to parallel the alphabetical sequence of the words and phrases—the code is in danger. Exception may be made of the case of a code which is *invariably* used with an encipherment of such a character as completely to destroy the traces of the original alphabetical arrangement. These German codes, however, were not intended to be so used, and were not so used. The early identifications made in 18470 by analysis would have been made if the code had been entirely nonalphabetical; but they would not have led to further identifications of words in their alphabetical neighborhood. Any word identified in an even partially alphabetized code is a potential clue to the identification of other words alphabetically near them.

In these codes the alphabetization was quite insufficiently changed. In the case of 13040 the original alphabetical arrangement was split up four pages at a time—for the moment we will disregard the shuffling of the blocks-of-ten on each page. In other words, the entire vocabulary was split up into only 48 parts. Given 48 words, *provided one were in each of these parts*, and a fairly large number of messages, the cryptographer would be off to a running start. In 18470

the arrangement was somewhat different, and the compilers may have believed they were splitting up the vocabulary one page at a time—dividing it into 246 units; but the *systematic* separation of the pages diminished the advantage so gained (cf. pp. 21; 34 *ff*; 44; and note 19). New words were identified through noting their distance from other words already known (cf. p. 48), and the dictionary could be used to help in making new identifications (cf. p. 49*f*.). A real page by page split-up would at least have been a decided improvement; but when this was employed later in making 1777 and 12444 from 18470 it was too late.

This weakness of partial alphabetization was greatly increased by the insertion of the two numerals per page running in regular order parallel to the alphabetically arranged vocabulary. This fault is common to 13040 and 18470 (cf. pp. 5; 30 *ff*; 36*f*.), and the fixing of the meaning of a numeral group was a decided help to identifying words on the same page. A separate set of tables for the numerals—one for encoding and another for decoding, with code groups taken at random throughout the book—would have alleviated but not cured the weakness inherent in the existing arrangement.

Other minor weaknesses in construction remain to be mentioned. In 13040 all proper names are separated from the vocabulary proper. In 18470 place names are to some extent and personal names completely separated from the rest of the book. All the names in 13040 and the personal names in 18470 are thereby marked off to the eye by the high numbers of their code groups (cf. pp. 6, 17, 28, 59). The partial mixing-in of place names with the rest of the vocabulary in 18470 only slightly increased the difficulty of identifying code groups as names of places (cf. p. 28).

The systematic insertion of stops in 13040 (cf. p. 5), and of stops and certain particles in 18470 (cf. p. 58*f*.), does no possible good so far as guarding secrecy is concerned, and may do some positive harm in helping to fix the alphabetical position of the blocks in which they occur. In fact the periodic recurrence of the particles in 18470 might help to fix the alphabetical position not only of blocks but also of pages. In practice, however, in M. I. 8, this periodicity was not discovered in time to be of service in locating the alphabetical position of words. The same statement applies to the regular allocation of numerals to the fifth and tenth blocks alphabetically (cf. p. 34).

So much for faults in construction and their contribution to the decipherment of the codes. We proceed to discuss the effect of errors committed in using the codes.

Faults inherent in code construction can be overcome by skillful use of encipherment, but in the case of these codes no attempt was made to do this. A mere renumbering of pages such as produced 5950 from 13040, and 2310, 1777, and 12444 from 18470 (cf. pp. 8; 18 *ff*.), is entirely insufficient for the purpose, and doubly so when, as in this case, the basic code continues to be used along with the encipherment in the transmission of messages. In 1777 and 12444 we have at least a complete change in pagination; the fault is aggravated when, as in the case of 5950 and 2310, the page numbers are changed four pages at a time.

So, too, the simple table used in the encipherments of both 13040 and 18470 for changing the penultimate digits of the code groups (cf. pp. 8, 18) is inadequate. It will be recalled that the use of this table led to the uncovering of the 1777 and 12444 encipherments before any identifications in vocabulary had been made.

Of the other encipherments used in the case of 13040—the additive (cf. p. 8; 13*f*.) and the sliders (cf. p. 98 *ff*.)—the writer cannot speak with authority, since the fact of the existence of these devices was communicated by the British and only individual cases of their use were deciphered in M. I. 8.

Granted the method of encipherment, further mistakes were made in the use of the encipherments.

It was certainly poor practice to send the message (see p. 84) containing a discussion of the enciphering systems. This, however, was mild in comparison with sending the same telegram twice—once in the basic code, and once in the encipherment (cf. pp. 19, 86).

The occasional publication of a paraphrase of a code message, such as that noted above (p. 53) in connection with the announcement of an extended zone of submarine activity, is almost unavoidable, even though not unattended with danger to the code employed. Such a paraphrase should be skillfully made, and need not be so valuable to the decipherer as was the message referred to. The blunder is infinitely worse, however, and is entirely inexcusable, when the code text and the published clear-text agree exactly, as in the case of the war-bond message cited above (p. 51).

The worst instance of carelessness in code use with which the writer ever came into contact occurred in connection with 13040. That code was in any case too old for use in important communications. It was written in the old German orthography. Such a word as velociped occurred in the body of the vocabulary, but automobil is found in a supplement, and U-boot in a supplement to proper names! A code book is not like wine that improves with age; it resembles a wooden ship which tends to develop leaks.

The writer, during the war, was on one occasion requested by the State Department to read a 1,500-word message in 13040 which had been sent from Berlin to Ambassador Bernstorff in Washington and which was concerned with the interminable submarine controversy. When the task had been completed he was asked to compare his decipherment with a typed copy of a German text and to note any differences in the two. There were no differences—the two documents were identical in every word, in every letter, in every cross of a t and in every dot over an i. And what was the clear-text document? It was a memorandum handed by Bernstorff to the Secretary of State!

There was no American cryptographic bureau in existence at the time when that message had been sent. If there had been, the usefulness of 13040 would have vanished from that moment.

We may conclude with mention of a few lesser sins committed in the use of the codes. The use of one code for an introduction to a forwarded message in another, while possibly unavoidable, was none the less a practice which aided the decipherer by showing a break at the point where the change in code presented a difference in the appearance of the code groups. It may have been largely a matter of luck that this practice led to important results (cf. pp. 28, 30).

So, too, the numbering of messages by means of the code proper instead of by means of the Dreinummerheft helped, through the identification of numbers, to betray the sequence of the code pages (cf. p. 32). The writing of the message numbers in code at the ends of telegrams, helpful as it was to the decipherer (cf. p. 34), is possibly hardly to be called poor practice except where the repetition was preceded by the word Nummer. The general carelessness exhibited in the use of that word has been referred to above (p. 27, note 12).

Another minor fault not unattended by consequences was the use of the Dreinummerheft in the body of messages instead of at the beginning only (cf. the note just referred to).

(27) Specimen Messages in 18470, 1777, and 12444

(1) The following telegram (18470 messages, pp. 698–705, 707–713, 714–720, and 726–729), sent in several parts from Madrid to Berlin, and dated September 11, 1918, has been referred to above (pp. 32, 40). Some garbled groups are restored in parentheses.

731 Nr. 12
740 22
582 vom 11 Sept. [1918]
18472
12770 Memorandum
12762 stop
18564 In
23672 Beantwortung
13622 Begleitschreibens
18185 von dem
9841 koeniglichen
7047 spanischen Botschafter
6831 an den
20528 Herrn
21499 Staatssekretaer
13630 des
32337
22337 Auswaertigen Amtes
3250 am
10488 14ten
21891 vorigen Monats
9578 uebergebenen
12770 Memorandums
26388 beeilt
30137 sich
19372 kaiserliche Regierung
27595 Folgendes
30723 zu
38875
(28875) erwidern
24461 stop
28922 Die
19372 kaiserliche Regierung
24780 hat
29465 keine
19121 Gelegenheit
16866 versaeumt
9170 um
10207 darauf
24610 hinzuweisen
8505 dass sie
24033 nicht nur
15665 gegenwaertig
18670 in den
13426 besser
2542
(3542) superlative
13008 Beziehungen
10054 mit
7043 Spanien
13123 zu
11069 leben
14555 wuenscht
28198 sondern dass
30140 sie
8412 auch
25335 hofft
29672 nach dem
14179 Krieg
18654 in
25779 enger
30711 Freundschaft
10051 mit
7043 Spanien
19908 zusammen (leben?)
12563 zu
9885 koennen
13983 und
8505 dass sie
7043 Spaniens
7555 Macht
13983 und
11510 Groesse
18655 in
13644 beiderseitigem
18908 Interesse
10133 und
15320 im Gegensatze zu
11601 der
8016 Politik
6881 anderer
7498 Laender
10058 mit allen
10043 Mitteln
29513 zu
27213 foerdern
13209 bereit
15769 ist
11451 stop
15162 Die
19372 kaiserliche Regierung
25760 empfindet
28816 es
10230 daher
9437 schmerzhaft
8535
(8545) dass
9841 koenigliche
7064 spanische Regierung
18654 in
16793 Vernachlaessigung
30916 dieser
11683 guten
7251 Absicht
1901 an der
14248 willkuerlichen
26194 Schaedigung
6045
(7045) spanischer
18908 Interessen
30511 durch
1142 Deutschland
13123 zu
18716 glauben
9062 scheint
23851 stop
17702 Die
4786 Ankuendigung
3211 der
9841 koeniglichen
7064 spanischen Regierung
8505 dass sie
27166 fuer
15470 jeden
30511 durch
1186 deutsche
14733 Unterseeboote
17810 verursachten
16741 Verlust
1988 an
7045 spanischen
9728 Schiffen
23890 comma
17021 der
18130 vom
20301 Augenblick
3211 der
9574 Uebergabe
9230 des
12770 Memorandums
25507 erfolgen
28155 sollte
22600 comma
24532 entsprechenden
1186 deutschen
9736 Schiffs
23352 raum
18652
or
18654 in
13441 Besitz
23962 nehmen
14598 wuerde
12270 comma
6673
(7673) liess
11989
(11089) legitim
30910 diese
4851
(4871) Annahme
13123 zu
22392 stop
1912 Die
19372 kaiserliche Regierung
23355
(23655) bedauert
11042 lebhaft
11870 wenn
13200 berechtigte
6045
(7045) spanische
18908 Interessen
30516 durch die

10221	dem
1146	deutschen Reich
18149	von seinem
27639	Feinde
8499	auf
18562	gezwungen
30278	e
8388	Art
3211	der
14154	Kriegsfuehrung
27354	gedraengt
11849	werden
16373	und
21356	steht
9470	nicht
1920	an
7230	comma
25652	erneuert
20352	ausdruecklich
30320	festzustellen
8549	dass
1142	Deutschland
24033	nicht nur
15418	jede
7250	Absicht
2211	
(3211)	der
26194	Schaedigung
6045	
(7045)	spanischer
11069	Lebens
18908	interessen
30331	fern
7647	liegt
11010	comma
28198	sondern dass
28816	es
8412	auch
30368	fest
24520	entschlossen
15780	ist
3139	alle
13989	Massnahmen
29513	zu
22876	treffen
30000	comma
29923	und
9592	
(9593)	zu
15472	jeder
17956	Verstaendigung
21902	die
25217	Hand
24753	zu
13010	bieten
30511	durch
12177	welche
30910	diese
18908	Interessen
19425	geschuetzt
22963	und
17213	
(27213)	foerdern
2422	Past Participle
11348	
(11848)	werden
21037	soweit
30968	dies
19044	irgendwie
10018	mit der
24876	heiligen
10881	Pflicht
23281	der
26996	Reichsverwaltung (?)
21968	vereinbar
15769	ist
15762	den
1142	Deutschland
8499	auf
18562	gezwungenen
29248	Existenz
28256	kampf
16402	zum
15212	gluecklichen
25722	Ende
25703	zu
30834	fuehren
17162	
(27162)	stop
27112	Fuer die
31711	Freundschafts
15967	gesinnungen
1142	Deutschlands
13010	bietet
9371	schon
17702	die
18407	Vergangenheit
19838	zahlreiche
13154	Beispiele
13211	stop
13232	Bereits
18190	vor
18555	zwei
15718	Jahren
25725	
(24725)	hat sich
15162	die
19372	kaiserliche Regierung
20018	zur
9695	Ueberlassung
1186	deutscher
18654	in
6055	
(7455)	spanischen
15181	Haefen
7648	liegender
9728	Schiffe
13209	bereit
25582	erklaert
25471	stop
30115	Sie
26221	bot
30333	ferner
7043	Spanien
26722	die
7643	Lieferungen
1186	deutscher
8698	Kohlen
12451	stop
28119	sogar
18654	in
6196	hollaendischen
17230	oder
4083	daenischen
15181	Haefen
1920	an
4861	stop
8517	Dass (die)
9841	koenigliche
7064	spanische Regierung
8461	
(8401)	auf
13619	beide
30711	freundschaftlichen
6856	Angebote
8430	auch nicht
29385	eingehen
2470	Past Tense
17230	oder
7880	nicht
29385	eingehen
9805	konnte
15721	ist nicht
1142	Deutschlands
9236	Schuld
22621	stop
9190	Umso
9611	ueberraschend
24514	er
15789	ist es
27111	fuer die
19372	kaiserliche Regierung
11874	wenn
15447	jetzt
12952	die
9846	koenigliche Regierung
29527	
(12952)	die
2501	
(7250)	Absicht
3169	
(13169)	bekundet
30910	diese
18764	gleichen

1186 deutschen
9728 Schiffe
17702 die
11499 ihr
19705 seinerzeit
20399 aus
30734 freien
21652 Stuecken
1938 angeboten
15631
(14631) waren
17139 nunmehr
16040 gewaltsam
18654 in
13441 Besitz
8553 zu
23962 nehmen
17193 und
17540 ohne
28915 Einwilligung
1142 Deutschlands
18654 in
30987 Dienst
25703 zu
21265 stellen
21342 stop
1542?
(15320) Im Gegensatz zu
22699 seinen
15692 Gegnern
27074 die
10574 den
24084 Neutralen
12049 unter
11496 ihnen
8414 auch
7043 Spanien
24033 nicht nur
15470 jeden
16729 Verkehr
10054 mit
1142 Deutschland
4675 Oesterreich
30491 der
6248 Tuerkei
13983 und
5589 Bulgarien
16832 versagen
28197 sondern auch
21752 speziellen
25231 Handel
10055 mit
6849 anderen
24084 neutralen
9498
(7498) Laendern
1500 [
14916 wie
6194 Holland
4082 Daenemark
6666 Norwegen
13983 und
4227 Schweden
1509]
13515 beschraenken
17230 oder
19271 ganz
20855 verbieten
24780 hat
1142 Deutschland
25211 dem
7045 spanischen
25231 Handel
21037 soweit
24515 er
28913 das
21723 Sperr
19236 gebiet
14071 meidet
8703 das
10592 denkbar
11695 groesste
25421 Entgegenkommen
13381 bewiesen
13211 stop
27305
(27205) Fortsetzung folgt
18470
3239 Erste
27206 Fortsetzung von
6705 12
22417 22
29830 So
14593 wurde
11841 der
18811 gesamte
7045 spanische
29318 Einfuhr
25231 handel
20338 aus
24083 neutralen
17193 und
19743 selbst
20338 aus
27610 feindlichen
7398 Laendern
12952 die
29400 nicht
18775
(18675) in der
21723 Sperr
16413 zone
7645 liegen
1147 deutscherseits
29451 keiner
13517 Beschraenkung
14778 unterworfen
18745 gleichwohl
24514 er
18654 in
23564 Bann
14645 waren
14915 wie
10897 Petroleum
23373 und
23614 Baumwolle
13405 besteht
21037 soweit
17144 nur
26722 die
14646 Waren
27169 fuer
7045 spanischen
26020 nationalen
21909 Verbrauch
12411 und nicht
20028 zur
14295 Wieder
20320 ausfuhr
1920 an
1142 Deutschlands
27639 Feinde
13489 bestimmt
30199 sind
22621 stop
30202 Ebenso
14594 wurde
11841 der
7045 spanische
20320 Ausfuhr
25231 handel
29672 nach dem
24084 neutralen
20485 Auslande
16723 verhaeltnismaessig
30771 freigeben
2420 Past participle
23373 und
10289 darueber
24941 hinaus
11439 ihm
28119 sogar
29644 nach
27610 feindlichen
7498 Laendern
14916 wie
20093 zum Beispiel
12532
(12533) den
5370 Vereinigten Staaten
18139 von
6609 Nord Amerika
19838 zahlreiche
17382
(16382) Zugestaendnisse
7510 gemacht
13983 und

30510 durch
19129 Geleitsbrief
1678 Accusative Plural
30121 sichern
2420 Past Participle
3620 stop
20345 Aus der
19831 Zahl
11841 der
29833 so
18139 von
1142 Deutschland
20082 zur
20320 Ausfuhr
1908 an seine
15692 Gegner
30771 freigeben
2407 Past Participle
7045 spanischen
20320 Ausfuhr
14646 waren
22616 seien
24922 hier
17144 nur
30828 Fruechte
12136 Wein
12677 Kork
13983 und
17597 Oliven
24337 erwaehnt
25471 stop
28922 Die
30770 Freigabe
12117 weiterer
27168 fuer
7045 spanisches
12521 wirtschaftliches
11069 Leben
14920 wichtiger
20320 Ausfuhr
8373 artikel
14594 wurde
1147 deutscherseits
1938 angeboten
6782 stop
23671 Der
7045 spanische
30827 Frucht
25231 handel
14594 wurde
22351 ausserdem
18139 von
1142 Deutschland
25981 noch
13492 besonders
13695 beguenstigt
30511 durch
30770 Freigabe

90481—37——6

30491 der
15181 Haefen
18138 von
4137 franzoesisch
1792 Marokko
21038 sowie
21090 des
15180 Hafens
18137 von
22214 Cette
12176 welch
7723 letzterer
8414 auch
27111 fuer die
17906 Versorgung
20831 der
7367 Schweiz
10055 mit
7045 spanischen
14646 waren
30982 dient
8261 stop
17299 Obwohl
26722 die
7064 spanische Regierung
18138 von
1142 Deutschlands
27639 Feinden
27553 das
30246 Durchlassen
7045 spanischer
14646 Waren
29646 nach
1142 Deutschland
11240 nicht
29513 zu
25668 erreichen
16852 vermochte
24725 hat sich
15162 die
19372 kaiserliche Regierung
6875 angesichts
27481 dringender
26485
(26385) Beduerfnisse
7043 Spaniens
28119 sogar
13209 bereit
30476 gefunden
27572 die
20320 Ausfuhr
16019 gewisser
1186 deutscher
8103 Produkte
14915 wie
16346 Zucker
25880 rue
13293 ben

23854 samen
12555 Wirk
28324 nadeln
20501 Chemikalien
30513 und
8378 Arznei
10042 mittel
29644 nach
7043 Spanien
8553 zu
15924 gestatten
17540 ohne
14532
(24532) entsprechende
15521 Gegenleistungen
1678 Accusative Plural
13123 zu
16733 verlangen
14732 stop
11874 Wenn
18591
(19591) trotz
30918 dieses
27025 deutlichen
13433 Bestreben
24145 s
19373 kaiserlicher Regierung
13200 berechtigte
7045 spanische
18908 Interessen [sc. zu]
30122 sichern
26176 Schaden
10247 das heisst
15844 insbesondere
15861 der
17741
(16741) Verlust
17045
(7045) spanischer
9728 Schiffe
23373 und
10811 Personen
26176 schaden
28930 eingetreten
15769 ist
29831 so
23655 bedauert
30966 dies
19373 kaiserliche Regierung
11042 lebhaft
10133 und
22491 aufrichtig
20451 stop
30966 Dies
19177 gilt
13492 besonders
8413 auch
2711

(27111?) fuer die [Omission?]
18686 indem
24661 ein
30661 diplomatischer
17886 Vertreter
20831 der
9846 koeniglichen Regierung
18655 in
15558 Gefahr
18867 geraten
15769 ist
18912 die
30516 durch
30089 technische
11936 Unmoeglichkeit
14840 einer(?)
20102
(30102) sicheren(?)
13296 Benachrichtigung
20271 der
14731 Unterseeboots
8667 kommandeure
15867 innerhalb
28563 kleinsten
20125 Zeitraums
18137 von
11886 wenigen
29916 Tagen
7779 leider
29400 nicht
4309 abwenden
2420 Past Participle
11849 werden
9805 konnte
15421 stop
19373 Kaiserliche Regierung
24725 hat sich
21242 stets
13208
(13209) bereit
25582 erklaert
9540 ueber
15470 jeden
28958 einzelnen
28732 Fall
30491 der
17920 Versenkung
17231 oder
13554 Beschaedigung
7045 spanischer
9728 Schiffe
24133 zu
18022 verhandeln
12040 stop
30142 Sie
24781 hat
18661 in naechsten
28734 Faellen
14917 wie
20092 zum Beispiel
18863 gerade
18116 vor kurzem
27111 fuer die
7045 spanischen
9728 Schiffe
1540 quotation mark

[Here there is evidently an omission in the intercepted text, which then continues]

18472
3258 Zweite
27206 Fortsetzung von
6705 12
22417 22
22392 stop
11873 Wenn
29673 nach den
30308 Feststellungen
1670 Dative Plural
11601 der
9841 koeniglichen
7064 spanischen Regierung
10395 20
7823 Prozent
10850 des
7045 spanischen
9736 Schiffs
23352 raums
16773 verloren
15606 gegangen
30199 sind
29830 so
25601 erlaubt
30137 sich
19372 kaiserliche Regierung
10207 darauf
24610 hin[zu]weisen
8501 dass in
30914 diesem
16741 Verlust
14322 die
11566 grosse
19831 Zahl
7045 spanischer
9728 Schiffe
28632 einbegriffen
22620 sei
13302
(17702?) die
30510 durch
8853 Minen
11347
(12347) unbekannten
20703 Ursprungs
16840 vernichtet
14535 wurden
17231 oder
0732
(8732) die
15312 im
30987 Dienst
29021 der
15692 Gegner
1142 Deutschlands
12411 und nicht
7043 Spaniens
30134 sich
20425 ausschliesslich
10012 mit dem
25232 Handel
10055 mit
23564 Bann
14645 waren
26339 befassen
2471 Past Tense
3620 stop
19372 Kaiserliche Regierung
23635 bedauert
11042 lebhaft
11879 wenn der
12870 Mangel
1920 an
9736 Schiffs
23352 raum
18654 in
7043 Spanien
11772 einen
25655 ernsten
14415 Umfang
4877 angenommen
24780 hat
25050 stop
30144 Sie
28293 kann
15478 jedoch
29400 nicht
16352 zugeben
8517 dass
9326 Schuld
24900 hierfuer
20425 ausschliesslich
17230 oder
8419 auch
18663 in naechster Linie
15762 den
13200 berechtigten
1186 deutschen
14179 Kriegs
13989 massnahmen
18298 zuschreiben
2420 Past Participle
12539 wird
20691 stop
20831 Der

9841 koeniglichen
7064 spanischen Regierung
28293 kann
28818 es
25630 nicht
12347 unbekannt
22684 sein
8549 dass
19838 zahlreiche
7045 spanische
9728 Schiffe
18661 in naechsten
28734 Faellen
30491 der
18811 gesamte
13462 Bestand
16019 gewisser
17146 nur dem
26035 Namen
19644
(29644) nach
7045 spanischer
9729 Schiffs
15941 gesellschaften
15311 im
20425 ausschliesslichen
18908 Interesse
15861 der
15692 Gegner
1142 Deutschlands
28797 fahren
29251 stop
16019 Gewisse
23008 Reederei
25749 en
30199 sind
13133 bekanntlich
28199 sogar
21037 soweit
15606 gegangen
30136 sich
17300 Requisition
15357 ihrer
9728 Schiffe
30516 durch
7064 spanische Regierung
13123 zu
24570 entziehen
16199 indem sie
30134 sich
12121 weigern
2470 Past Tense
30792 den
10389 Aufenthalts
26874 ort
15357 ihrer
9728 Schiffe
6854 anzugeben
4861 stop
1911
(1912) Die
7064 spanische Regierung
12528 weiss
3020
(30202) ebenso
25849
(8549) dass
19838 zahlreiche
7045 spanische
27111 fuer die
26088 nationalen
18908 Interessen
27481 dringend
13245 benoetigten
9728 Schiffe
18139 von
1142 Deutschlands
15692 Gegnern
24753 zu
18277 Zwecken
28785 Fahrt
25745 en
18564 zwischen
25733 Entente
7498 laendern
10672 pressen
2422 Past Participle
11849 wurden
3682 stop
3014
(30142) Sie
-2150
(12528) weiss
8412 auch
7546
(8546) dass
19743 selbst
7045 spanische
12978 Kuesten
9728 schiffe
15319
(15312) im
-8908
(18908) Interesse
14681 der
25733 Entente
28897
(28797) fahren
28722 stop
19595 Trotzdem
9807 koennte
18903 das
12770 Memorandum
13831 der
9841 koeniglichen
7064 spanischen Regierung
29830 so
17954 verstanden
11848 werden
3209 als ob
30142 sie
30734 freie
28785 Fahrt
27165 fuer
3139 alle
9728 Schiffe
7045 spanischer
30481 Flagge
26589
(27589) fordern
12284 wolle
10247 das heisst
19743 selbst
27166 fuer
28146 solche
28122 die
14195 Kriegsmaterial
20027 zur
19614 toetlich
1658 delete 4 letters
14360 ung
1186 deutscher
28100 Soldaten
30834 fuehren
17230 oder
30135 sich
19251 gar
12055 unter dem
19421 Schutze
27610 feindlicher
14183 Kriegsschiffe
26357 begeben
15118 haben
16031 stop
28676 Ein
28182 solcher
3279 allgemeiner
30734 Frei
23792 brief
25161
(27161) fuer
23564 Bann
14645 waren
15768 ist
13065 bisher
25981 noch
18139 von
29451 keiner
7555 Macht
13831 der
12109 Welt
22382 ausgestellt
12295 worden
3681 stop

3139 Alle
4793 zu
26321 Beginn
30918 dieses
14179 Krieges
18654 in
12602 Kraft
26372 befindlichen
14179 Kriegs
23038 regeln
15118 haben
16945 vielmehr
21902 die
24564
(23564) Bann
1464
(14645) waren
18001 dem
16763 Zu
11595 griff (?)
27210 des
13297 benachteiligten
14152 Kriegsfuehrenden
20352 ausdruecklich
30771 freigeben
2422 Past Participle
28722 stop
13682 Bei
24036
(20036) Zurschaustellung
30724 fremder
15048 Hoheits
20107
(20106) zeichen
30510 durch
1142 Deutschlands
27639 Feinde
14598 wuerde
14962 die
16077 Gewaehrung
30734 freier
28785 Fahrt
27166 fuer
24083 neutrale
9728 Schiffe
18670 in den
18139 von
1142 Deutschland
9178 um die
19237 Gebiete
22660 seiner
4159 europaeischen
27639 Feinde
22963 und
29320 einige
13449 Besitzungen
16272 gezogene
21723 Sperr
16413 zone
1672 Dative Plural
22351 ausserdem
8580 dazu
40834
(30834) fuehren
8586
(8546) dass
18655 in
11496 ihnen
3281 alsbald
17161 nur
9728 Schiffe
10054 mit
24083 neutraler
30481 Flagge
6779 antreffen
2421 Past Participle
14539 wuerden
12291 stop
18475
9496 Schluss
18138 von
30020 Telegramm Nr.
6705 12
22417 22
6782 stop
18659 In der
37481
(27481) dringenden
9736 Schiffs
23352 raums
7691
(17690) not
7043 Spanien
1667 Genitive Singular
15766 ist
1..42
(1142) Deutschland
..119
(28119) sogar
13209 bereit
27161 fuer
24753 zu
11914 Unrecht
17920 versenk
30083 te
7045 spanische
9728 Schiffe
15571 Gegen
25617 ersatz
18655 in
2627
(22747?) Tonnengehalts
4422
(10422) aequivalent
4793 zu
7713 leisten
10247 das heisst
1186 deutsche
8728
(9728) Schiffe
24532 entsprechenden
23352 Raum
15607 gehalts
1979
(1989) an
7043 Spanien
4357 abtreten
2712 Infinitive with zu
3620 stop
20090 Zum
13309
(13308) Beweis
27111 fuer die
22491 Aufrichtigkeit
30918 dieses
6856 Angebots
25582 erklaert
30137 sich
19372 kaiserliche Regierung
24904 hiermit
21776 spontan
13209 bereit
6711 anstatt
27169 fuer
7045 spanischen
10275 Dampfer
3383
(23843) Sar
30942 din
25680 ero
1312
(13232) bereits
13093 billigen
3408
(2408) Past Participle
19183 Geldersatzes
7043 Spanien
15671 ein
1186 deutsches
9727 Schiff
24133 zu
9695 ueberlassen
9162 stop
15575 Gegen
18188 von der
7064 spanischen Regierung
18654 in
24331 Erwaegung
16272 gezogene
7250 Absicht
19746 selbstaendig
20027 zur
13443 Besitzergreifung
10353 eines

1186 deutschen
9727 Schiffs
21703 zu
9364 schreiten
12265 womoeglich
8412 auch
18655 in
28180 solchen
28741 Faellen
18673 in denen
24661 ein
7045 spanisches
9727 Schiff
15867 innerhalb
19050 des
31723
(21723) Sperr
19236 gebiets
17920 versenkt
12296 worden
11086 legt
15478 jedoch
19373
or
19372 kaiserliche Regierung
24904 hiermit
20352 ausdruecklich
17831 Verwahren
12461 ein
12463 und
13725 bittet
22522 die
9841 koenigliche
17064
(7064) spanische Regierung
30137 sich
2555
(25654) ernste
27591 Folgen
24373 eines
28180 solchen
9294 Tuns
18190 vor

2300
(20300) Augen
13123 zu
25256 halten
18652
(18672) stop
19373 Kaiserliche Regierung
25335 hofft
8517 dass
9841 koenigliche
7064 spanische Regierung
3281 alsbald
10018 mit der
1145 deutschen Regierung
18654 in
18024 Verhandlungen
8547
(9547) ueber diese
29923 und
2913
(12913) kuenftige
12117 weitere
21902 die
7045 spanischen
18908 Interessen
3256 am naechsten
13526 beruecksichtigen
2438 Present Participle
7966
(7866) Punkte
28978 eintreten
29103 und
30516 durch
14450 umgehende
18188 von der
19372 kaiserlichen Regierung
19790 seit
11399 laengerer Zeit
24443 erbetene
24528 Ersendung
27343
(29343) eines
7045 spanischen

12853 Marine
24124 sachverstaendigen
29645 nach
6024 Berlin
23752 einen
30711 freundschaftlichen
20468 Ausgleich
13592 beschleunigen
12536 wird
20691 stop
21902 Die
22708
(25708) enge
1186 deutsch
7045 spanische
30711 Freundschaft
13010 bietet
26382 die
16072 Gewaehren
1651 delete two letters
10214 dazu
8574
(8575) dass ein
13619 beide
30093 Teile
26301 befriedigendes
25534 Ergebnis
29021 der
18024 Verhandlungen
12480 nicht
20396 ausbleiben
12535 wird
22132 stop
2191 San Sebastian
29563 den
4848 10ten
27892 September
10326 19
8467 18
9496 Schluss

(Signed) RATIBOR

(2) The following message (18470 messages, p. 949), sent from the Foreign Office in Berlin to the German Ambassador in Spain, presents a decided contrast in contents to the message just quoted.

379	Nr. 16
032	30
258	vom 16 Nov [1918]
18478	
13788	Bitte
27377	dortiger Regierung
10025	mitteilen
8549	dass
3129	
(3139)	alle
29093	Einschraenkungen
10374	aufgehoben
20195	
(30195)	sind
3690	comma
12177	welche
18180	von
11995	uns
8230	dem
25263	Handelsverkehr
24083	neutraler
9728	Schiffe
10051	mit
11981	unseren
27639	Feinden
22634	sei
28818	es
30510	durch
27076	die
1145	deutsche Regierung
19743	selbst
3694	comma
22635	sei
28815	es
30510	durch
1186	deutsche
10694	Privat
12014	unternehmen
3692	comma
22634	sei
28818	es
15572	gegen
13489	bestimmte
8972	Konzessionen
14917	wie
27076	die
10551	der
20230	
(20320)	Ausfuhr
18180	von
9737	Schiffbau
13918	material (ien)
3690	comma
17230	oder
25054	nicht
3692	comma
10320	auferlegt
14646	waren
3622	stop
30910	Diese
8730	Mitteilung
25508	erfolgt
19142	gemaess
16520	Ziffer
23525	32
10567	des
22162	Waffenstillstands
17878	vertrags
3622	stop

(Signed) SOLF

(3) This message (from 1777 messages, p. 226, *ff.*), with its rather unusual subject matter, figured, in 1931, in claims for damages brought against Germany before the Mixed Claims Commission on the charge of infecting horses purchased by the Allies. It was sent from Madrid to Berlin. The first column contains the 1777 code groups, the second the 18470 equivalents. Restorations of garbled groups are enclosed in parentheses.

424	Nr. 11	
157	23	
835	vom 19ten Aug. [1918]	
45458	73458	Doenhoff
14437		
(11437)	9627	uebersendet
1282	2472	past tense
22223	22413	Aufzeichnungen
2987	1677	Acc. Plural
12020	10210	des
4723	30613	Direktors
7786	26476	Bakteriologischen
15606		
(15607)	18947	Instituts
27064	18654	in
8491	5581	Buenos Aires
5716	27306	Doktor
50297		Krause
2961	1651	delete one letter
4939	9529	ueber
9623	18013	Verhuetungsmittel
19541	20831	der
5832		
(5823)	27813	Serum
26136		
(26164)	12654	krankheit
14520	30510	durch
19927	25617	Ersatz
27699	17289	oder
28160	16750	Vermischung
9670	18060	des
1411	10801	Pferde
5823	27813	serum
2605	24145	s
28966	10056	mit
1817	17707	Rinder
5823	27813	serum
10152	26992	stop
50297		Krause
2961	1651	delete one letter
26844	10134	kommt
22333	11323	zu

30254	27594	folgenden
6150	10790	praktisch
19468	24358	erwiesenen
1016	9406	Schlussfolgerung
2982	1672	Dat. Plural
24667	3657	stop
20349	3239	Erstens
18213	1903	Das
25897	18587	zweimal
8559	8499	auf
9826	23716	56
1252		
(1352)	1592	dash
9826	23716	56
13108		
(12108)	15248	Grad
1312	1502	dash
14212	28602	eine
16982	25272	halbe
12654	21694	Stunde
1317	1507	dash
9780	25570	erhitzen
1238	2428	Past Participle
1817	17707	Rinder
5823	27813	serum
28020	17810	verursacht
29903	19743	selbst
27080	18670	in den
3755	11695	groessten
10887	12777	Mengen
27063	18653	in
6812	15402	ji
25347	16537	ziert
20292	27682	fast
6675	29465	keine
5823	27813	Serum
26164	12654	krankheit
1312	1502	dash
6196	10786	300
29621	8811	Milzbrand
21604		
(21044)	28734	faelle
16600	29240	comma
2556	13196	40
4961	9551	Typhus
21044	28734	faelle
1318	1508	dash
24638	3628	stop
20368	3258	Zweitens
18213	1903	Das
21449	18139	von
1817	17707	Rindern
29226	16016	gewonnene
4755	30695	Diphtheri
30988		
(20988)	30278	e
24628	3618	hyphen
22733	29923	und
8086	27976	Tet
30432	4422	a
6473	17163	nus
5823	27813	serum
15832	28822	erzeugt
4269	13659	bei
4755	30695	Diphtheri
20988	30278	e
9853	23793	und
8486		
(8086)	27976	Tet
30432	4422	a
6473	17163	nus
12020	10210	des
10889	12779	Menschen
20292	27682	fast
6675	29465	keine
5823	27813	Serum
26164	12654	krankheit
24872	8962	stop
18237	1927	Drittens
4267	13657	Bei
21427	18117	Vor
10552	15892	injektion
21490	18180	von
4755	30695	Diphtheri
20988	30278	e
24622	3612	hyphen
1817	17707	Rinder
5823	27813	serum
27153	28293	kann
23051	12891	man
11124	28314	nachher
6096	21186	sub
23346	13836	ku
22731	29921	tan
4755	30695	Diphtheri
20988	30278	e
24621	3611	hyphen
1411	10801	Pferde
5823	27813	serum
17063		
(27063)	18653	in
6812	15402	ji
25344	16534	zieren
14600	17540	ohne
24568		
(29568)	15558	Gefahr
13133	30723	zu
19760	11050	laufen
5823	27813	Serum
26164	12654	krankheit
22333	11323	zu
15832	28822	erzeugen
16661	29251	stop
4266	13656	Bei
9061	14451	umgekehrter
6212	10402	Anwendung

5960	22850	tritt
26942	9532	die
5823	27813	Serum
26164	12654	krankheit
8557	8497	auf
11352	22392	stop
18256	1996	Viertens
18222	1912	Die
25460		
(28160)	16750	Vermischung
20367	3257	2
1358	1598	dash (fraction)
18236	1926	3
1817	17707	Rinder
24622	3612	dash
20348	3238	1
1340	1530	dash (fraction)
18186		
(18236)	1926	3
1411	10801	Pferde
5823	27813	serum
1310	1500	bracket
20367	3257	2
1358	1598	dash (fraction)
18236	1926	3
1817	17707	Rinder
24622	3612	dash
20348	3238	1
1359	1599	dash (fraction)
18236	1926	3
1411	10801	Pferde
5823	27813	serum
1319	1509	bracket
24651	3691	comma
26484	12574	wobei
19302	21242	stets
26975		
(26973)	9563	das
9616	18006	Verhaeltnis
29444	16334	zu Gunsten
13990	14280	des
1817	17707	Rinder
5823	27813	serums
25634	22124	wahren
1234	2424	Past Participle
2574		
(5275)	11865	werden muss
9300	20640	comma
15832	28822	erzeugt
20910	30200	ebenso
6675	29465	keine
5823	27813	Serum
26164	12654	krankheit
24872	8962	stop
18519	6809	Fuenftens
1817	17707	Rinder
30308	19248	geben
20914	30204	ebenso wie
13223	28913	das
1411	10801	Pferd
15100	21040	sowohl
4751		
(4755)	30695	Diphtheri
20988	30278	e
24628	3618	dash
20326	3216	als
8524	8414	auch
8086	27976	Tet
30432	4422	a
6473	17163	nus
5823	27813	serum
24612	3602	stop
2156	6796	11
9976	20366	23

(Signed) RATIBOR

(4) This telegram (1777 messages, p. 177) was sent from Berlin to Madrid on July 6, 1918. Mirbach was the German Ambassador to Russia.

The first column contains the 1777 message, the second the transposition into 18470. One garbled group has been restored.

692		Nr. 9
288		08
433		vom 6ten Juli
1777		
24790	15680	Geheim
21372	27162	stop
14520	30510	Durch
19795	11085	Legationssekretaer
22336	11326	Lange (?)
28281	24571	entziffern
9712	25502	stop
30626	18816	Gesandtschaft
7033	3723	Moskau
14922	27412	drahtet
18588	6878	6ten
13077	4767	7ten
24668	3658	stop
24190		
(34190)	42190	Mirbach
3822	28112	soeben
9591	19481	einem
8506	8446	Attentat
27064	18654	in
30626	18816	Gesandtschafts
30307	19247	gebaeude
24250	20090	zum
22635	26825	Opfer
29574	15564	gefallen

5391	30881	stop
26268	19658	Tod
14520	30510	durch
29083	17073	Revolver
9553	19493	schuss
27064	18654	in
11131	28321	Nacken
6453	17193	und
23850	26290	Bomben
6387	14577	wurf
17545	11935	unmittelbar
13240	28930	eingetreten
24617	3607	stop
24106	29646	Nach
23527	12117	weiterer
11172	28362	Nachricht
17772	9062	scheint
15868	28858	es sich
8280	9170	um
18128	7518	Mache
28971	10061	der
14743	25733	Entente
14713	25703	zu
16942	25232	handeln
10921	24811	stop
11172	28362	Nachricht
26447	12537	wird
2332	24922	hier
18044	28434	morgen
25703	16843	veroeffentlicht
17933	20923	und
27064	18654	in
17975	20965	vorstehendem
24460	29850	Sinne
26852	10192	kommentiert
30098	4888	9
14397	3187	08

(Signed) BUSSCHE

(5) This message from 12444 messages, p. 32, which was sent from Berlin to Madrid, dated December 23, 1918, and intercepted December 24, probably repeats information telegraphed from Brest Litowsk to Berlin on December 21, since the present message refers to December 22 as still in the future.

The first column contains the 12444 code groups, the second the 18470 equivalents. One garbled code group is restored in parentheses.

12444		
555		Nr. 14
778		50
457		vom 23sten Dez.
23220	21410	Stab
28067	10057	mit
10350	22690	seiner
29741	13631	Begleitung
30979	15769	ist
16469	22459	21sten
1354	4494	abends
18682	5572	Brest
17894	2584	Litowsk
22885	28975	eingetroffen
25011	23401	stop
16428	22418	22sten
7827	20917	vormittags
29418	25508	erfolgt
7987	20077	zunaechst
29908	22348	Aussprache
28025	10015	mit den
14059	21999	Verbuendeten
10410	29600	comma
30019	28309	nachmittags
19666	18156	voraussichtlich
26703	24343	erste
15326		
(15426)	16616	Voll
23080	29870	sitzung
28025	10015	mit den
12992	3082	russischen
2746	14936	Widersachern (?)
22597	10487	14
27178	13068	50

(Signed) BUSSCHE

(6) The following telegram, sent from Berlin to Madrid under date of December 23, 1917, is taken from 12444 messages, page 33, *ff*. A transcription into 18470 is here appended in the second column.

In the text of the message the last two groups are meaningless and are probably a dittography of the same two groups appearing about the middle of the message. At the group 23260, the twelfth group from the end, the encoder suffered a lapse: his copy undoubtedly read "statt", but he looked up and encoded the similarly sounding but here perfectly meaningless word "staat". This might be called a mental garble.

The telegram is extremely interesting from the light that it sheds on the history of the various codes in the 18470 series. We are definitely informed, apropos of the trouble that Berlin was experiencing in the decoding of certain messages sent from Madrid, (1) that 1777 was the fifth variation of code 2310; (2) that 12444 was the sixth variation of the same code; (3) that 1777 was composed in Berlin according to proposals sent in a telegram from Madrid; finally (4) that these proposals had been sent on October 31.

It would be most interesting to read just what proposals were made in the Madrid message of October 31. Did they actually send a detailed table by wireless? If so, it is not to be wondered at that the table set up in Berlin failed to work. It is an everlasting pity that October 31 antedates the beginning of the A. E. F. interceptions, and curiosity concerning the contents of this message must remain ungratified.

Examination of the study below (p. 89 *ff.*) of "Additional Codes of the 18470 Family", based on certain material received by M. I. 8 from a "Dutchman", will show why Berlin refers to 1777 and 12444 as the fifth and sixth encipherments respectively of 2310. 2310 had been made by shuffling the pages of 18470 four pages at a time, and applying the customary table for the blocks-of-ten. It was no doubt—since the other derivatives are here called variations of 2310 (Abaenderungen des Chiffres 2310)—the first variant of 18470. The "Dutchman" describes codes 37000, 29000, 2500, and 20000, of which 29000 and 20000 have the same block-of-ten arrangement as 2310 and are accurately described as variants of that code. 2500 makes a second shift in the blocks-of-ten, applying the original table to the blocks of *2310*, so that 2500 also is accurately described as a variation of 2310. 37000, however, has the same block-of-ten arrangement as 18470 and cannot be called a variant of 2310. This gives us three derivatives of 2310 before the coming of 1777 and 12444.

One encipherment is missing. We might get out of the difficulty by assuming 2310 instead of 18470 to be the parent of all the others of the family; but objections to this view are given on pp. 90 *f.*; 96. Possibly another encipherment exists of which no trace has reached us.

555		Nr. 14	26395	22985	sechs
461		49	17474	10564	des
457		vom 23ten Dezember	27935	20525	Chiffres
550		unter Bezugnahme auf Telegramm	21876	20366	23
387		Nr. 26	20807	4847	10
845		73	9319	1509	bracket
387		Nr. 26	4550	3690	comma
082		76	7595	18585	zweite
400		und	2435	25225	Haelfte
387		Nr. 26	28066	10056	mit
499		77	19508	8448	17
12444			21239	27029	77
26703	24343	Erste	24342	19232	gegeben
2435	25225	Haelfte	24700	30840	comma
23831	30021	Telegramm Nr.	2512	30202	ebenso
3587	20477	26	23830	30020	Telegramm Nr.
20309	8249	73	3587	20477	26
30979	15769	ist	17476	10566	76
28065	10055	mit	3753	17193	und
27936	20526	Chiffre	3587	20477	26
28316	28706	124	21239	27029	77
25106	13546	44	4533	3623	stop
9310	1500	bracket	25320	30910	Diese
1300	4440	Abaenderung	23091	29881	sind
17187	6877	6	28022	10012	mit dem
9350	1590	dash	27935	20525	Chiffre

19508	8448	17
21239	27029	77
4553	3693	comma
2752	14992	wie er
7632	24922	hier
15925	10315	auf Grund
17460	10550	der
7830	20920	Vorschlaege
25286	27376	dortigen
23831	30021	Telegramms Nr.
21776	4766	7
22528	10418	13
19640	18130	vom
2957	23597	31ten
12573	17563	Oktober
28515	25005	hergestellt
30356	12296	worden
4552	3692	comma
21144	24034	nicht zu
25781	24571	entziffern
4533	3623	stop
6298	13788	Bitte
23832	30022	Telegramm Nr.
3587	20477	26
17476	10566	76
25993	13983	und
3587	20477	26
21239	27029	77
24381	19271	ganz
24700	30840	comma
23830	30020	Telegramm Nr.
3587	20477	26
20309	8249	73
19649	18139	von
9300	1540	quote
19209	11149	Lokal
3582	20472	ausschuss
2467	25257	haelt
19523	8413	auch
25378	30968	dies
26891	25981	noch
25875	27165	fuer
7847	20937	vorteilhaft
8640	3530	comparative
9304	1544	unquote
22430	1920	an
28066	10056	mit
13280	23970	neuem
27935	20525	Chiffre
28316	28706	124
25106	13546	44
20623	14213	wiederholen
23260	21450	staat (error for statt)
10484	29674	nach der
1300	4440	Abaenderung
17118	6808	5
9350	1590	dash
24764	30854	fuenf
17475	10565	des
27935	20525	Chiffres
21876	20366	23
20808		
(20807)	4847	10
28515	25005	hergestellt } These two groups have
30356	12296	worden } slipped in by error.

(Signed) BUSSCHE

(7) The following is a reproduction of one of the two messages that were found in two codes. (See p. 19.) This message was sent originally from Berlin to Madrid in 18470 under date of February 24, 1918 (18470 messages, pp. 138–139); it was then sent again in 12444 under date of March 4 (12444 messages, pp. 207–209). In the transcription given here the first of the three columns contains those groups that appear only in the 18470 version, the second column (the bulk of the message) contains the groups which are equivalent in the two versions, and the third column comprises the groups peculiar to the 12444 version.

The two versions correspond almost exactly. The original text of the two was identical except for the introductions. A word or two has dropped out here and there in both versions, and there are a few cases of garbling. These discrepancies, almost self-correcting when the message can be read, caused more or less trouble when the two versions were originally compared for the purpose of paralleling pages in the two codes. In some cases where the required relationship of penultimate and of ultimate digits was not exact, pages were at that time marked as provisionally equivalent; these cases are indicated here by a bracketed question mark after the second of the two pages in question. In some cases a variation in the ultimate digit was assumed to be due to the presence of variants in the code book.

There are some features of the two versions that are interesting from a cryptographic standpoint. Most important is the criminal carelessness of repeating a message in a different code. Time and labor could have been saved, and, far more important, the safety of the code could have been safeguarded by simply repeating the text of the original message and fitting it

with a new introduction. As it is, it is sure that the encoder of the 12444 version never looked at the 18470 original, for the new version is not a mere routine tabular transposition from the first message but a new encoding. A glance at the instances in which the versions depart from the page-for-page correspondence of the two codes will suffice to prove this statement. The 18470 message has Cef er ino, Unterseeboot, and Streitkraefte where the 12444 message has Cef eri no, U-boot, and Streit kraefte. The equivalents for die, der, and und differ throughout; and where the 18470 message has 7281 and 11041 for stops, the message in 12444 has stops from other pages.

Not only were the two versions encoded independently, but it is possible to say with practical certainty that they were encoded by different code clerks, and that the second encoder was less experienced than the first. The differences in procedure stand out as differently as differences in handwriting. The 12444 encoder has twice (for Unterseeboot and for Streitkraefte) wasted code groups. He has added "Dative Plural" after Geisel, a procedure probably taught to code clerks, but generally neglected in practice. Most convincing of all, he has neglected to use the nonalphabetical groups for und and the forms of the article that are so freely scattered through the book, and has amateurishly turned each time to the alphabetical page in question to find his word.

It is an interesting though easily explicable fact that, under these conditions, the two encoders have twice drawn their stops from the same pages; where 18470 has 12291, the 12444 version has 30300, and for the 21491 of the 18470 message the other version has the exact equivalent, 23251. 30300 is not the exact equivalent for 21491 (that would be 30351), and is probably not a stop at all: it is probably garbled, and may be an error for 30100 (=20640 in 18470), although even that is more likely a comma than a full stop. If 303 is in fact the correct page number, both encoders have followed the word wuerde, which is on alphabetical (XX) page 245 by a stop on the alphabetically adjoining page 244. The stops were scattered through the book precisely that they might be used in this manner. The correspondence between the other two stops, 21491 and 23251, is exact, and is due to the same cause.

18470	Both Codes	12444	18470	Both Codes	12444
814 N. 247					23830 Telegramm
580 vom 24sten Feb.					25977 247
728 Antw. auf Tel.					1517 ueberhaupt
549 Nr. 104					21164 nicht
18477					26747 erwaehnt
		535 (525) Nr. 284			20880 comma
		989 vom 4ten Maerz			8150 lautet
		728 Antw. auf Tel.			6364 in
		964 Nr. 115			20623 Wiederholung
		12444			8322 stop

18470	Both Codes	12444	18470	Both Codes	12444
		25916 Auf Telegramm		1186 12296 (15596) deutschen	
		7446 104	14731 Unterseeboot		1544 U
		3892 stop			5212 boot
		21286 Die			4522 dash
	19373 22982 Kais. Regierung			8667 15177 kommandeurs	
	25257 2467 haelt		15762 den		17484 den
15162 die		21285 die	15861 der	18953 20063 Instruktionen	17461 der
	13066 27176 bisherigen			1186 15596 deutschen	
	10676 8286 Pressenachrichten		21638 streitkraefte	22978 26388 See	27719 streit
	9546 1506 ueber die				29613 kraefte
		23990 Vorgaenge		30532 11942 durchaus	
		29792 bei		15938 (14938) 2748 widersprechen	
		9730 Versenkung		14596 16058 wuerde	
22891 der		17475 des (sic!)	12291 stop		30300 stop
	22290 11650 Cef			18952 30062 (20062) Instruktions	
24515 er		29488 eri		19142 170? gemaess	
15883 ino		26866 no		15116 5428 [?] haben	
	27163 25876 fuer			1186 15596 deutsche	
	22094 19054 unzuverlaessig			8667 15177 Kommandeure	
		10500 comma		24083 21193 neutrale	
	22595 1155 da			16030 29040 Gewaesser	
	9781 9491 geschildertes		11913 und		6673 und
	21872 23982 Vorgehen			24367 26777 erst	
25870 des		17475 des			

18470	Both Codes	12444	18470	Both Codes	12444
	23303 27413 recht				21286 die
	24083 21193 neutrales			25981 26891 noch	
	19236 24346 Gebiet			17508 12519 ohne	
	12329 9239 unbedingt			13284 15794 Bericht	
	16480 24591 [?] zu			15767 30990 ist	
4336 achten				12536 25560 [?] wird	
7281 stop		10401 stop		6816 17126 Angelegenheit	
	14699 3059 Wegnahme			19175 1785 genau	
	18139 19648 von			14768 5878 (5778) untersuchen	
	15642 14702 Geisel		20923 und		6670 und
		15083 Dat. Pl.		17626 8936 noetigenfalls	
	20337 21868 (21848) aus			17450 12860 Remedien ?	
	24083 21193 neutralem			28978 22888 eintreten	
	19236 24346 Gebiet			11340 16300 lassen	
	14596 16058 [?] wuerde		11041 stop		24791 stop
	24936 7646 hierzu			13788 6298 Bitte	
	18654 6364 in			8730 20940 mitteilen	
	26101 20411 scharf			1920 22431 an	
	3549 8608 [?] superlative in-em		30513 und	27377 2527 (2587) dortige Regierung	6672 und
	15522 12432 Gegensatz			17854 19964 verwenden	
	21354 17364 stehen			18654 6364 in	
	21491 23251 stop			10672 8283 Presse	
	19312 (19372) 22983 Kais. Regierung		8001 stop		

(Signed) BUSSCHE

(28) Additional Codes of the 18470 Family

After the preceding account had been written, M. I. 8 acquired photostats of skeletons of certain German codes and descriptions of these codes from some one in Holland. This material had originally been offered for sale to some American officials then in Holland in April 1919. Since no one conversant with codes was on the ground to examine the material, and no adequate description was forthcoming, nothing had been done in the matter at that time. 18470 and its encipherments 2310-2815-80574, 1777, and 12444 had long since been "broken" when, about Christmas 1919, the material originally offered in Holland was sent to Washington for inspection and possible purchase. In Washington it was photostated, and is accordingly now in the files of M. I. 8.

This material contains, besides parts of certain codes not germane to the present study, a skeleton of a code known as 2500, with tables for changing this code into four encipherments called by the "Dutchman" from whom the material was obtained 37000, 29000, 20000 and 18400. The last turned out to be identical with 18470, although in the messages received by M. I. 8 that designating number was never employed.

It was interesting to compare the new material with the identifications made in M. I. 8. The "Dutchman" added words to those already identified, while at other times the M. I. 8 skeleton contained identifications not in the new material. Occasionally there would be conflict in identification, and one skeleton or the other would require correction.

It is difficult to place the "Dutchman." The writer's recollection is that it was said in Washington in April 1919 that the man was a Hollander. H. O. Yardley in his book "The American Black Chamber" says he was a German, but later, in conversation with the present writer, he stated that he had merely taken this for granted, and that the man may very well have been a Hollander. There are objections to either possibility.

If the man was a Hollander, we can imagine his building up skeletons of German codes in use between Berlin and the Netherlands. The present writer has been informed on excellent authority that the Dutch Government actually had a Deciphering Bureau which, when occasion demanded, would cause information of an important-if-true nature to be issued, and would then carefully scan out-going and in-coming telegrams of foreign Governments in the effort to find the information repeated in code messages. On the other hand our "Dutchman" informs us that a certain code (18400) was used by a German consul at Nice in 1914, and 2 years later by the German Ambassador to Denmark. He knows, too, that one and the same code may, in its proper name division, contain different family names according to the foreign country with which it is to be used. It would be remarkable if a Hollander knew either of these facts, and astonishing if he knew them both. In his description of codes 9700 and 5300, not belonging to the 18470 family, of which he likewise furnished partial copies, the "Dutchman" has indicated certain additives, some of them running to many figures, which were used with these codes. To work out these long additives from the fractions of the codes at his disposal would have been a very rare cryptographic achievement.

We might suppose a person in possession of these data to have been associated with the German Foreign Office, but this supposition, too, has its difficulties. If he was in the Foreign Office, why did he have to build up codes piece-meal instead of copying them from a code book? And why does he betray complete ignorance of the real use of the Dreinummerheft (see p. 4 *f.*)? For of this little code-in-itself he tells us that the three-figure numbers "indicate the bureau for which the telegram is destined, etc." Now by "etc." he may mean anything at all, but the fact is that the three-figure groups *never* indicate "the bureau for which the message was destined", or anything even remotely like it.

Above all, if he was in the Foreign Office, why does he have to guess the meaning of certain code groups? For guess he does, as he himself tells us: "Where I could not till now fix a number but the text showed clearly that a number was meant, I put the word 'zahl'." Nor does the handwriting look like that of a German.

In any case, however, what really interests us is that we have here four additional codes which prove to be variants of 18470. Added to the three variants which we already have, this gives us seven variants of 18470, or a total of eight codes from the same alphabetical base.

Our study convinced us that 18470 was derived from an alphabetical base that we called XX, and that 2310-2815-80574, 12444, and 1777 were derived from 18470. (See p. 18 *ff.*) On the other hand, our "Dutchman", in connection with his collection of codes, says "Probably code 2500 is the original code book. From this code are derivated (sic!) the codes 18400 (=our 18470), 29000, 37000, 20000." We shall now have to see whether, in the light of new information, we must modify our conclusions, or whether we can fit the new encipherments into the framework already built up.

It will be granted at once that originally our code was compiled alphabetically, if only for the reason that there is no other practical way to perform such a task. Any one who will read what has been written above concerning the relationship of an archetype XX to code 18470 (see p. 34 *ff.*) will also grant that this intimate relationship is not in any way changed by the new material.

On the other hand, it does not necessarily follow from these facts that 18470 was *directly* derived from XX, or that it was the first code so derived, while the other codes of the series were derived from 18470. It would be perfectly possible to make a code systematically from XX, and then to change it systematically so as to produce another code whose relationship to XX would appear just as clearly as that of the first code.

Examination of our series of codes reveals the fact that 2310 actually bears the same systematic relationship to XX as does 18470. To produce 2310 from 18470 the pages of the latter were renumbered in blocks of four. Thus, 18470 pages 10, 11, 12, 13 became 2310 pages 58, 59, 60, 61, etc. (See the complete table p. 24.) It follows that 2310 will have the same kind of relationship to the original alphabetic Code XX as 18470 has; for whenever, in the course of the alphabetical sequence, the means, or the extremes, of a four-page block appear in 18470 (see p. 36 *f.*) the same is necessarily true of 2310 also.

Examination reveals further that this is true of no other code either of those furnished by the "Dutchman" or of those that M. I. 8 already had. In the case of 18470 we were able to predict in advance certain facts about the numerals occurring on various pages even before the numerals had been identified. (See pp. 31 *f.*; 34; 36.) This cannot be done with 12444 or 1777 because of the page-by-page change to which the code had been subjected to make these encipherments; and it cannot be done with any code added by the "Dutchman's" series because the occasional occurrence of pages with double numbers throws things askew. If 18470 were derived from 2500 or from any other of the codes with which we are dealing, such a state of affairs would not exist, and this state of affairs in itself suffices to prove that 18470 is not the offspring of any of those codes.

We can, however, provide additional proof, and since this proof will bring out certain features of code compilation in the German Foreign Office, it seems worth while to do so.

1. Code 13040 has on page 130 a series 10 groups reserved for a code indicator. Precisely the same state of affairs exists on page 184 of 18470. In both these cases this phenomenon is proof that we are dealing with an original and not with a derived code. In all other codes of the same family as 18470 the "Chiffre Nummer" has a distinct meaning—indicates a word

or phrase—besides serving as the code indicator. In code 20000 for example, the group 20000 (the equivalent of 9500 in 18470) signifies "ueber."

2. Further proof is furnished by an examination of the use of the device of giving a page a double number in order to render identification more difficult.

When 13040 was compiled this device was employed in the case of 26 pages. For this purpose pages were chosen which, almost without exception, contain words frequently used, and the double numbering of the pages was an effort to cut down repetitions in messages. Besides grammatical directions and two pages of supplementary matter, the pages with double numbers contain the following words: Aus, das, der, des, die, ein, hat, ihm, in, kaiserlich, melden, mit, nicht, sei, sie, unter, von, wird, wurde—every one with the possible exception of kaiserlich and melden immediately recognizable as a common word.

No such phenomenon appears in 18470, and for a reason that is easily seen. We do not know when either 13040 or 18470 was compiled, but we do know that 18470 is the later of the two. This is absolutely certain, because 13040 uses the old German orthography and 18470 the new. (En passant, it is an astounding fact that the German Foreign Office entrusted its correspondence with its representative in the greatest neutral country of the world to this code, which may well be called antediluvian.) Now when 18470 was compiled a different procedure was adopted. Instead of assigning double numbers to some 20 pages containing frequently used words, some extremely common words (der, die, und, nicht, etc.) were sprinkled through the book on page after page regardless of alphabetical sequence, and double-numbered pages were dispensed with. (See pp. 38*f.*; 58*f.*)

With the exception of 18470, 12444, 1777, and 2310 all the codes of the family contain pages with double numbers. This in itself would be good reason to regard all these codes as derived from 18470 and not 18470 from any of them, for it is most improbable that, once the pages of a code had been given double numbers, this system would be discarded in making a variant of the code. We may point, too, to the parallel case of 13040 and 5950, where we not only find the system of double page numbers carried out, but see the same pages receiving double numbers in 5950 as had them already in 13040.

Since this system of assigning double numbers to certain pages plays such a prominent part in German code encipherment, it seems worth while to make a further study of these pages and endeavor to discover the considerations that governed the double numbering.

37000, 29000, 20000, and 2500 all contain pages with double numbers. Except in a few cases, however, these pages are not the same in the various codes. Moreover, some of the codes contain substantially more pages with double numbers than others. The following lists show the common words (where any such can be pointed out) that are found in the various codes on the pages with double numbers. The "Dutchman" is not absolutely accurate in his assigning of double numbers, and the present writer has made some additions as a result of comparing the "Dutchman's" various tables. (These additions will be found penciled on the "Dutchman's" tables in the files of M. I. 8.)

DOUBLE-NUMBERED PAGES IN 37000

The table gives the numbers of the page, then the equivalent page in 18470, and then the word on the page which, being one of frequent occurrence, may be regarded as having caused the giving of a double number to the page. This same procedure is followed in the other tables. (37 indicates 37000; 18, 18470. So in the other tables 20 indicates 20000; 29, 29000; and 25, 2500).

90481—37——7

37	18	
521–522	15	Gram. Dir.
523–524	16	Do.
186–187	24	Do.
486–487	32	Als
507–508	35	Gram. Dir.
509–510	36	Do.
249–250	82	Dem ?
252–253	84	Auf
382–383	88	Minister
189–190	90	(?)
234–235	95	Ueber
418–419	100	Mit
315–316	104	(?)
317–318	105	Der (Alphabetical)
345–346	114	Ich; Ihn
267–268	118	Werden
269–270	119	Uns; Unser
84– 85	122	Worden
88– 89	125	Wird
24– 25	130	Bis
26– 27	131	(?)
429–430	140	Mein
46– 47	142	Wir; Wieder
50– 51	145	Wurde; Wuerde
295–296	146	Waren
299–300	149	Wie
331–332	151	Haben
334–335	153	Ihr; Im
304–305	161	(?)
393–394	164	Zu (Alphabetical)
502–503	171	Nur; Ob
262–263	186	In
140–141	192	(?)
96– 97	203	Aus
73– 74	210	Sowie ?
58– 59	214	Staat ?
386–387	226	Sein
42– 43	235	Bank ?
580–581	240	Nicht (Alphabetical)
159–160	244	Erbeten ?
309–310	247	Hat
515–516	266	(?)
135–136	288	Es
149–150	291	Euer; Euch
36– 37	296	Nach

NOTE.—A question-mark after a word means that the word may not be of such frequent occurrence in the language as to have caused the page to get a double number. A question-mark instead of a word means that no word could be found on the page in question of such frequent occurrence that it may be supposed to have caused the page to receive a double number. This note applies also to the other tables of this series.

DOUBLE-NUMBERED PAGES IN 20000

20	18	
189–190	15	Gram. Dir.
191–192	16	Do.
28– 29	19	An
332–333	22	Geog. Names
335–336	24	Gram. Dir.
319–320	27	Do.
33– 34	31	Alle
35– 36	32	Als
165–166	34	Geog. Names
167–168	35	Gram. Dir.
169–170	36	Do.
67– 68	43	(?)
69– 70	44	Ab
89– 90	71	(?)
105–106	75	Machen ?
118–119	81	(?)
256–257	85	Dass
387–288	88	Minister
389–390	89	Konsulat
156–157	91	Um
159–160	93	(?)
199–200	95	Ueber
375–376	99	Minister
377–378	100	Mit
379–380	101	Kommen
289–290	102	Das (Alphabetical)
139–140	106	Praesident
153–154	113	Lassen
61– 62	114	Ich; Ihn
338–339	118	Werden
340–341	119	Uns; Unser
342–343	120	Unter
344–345	121	Welcher ?
242–243	123	(?)
244–245	124	Und (Alphabetical)
448–449	127	Melden
460 (450?)–1	128	Mann
124–125	130	Bis
129–130	134	Betrag ?
132–133	136	Bei
428–429	141	Krieg ?
312–313	146	Waren
316–317	149	Wie
94– 95	151	Haben
97– 98	153	Ihr; Im
206–207	157	Ist
504–505	158	(?)
508–509	161	(?)
17– 18	162	(?)
20– 21	164	Zu (Alphabetical)
585–586	170	(?)

20	18	
587–588	171	Nur; Ob
589–590	172	Ober
537–538	175	Ohne
539–540	176	Note ?
578–579	178	Vertrag ?
45– 46	185	Zwischen ?
479–480	188	Gesandtschaft
399–400	194	(?)
403–404	197	Sekretaer ?
327–328	200	Zum; Zur
329–330	201	(?)
511–512	203	Aus
513–514	204	(?)
99–100	210	Sowie ?
56– 57	215	(?)
58– 59	216	(?)
499–500	220	(?)
475–476	225	Da
350–351	226	Sein

20	18	
419–420	230	Regierung
422–423	232	(?)
439–440	235	Bank ?
82– 83	242	(?)
85– 86	244	Erbeten ?
145–146	247	Hat
148–149	249	Hiesig
111–112	251	(?)
74– 75	256	(?)
466–467	269	Reichs-
179–180	270	Die (Alphabetical)
236–237	274	Dringend ?
261–262	283	Nicht (Alphabetical)
11– 12	287	Falls ?
52– 53	292	(?)
284–285	296	Nach
549–550	299	Tag ?
217–218	303	(?)
230 (220?)–1	305	(?)

See note on p. 92.

DOUBLE-NUMBERED PAGES IN 29000

29	18	
413–414	11	Geog. Names (Deutschland)
183–184	15	Gram. Dir.
185–186	16	Do.
247–248	24	Do.
225–226	27	Do.
215–216	35	Do.
217–218	36	Do.
140–141	48	(?)
244–245	73	Geog. Names
431–432	84	Auf.
319–320	91	Um
331–332	94	Schluss ?
439–440	102	Das (Alphabetical)
406–407	109	(?)
88– 89	111	(?)
417–418	114	Ich; Ihn
58– 59	122	Worden
60– 61	123	(?)
62– 63	124	Und (Alphabetical)
264–265	127	Melden
452–453	153	Ihr; Im
194–195	156	Gegner ?
117–118	171	Nur; Ob

29	18	
122–123	175	Ohne
303–304	182	(?)
284–285	186	In
288–289	189	Interesse ?
208–209	193	Kais. Regierung
261–262	197	Sekretaer ?
127–128	219	(?)
130–131	221	War
363–364	224	(?)
298–299	226	Sein
148–149	243	(?)
348–349	246	(?)
366–367	250	(?)
170–171	255	Erhalten ?
40– 41	258	(?)
71– 72	276	(?)
54– 55	279	(?)
35– 36	291	Euer; Euch
399–400	295	Muss
96– 97	298	Sind
100–101	301	Sich; Sie; Sind
82– 83	302	(?)

See note on p. 92.

DOUBLE-NUMBERED PAGES IN 2500

25	18		25	18	
156–157	10	Geog. Names (England)	55– 56	171	Nur; Ob
158–159	11	Geog. Names (Deutschland)	57– 58	172	Oder
161–162	13	Do.	14– 15	178	Vertrag ?
343–344	30	Do.	16– 17	179	(?)
27– 28	44	Ab	124–125	186	In
29– 30	45	Geog. Names	187–188	193	Kais. Regierung
64– 65	58	Do.	167–168	226	Sein
298–299	85	Dass	31– 32	230	Regierung
371–372	88	Minister	309–310	238	(?)
346–349	98	Konsul; Koennen	87– 88	243	(?)
224–225	106	Praesident	238–239	247	Hat
253–254	114	Ich; Ihn	241–242	249	Hiesig
75– 76	122	Worden	82– 83	255	Erhalten ?
79– 80	125	Wird	35– 36	266	(?)
387–388	127	Melden	39– 40	269	Reichs–
98– 99	132	Bericht	120–121	272	(?)
70– 71	135	(?)	278–279	274	Dringend ?
417–418	140	Mein	306–307	288	Es
94– 95	145	Wurde; Wuerde	327–328	291	Euch; Euer
172–173	146	Waren	150–151	294	Kein
178–179	155	Gegen ?	152–153	295	Muss
180–181	156	Gegner ?	245–246	300	Telegramm
51– 52	168	(?)	247–248	301	Sich; Sie; Sind

See note on p. 92.

We observe that code 37000 has 45 pages with double numbers, while 29000 has 45, 2500 has 46, and 20000 has 89. Since there is some uncertainty at times about the page equivalence and double numbering, it is possible that 37000, 29000 and 2500 actually have the same number of pages with double numbers, and that 20000 has twice as many. There would be nothing astonishing in a code compiler's selecting a certain number of common words for such treatment and later doubling or halving the number. But what is really striking is the great variation in the common words found on the double-numbered pages. The German language does not change, or, if it does, it changes with glacierlike slowness; words that were common when one of these codes was compiled were just as common when the others were designed.

Still we find that *only three pages* have double numbers in all four of the codes. These pages contain the common, but not exceedingly common, words ich and ihr, nur and ob, and sein, of which only ich has a double-numbered page in 13040. The pages of 18470 receiving double numbers in more than one code with common words appearing on them are the following:

2500 and 29000	11	156	193	243	255	295	301					
	Names	Gegner ?	Kais. Reg.	?	Erhalten?	Muss	Sind; Sich; Sie					
2500 and 20000	44	85	106	172	178	230	249	269	274			
	Ab	Dass	Praesident	Oder	Vertrag?	Regierung.	Hiesig	Reichs	Dringend			
2500 and 37000	125	140	145	266	288							
	Wird	Mein	Wurde; Wuerde	?	Es							
29000 and 20000	27	91	102	123	124	175	197					
	Gram. Dir.	Um.	Das (Alph.)	?	Und (Alph.)	Ohne	Sekretaer ?					
29000 and 37000	84											
	Auf.											
20000 and 37000	32	95	100	118	119	130	149	151	161	164	203	
	Als	Ueber	Mit	Werden	Uns; Unser	Bis	Wie	Haben	?	Zu (Alph.)	Aus	
	210	235	244	296								
	Sowie ?	Bank ?	Erbeten ?	Nach								

2500, 29000 and 20000	127 Melden					
2500, 29000 and 37000	122 Worden	186 In	291 Euer; Euch			
2500, 20000 and 37000	88 Minister	146 Waren	247 Hat			
29000, 20000 and 37000	15 Gram.	Dir.	16 Ditto	24 Ditto	35 Ditto	36 Ditto	153 Ihr; Im
2500, 29000, 20000 and 37000	114 Ich;	Ihr	171 Nur;	226 Ob	Sein		

No less than 85 pages have double numbers in one code only. Even more striking is the fact that a recapitulation shows that in one code or another 145 different pages are given double numbers—and that in a total of 300 pages. In fact, if we eliminate pages with proper names, of which only eight have received double numbers, the total number of pages amounts only to 254. In other words, more than half the code has been given double numbers at one time or another.

It is, accordingly, obvious, that the principle of frequency of occurrence has not been the sole guide in assigning double numbers to the pages of these codes. This principle, indeed, is not so well observed in the case of 29000 and 20000 as it is in 37000 and 2500. In general, however, it seems safe to say that the double numbering of pages was employed only partially to conceal the repetition of frequent words, and had as its main object the enlargement of the apparent range of the codes.

3. 37000 differs from 18470 only in the renumbering of the pages and the assignment of double numbers to some of them. 29000 and 20000 exhibit a rearrangement of the 10-word blocks on the various pages such as was made in changing 13040 to 5950, and in changing 18470 to 12444 and 1777, and 2500 shows a further shift in these blocks. This whole shift of 10-word blocks is shown in the following table:

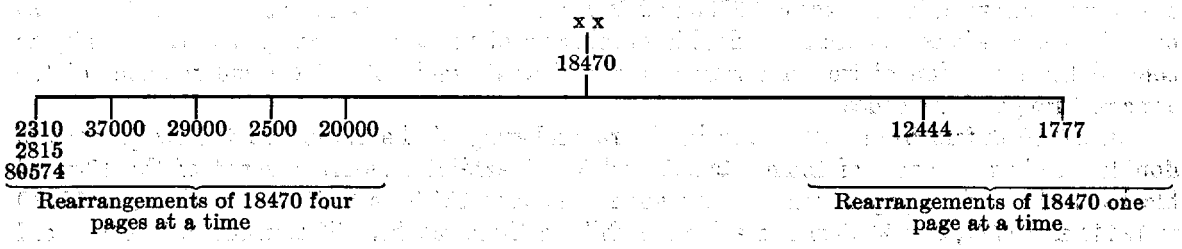
18470 37000	29000 20000	2500
0	1	2
1	2	3
2	3	4
3	4	0
4	0	1
5	6	7
6	7	8
7	8	9
8	9	5
9	5	6

2500 bears the same relationship to 29000 and 20000 as those codes do to 18470 and 37000; in other words, 2500 has undergone a double shift.

The 10-word blocks of 37000 are arranged just as in 18470. Those of 29000 and 20000 have been arranged just as in 2310-2815-80574, 12444, and 1777—and, incidentally, in the same way as the 10-word blocks of 13040 were rearranged in making 5950. The double shift in 2500 is the only one of the kind known to the present writer.

2310 differs from 18470 merely in a change of pagination and a shift of 10-word blocks. It was made from 18470 precisely was 5950 was made from 13040—by renumbering the pages four at a time. For this reason everything that has been pointed out concerning the relationship of 18470 to the archetype XX holds true of 2310 also. It would indeed be difficult to say whether 2310 preceded 18470 or 18470 preceded 2310, if it were not for two considerations—the provision for the "Chiffre Nummer" in 18470, and the lack of such provision in 2310; and the relationship of the 10-word blocks in the two codes, these blocks holding the position in 2310 that they regularly have in derived and not in original codes.

We cannot say in what order the various encipherments were made. It seems certain that 12444 and 1777, in which the numbers of the pages were changed one at a time, are later than any of the others in which the pages are shifted four at a time.[23] It seems beyond doubt that 18470 is the first of the codes, and was made directly from the alphabetical archetype XX. A stemma of the various codes of the family may accordingly be made as follows:



II. THE "FUENFBUCHSTABENHEFT"

During the year 1921 the numbers of the Dreinummerheft ceased to appear at the beginnings of German code messages, and were replaced by a series of five-letter words. To these words, which obviously formed a new numbering and dating code, the name *Fuenfbuchstabenheft* may be arbitrarily assigned.

This new numbering and dating code had not, so far as the experience of M. I. 8 went, been used during the war. Its solution, however, shows the importance of continuity in cryptographic work, for, as will presently appear, the decipherment of the new code was checked by tying it up to the old war-time "Nummerheft."

A careful inspection of the five-letter groups showed the following facts: (1) they were composed with a two-letter difference—that is, each word differs from every other word in at least two letters; (2) outside of a few messages beginning with code words whose initial letter is K, the first code word in the message uniformly precedes the second alphabetically; (3) in messages orginating in the same place (Moscow or Berlin) the initial code words of the messages progressed alphabetically from message to message, and the second words progressed similarly.

[23] See, in this connection, the code telegram (12444 messages, p. 33 *ff.*) reproduced above (p. 84 *f.*) and the accompanying comment.

As a result of these observations a mutilation or construction table was made for the five-letter words. This table is reproduced here:

ba	be	bi	bo	bu	by			
--	da	de	di	do	du	dy		
--	--	fa	fe	fi	fo	fu	fy	
--	--	--	ga	ge	gi	go	gu	gy
ky	--	--	--	ka	ke	ki	ko	ku

l	z	x	t	s	r	p	n	m	ar	ep	in	om	ul
m	l	z	x	t	s	r	p	n	ap	en	im	ol	uz
n	m	l	z	x	t	s	r	p	an	em	il	oz	ux
p	n	m	l	z	x	t	s	r	am	el	iz	ox	ut
r	p	n	m	l	z	x	t	s	al	ez	ix	ot	us
s	r	p	n	m	l	z	x	t	az	ex	it	os	ur
t	s	r	p	n	m	l	z	x	ax	et	is	or	up
x	t	s	r	p	n	m	l	z	at	es	ir	op	un
z	x	t	s	r	p	n	m	l	as	er	ip	on	um

It was assumed that, according to German usage, the opening five-letter word of a message would give the message number, and it was noticed that these words uniformly occupied a position near the beginning of the alphabet. The supposition, therefore, seemed warranted that these code groups formed the beginning of the new Nummerheft. This supposition was checked by assuming that when the Nummerheft was changed messages numbered in the new system would bear numbers consecutive with those of messages in which the old Dreinummerheft had been used. It seemed certain that the date would follow the message number.

The beginning of the calendar was approximately fixed by assigning to several messages a date of sending corresponding to the date of interception, and then working back with the aid of the Mutilation Table to fix the beginning of the calendar. The word GUNEP, from its position in the messages, and its frequent occurrence, was assumed to mean Antwort auf Telegramm.

The occurrence in a Berlin-Moscow message of GUNEP BOROP FOSOL served to confirm the assumptions that had been made: These words, if the suppositions were correct, would mean Antwort auf Telegramm Nr. 159. vom 13ten April, and a search disclosed that Moscow-Berlin telegram no. 159, numbered in the old Dreinummerheft, had actually been sent on April 13.

A series of code words beginning with K, and varying with the number of words in the message, was taken to represent the number of significant code words in the message. When KIRUZ was taken on this basis to represent 15, it was found that the other words in that alphabetical neighborhood fitted in to represent the numbers from 1 to 100. KYZON (Stop or Null) and KYZIP (und) were guessed by studying their occurrences.

The meaning of some words remained obscure when the work was discontinued, but the bulk of the Fuenfbuchstabenheft was accounted for.

III. GERMAN METHODS OF CODE ENCIPHERMENT

Several German methods of code encipherment are known in addition to those that have been described in the preceding pages. Besides the encipherments of 13040 described above

(p. 8 *ff.*), it is known that the Germans disguised this code by means of "sliders", although no examples of this encipherment were found in M. I. 8.[24] The end achieved by this method is the replacing of some or all of the digits of each code group by other digits, just as letters of the alphabet are replaced by others in a substitution cipher. To complicate matters further, one scheme may be employed for the first column, another for the second, and so on as in a multiple-alphabet cipher. The end desired may be achieved by the use of a device which makes use of sliding paper tapes—hence the name "slider". A further description of such a device will be given presently.

A number of messages written in a slidered encipherment of the German Naval Code—the Verkehrbuch, called for convenience 55515—came to light in M. I. 8 and were read there. Copies of three different sliders had been received from the British. The problem was, assuming that sliders had been used, to find out which one of them had been employed, and at what figures it had been set.

The sliders seem no longer to be in the files. Several decoded messages are on hand, however, which contain both the text as sent and the basic text of the Verkehrbuch. These messages bear the notation, made at the time when the messages were read, "slider 1 set at 718", and from them slider 1 has been reconstructed. A copy follows. The column of figures at the side is stationary. The three other sets of figures represent sliding tapes which can be set with any desired figure opposite 0 of the stationary column. The first and fifth figures of code groups remain unchanged. When the tapes are set at some point previously agreed upon, the code figures to be enciphered are found in the stationary column and are replaced, in order, by the figures opposite on the tapes.

Basic code	Second figure becomes	Third figure becomes	Fourth figure becomes
0	7	1	8
1	0	9	3
2	9	4	4
3	2	6	6
4	6	2	5
5	3	7	2
6	5	3	7
7	8	5	1
8	1	0	9
9	4	8	0
	7	1	8
	0	9	3
	9	4	4
	2	6	6
	6	2	5
	3	7	2
	5	3	7
	8	5	1
	1	0	9
	4	8	0

First and fifth figures remain unchanged.

With the tapes set at 718, the code group 41259 would be enciphered 40429.

[24] A specimen that turned up years later in the files of the State Department is discussed on page 101 *f.*

It was known that for messages passing between Washington and Buenos Aires slider no. 1 set at 718 had been most commonly used, and all the messages passing between these two points that were then in our hands were read by trying this encipherment. On the other hand, a number of messages passing between the German Ambassador to Chile and his colleague in Peru would not give a reading on this basis, and it was necessary to make tests to ascertain how they had been enciphered.

The cryptographer's golden rule," Guess a word", was applied. Of three telegrams sent by Ambassador Erckert from Santiago to Lima in September 1917 one was in 26040 and had been read. This message was numbered 3, and when it was read it was assumed that the other two of the series would prove to be numbers 1 and 2. Efforts made to read these two on the supposition that they might be in a slidered encipherment of 13040 were unavailing. The attempt was then made to read them as encipherments of 55515. Tests for 1 or Nummer 1 proved unavailing. On the other hand the test for 2 was successful and resulted in the reading of the whole series of messages between Lima and Santiago. Of the two different code groups for 2 provided by the code book, that one was chosen which has the same initial digit and the same final digit as the first group in the code message. Slider no. 1 was then so set as to bring the three middle digits of the code group opposite the three middle digits of the unenciphered code group for 2, namely 8, 3, and 9. The result of this process was to set the slider at 256, which proved to be the correct key.

It may be remarked incidentally that the reason why no. 1 had not been found by this method was that in that message the actual number was preceded by the code group for "Telegramm Nr." It may be added that when these messages had been studied before, it had appeared queer that no. 3 had been sent so late in the year as September. The supposition had been made at that time that the Ambassador had only then begun numbering his messages, and that in that case his no. 1 would probably refer to that fact. A note had been made concerning no. 1: "Test for, 'Werde kuenftig Depeschen nummerieren.' " When the message was read, it proved to contain the words, "Ich bitte Sie nummerieren Telegramme Briefe von jetzt ab."

The following message, sent from the German Embassy in Buenos Aires to Ambassador Bernstorff in Washington is an example of the messages enciphered with slider 1 set at 718. The message shows the difficulties of German communication, since it was first sent in one form (through a Swedish intermediary), and then relayed in another form at Buenos Aires. The first column of figures reproduces the enciphered code as sent, the second gives the underlying code of the Verkehrbuch, and the third gives the clear text.

24946	29126	42
10083	11803	Berlin
62790	63580	telegraphiert
35505	36795	colon
21845	28925	28
68035	67815	vom
50297	51487	19ten Mai
24018	29878	Antwort auf Telegramm
21024	28854	23
34759	39549	Euere
34353	39643	Exzellenz
34954	39144	sind ermaechtigt zu
15426	16256	Ind
16467	14237	er
61044	68824	weitere
68284	67404	20,000
17136	10016	bracket
21052	28842	20
29819	22979	taus
16969	14139	end bracket
35522	36752	Dollars
77154	70044	zu
40846	41926	geben
21854	28944	29
68035	67815	vom
50297	51487	19ten Mai
40578	41768	Fuer
49050	42840	Gesandtschaft
27137	20017	Peking
35507	36797	colon
21060	28830	18
50297	51487	19ten Mai
24329	29659	Im Anschluss an
62658	63348	Telegramm Nr.
21500	28790	16
36663	34333	Bitte
39581	32701	bei
35347	36627	direkten
17152	10042	Dat. Mehrzahl
64375	69665	Zahlung
24115	29075	an
12280	13400	D
10103	11093	as
68038	67818	von
55856	56946	Quittungen
21771	28561	absehen
55575	56765	Punkt
33892	35982	Das
61857	68947	wird
39581	32701	bei
64375	69665	Zahlung
68199	67089	durch Vermittlung von
21224	28454	Dritten
24149	29029	als
12811	13971	Eduard
20510	21770	Schu
29747	22527	ster
55856	56946	quittieren
55510	56770	Punkt
64826	69956	Zimmermann

The British say that the slidered encipherment was used "no doubt . . . to protect the Swedish intermediary, as it might otherwise have been noticed that the same set of figures which arrived at Buenos Aires as a Swedish telegram was sent [further] as a German one." They point out also that "it was the resemblance between the German and Swedish telegrams which first suggested that they were identical messages disguised by the use of a slider." In the message quoted above, for example, we note the constant identity of the first and last figures in each code-group of the message in the basic code and in the corresponding group of the slidered encipherment. Similar parallelisms would appear in the case of messages enciphered by means of the other sliders.

The British instructions accompanying the sliders contain no description of how they were reconstructed after the method of encipherment had once been suspected. We can readily see, however, that the reconstruction followed almost as a matter of course upon the suspicion of the identity of the telegrams, for the paralleling of two identical messages group by group will solve the problem almost automatically. If, for example, we take only the first five groups of the message just quoted and compare the basic code with the slidered encipherment, we have

Basic code	Encipherment
24946	29126
10083	11803
62790	63580
35505	36795
21845	28925

From these few groups we can conclude (1) that the first and fifth figures of each group remain unenciphered; (2) that the enciphered equivalents of basic code 4, 0, 2, 5, and 1 when occurring as second figures of a group are respectively 9, 1, 3, 6, and 8; (3) that the equivalents of basic 9, 0, 7, 5, and 8 as third figures are respectively 1, 8, 5, 7, and 9; and (4) that the equivalents of basic 4, 8, 9, and 0 [4 is here repeated] as fourth figures are respectively 2, 0, 8, and 9. The remainder of the slider is built up in a similar way.

The British, then, recognized the equivalence of the two messages and reconstructed the slider. In M. I. 8, the message existed in only one form; on the other hand, the sliders were provided, and the task was to find the right slider and the correct setting.

An example of a slidered encipherment of a 13040 message came to light in the files of the State Department while this study was being made ready for the press. The encipherment was identified by the indicator 11076 which the British had said was used to introduce these messages. The message follows, with the equivalent 13040 text and the decipherment. The enciphered code is in the first column, the 13040 text in the second. One or two groups remain doubtful.

791		Nr. 172 } The first number is the Buenos Aires serial number, the other that
122		Nr. 93 } of Berlin.
473		Vom 25ten August
11076		Y (the indicator for this encipherment)
92377	23666	Erstens
3660	5339	Antwort auf Telegramm Nr.
03544	15722	58
5846	6923	und
06467	14236	im Anschluss an
01613	18371	heutiges
07532	10715	drahtloses Telegramm
19306	82693	Albert
3495	5284	annulliert
6932	4115	Imperfect Subjunctive
90421	21257	Vertraege
00180	11009	Zahlen
6933	4111	Perfect Indicative
1897	8986	Gua
5743	6521	ran
92738	23510	ty
09055	12844	Trust
08489	17208	fuer
3069	5838	} These two groups together almost surely spell Konto.
2572	3765	delete 2 letters? }
5553	6741	Reichscasse or Reichsbank
01554	18742	Dollars
02422	13255	15
99099	22888	00
99801	22997	000
92153	23041	stop
02578	13760	Ferner This may possibly belong before the preceding group; or possibly it introduces a new paragraph [note "erstens" above] which has disappeared.

The problem in the reading of this message, as in that encoded in the encipherment of the Verkehrbuch and just described above, was to find the setting of the slider. It was known from the British instructions that in these encipherments of 13040 the first two figures (in 4-figure groups the first figure only) were enciphered by column 1 of the slider, the next figure by column 2, and the last two figures by column 3. The setting for the first two figures can be found without difficulty. Inspection shows that the predominating initial figures in the 5-figure groups of the

encipherment are 0 and 9. Since the predominating initial figures in the 5-figure groups of 13040 are 1 and 2, we must have either 0=1 and 9=2, or 0=2 and 9=1. A trial with the slider shows that only the first arrangement is possible. Even this trial is hardly necessary, for 13040 contains 100 pages of 5-figure groups beginning with 1 and only 40 beginning with 2, so that the predominance of initial 0 over initial 9 in the encipherment would in itself lend a very strong presumption that 0=1 and 9=2.

The matching up of the other figures cannot be done with equal quickness and certainty. In the message just given it was found that the first column of the slider had been set at 7, and, since 718 had been so frequently used as the setting for the Verkehrbuch messages, that arrangement was tried and proved correct. If it had been found to be incorrect, guessing a word and the test for der, die, or und (see page 14) could have been tried next. At the very worst, however, there would be only 100 possibilities for the setting of the slider for the last three figures of the code groups.

On November 8, 1917, Dr. Kraske, who had been attached to the German Ministry in San Jose de Costa Rica, following the breach of relations between Costa Rica and Germany, sent a message to Kracker, German Minister in Colombia, containing the following request: "If you should consider it desirable to send me a communication in code, please transpose the numerals of this code [13040], which I shall preserve as long as practicable, into A B C code words, and address your communication without signature to Dr. E. Kraske, Casilla No. 482, San Jose de Costa Rica." No messages of the kind described were brought to light in M. I. 8.

Although not strictly concerned with diplomatic code, other methods of code encipherment used by the Germans during the war may be appended here.

The code used in America and between America and Berlin by von Papen was a simple straight alphabetic code of 10,000 code groups. Several neat methods, however, were used to encipher the code. Groups beginning with 9 were enciphered by writing the 9 as two digits—91, 92, etc. This gave a false appearance to the range of the code and also provided the groups above 9,000 with several variants. This procedure was used so constantly that it is hardly to be regarded as an encipherment. The following method furnished a pretty disguise for the code:

(1) Remove the first figure of the code group.

(2) Put the first figure at the end of the code group, enciphering it—at the same time—as follows (N. B.—Only the first figure of the group is enciphered; the others remain unchanged):

Original figure	0	1	2	3	4	5	6	7	8
Is enciphered by any one of the 5 numbers beneath it.	7	12	17	22	27	32	37	42	47
	8	13	18	23	28	33	38	43	48
	9	14	19	24	29	34	39	44	49
	10	15	20	25	30	35	40	45	50
	11	16	21	26	31	36	41	46	51

In the case of groups beginning with 90–98, the first *two* figures were transposed to the end and enciphered thus (our table is not complete):

Original figures	90	91	92	*	*	*	98
Are enciphered by any of the numbers beneath them.	52	57	72				96
	53	58	73				
	54	59	78				
	55	60					
	56	61					

Examples: 2364 becomes 36417 or 36418, etc.; 90129 becomes 12952 or 12953, etc.

A second encipherment of this code consisted in a substitution of groups of letters for the groups of figures according to the following tables:

For enciphering last 2 figures		For enciphering all except last 2 figures (whether there are 2 or 3 does not matter)			
03	na	00	anf	903	lop
04	nu	01	apa	909	moh
05	ob	02	arn	911	myr
07	ol	06	bla	912	nam
11	ot	13	cep	913	neb
13	ow ox	14	cho	914	nil
21	se	15	ciz	926	ops
23	ta	19	cyw	940	rhu
27	uc	25	dup	980	voc
29	uf	26	dwa		
30	ug	29	eck		
39	wi	36	eng		
44 ?	xi	41	fes		
45	yi	43	fju		
46 ? 48 ?	yu	45	fow		
50	ab	53	gov		
53	af	55	gux		
55	ah	60	hif		
56	aj	61	hot		
60	be	62	huw		
63		69	imp		
64	de	73	isz		
65	do	77	jos		
67	ek	78	juw		
68	el	81	kex		
71	er	82	kih		
72	et	86	kru		
73	ew	87	kum		
74	ex				
77	fo				
79	go				
84	id				
85	if				
86	im				
34 ?	uv				

M. I. 8 did not have the complete table. The material came from the Department of Justice.

The following is part of a message in this encipherment:

94077	1368	6121	92684	8773	0113	0003	5504	91150	6084	3677	8205
rhufo	cepel	hotse	opsid	kumew	apaow	anfna	guxnu	myrab	hifid	engfo	kihob

It will be noticed that the encipherment falls within the cable requirements of that time, that the code words be pronounceable.

Finally, the von Igel-von Papen code was disguised in a way that permitted it to be sent as what appeared to be an ordinary clear-text telegram. Each digit was assigned two or more letter equivalents, thus (we have only part of the table):

0	k	4	g, n
1	a, i, d	5	e, t
2	s, j, z	6	v, p
3	b, o		

The telegram would then be written out in the unenciphered code. One of its letter equivalents would then be substituted for each figure. Each letter would then be used as the initial of a word, the words being so chosen that they would make more or less connected sense. The last process is precisely similar to that followed in the game of "Telegrams." These words were then sent as an ordinary telegram, and the recipient, by reversing the process, would recover the code telegram. An illustration will make the process clear: To send the word Iren in the code, two groups were necessary—4602=Ir and 2513=en. Letters were substituted for each digit in the code groups $\begin{Bmatrix} 4602 & 2513 \\ gvks & zeio. \end{Bmatrix}$ Words were then written with these letters as initials: Germania Versicherung Kontrakt sicher zugesagt Executor ist offenbar.

Madame Victorica, the German agent, used an encipherment of the A B C code differing very slightly from the last-mentioned encipherment of the von Papen code. As employed by Victorica, vowels were not assigned numerical values, and words beginning with vowels were blanks in the code. This feature made it easier to compose the code telegrams. The following is an example of Victorica's use of this code:

Table of values:

1	t, d	6	b, p
2	n, z (x?), y	7	f, ph, v
3	m, w	8	h, c, ch, j
4	qu, r	9	g, k
5	s, sh	0	l, z (?)

The following message was sent to Victorica on February 24, 1917:

Give Victorica the following message from her lawyers Lower terms impossible Will give further instructions earliest and leave nothing untried Very poor market will quote however soonest our terms Want meanwhile bond Have already obtained license.

Beginning at the words "lower terms impossible" and arranging the initial letters, with the vowels omitted, in groups of five, we have:

LTWGF LNVPM WQHST WMBHL. The numerical values are now substituted:
01397 02763 34851 33680

These groups are now looked up in the A B C code:

01397 On account of political affairs
02763 You must arange immediately or it is useless
34851 Safe as possible
33680 Remittance sent today

The German Naval Code known as H. V. B. (Handelsverkehrbuch) has code words composed of letters, not figures. It contains 2 sets of code words, 1 of 10 letters each and 1 of 4 letters each. These code words were enciphered by means of a single alphabet substitution, precisely as in a cipher of the single alphabet substitution type.

The code used by Dr. Albert with Ambassador von Bernstorff was enciphered by a transposition of figures similar to that used in the first encipherment of the von Papen code described above. In the Albert code the first two figures were transferred to the end, but there was no further encipherment.

○