The GEE System—I

~~Top Secret Dinar~~

The first of three installments describing the attack on [redacted] perhaps the most important cryptographic system used by Germany in World War II. Introduced by Brigadier John H. Tiltman.

INTRODUCTION

I approach the task of writing this note with some diffidence, as the diagnosis and solution of the printing mechanism which was the cause of the vulnerability of this one time pad system was entirely the work of U.S. cryptanalysts and was quite one of their most important successes. I and my Research sections at G.C.H.Q. only joined in at the exploitation stage. But we did work in this field for three or four months starting in January 1945, our chief contribution being the reconstruction of the first few wheel patterns which led to the solution of a large part of the material passing between Berlin and Tokyo.

The system was intended by the Germans to be a one-time system to be used for the most important and secret diplomatic messages, and there is every reason to believe that its vulnerability was never suspected by the German Foreign Office, as it was in use for over ten years, during which reliance was placed on a one-part code (re-edited more than once) and no attempt was made to avoid by bisecting or other means beginning stereotypes. In fact, I have seen captured pads bearing on the back as many as eight signatures testifying to the fulfillment of the various security measures in production.

The solution caused such a revolution of thought in the minds of consumers of intelligence that, for about two years after the war ended, if, in reply to queries from higher authority as to prospects in quite other fields of research, I explained our lack of success as due to use of one time pads, I could sense the suspicion that we were not really trying!

The Germans were to a large extent committed for the duration of the war to the main cryptographic systems with which they entered it, and, although there has been much improvement in cryptographic systems since the war ended and this particular way of producing one time pads is hardly likely to be used again, there are important lessons to be learnt from careful study of old systems such as this which presented difficult problems of initial diagnosis.

Brigadier J. H. Tiltman

SECTION I.—THE MECHANICS OF THE SYSTEM

1. INTRODUCTION

The most voluminous German diplomatic system in use during most of the second World War and the one considered most secure by its users was known to the ASA as [redacted] It consisted in the one-time additive encipherment of the main German diplomatic code, a one-part, five-digit 57,000-group code known as the *Deutsches Satzbuch*. From a variety of sources, including cryptographic instruction messages in the solved [redacted] and captured additives, the essential mechanics of the system were known. When the attack on the system began, what remained for solution was the prediction of the unknown additive.

2. ELEMENTS IN THE SYSTEM

The two elements necessary for the processes of encrypting and decrypting in [redacted] are the code book and the pad of additive sheets.

a. The Code Book.—From the first appearance of traffic in [redacted] until 1 January 1942, the German Code Book No. 3 (the third edition of the *Deutsches Satzbuch*) was used. From 1 January 1942 until 19 April 1945, when traffic stopped, the German Code Book No. 4 was used. Both code books were also used during the same period in [redacted] (the double-additive system or the *Grundverfahren*) and in plain code traffic [redacted] The codes have both four-letter and five-digit equivalents for the plaintext meanings, which are well chosen and easily used. Code Book No. 3 contains approximately 31,500 code groups; No. 4 contains approximately 57,500. The repeated use of these codes indicates that the German Foreign Office based its confidence in the security of the system on the encipherment.

b. One-time Additive.—Each sheet of [redacted] one-time additive has 48 five-digit groups arranged in 8 rows of 6 groups each. The sheets were bound into volumes of 100 sheets each. These volumes we refer to as pads; the Germans called them *Baende* or *Bloecke*. Each pad of additive sheets had (1) a designation of whether the volume or pad is in deciphering or enciphering form (*Entzifferung* or *Verzifferung*); (2) a pad number and sometimes a color designation (*Band*

[1] This system, the next most important German system in volume and security to [redacted] was an enciphered code, using the same code as GEE and encipherment by additive taken from a 10,000-line book and superencipherment by additive. [redacted]

[2] The earliest intercepted message in the files of the ASA is dated 1934, but TICOM has revealed 1925 as the earliest possible date, for at that time the Germans purchased the first machine to generate this type of additive.

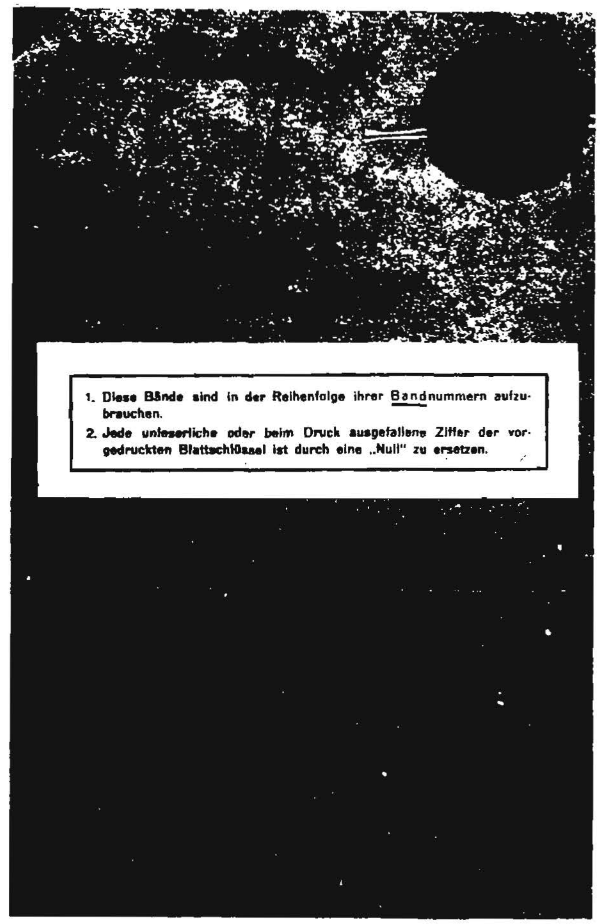
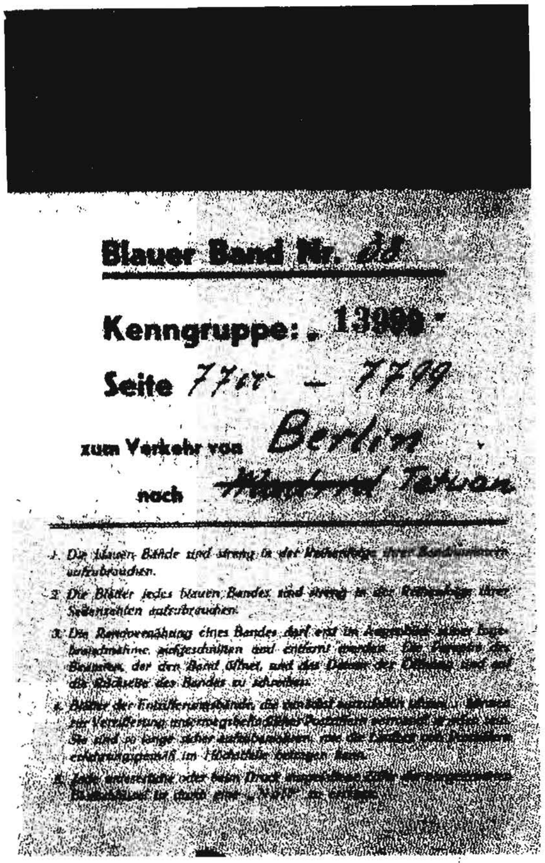


Fig. 1a.—*One type of cover of* [redacted] *pad.*

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36



[redacted]

Blauer Band Nr. 38

Kenngruppe: „13000"

Seite 7700 – 7799

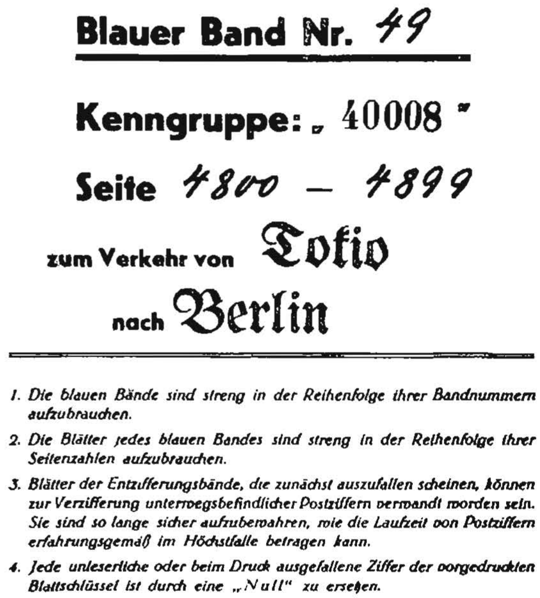
zum Verkehr von Berlin

nach ~~[illegible]~~ Tokyo

1. Die blauen Bände sind streng in der Reihenfolge ihrer Bandnummern aufzubrauchen.
2. Die Blätter jedes blauen Bandes sind streng in der Reihenfolge ihrer Seitenzahlen aufzubrauchen.
3. Die Randvernähung eines Bandes darf erst im Augenblick seiner Ingebrauchnahme aufgeschnitten und entfernt werden. [illegible]
4. [illegible]
5. [illegible]

Fig. 1b.—Another type of cover of a [redacted] pad.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36



Blauer Band Nr. 49

Kenngruppe: „40008"

Seite 4800 – 4899

zum Verkehr von Tokio

nach Berlin

1. Die blauen Bände sind streng in der Reihenfolge ihrer Bandnummern aufzubrauchen.
2. Die Blätter jedes blauen Bandes sind streng in der Reihenfolge ihrer Seitenzahlen aufzubrauchen.
3. Blätter der Entzifferungsbände, die zunächst auszufallen scheinen, können zur Verzifferung unterwegsbefindlicher Postziffern verwandt worden sein. Sie sind so lange sicher aufzubewahren, wie die Laufzeit von Postziffern erfahrungsgemäß im Höchstfalle betragen kann.
4. Jede unleserliche oder beim Druck ausgefallene Ziffer der vorgedruckten Blattschlüssel ist durch eine „Null" zu ersetzen.

Fig. 1c.—A third type of cover of a [redacted] pad.

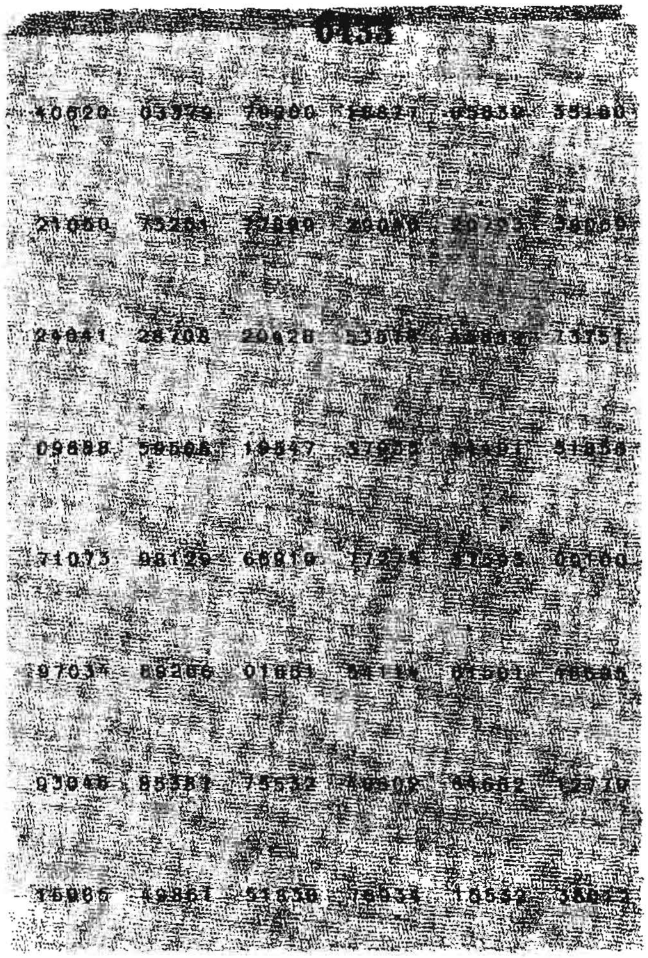


Fig. 2a.—A page of one-time additive. Notice the perforations which permit the destruction of a page as it is used.

1701 **2734**

88975	39765	38800	40284	22791	53812
88286	14678	61703	74155	12916	35381
68545	92218	65668	41955	67504	27963
87990	69874	45380	71843	02355	39983
44696	48947	57279	60712	13030	45629
00066	34555	36206	15427	57169	28332
85772	59723	54631	18966	50044	70126
50351	18051	30869	30388	32924	37572

Fig. 2b.—Another type of one-time additive sheet. Note the two identifying numbers.

Nr. 41 or *Blauer Band Nr. 49*); (3) a series number or a five-digit recognition group (*Serie 52* or *Kenngruppe*: *40008*); (4) the range of the five-digit serial pad numbers (*Blatt 9000–9099* or *Seite 4800–4899*); (5) the circuit and direction for which the pad was to be used (*von Tokio nach Berlin*); and (6) directions what to do in case digits of additive could not be read on the sheet. Each sheet of additive had a four-digit serial number printed in red at the top; and in the case of volumes of additive made up later in the use of the system, there was also on each sheet a four-digit number printed in black to be used as an indicator in transmission. (See figs. 1*a*, 1*b*, 1*c*, 2*a*, and 2*b* for photographs of front matter from volumes of additive and the additive sheets.)

Plain	*Multex*	*12*	*89*	*12. November*
Code	50864	04330	13024	62895
	Schmidt	*Text*	*heutigen*	*Fuehrer-*
	65165	73032	33317	27303
	kundgebung	(Combine two preceding words)	*aus*	*Anlasz*
	43314	00093	07002	04485
	Feirlichkeit-	(Genitive plural)	*9. November*	*wird*
	25266	00147	62570	88382
	Montag	*8 Uhr*	*mitteleuropaeische zeit*	*durch*
	50451	15374	50045	19355
	NP	*D*	*uebertragen*	.
	54454	15475	75481	00001
	Bitte	*Hell-*	*empfaenger*	besetz
	12337	32831	21396	11070
	. Paragraph	*Empfangsbestaetigung*		
	00007	21402		

Fig. 3a.—The encodement of a [redacted] message.

3. ENCRYPTMENT

In the typical process of encoding, the plain text of the message to be sent was first converted into five-digit code groups. (See Fig. 3*a*.)

This code text was then enciphered by the addition (noncarrying) of the key provided on a sheet of the pad, the first group of the code text and the first group of the key coinciding (see Fig. 3*b*).

To prevent wasting an inordinate number of additive groups of a page of additive, the German code clerks were allowed to send up to four final groups of the text of the message in plain code if the words were not compromising. In these cases the last part of the plain text was encoded and the four-letter code groups (not the five-digit groups necessary when additive was to be applied) were re-divided into five-letter groups for transmission, and if the last group was not a five-

	6 0 8 1 ("Black" nonserial number used as indicator in transmission)			4 8 0 6 ("Red" serial number used generally for reference in servicing unreadable messages)		
Code text	50864	04330	13024	62895	65165	73032
Additive	43415	27267	02983	26631	22763	35178
Resulting Cipher text	93279	21597	15907	88426	87828	08100
Code	33317	27303	43314	00093	07002	04485
Additive	34418	11312	91904	11751	45729	92241
Cipher	67725	38615	34218	11744	42721	96626
Code	25266	00147	62570	88382	50451	15374
Additive	96193	96401	39302	02492	03638	62865
Cipher	11359	96548	91872	80774	53089	77139
Code	50045	19355	54454	15475	75481	00001
Additive	41197	09021	58046	03071	95826	70990
Cipher	91132	18376	02490	18446	60207	70991
Code	12337	32831	21396	11070	00007	21402
Additive	24126	99760	39549	00462	93615	87426
Cipher	36453	21591	50835	11432	93612	08828
Additive	76112	31794	36791	20719	93647	48991
Additive	12955	18427	49402	95273	56243	19057
Additive	03267	06903	82387	77072	94364	51578

The cipher text to be sent reads:

93279	21597	15907	88426	87828	08100	67725	38615
34218	11744	42721	96626	11359	96548	91872	80774
53089	77139	91132	18376	02490	18446	60207	70991
36453	21591	50835	11432	93612	08828		

Fig. 3b.—The encipherment of a [redacted] message.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

letter group, the remainder of the five letters was supplied by some or all of the letters of the code equivalent for *Fuellgruppe* or "Null," (GBUE). In other cases of non-comprising final groups in plain code, the code clerk simply used the switch group DESAB (an abbreviation for *Deutsches Satzbuch*) to precede the five-digit groups of plain-code text.

The resultant message text was next provided with indicators immediately preceding, and repeated immediately following, every 48 groups of cipher text; with precedence designation, an external serial message number, the encryption date, and an indication of the number of parts; and with a group count. A signature in plain text and

```
239 S TOKYO 149/147  12  5555  GG AUSWAERTIG BLN
CITISSIME  1289 / 12 DREI TEILE 8174  02639 81659 07956
85939 48685 26308 47853 11286 41910 42614 31842
38532 56204 90819 01340 52580 21846 55788 81680
40543 81611 18082 16648 64097 74961 22132 16000
95721 74528 68240 65719 63094 74997 34632 60272
64582 52761 78619 98643 87016 12308 01555 25010
45664 70203 75327 74842 14154 8174  6324  25564
28846 51755 25081 59206 75145 52845 44377 91167
39264 28248 77504 96052 94435 95560 45226 21426
74440 72488 40649 96107 40713 45989 83861 81931
11527 89486 01205 04547 09455 93265 11120 56672
43753 68929 17859 82386 80935 15828 33178 70263
25440 36918 49504 66061 77232 11517 52247  6324
1430 83983 22498 18532 93369 07021 33245 50303
33817 64618 62777 03804 38037 72960 65333 13752
43812 25686 08147 07804 33827 30292 13760 28628
06500 23227 90150 32227 10888 77189 40335 77997
00780 89164 55177 74974 17600 99487  1430 00037
STAHMER
```

Origin
Destination
Precedence designation
External serial message number
Day of encodement
First "black"* sheet indicator
Repetition of 1st indicator
2d "black" sheet indicator
Repetition of 2d indicator
3d "black" sheet indicator
Repetition of 3d indicator
Group count to last indicator
Signature

*I.e., the indicator used in transmission, distinct from the "red" indicator, used for reference to unreadable messages.

Fig. 3c.—The complete message.

a heading completed the message (see Fig. 3c). This was a typical case. There were of course numerous variations.

4. DECRYPTMENT

For some time it was thought that the German Foreign Office made up complementary versions of the pad sheets for the receiving ends, as was the case in the [redacted] additive, in order to make both enciphering and deciphering processes a matter of addition. When we learned how these sheets were produced, however, we became certain that the process of deciphering was one of subtracting the additive groups from the cipher text as received. The process of deciphering was then simply the reversal of the enciphering process. The cipher text received was written above the additive groups of the deciphering sheet and the additive subtracted without carrying from the cipher text. The resulting text was plain code which the code clerk looked up in the code book and converted into its German equivalent.

5. INDICATOR SYSTEMS

Three main types of indicators appeared in [redacted] traffic. They are: (a) pad-sheet indicators (clear and disguised) and other external numerical indicators, (b) economy-measures indicators, and (c) special indicators.

The characteristics of pad-sheet indicators can be classified on the basis of the two networks on which German diplomatic traffic was transmitted. The traffic on the regular commercial German Diplomatic Network (Clandestine SGDN), as generally disguised.

a. Regular Commercial German Diplomatic Traffic.—[redacted] traffic on the German Diplomatic Network had all indicators in the clear, and could be divided into two types, one having pad-sheet indicators running in series and the other having pad-sheet indicators which did not run in series. The traffic with clear serial pad numbers had the following characteristics in the clear: international call signs, station of origin and destination, message number, date of encipherment, four-digit pad-sheet indicators running in series (preceding each block of 48 groups of five-digit cipher text), a group count, and a signature. The group count was a five-digit group composed of three zeros in the first three positions and two digits giving the number of cipher groups back to the last four-digit indicator. For example, [redacted] preceded the signature. An example of this type of message is presented in Fig. 4. Another type of commercial pad traffic had the

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[redacted]

STAHMER → Signature

Fig. 4.—A typical [redacted] message sent on the GDN with serial pad sheet numbers.

same indicator characteristics with the exception that the pad sheet numbers are three-digit instead of four-digit and that there may be a five-digit discriminant (*Kenngruppe*) preceding either the first pad-sheet number or all of the pad-sheet numbers. An example is given in Fig. 5.

The other type of traffic, that with nonserial indicators, on the regular commercial German Diplomatic Network had the so-called "four-figure repeat" indicators for the pad sheets. The traffic had the international call signs in clear, as well as station of origin and destination, external serial message number, date of encipherment, group count, and signature. The four-figure pad-sheet indicators coming at 48-group intervals did not run in serial order and seemed to be well distributed, apparently at random, among the 10,000 numbers possible.


```
CUD2 DE DGD 10310KCS S3R3 18MY 1508Z US4/05352

S BERLIN 326 379/378 18 1550 ETAT GG 1/50

DIPLOGERMA LISSABON
                                                    → Kenngruppe
1298/17 28200 928 86704 29383 87796 46837 15828 61599 05306
                                                    → Three-digit page number
                4 lines (38 groups) omitted

PGE 2/50 326 DIP
                                                    → Repetition of kenngruppe
38689 11111 49017 28200 929 23506 96441 86833 91296 45153
                                                    → Second page number
                4 lines (40 groups) omitted

PGE 3/50 326 DIP

95877 07289 41301 28200 930 40239 66446 05207 86979 17011

                4 lines (40 groups) omitted

PGE 4/50 326 DIP

56917 29881 93175 28200 931 46157 31954 50747 98719 72825
74208 35782 96920 04759 23833 70194 01169 12858 88069 57837
2001 11444 29707 07687 25715 64649 00021

                        AUSWAERTIG
```

Fig. 5.—A [redacted] message sent on the GDN with serial three-digit indicators.

Because these indicators did not run in series, it was found necessary to repeat them at 48-group intervals so that garbles would give only a minimum of trouble. Therefore, the indicators and repetition of them are spaced throughout the cipher text thus: 4221 . . . . (48 groups of cipher text) 4221 0958 . . . . (48 groups of cipher text) 0958 7203 . . . (48 groups of cipher text) 7203 6466 . . . . (21 groups of cipher text) 0021 (group count back to the last indicator) 6466 SIGNATURE. An example of this type of message is given in Figs. 6 and 3.

b. A Kind of Traffic on Both International and Clandestine Circuits.—Traffic with nonserial pad-sheet indicators also appeared with other characteristics, both on the regular commercial net and the Special German Diplomatic Network. The call signs, therefore, might be either international trigraphic call signs or letter-digit-letter disguises. (Appendix A contains a summary of the system of disguising call signs on the SGDN, some means of penetrating the disguise, and some remarks on the operating signals used.) If the in-

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

ternational call signs were used, then the stations of origin and destination would be in the clear. If the letter-digit-letter disguises were used, no other designation or station appeared.

```
IWHB 88 10/9/43 0945/10/43 13345KCS

DFK DE CUD2 SSS 423 LISBOA 103 10 0005

GERMANY COVT AUSWAERTIG BERLIN
                                                                  → First nonserial indicator
1038 / 09 3015 27562 11297 25633 38421 85585 42075 37711 27165

              4 lines (38 groups) omitted
                                                                  → Repetition of first indicator
61328 77958 3015 1737 32996 71075 39996 40593 47026 18650
                                                                  → Second nonserial indicator
              4 lines (40 groups) omitted
                                                                  → Repetition of second indicator
27960 00047 1737

                    HUENE
```

Fig. 6.—A [redacted] message sent on the GDN with nonserial indicators.

On this particular type of traffic, there usually occurred the special discriminant REMAX, after the external message number and the date of encryptment. All other indicators except the signature usually came in the clear. There was one difference between this type of nonserial indicator traffic and the "four-figure-repeat" traffic, and that was that this type of traffic never seemed to repeat the indicator for checking purposes. An example is presented in Fig. 7.

```
                                                                  → SGDN call sign disguise:
                                                                      AC: Ankara
J2U DE DFE/DOG 9810 KCS S3R3 07JA1832Z USC1/03610/JA              (Note: No stations of
                                                                      origin or destination)
KA 105 WDS 1/50                                                   → Discriminant

REMAX 7430 18258 36965 65987 65966 64754 09366 82695 22359        → First nonserial, unrepeated
                                                                      pad sheet indicator
              4 lines (40 groups) omitted

KA 2/49                                                           → Second indicator
9453 78873 25915 58508 40001 13718 97051 53244 97487 82994

              4 lines (39 groups) omitted

KA 3/06                                                           → Third indicator
3126 97350 04789 23399 95514 00004
                                                                  (Note: No signature)
```

Fig. 7.—A [redacted] message with a REMAX discriminant.

c. Traffic on the Special German Diplomatic Net.—On the clandestine Special German Diplomatic Net,[3] in addition to the REMAX traffic already described, four types of indicators occurred: (1) four-digit indicators disguised by means of conversion measures instituted on 2 April 1940, which remained in effect until 10 April 1943; (2) four-digit indicators disguised by means of conversion measures instituted on 10 April 1943, which remained in effect at some stations until traffic ceased in April 1945; (3) indicators disguised by the chain addition, and (4) indicators derived from the first, second, and last groups of text.

As for the first type, on 2 April 1940, we read in the [redacted] system, a message from Berlin to Dublin giving complete details for the disguise of pad-sheet indicators in [redacted] traffic. On 19 December 1941, a message instituting the same measures of disguise was sent from Berlin to all stations on circular links. (The message from Berlin to Dublin was not complete; therefore, the following transcription of the message is from the 19 December 1941 version.)

```
From:         Berlin                  Intercept Station: 7
To:           Broadcast (Circular)    Intercept Date: 21 Dec '41
Date:         19 December 1941
System:       [redacted]
Message No.:  MULTEX 1095
Keyword:      ZIRIOSIR
Kenngruppe:   20202
```

Confidential Matter B. MULTEX 1095, 19 December 1941.

Section C of the Decree PERS ZB 387, Secret Government Matter/39 (Decree of 1 May 1941)

Telegrams proceeding from Berlin via secret radio channels vary from the customary telegraphic form as follows:

a. The address is omitted.

b. Number, date reference, and signature are secretly enciphered.

c. In the case of special press reports all four figure page numbers are disguised (three-figure page numbers, as provided for the red, yellow, violet, etc., volumes, are not disguised). (Only at posts which use the sparfassung of the sonderverfahren: In using the lower half of a page Berlin omits the open word "zwei".)

[3] The Special German Diplomatic Net (SGDN) was a special private network established by the Germans to carry their diplomatic traffic exclusively; it had its own call signs and procedures.

Conversion of the disguised page numbers into the original page numbers: Look up the four figures of the disguised page number *in order in the following conversion table* and replace each of them by the figure standing to its right in the table.

Conversion Table: 0 = 3, 1 = 7, 2 = 9, 3 = 0, 4 = 6, 5 = 8, 6 = 4, 7 = 1, 8 = 5, 9 = 2.

Under the four figures obtained from this conversion write in order the first four figures of the five-figure group following immediately upon the disguised page number in the telegram. Subtract these four figures according to the method of <u>schluesselsubtraktion</u> (i.e., without carrying tens) from the four figures standing above them. The four-figure number which results is the desired original page number.

Example:

Beginning of a telegram which has arrived with disguised page-number: "7189 13267 etc."

7189 by means of the TAUSCHTAFEL (conversion table) is converted into 1752. 1752 minus 1326 gives the original page number, 0436. . . .

This method of encipherment and decipherment is needlessly complicated, however, because *the same process can be performed in a* single operation by the use of a conversion square, reconstructed in the ASA[4] and called the Old Conversion Square. The cell is identified by row and column co-ordinates (the first and second digits, respectively, of the dinome).

Old Conversion Square

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

[4] Reconstructed *before* contents of MULTEX 1095 were read.—Ed.

Deciphered, the four-digit number 0436 is the original page number, as illustrated. When all pad sheets of a given message have been undisguised, *there should* result a clear series of pad-sheet numbers. This type of traffic has Special German Diplomatic letter-digit-letter-call signs, no stations of origin and destination indicated in any other fashion, no external message number or date of encryptment in clear, but there is a group count at the end of the message giving the number of groups to the last four-figure indicator. A typical message is given in Fig. 8.

Concerning the second type of SGDN message, on 9 March 1943, Berlin sent a message (Multex No. 230) to all stations on the circular links giving the new measures for the disguise of four-figure pad-sheet numbers. These measures went into effect on 10 April 1943. A *transcription of the parts of the message which have reference to* [redacted] follows:

From: Berlin (AUSWAERTIG)

TO: Circular

Date: 9 March 1943

[redacted]

MULTEX #230

Classified Matter B.

In connection with Multex #209 of the 4th.

Section B: <u>Measures for disguising telegrams from other offices forwarded via special channels</u>.

1. In order to prevent foreign authorities from identifying the radio station with the help of telegrams which arrive in the normal, official manner and later must be forwarded to the (department?) or to an *office abroad via special channels*, the following is to be rigidly observed:

2. <u>Plain text</u> or <u>nonsecretly</u> enciphered telegrams arriving via normal official channels are to be secretly enciphered and disguised before being forwarded to another office via special channels.

3. <u>Secretly</u> enciphered telegrams arriving via normal, official channels or via special channels, before forwarding via special channels to another office, are to be deciphered, re-enciphered, (with new keys), and disguised.

4. If the deciphering of such a telegram is not possible at the forwarding office because of the lack of the required secret cipher material, the telegram is first to be disguised in the normal manner so that it consists only of five-digit groups. . . .

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Section C: Removal of the disguise in telegrams sent via special channels.

1. Telegrams arriving from the foreign office.

Conversion Table: 1. Line: 0 2 4 6 8
2. Line: 9 3 7 1 5

The 5 numbers of the second line are to be placed directly under the 5 numbers of the first line.

1. Telegrams arriving from the Foreign Office via special channels have only . . . changes in the otherwise customary external form . . .

2. Only these are not to be disguised.

A. In the case of sonderverfahren [redacted]. The four-digit page numbers . . . are not disguised . . .

3. Undisguising of the page number . . .

A. The four-digits of the disguised page number are to be looked up in the above-mentioned conversion table and are to be replaced by the numbers either above or below them.

B. Each of the first four digits of the first secret-text group, which follows immediately upon each of the page numbers to be deciphered, is to be multiplied by 2. The results of the multiplication—omitting possible tens places which might come out (2 × 0 = 0, 2 × 3 = 6, 2 × 5 = 0, 2 × 8 = 6, etc.)—are written down as a four-digit group and conversion table.

C. The four-digit number as given in B is to be subtracted . . . from the four-digit number obtained in A. The four-digit number thus obtained is the desired original page number.

D. Example: Beginning of a telegram with an enciphered page number: 7189 40856 and so on. 7189 is converted to 4650. The first four digits of 40856, after being multiplied by 2, result in 8060. 8060 is converted to 5019. 4650 minus 5919 gives as a result the original page number 9741.

Again, the same example given in the message can be performed by the four-figure indicator by means of a cipher square, reconstructed in the ASA and called the *New Conversion Square*, given below; the cell identified by the row and column co-ordinates (the first and second digits, respectively, of the digraph) gives the plain indicator.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

	1	2	3	4	5	6	7	8	9	0	
1	3	9	5	1	7	3	9	5	1	7	1
2	0	6	2	8	4	0	6	2	8	4	2
3	9	5	1	7	3	9	5	1	7	3	3
4	4	0	6	2	8	4	0	6	2	8	4
5	5	1	7	3	9	5	1	7	3	9	5
6	8	4	0	6	2	8	4	0	6	2	6
7	1	7	3	9	5	1	7	3	9	5	7
8	2	8	4	0	6	2	8	4	0	6	8
9	7	3	9	5	1	7	3	9	5	1	9
0	6	2	8	4	0	6	2	8	4	0	0
	1	2	3	4	5	6	7	8	9	0	·

Thus, Enciphered indicator	7189
First group of cipher text	40856
Plain indicator	9741

This is the original page number as in the illustration. When all pad-sheet indicators of a given message have been deciphered, there should result a clear series of pad-sheet numbers. This type of traffic has exactly the same external characteristics as the traffic with pad-sheet indicators disguised by the Old Conversion Square. See Fig. 8.

The third type came with only five-digit groups, its pad sheets being disguised by chain addition; it had letter-digit-letter disguised call signs, no external message number, no date of encryptment, no group count, and no signature in clear.

The method of disguise is one based on the fifth GAT[5] of the message. This fifth group is in reality the first group of cipher text, the first four groups being part of the disguised indicator. The *chain sum* is a number formed by adding successively the digits of the in-

[5] Group As Transmitted.

```
STATION 4                      13 AUGUST 1941
                                                         → SGDN Call sign –
                                                           AO – Lisbon
[CIP]  DE DGC  (9880 KCS)   SHEET ONE   S3R3 H 20          Note: No station in
                                                           clear
QGI 221WDS   1/49
                                                         → First disguised indi-
[0746] 98698 24517 87495 43536 34549 13756 95058 34456 04734   cator (yields 4305)

              4 lines (39 groups) omitted

2/49
                                                         → Second disguised in-
[7194] 74203 18482 31272 65510 82912 47592 86736 89420 65497   dicator (yields
                                                           4306)
              4 lines (39 groups) omitted

3/49
                                                         → Third disguised indi-
[9307] 87347 54273 20496 73994 07508 02248 74649 49262 07659   cator (yields 4307)

              4 lines (39 groups) omitted

4/49
                                                         → Fourth disguised in-
[2929] 59949 50860 42716 14618 35362 18572 68872 20759 72143   dicator (yields
                                                           4308)
              4 lines (39 groups) omitted

5/25
                                                         → Fifth disguised indi-
[3319] 67738 54944 66709 29719 34304 88608 02345 39076 95186   cator (yields 4309)
54998 17718 86553 73628 13352 86034 74113 83774 76039 06873
50768 92598 06217 71321 [00023]                          → Group count to last
                                                           indicator
```

Fig. 8.—A [redacted] message sent on the SGDN with disguised serial indicator.

dicator (the first to the second, the second to the third, and so on, until the last which is added to the first) to produce a five-digit number. In the decryptment, such a disguised fifth group is subtracted from the first group of the message; the chain sum of the first group, from the second group; the chain sum of the second group from the third, and the chain sum of the third group from the fourth. The result of these processes will be: first a discriminant, 12345, which indicates that the traffic is [redacted] traffic; second a group composed of a sum check (the first digit) of the pad-sheet number and the four digits of the pad-sheet number; third, a repetition of the second group (sum check and pad-sheet number); and fourth, a *Schlussgruppe* (literally, closing group), composed of the day of the month in the first two digits, a zero, and the group count either to the next set of indicators or to the end of the message. An example follows:

First five groups of message:	39667	87676	15770	66419/	/93493
Chain sum of the 5th group:	27322				(first
Plain discriminant	12345				group of
Chain sum of the first group:		25230			cipher
Sum check and pad-sheet number:		62446			text)
Chain sum of the second group:			53334		
Repetition of sum check and pad-sheet no.			62446		
Chain sum of the third group:				62471	
Date and group count:				04048	
53rd, 54th, 55th and 56th groups:		11608	99026	83223/	/68115
Chain sum of the 56th group:		*49261*			(first
Sum check and next pad-sheet no.		72447			groups
Chain sum of 53rd group:			27689		of cipher
Repetition of sum check and pad-sheet no.			72447		text of
Chain sum of 54th group:				89285	2nd pad
Date and group count:				04048	sheet)

Next, 48 groups following, *beginning to count with the 56th group*—which is real cipher text—there are similar indicators. Groups 104, 105, 106 are the extratextual groups, and group 107 is the first group of cipher text of the next pad sheet and is used to make the first chain sum. The discriminant 12345, does not appear in any of the succeeding sets of extratextual groups for the other pad sheets in the message. Therefore, the number of extratextual groups involved in the disguise of the first pad-sheet indicators is five, and in the digits of all other pad sheets in the message, four. Figure 9 gives an example of messages of this type.

The method of disguising pad-sheet numbers by chain addition went into effect on 10 April 1943, the same date as the introduction *of the new conversion measures for traffic with four-figure pad-sheet* indicators. The messages sent forth are given in the appendix to this section. Berlin sent these messages to all stations on circular links. And, finally, a fourth type of traffic with only five-digit groups was used by stations of the SGDN in 1942 and 1943; it had disguised letter-digit-letter call signs, no stations of origin or destination in clear, no group count in clear, no message number or date in clear, and no indicators in clear.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

```
DFE DE OG J6S  10485KCS  S3R3 QRN  27JN1914Z  US4/10099     SGDN call signs - Ankara

KA 441W 1/50
  1      2      3      4      5                             Group 1 - discriminant
87084  74127  34319  94440  07879  11909                    Groups 2, 3 = pad-sheet
75669  55842  15064  77402  (44 groups omitted)               number preceded by sum
12345 2/9355 2/9355  27048                                    check
                                                            Group 4 - date and group
KA 2/50                                                       count
                                                            Group 5 - first group
                                                              cipher text
                53     54     55     56
20355  82384  24091  93259  42786  63259  89300             Second pad-sheet indicator
                            25748  (42 groups omitted)
             3/9356 3/9356  27048
                      104    105    106    107
28227  22859  55068  01823  58300  58343  97507  89898      Third pad-sheet indicator
                     62576  19053  31305
                     4/9357 4/9357 27048
```

Fig. 9.—A [redacted] message sent on the SGDN with disguised indicator and date and group count preceding the text.

If the first five-digit group of such a message is subtracted from the last five-digit group, digit for digit, the result is the so-called *Schlussgruppe*, containing in its first two digits the date of encryptment; in its third digit, a zero; and in its last two digits, the group count to the position of the last pad-sheet indicator. The pad-sheet indicator for the first pad sheet is found by subtracting the first digit of the second five-digit group in the message successively from digits 2, 3, 4, and 5 of that group. The second pad-sheet indicator results from the same process performed on group 51. The pad sheets when undisguised, should yield a clear series. The example given in Fig. 10 has the original pad-sheet number written above the group from which it results.

6. ECONOMY MEASURES (SPARFASSUNG)

If a message to be enciphered in [redacted] did not happen to be an exact multiple of 48 groups of code (the number of groups on the pad sheet), the sheet was not completely used. The German Foreign Office felt it necessary to set up economy measures for the purpose of making use of all the groups of additive left over on the sheets at the end of messages not exact multiples of 48 groups.

The first of two attempts at using the left-over groups, an attempt to make use of all groups of additive on each sheet, proved unsuccessful after some time because the complexity of the measures confused the code clerks; the second attempt, which proved successful, was designed to make use of half-sheets of additive.


```
DGC DE [FQ (GST)]  S3R3   12740 KCS at 1142 13/3  ----------> SGDN call signs

136 W 1/50
        4278 -----------------------------------------------> First pad-sheet number
[85936] [82056] 69095 88718 34067 73271 91953 45077 42646 72353
                -------------------------------------------> Disguised first-pad sheet
              4 lines (40 groups) omitted                       number

2/50
  4279 -------------------------------------------------------> Second pad-sheet number
[37502] 89741 88619 39994 26356 04618 70617 80632 97342 36302

              3 lines (30 groups) omitted

                                                      4280 --> Third pad-sheet number
74255 98102 21246 60305 87738 55618 56029 41500 66826 [59735]

3/36
42565 27546 14274 46390 58993 01997 95168 01459 32889 88759
07551 10146 58549 64025 52488 12204 93129 55500 87866 06143
83934 69479 38620 49004 74681 00760 01685 74302 05279 65544
70583 46549 10529 80312 30249 [98951] --------------------> Last group of message
                               85936 ---------------------> First group of message
                               13035 ---------------------> Schlussgruppe
```

Fig. 10.—A [redacted] message sent on the SGDN with disguised indicators with the disguised date and group count at the end.

The date for the institution of the first set of *Sparfassung* measures is not certain. The first evidence in the way of external information about these early measures, however, came in a message sent in [redacted] on 3 February 1940:

```
From:   Berlin (CIRCULAR)
To:     Guatemala, Mexico
Date:   3 February 1940
[redacted](Keyword:  ALTAAFEN)
Message Number:  30
```

```
An indicator of the group of the BANDBLATT with which you begin
encipherment is necessary even when the telegram begins with
the first group of a new BLATT. (. . . )
```

The measures were used, apparently, only for the South American, Central American, and Mexican stations. The indicator used for designating the group of the pad sheet was a five-digit group. The first digit of the group indicated which line of the pad sheet to begin with, and the second digit gave the number of the group in the line. The last three digits of the group were nulls selected at random by the clerk. For example, if in the first two uses of the pad sheet, only 33 groups of the sheet were used, the third use of the pad sheet would begin with group number 34. The indicators for such a situation might be 3073 64972 DREI, meaning that the third use (DREI) of pad sheet 3073 was begun with the sixth line, fourth group (16 groups to a line).

Beginning 6 September 1941, however, new economy measures were instituted. The details of these measures came in a [redacted] message of the same date. According to this system, the lower half of each incompletely used pad sheet was to be used beginning with line 5; the word "Zwei" was to serve as a warning of this. The pad-sheet indicators for the *Sparfassung* measures would be like the following: 3089 *Zwei* 21105 i.e., the second use of the pad sheet 3089 began with the first group of the fifth line of the pad sheet and that the first group of cipher text produced by that encipherment was 21105. The measures remained in effect until 15 January 1945.

7. SECURITY CLASSIFICATION

Priority designations, etc.—The following types of external designations receive attention because they figure in the external appearance of [redacted] traffic: (a) security classifications, (b) priority designations, (c) addresses, (d) distribution directions, (e) special discriminants, and (f) special volume and special-use indicators.

a. Security Classifications.—On 22 February 1943, we read in the backlog of [redacted] a message sent on 13 November 1940, containing security classification. The message contained specific definitions of *Verschluszsache A, B,* and *C* (classified matter A, B, and C), categories of classified material which correspond in many respects to our classifications Restricted, Confidential, and Secret. These classifications were enciphered in [redacted] messages and never appeared in the clear. They frequently served as cribs and so deserve mention here.

Previous to 24 April 1941, the designations, *Vertraulich* (Confidential), *Geheim* (Secret), *Strengst Geheim* (Most Secret) and *Geheime Reichssache* (Secret Government Matter) had been authorized to be sent in the clear as classification for material sent in either [redacted] or [redacted] After 24 April 1941, however, the designations *Vertraulich* and *Strengst Geheim* were discontinued, and the system of classification was simplified to one of designating material sent as either *Geheim* or *Geheime Reichssache.*

b. Priority Designations.—On 3 April 1940, the designations *Cito* (Urgent), *Citissime* (Very Urgent), and *Super Citissime* (Super Most Urgent) were authorized to be sent in the clear on messages to indicate the urgency with which they should be decrypted and handled. On 9 June 1941, the designation *Nachts* was specified to be put in the clear on telegrams which were so important that they should be decrypted immediately upon arrival, even though at night. On 23 July 1940, the English designations Urgent, Very Urgent, Most Urgent, Super Urgent, and Super Most Urgent were authorized to be sent in clear only on traffic sent via the *Sonderweg* (the secret government channel, i.e., not commercial, but clandestine channels). Later, the German designations *Dringend* (Urgent), *Sehr Dringend* (Very Urgent), *Sehr Dringend Nachts* (Very Urgent Night), and *Aeusserst Dringend* (Extremely Urgent) were used for both regular commercial transmissions and for transmissions by the clandestine link. On 28 August 1941, The Designation *Emil* was to replace *Citissime* on military situation telegrams, and in very urgent cases both *Emil* and *Citissime* were to be used.

c. Addresses.—Before December, 1939, messages sent to naval attaches (*Marineattaches*) were prefaced with the address *Marineattaches* in the clear. On 12 December 1939, however, it was decreed that three successive identical digits in the third group of the message should indicate that the message was addressed to the naval attache. Traffic to Tangier for 1942 and 1943 had very often the designation *Gernava*, an indication that the message was to be turned over to the German naval attache.

The designations *Milon, Lucie,* and *Maria* (to indicate traffic for the military attache, the air attache, and the naval attache respectively) to be sent in the clear on circular and broadcast traffic were instituted on 3 December 1941, for the most stations and on 19 October 1942, for Buenos Aires. *Maria* was actually never seen in the traffic and *Milon* came later to be used on traffic sent as a matter of course to both the military and air attaches. *Lila* was the designation used for all traffic destined for Von Ribbentrop personally. The distinction between traffic for the embassies and traffic for the consulates lay in the designations, *Diplogerma* and *Consugerma.*

Early in the use of the [redacted] system by the German Foreign Office, a system of distribution directions was set up involving colors. The messages prefaced with the word *Gelb* (yellow), which served both as a kind of indicator and an address, were messages enciphered by means of the so-called *All Schluessel* (universal key) and were to be copied and decrypted by all stations holding the cryptographic materials necessary. The designation *Rot* (red) was used on messages for stations holding the *Ring-Schluessel* (circular key). On *Rot* messages, when stations of origin and destination were not indicated in the clear, a five-digit discriminant (*Kenngruppe*) was used to distinguish among the different circular keys. The designation *Gruen* (green) was used on messages for stations holding a particular *Landes-Schlues-*

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

seln (continental key). Again a five-digit discriminant was used to distinguish among the different *Landes-Schluesseln*. The designation *Blau* (blue) was used with a five-digit discriminant on messages from one particular station to another particular station holding the same *Einzel-Schluessel* (single key). Very early in the use of [redacted] the colors were used for the same purposes as in the [redacted] system. And others such as *Weisz* (white), *Schwarz* (black), *Violett* (violet), *Lila* (purple), and *Braun* (brown) were used probably to indicate traffic for specific correspondents. With the circular designation *Rot* the following address groups were used for specific combinations of stations: 04440, 08822, 17111, 28200, 28868, 33735, 35599, 46444, 57513, 59999, 62400, and 82282. In addition on 26 April 1945, the designation *Silber* was used on messages transmitted directly to Bern after Berlin stopped functioning as a station. The messages were to be forwarded to the place where the Foreign Office had taken up headquarters in Stockholm.

d. Special Discriminants.—All forms of [redacted] were considered the same system, and, therefore, there are no special systems. But there are some kinds of traffic which resemble [redacted] but which cannot be proved to be [redacted] One of the most important is traffic which bore the discriminants *Opera* and *Opera Friend*. Some of the messages with such designations begin with [redacted] encipherment but obviously contain portions which are not [redacted] traffic. Others cannot even be determined to have any portion in the [redacted] systems.

e. Special-Volume or Special-Use Indicators.—Very little is known about the indicators which designated special volumes of pad sheets or special use of the volumes. The group *Lila* already mentioned, was apparently an address for Ribbentrop; it was used in connection with pad sheets mentioned in [redacted] messages as "special" volumes made up specifically for Ribbentrop. The indicators *Salon* and *Aster* seem to have been of the same sort. They were used only in connection with certain pad-number series which stand out distinctly from the regular pads. The indicator *Adler* which appears primarily on traffic to stations in the Far East may actually be an address of military and air attaches because all traffic read up to the present with such an indicator has dealt with the military situation and bore an address of either a military or an air attache. The series of pad sheets with *Adler* as an indicator are distinct from the regular pad-sheet series and therefore should be considered as special volumes.

8. TRAFFIC STATISTICS

Besides all these data about the cryptography and externals of the messages, we had an enormous volume of traffic to work with. From

1934 (when more or less serious interception of German cipher traffic was resumed, as far as can be determined from the traffic on hand) until traffic ceased on about 15 April 1945, our intercept stations picked up 156,065 [redacted] messages involving a total of 357,802 pad sheets. The stations which received a volume of traffic exceeding 1,000 messages for the whole period were the following, in order according to the volume of traffic in terms of pad sheets:

Station	*Messages*	*Pad Sheets*
Tokyo	20,071	54,756
Lisbon	23,113	54,476
Circular	4,843	21,716
Madrid	8,470	19,613
Tangier	6,568	14,073
Athens	5,431	11,335
Buenos Aires	5,563	11,333
Ankara	4,193	9,798
Rio de Janeiro	5,262	9,400
Shanghai	4,620	8,434
Santiago	2,985	6,199
Sofia	2,243	5,012
Bangkok	1,992	4,605
Mexico City	1,994	4,031
Belgrade	1,760	3,915
Bucharest	1,544	3,224
New York	1,536	2,746
Bern	1,016	2,529
Tarabya	1,048	2,462
Hsinking	1,220	2,436
Tirana	1,318	2,378
Fasano	1,236	2,372

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

APPENDIX TO SECTION I

A Message concerning the use of [redacted]

From: Berlin (AUSWAERTIG)

TO: Circular (Tokyo, Shanghai, Peiping, Hsinking, Buenos Aires, Bangkok)

4 March 1943

[redacted]

MULTEX #209

Classified Matter B.

In connection with telegram of the 1st, Multex 199, Appendix to Decree PERS Z B 99 Secret Government Matter /43:
Instructions for Disguise Procedure.

SECTION A:

Disguise Measures in the Transmission of Telegrams via Sonderweg.

I. General.

1. All telegrams prepared at the foreign service posts to be sent by unofficial secret transmission service ("Sonderweg") may consist only of consecutive five-digit cipher groups without any additions whatsoever and must, therefore, be stripped of all characteristics typical of the German cipher telegrams (page number, keywords in the grundverfahren, final groups, etc.); i.e., they must be "disguised."

2. a. All telegrams dispatched via Sonderweg must be completely enciphered by the SECRET cipher process.

b. If, for special reasons, one and the same telegram is sent both via the normal public telegraph or radio channels and via the unofficial "Sonderweg," it is to be differently enciphered for transmission via each of the two channels, i.e., in sonderverfahren, with different pad pages for each of the two channels, in grundverfahren with different hilfszahlen and different zahlenwuermer for each of the two channels. The telegram to be dispatched via sonderweg is also to be disguised.

c. It is permissible to send one and the same telegram in clear or with nonsecret encipherment via an official intelligence channel and simultaneously with secret encipherment and disguise via Sonderweg.

3. External form of the telegrams;

a. Omit address.

b. Message numbers, references and signatures, as well as special additions which are commonly given in clear (cito, citissime, etc.), are to be treated as message text, i.e., are to be enciphered with the secret text. (The indicator REMAX must not be enciphered along with the secret text but should

be put in clear in front of the completely disguised telegram. Special instructions regarding the treatment of this indicator have been issued to the radio officials of the posts concerned.)

c. Indications of the number of parts and the numbers of the separate parts of messages consisting of several parts are to be omitted.

In the grundverfahren, fairly long telegrams are to be divided into parts of which each (save the last) must consist of exactly 48 secretly enciphered code groups.

d. The separate parts of a message consisting of several parts should, after disguising, be joined together without recognizable separation or paragraphing to form a single message.

e. The "final group" of a message, both in sonderverfahren and grundverfahren, is to be formed from the message date (in grundverfahren, the date of the daily key employed) and the group count.

II. The Disguise.

1. Preparatory measures.

Before the secret text groups of each telegram or the first part of a telegram consisting of several parts, put the following in the order indicated and disguise:

a. In the sonderverfahren:

The indicator "12345" (12345) (as an indication of the use of the sonderverfahren), the page number, the repetition of the page number, and the final group (SCHLUSSGRUPPE).

Before the secret text groups of each additional part place the following and disguise: the page number, the repetition of the page number and the final group. At the end of the secret text of the telegram or a part there should be no date of any sort. In the case of telegrams enciphered by the use of several pad pages, the pages should be completely used up.

b. In the grundverfahren:

The indicator of the key book used, the first hilfszahl, the second hilfszahl, and the final group.

Hilfszahlen should not be converted into four-letter code words ("key words"). At the end of the secret text of a telegram or part there should be no date of any sort.

2. Disguise for sonderverfahren:

a. Form the "quersumme" of the four digits of the page number of the first hilfszahl by adding the first, second, third, and fourth digits without carrying (e.g., the quersumme of 4036 is 3). Place the number derived as quersumme in front of these four digits so that a five-digit number is produced.

Form the quersumme of the four digits of the repetition of the page number or the second hilfszahl and place the resulting number in front of these four digits.

b. From the five digits of the first secret text group which immediately follows the "final group" of the tele-

gram or part, form the "kettenzahl" by adding the following digits of the first secret text group without carrying:
First and second digits, second and third digits, third and fourth digits, fourth and fifth digits, fifth and first digits. Write down the result of each of these five additions so that a new five-digit number, the "kettenzahl" is produced, (e.g., the kettenzahl of 72601 is 98618).

c. Add the kettenzahl formed from the first secret text group to the indicator by the method of schluesseladdition.

d. From the five-digit number thus obtained, form the kettenzahl and add this to the repetition of the page number or the second hilfszahl—augmented by prefixing the quersumme--by the method of schluesseladdition.

e. From the five-digit number thus obtained, form the kettenzahl and add this to the final group (schlussgruppe) by the method of schluesseladdition.

f. Example:

A telegram of 59 secret text groups which was enciphered on the 23rd of the month in the grundverfahren with the key book "13131" and by the use of the hilfszahlen 7893 and 3987 for the first part and the hilfszahlen 1642 and 2461 for the second part.

The first secret text group of the first part, "64379"; the first secret text group of the second part, "22061."

Placing the QUERSUMME 7 before the first HILFSZAHL gives 88793. Placing QUERSUMME 7 before the second HILFSZAHL 3987 gives 73987.

The kettenzahl of the first secret text group of the first part, 64379, is 07065. Adding 07065 to the indicator 13131 gives 10196. The kettenzahl of 10196 is 11057. Adding 11057 to the first hilfszahl 77893—augmented by prefixing the quersumme--gives 88840. The kettenzahl of 88840 is 66248. Adding 66248 to the second hilfszahl 73987--augmented by prefixing the quersumme p gives 39125. The kettenzahl of 39125 is 20378. Adding 20379 to the final group 23048 gives 43316. Thus the following groups should be placed before the 48 secret text groups of the first part: 10196 88840 39125 43316.

Placing the quersumme 3 before the first hilfszahl 1642 gives 31642. Placing the quersumme 3 before the second hilfszahl 2461 gives 32461. The kettenzahl of the first secret text group of the second part, 22061, is 42673. Adding 42673 to the first hilfszahl 31642—augmented by prefixing the quersumme--gives 73215. The kettenzahl of 73215 is 05362. Adding 05362 to the second hilfszahl 32461--augmented by prefixing the quersumme--gives 37723.

The kettenzahl of 37723 is 04956. Adding 04956 to the final group 23011 gives 27967. Thus the following groups are to be placed before the 11 secret text groups of the second part: 73215 37723 27967. (Continuation follows.)

Confirmation of receipt.
SELCHOW
Auswaertig

SECTION II.—EARLY ATTEMPTS AT SOLUTION

1. SUMMARY OF ATTEMPTS AT SOLUTION

In July 1940, Dr. Emil Wolff, an employee of the I. G. Farbenindustrie and a passenger on the Japanese steamer *Yasukuni Maru*, suspected of being an agent for the German Reich, was apprehended by a special agent of the Federal Bureau of Investigation, Mr. Richard E. Smith, and Major L. D. Carter of the United States Army. In Wolff's possession was a trunk of secret documents including code and cipher materials, which the F. B. I. searched thoroughly and photographed. This material was forwarded immediately to the SIS (the ancestor of ASA) for study. It included some 3,600 sheets of one-time key.

A standard IBM index (the "XYZ") was made of the one-time key material, and it was diagnosed as "random"; i.e., the number of five-digit coincidences theoretically expected at random occurred. At that time, the [redacted] system had not been broken into, and no information was available from its messages concerning [redacted] Therefore, research on the system was abandoned because there seemed to be sufficient indication that it was a one-time pad system, and that further research without more extensive information and no other cryptanalytic aids would be a waste of time. Later we gradually learned more and more about the system but even when we understood its nature completely and the cryptanalytic problem became merely that of reconstructing the keys, this task for a long time was believed impossible.

In September, 1943, shortly after the completion of the derivation of additive in the second additive book used in the double additive encipherment system, [redacted] research began again on [redacted] This time the point of view in the research and the methods of attack were considerably altered by the fact that much more had been learned about the system from messages read in [redacted] and that more experience had led to a sounder interpretation of "random" applied to text.

Research was resumed in September 1943 and was carried on from that time until January 1944 by one person working full time with the assistance of five people working part time. Then the staff was gradually increased to approximately twenty full-time persons until the initial entry into the system about the middle of November, 1944, when all available personnel with [redacted] experience and with cryptanalytic experience on the [redacted] system were drafted to carry forward the solution and production of the [redacted] system. At the peak of production, the [redacted] unit included 123 persons working full

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

time; emphasis was then put on the production of Berlin-to-Tokyo and Tokyo-to-Berlin traffic in an effort to produce all information of military operational application before the end of the Japanese War. Eventually messages on a number of circuits were read and theoretically all the traffic became readable. Indeed, message texts enciphered with about 14,000 one-time pad sheets were read.

The first attempts at solution were made on the basis of the compromised pads in Wolff's trunk. The second consisted in several attacks on two-deep overlaps after [redacted] messages, read in 1944, had revealed situations under which the German Foreign Office approved the re-use of additive. And the third was the complete IBM index study made of all compromised material. This index of 380,000 cards was completed about the middle of November 1944.

2. THE "XYZ" INDEX OF 1940 COMPROMISED MATERIAL

The first attack was made on the basis of the "XYZ" index. Although it could not be located for subsequent research, and cannot now be found, it was apparently a standard IBM index containing in a single listing every five-digit group of additive on each of the sheets of additive compromised, the total amounting to approximately 170,000 listings. Each listing showed in numerical order the group to be indexed, and a few groups preceding and following. This apparently was examined and evaluated with a view only to determining whether or not the number of five-digit coincidences expected at random actually occurred. Apparently it was not noticed that in certain blocks of the index the digits in certain positions in the groups indexed produced crests in the distribution far greater than those expected to result from thoroughly mixed and evenly distributed text. As a result, the phenomenon which later came to light and proved to be the most important factor in the solution of the system was not observed at the time of the XYZ index.

3. ATTEMPTS TO SOLVE TWO-DEEP OVERLAPS

When personnel were made available for work on the [redacted] problem, it was necessary, first, to begin the enormous task of filing and logging the traffic so that research could progress systematically. At the same time, all information concerning [redacted] accumulated up to that time was studied. In the course of filing and logging traffic and of reviewing the cryptographic information available, three different two-deep overlap situations were discovered: (a) overlaps in several beginning or ending groups between two slightly different versions of a circular out of Berlin or a message sent from one secondary station to Berlin and to another secondary station; (b) overlaps made possible by a message from Berlin on 29 September 1939 in the [redacted]

system authorizing Buenos Aires to use [redacted] Actual overlaps were found in the first two cases, but no traffic was discovered in the third case.

a. Beginning and ending overlaps.—In the first case, it was observed from filing and logging traffic that in some situations where messages were sent from one station to more than one other station, there appeared several groups of cipher text either at the beginning of the message or at the end (or at both places) [redacted]

The difference between the first two textual groups can be accounted for on the grounds that the [redacted] With the cipher groups exhibiting the same sum (1), the assumption is most reasonable.

In the case of the other pair of groups which overlap, the results are somewhat more fruitful. The solution for the one which is followed by the group count "0019" is a signature since the Germans put the signature meticulously at the end of the message; and since the most common final signature on [redacted] messages out of Berlin was *Auswaertig* (Foreign office), the exact signature was assumed to be just that. And the best possible confirmation for the validity of the assumption results from the other version: the group with the highest frequency in all German traffic using the German Code Book is "00007" (PUNKT ABSATZ = Period Paragraph). But at best the recovery is not extensive.

The second example is one involving more groups:

TOKYO-BERLIN 1 July 1943

	Pad Sheet								
	1856	01817	76923	73578	19771	78665	40318	2501	(Same)
		Unsolved							
Additive =				61726	67190	42000	04067	25024	
Code =				12852	52681	36665	46351	00007	
Meaning =	BOTSCHAFT			NANKING	INFORMIERT	LUFTPOST	PUNKT	ABSATZ	

TOKYO-NANKING

	Pad Sheet								
	1856	01152	75112	92764	77750	23383	04064	42364	Same
		Unsolved			67190				
Additive =				61726	67190	42000	04067	25024	
Code =				31048	10660	81383	00007	27340	
Meaning =	HABE			BERLIN	VERSTAENDIGT	PUNKT	ABSATZ	FUELLGRUPPE	

The solution of the two-deep overlap given above appears most likely: (a) [redacted]

b. The Buenos Aires overlaps.—In the second case, the following message was sent in the [redacted] system from Berlin to Buenos Aires on 29 September 1939, providing for the use of the [redacted] The message was read in 1944 in the backlog:


```
From:    Berlin                       CI 881
To:      Buenos Aires                 Translated:
Date:    29 September, 1939           26 April, 1944
System:  [redacted] (Keyword- KEGAFUBA)
No message number
```

In answer to telegram of the 26th #479. [redacted]

1. To make new encoding pages out of the page series 11 (000-499) for immediate use:

a. New numbers: Omit "ROT." Add "6000" to each original page number of three digits.

b. New pages: Copy the printed five-digit figure group from each original page. [redacted]

2. For the usual decoding of corresponding telegrams, therefore, save in order the original pages for #1.

The period of time during which pad sheets were to be used for [redacted] was indicated by the following message also read in the backlog:

```
From:    Berlin
To:      Buenos Aires
Date:    24 November, 1939
System:  [redacted] (Keyword - LUGABORA)
No message number
```

In reply to telegram of the 23rd #765.
1. Thirty BAENDE are expected to arrive there the middle of January.

Several of these Buenos Aires overlaps were found, but they were not solved with any degree of certainty because the shift in [redacted] although apparently an advantage in producing more text, displaced the stereotyped beginning of one of the messages so that there was no reliable check on the solution; i.e., [redacted]

c. [redacted]—The third overlap situation was known as a result of another message read in [redacted]

```
Date:    30 July 1944
Msg. No. 9 (NEBAAFON, Kenngruppe: 59971)
System:  [redacted] (C. I. 966, translated 8/10/44
```


(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

The cipher material in [redacted] used for cipher traffic between the [redacted] Embassy and the consulate there, has been destroyed. Please, therefore, use there only the blocks [redacted]

Traffic between [redacted] with Ankara, however, was not forthcoming.

No plain text of any value was recovered from the two deep overlaps. The value of the work done on them was two-fold: (a) it confirmed the suspicion that Berlin's invariable systematization of procedure in communications would lead to [redacted] conforming to a great extent with the [redacted] which we were thoroughly familiar with in [redacted] and (b) through the discovery of several genuine overlap situations, it led to the suspicion that the German Foreign Office might as a general principle [redacted] thinking that security would not be endangered thereby. The first of these discoveries was of the utmost importance to the actual solution.

4. THE 380,000-CARD STANDARD IBM INDEX OF ALL AVAILABLE ADDITIVE

In the attack on [redacted] it was assumed that the only cryptanalytic method which might produce results was that of [redacted] In studying the [redacted] additive two types of results were held possible; (a) the discovery of further duplication of additive, or [redacted] in which case the system would [redacted] (b) the discovery of patterns in the construction of the additive which might reveal the nature of the method whereby it was generated. The second possibility was suggested by a consideration of the extensive use of the [redacted] system, by the tremendous volume of traffic involved, and by a realization of the problems in the matter of generating random material in an economic, efficient, systematic fashion. If the system was to be assumed to be a legitimate one-time system, the only hope of solution lay in discovering the German's [redacted]

Therefore, when the index of available additive was made, it took the form which would best reveal either [redacted] and a shift of starting point or patterns of similarity in the material. That is, every group of additive available to be indexed was listed together with two groups preceding and five following. It was assumed that since shifts in starting point in [redacted]

[redacted] in the special cases of two-deep overlaps were simply shifts to a different five-digit group, future groups intact. The index, therefore, would reveal additive identity, even though the starting point were shifted. [redacted] Then, in the case of patterns of similarity, it was assumed that a standard IBM index would possibly reveal more obvious patterns if they existed and could be seen.

The additive available for study at the time the index was made up consisted of three different types. The first type was the compromised additive taken by the F. B. I. from Wolff in 1940 (3,600 sheets or 172,800 groups). The second type of additive was what was called [redacted] additive. It was noticed from a study of the logs of the [redacted] traffic that on 15 January 1942 there began to appear [redacted] system (which had been read almost completely) and the [redacted] system. The plain-code version of the [redacted] text of a circular could simply be subtracted from the cipher-text version of the [redacted] circular and additive [redacted] The third type of additive was solved with a fair degree of certainty on two-deep overlaps; about 200 groups of this type of additive were available. We called this [redacted] additive. Eventually, therefore, the index as finished contained appoximately 380,000 groups.

All this additive was thrown into one index which was set up thus:

a	b	c	d	e	f	g				
B6061	5	25	91324	54340	02478	02383	10801	38244	74751	96922
A4356	4	19	33204	71016	02478	97048	16173	08582	34975	68458
A9913	5	25	18352	25072	02478	32473	58971	72212	92414	46097
A7667	8	43	77949	53780	02478	90660	38838	39969	37687	71443
					4	(Total of groups 02478)				
A4278	6	35	63670	90464	02479	32549	89911	60064	71737	86643
A5495	8	47	52204	57355	02480	77263				
C9627	5	29	59032	30422	02480	92387	51010	41676	66075	21002
A3424	8	48	37713	67827	02480					
					3					
B8937	4	16	61560	18406	02481	31980	75885	19568	72658	84771
B6323	5	25	34320	99263	02481	58299	30923	38388	78938	73442
A4190	4	23	64305	63091	02481	66216	86240	86054	53308	30551
					3					

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

a. *Version.*—Originally a designation used to differentiate additive derived for the [redacted] used by the Germans at different periods; it later lost significance.

b. Pad sheet number.

c. Line number.

d. Group number.

e. Groups preceding.

f. Control group (sort column).

g. Groups following.

In this index the significant facts were observed which led to the discovery of patterns in the additive and eventually to such a complete understanding of the structure of the additive that all pad sheets ever used can in theory be reconstructed. In the course of the research, the nature and the essential functions of the [redacted] were also revealed. Then, sometime in February, 1945, after the explanation of [redacted] had already got under way, a paper from British files showed that the idea [redacted] additive apparently originated with a company of British engineers in London from whom the German Government had bought three such devices in 1932 with no provision that its nature be kept secret. Finally the exact nature of the machine was proved from an examination of files captured in Germany.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36