DOCID: 4326479 AHA # 16 [redacted] (14) S-290

Country: U.S.A./GERMANY
Time Frame: 1925 -
Prime Keys: GERMAN DIPLOMATIC System: GEE One-Time Pad (in use since 1925; first intercepted 1934). System mechanics; indicator systems; international & Clandestine traffic; Special German Diplomatic Net. Argentina (Buenos Aires) over-laps Techniques of solution; C/A development. Machine processing. Weakness in German security. TICOM. GEE and GEC messages. IBM. M-1005 Machine. German machine additive generation described.

Source Title: The Solution and Exploitation of German One-Time Pad System, GEE.
Origin: [SIGNAL SECURITY AGENCY]Army Security Agency—published, WDGAS-93 May 47
Pages: 182
Classification: ~~TOP SECRET CREAM~~

ARMY SECURITY AGENCY

WW-II

The Solution & Exploitation of GERMAN One-Time PAD System: GEE

29 May 1947

~~TOP SECRET CREAM~~

B 9103

ARMY SECURITY AGENCY

Washington 25, D. C.

THE SOLUTION AND EXPLOITATION OF THE GERMAN ONE-TIME PAD SYSTEM, GEE

Prepared under the direction of the

CHIEF, ARMY SECURITY AGENCY

May 29, 1947

~~TOP SECRET CREAM~~

WARNING

This document contains information affecting the National Defense of the United States within the meaning of the Espionage Act, 50 U.S.C., 31 and 32, as amended. Its transmission or the revelation of its contents in any manner to any foreign agency or other unauthorized person is prohibited by law.

TABLE OF CONTENTS

FOREWORD

The draft of this paper was prepared by T. A. Waggoner, assisted by Miss Ruth Jache, in late 1945 and early 1946. It was edited by WDGAS-93 Recorder in 1946 and published in 1947 by the same group with a new designation WDGAS-95-E.

ABSTRACT

GEE, the most voluminous German diplomatic system in use during the second World War and the one considered most secure by its users, was solved through the analysis of captured keys which revealed the nature and operation of the additive generating machine so that the specific keys though used once and only once could be predicted in full upon partial recovery through cribs and superimposition to give a new kind of overlap.

SECTION I

The Mechanics of the System

Paragraph

1. Introductory.--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 GEE. It consisted in the one-time additive encipherment of the main German diplomatic code, a one-part, five-digit 57,500-group code known as the Deutsches Satzbuch. From a variety of sources, including cryptographic instruction messages in the solved GEC[1] 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 GEE are the code book and the pad of additive sheets.

---

[1]This system, the next most important German system in volume and security to GEE, 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.

a. The code book.--From the first appearance of traffic in GEE[2] 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 GEC (the double-additive system or the Grundverfahren) and in plain code traffic (GED). The codes have both five-letter and five-digit equivalents for the plain-text 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 GEE 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 from (Entzifferung or Verzifferung); (2) a pad number and sometimes a color designation (Band 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

---

[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.

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 figure 1a, 1b, 1c, 2a, and 2b for photographs of front matter from volumes of additive and the additive sheets.)

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 figure 3a.)

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 figure 3b).

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-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," (QBUE). In other cases of non-compromising 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

Figure 1a. One type of cover of a GEE pad.

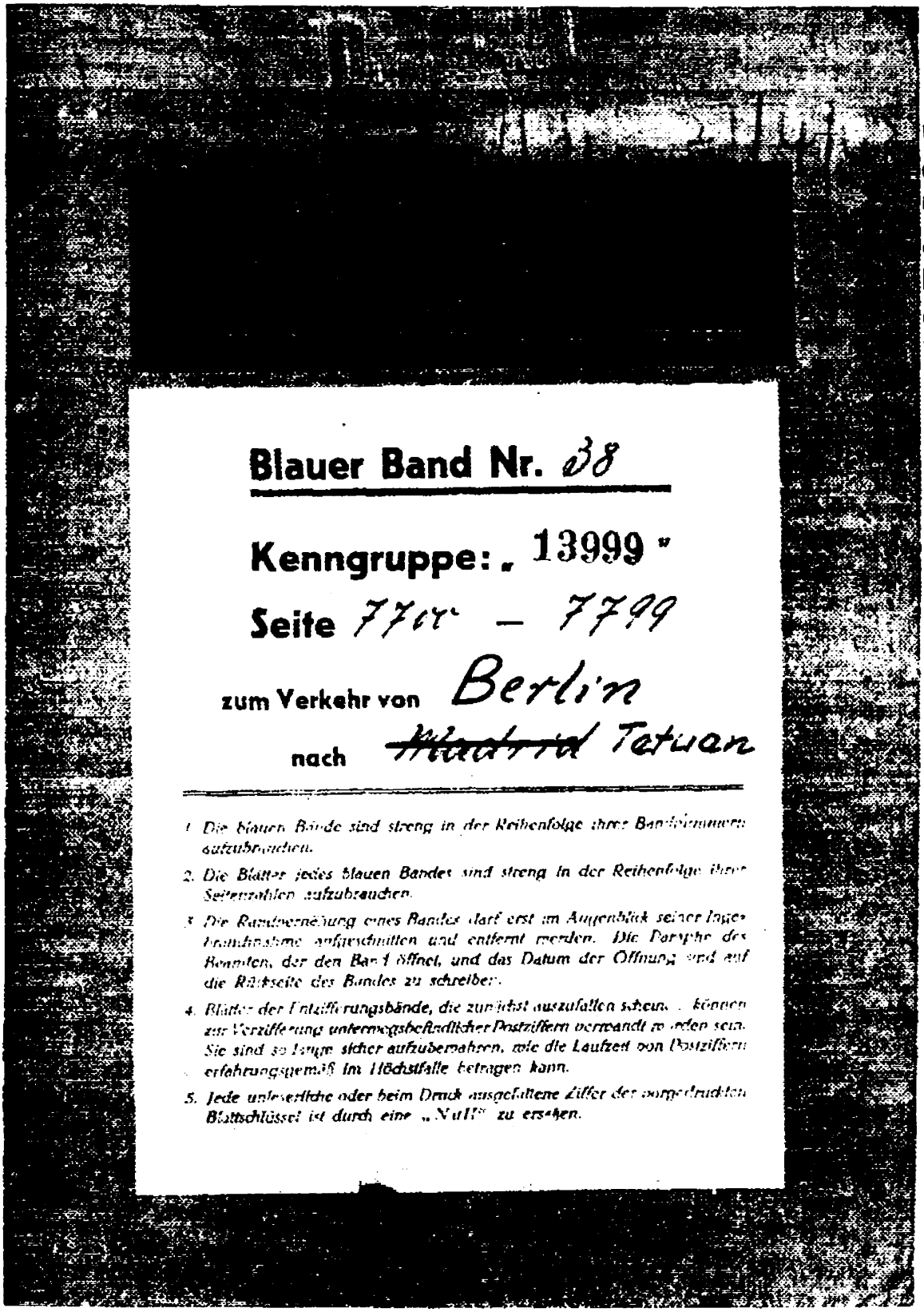
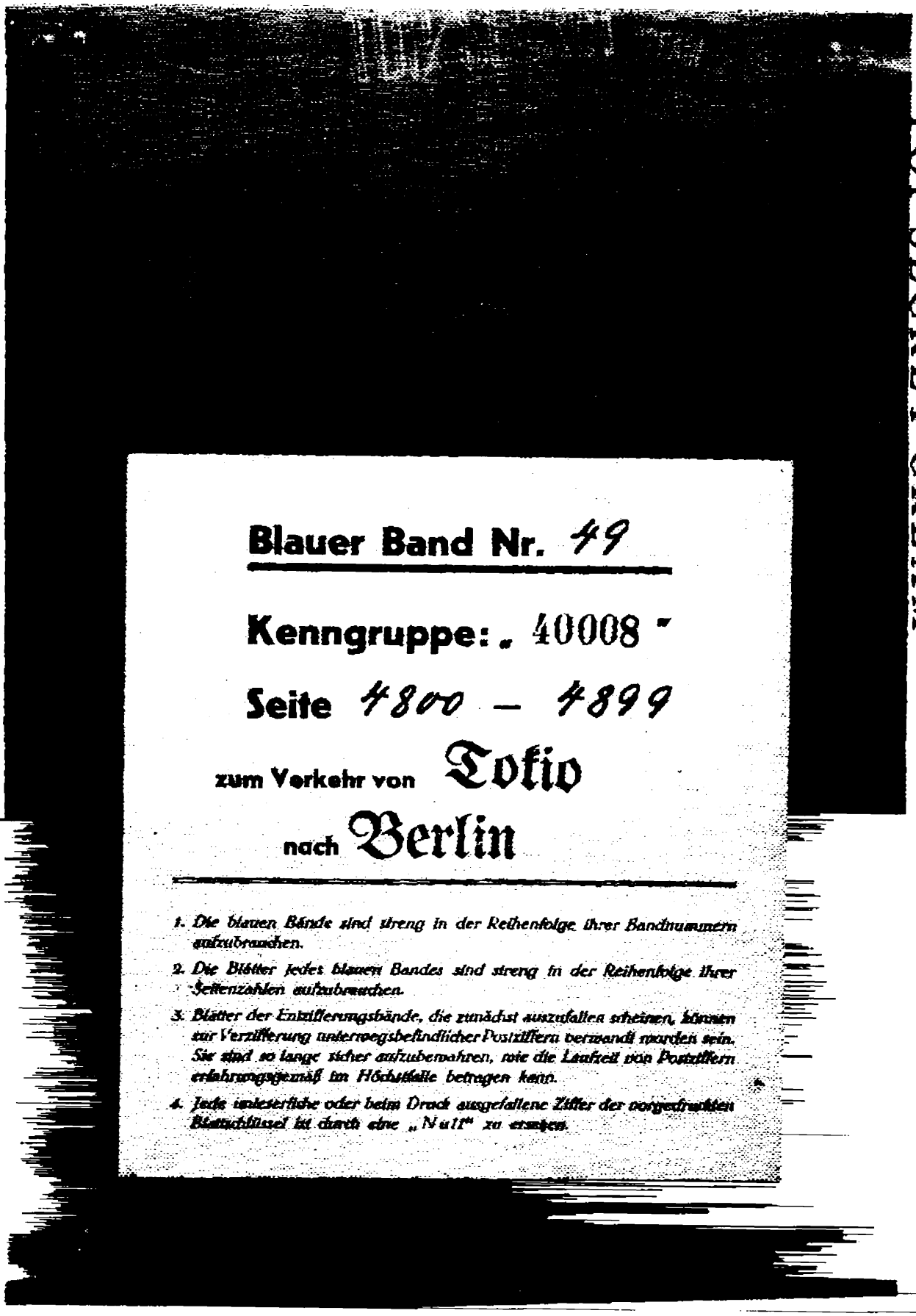


Figure 1b. Another type of cover of a GEE ind.



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.*

Figure 1c. A third type of cover of a GEE pad.

TOP SECRET CREAM

6431

19130	53046	42634	85649	23181	63885
29540	02037	43341	60121	90072	07667
72724	95318	63598	77376	34617	61170
63632	74299	06061	14342	77460	92217
92557	72064	42732	39596	26992	31897
25950	77803	51354	17775	75251	40250
05799	41095	23483	93256	59060	94854
83124	37205	10926	99024	38963	26369

M

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

3101 2732

03781 81281 76499 32606 06422 60683

66793 40780 33218 88431 04865 83660

03338 37589 98113 15066 38918 18520

60003 06483 46344 01902 85590 85753

57771 52512 43888 24820 92705 79341

74755 98288 20139 37900 39780 52846

48483 28118 23043 25649 19102 65255

78446 62378 02780 01172 70619 43961

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

Plain	Multex	12	89	12. November	Schmidt	Text
Code	60864	04330	13024	62895	65165	73032
	heutigen	Fuehrer-	kundgebung	(Combine two preceding words)	aus	Anlass
	33317	27303	43314	00093	07002	04485
	Feierlich-keit-	(Genitive plural)	9. November	wird	Montag	8 Uhr
	25266	00147	62670	86382	60451	15374
	mitteleuropae-ische Zeit	durch	NP	D	uebertragen	.
	50046	19355	54454	15475	75481	00001
	Bitte	Hell-	empfaenger	besetz	. Paragraph	Empfangs-bestaetigung
	12337	32831	21396	11070	00007	21402

Figure 5a. The encodement of a GEE message.

	6081 ("Black" nonserial number used as indicator in transmission)			4806 ("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

Figure 3b. The encipherment of a GEE message.

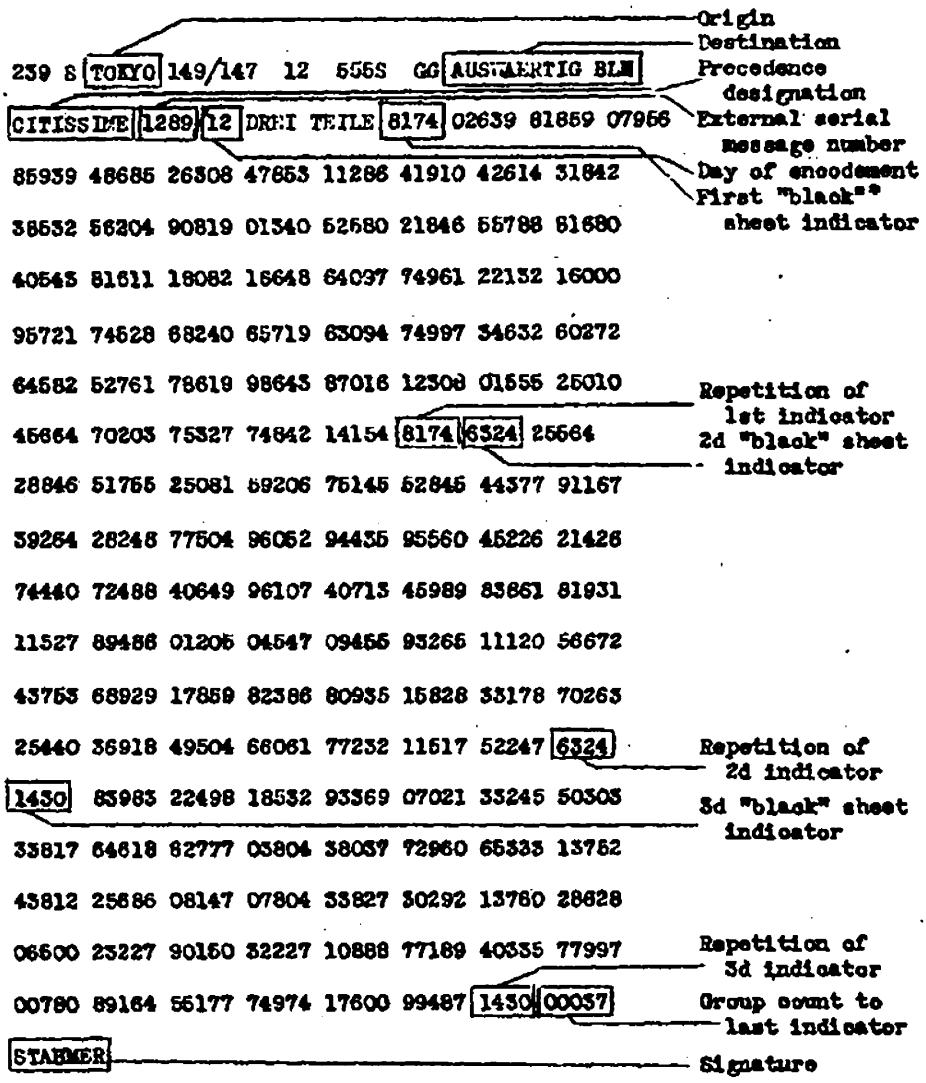
encryption date, and an indication of the number of parts; and with a group count. A signature in plain and a heading completed the message (see figure 3c). This was a typical case. There were of course numerous variations.

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 GEC 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 GKE 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 (GDN) usually had all indicators in the clear; pad-sheet indicators on traffic on the Special German Diplomatic Network (Clandestine SDGN), were generally disguised.

a. Regular commercial German diplomatic traffic.--GKE traffic on the German Diplomatic Network had all indicators in the clear, but it could be divided into two types,



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

Figure 5c. The complete message.

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, the final group 00021 would indicate that 21 groups earlier in the message there appeared or should appear the last four-digit pad-sheet indicator. The group count almost always followed the last group of cipher text and preceded the signature. An example of this type of message is presented in figure 4. Another type of commercial pad traffic had the 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 figure 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 seem to be well distributed, apparently at random, among the 10,000 numbers possible. 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

DGO DE JNE 10160 KCS 21AU2022Z 93R3 US5/22658/59/AU — International call signs; Station of origin

192 S TOKYO 200/199 21 50S ETAT GG CTF CK 1/48 — Station of destination

AUSWAERTIG BERLIN — External message number

2558/11 1249 35421 70196 87298 92034 10380 07796 60956 43417 — Day of encodement; First pad sheet number

4 lines (36 groups) omitted

192 AUS 2/50

08698 25815 76457 65716 1250 18762 21554 30951 66202 70156 — Second pad sheet number

4 lines (40 groups) omitted

192 AUS 3/50

02709 53365 30545 1251 74446 11398 38574 20993 57029 17614 — Third pad sheet number

4 lines (40 groups) omitted

192 AUS 4/49

35004 00070 1252 08616 51987 89631 56716 63747 89129 40682 — Fourth pad sheet number
13832 07285 86943 57120 87378 30909 89079 78835 15212 98785
41040 81925 89055 23893 26043 07596 81464 05905 46746 96043
18769 22671 41610 55145 87180 48183 75451 31492 20678 59244 — Group count to last pad sheet number
81455 81558 76400 47865 84292 92280 90114 00044

STAHMER — Signature

Figure 4. A typical GEE message sent on the GDN with serial pad sheet numbers.

CUD2 DE DGD IO3LOKCS S3R3 18MY 1508Z US4/05352

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

DIPLOGEMA LISSABON

1298/17 28200 928 86704 29383 87796 46837 15828 61599 05306

Kenngruppe

Three-digit page number

4 lines (38 groups) omitted

PGE 2/50 326 DIP

38689 11111 49017 28200 929 23506 96441 86833 91296 45153

Repetition of kenngruppe

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
20001 11444 29707 07687 25715 64649 00021

AUSWAERTIG

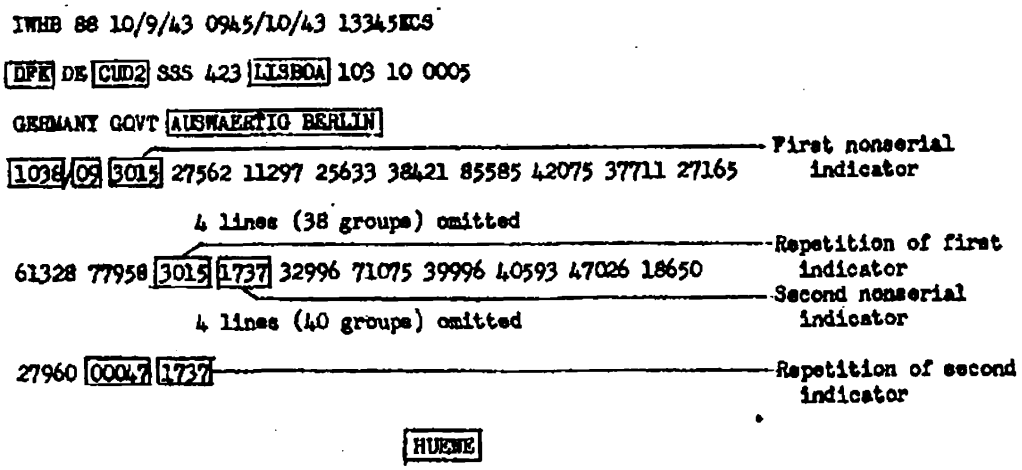
Figure 5. A GRE message sent on the GDN with serial three-digit indicators.

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 figures 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 international 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.

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 the fact that this type of traffic never seemed to repeat the indicator for checking purposes. An example of this type of traffic is presented in figure 7.

c. Traffic on the Special German Diplomatic Net.--On the Special German Diplomatic Net, the clandestine link, 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



17

Figure 6. A GKE message sent on the GDN with nonserial indicators.

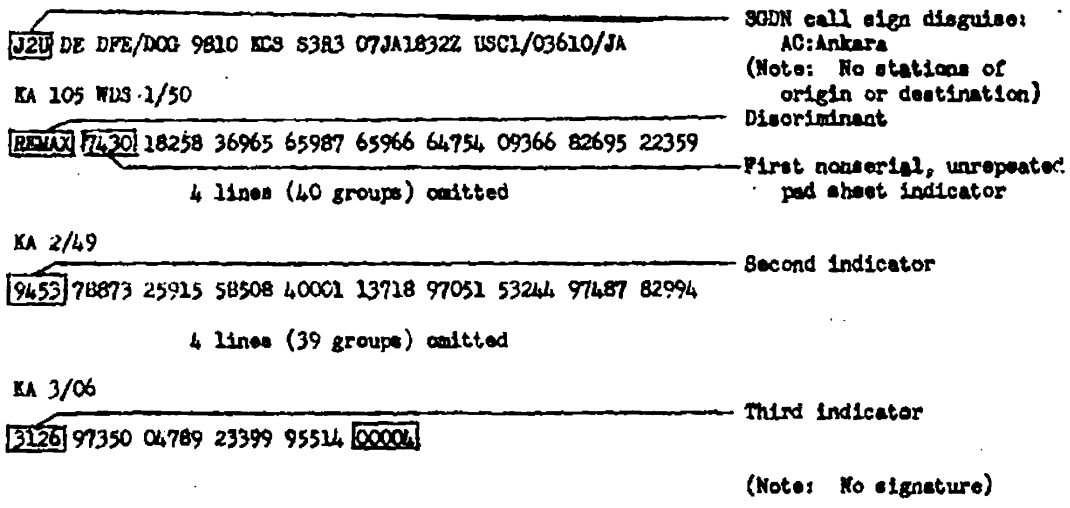


Figure 7 A GEE message with a REMAX discriminant.

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 GEC system, a message from Berlin to Dublin giving complete details for the disguise of pad-sheet indicators in GEE 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:	GEC		
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")

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 SCHLUESSELSUBTRAKTION [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 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	

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 figure 8.

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 indicator

0746 98698 24517 87495 43536 34549 13756 95058 34456 04734 (yields 4305)

4 lines (39 groups) omitted

2/49

Second disguised indicator

7194 74203 18482 31272 65510 82912 47592 86736 89420 65497 (yields 4306)

4 lines (39 groups) omitted

3/49

Third disguised indicator

9307 87347 54273 20498 73994 07508 02248 74649 49262 07659 (yields 4307)

4 lines (39 groups) omitted

4/49

Fourth disguised indicator

2929 59949 50860 42716 14618 35362 18572 68872 20759 72143 (yields 4308)

4 lines (39 groups) omitted

5/25

Fifth disguised indicator

3319 67738 54944 66709 29719 34304 88608 02345 39076 95186 (yields 4309)
54998 17718 86553 73628 13352 86034 74113 83774 76039 06873
50768 92598 06217 71321 00023 — Group count to last indicator

Figure 8. A CEE message sent on the SGDN with disguised serial indicator.

Concerning the second type of SGDN[1] 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 GEE follows:

From: Berlin (AUSWAERTIG)
To: Circular
Date: 9 March 1943
GEC
MULTEX #230
Classified Matter B.
In connection with Multex #209 of the 4th.

Section B: Measures for disguising telegrams from other offices forwarded via special channels.

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

3. Secretly 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.

---

[1] 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.

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. . . .

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 (GEE). 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 x 0 = 0, 2 x 3 = 6, 2 x 5 = 0, 2 x 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 5919. 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 coll identified by the row and column co-ordinates (the first and second digits, respectively, of the digraph) gives the plain indicator.

	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 figure 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 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 indicator (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 GEE 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:

	1	2	3	4	5
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 number	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. The 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 were

DFE DE OG J6S 1Q485KCS S3R3 QRN 27JN1914Z UB4/10099 SGDN call signs = Ankara

KA 441W 1/50

Group 1 = discriminant
Groups 2,3 = pad-sheet number preceded by sum check
Group 4 = date and group count
Group 5 = first group cipher text

1	2	3	4	5		
87804	74127	34319	94440	07879	11909	
75669	55842	15064	77402	(44 groups omitted)		
12345	2/9355	2/9355	27048			

KA 2/50

		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		

Figure 9. A GEE message sent on the SGDN with disguised indicator and date and group count preceding the text.

TOP SECRET CREAM

set 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 Special German Diplomatic Network 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.

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 figure 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 GEE 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 (G5I) 8383 12740 HCS 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 number

4 lines (40 groups) omitted

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 98961 — Last group of message

13936 — First group of message

13035 — Schlussgruppe

Figure 10. A GEE 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 GEC on 3 February 1940:

From: Berlin (CIRCULAR)
To: Guatemala, Mexico
Date: 3 February 1940
GEC (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 (6 groups to a line).

Beginning 6 September 1941, however, new economy measures were instituted. The details of these measures came in a GEC message of the same date (presented in the appendix of this section). 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 classifications, priority designations, etc.--The following types of external designations receive attention because they figure in the external appearance of GEE 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 GEC 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 GEE messages and never appeared in the clear. They frequently served as cribs and so deserve mention here. The message setting up these classifications is reproduced in the appendix to this section.

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 GEC or GEK. 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 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 GEC 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-Schluessel (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 GEE the colors were used for the same purposes as in the GEC 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, 28858, 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 GEE were considered the same system, and, therefore, there are no special systems. But there are some kinds of traffic which resemble GEE but which cannot be proved to be GEE. One of

the most important is traffic which bore the discriminants Opera and Opera Friend. Some of the messages with such designations begin with GEE encipherment but obviously contain portions which are not GEE traffic. Others cannot even be determined to have any portion in the GEE system.

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 GEC messages as "special" volumes made up specifically for Ribbentrop. The indicators Selon 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 GEE 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

More detailed statistics are on file in WDGAS-95-E.

Appendix to Section I

A. Messages concerning the use of GEE
B. Message regulating the economy measures
C. A message setting up the security classifications

A. Messages concerning the use of GEE.

From: Berlin (AUSWAERTIG)
To: Circular (Tokyo, Shanghai, Peiping, Hsinking, Buenos Aires, Bangkok)
4 March 1943
GEC

MULTEX #209

Classified Matter B.

In connection with telegram of the 1st, Multex 199, Appendix to Decree FERS 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 ZAHLENWUERFER 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 or 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 telegram 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 20378 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

From: Berlin (AUSWAERTIG)
To: Circular
March 4, 1943
GEC

Multex #211

Classified Matter B.

The supplement to decree PERS ZB 99 g.RS/43 "Instructions to the VERSCHLEIERUNGVERFAHREN" which is still on the way; upon receipt is to be inserted in Section A, Part II, number 2, between paragraphs D) and F): "E". From the five-digit number thus obtained form the "KETTENZAHL" and add this by the SCHLUESSELADDITION method either to the repetition of the BLATT NUMMER --SEITENZAHL which is to be enlarged by placing before it the QUERSUMME, or to the "second HILFSZAHL." At the end of Section B the following is to be inserted at the end of the text of paragraph 4: "The ZIFFERTEXT thus formed (consisting of the introduction converted into code book groups and of the five digit groups of the disguised telegram to be forwarded which follow them) are secretly encoded further in the usual manner by means of the SONDER or the GRUNDVERFAHREN, like a plain text converted into code book groups. The completed secretly encoded telegram must still be disguised in the usual manner before being sent through the special channels."

Confirmation of receipt.

SELCHOW

From: Berlin (Auswaertig)
To: Circular (Tokyo, Bangkok, Nanking)
13 March 1943
GEC ORFEFIIT

Multex #246

Classified matter B.
In connection with telegram of the 19th, Multex #230.

II. Telegrams arriving from other foreign diplomatic offices.

a. From the five digits of the fifth cipher group of the telegram arriving in disguise form the KETTENZAHL (see Section A, II, 2b) and subtract this from the first cipher group of the disguised telegram by the method of SCHLUESSELSUBTRAKTION. The resulting five-digit number is the "indicator."

(If the indicator is "12345," the telegram is enciphered in the SONDERVERFAHREN; if not, it is enciphered in the GRUNDVERFAHREN.)

b. From the five digits of the first cipher group of the disguised telegram form the KETTENZAHL and subtract this from the second cipher group of the telegram by the method of SCHLUESSELSUBTRAKTION. The resulting five-digit number is, after deletion of the first digit (QUERSUMME), the page number or the first HILFSZAHL.

c. From the five digits of the second cipher group of the disguised telegram form the KETTENZAHL and subtract this from the third cipher group of the telegram. The resulting five-digit number is, after deletion of the first digit (QUERSUMME), the "repetition" of the page number or the second HILFSZAHL.

d. From the five digits of the third cipher group of the telegram form the KETTENZAHL and subtract from the fourth cipher group of the telegram. The resulting five-digit number is the final group of the telegram.

e. If the telegram arriving in disguise consists of more than 52 cipher groups, proceed as above described. The 49th, 50th, and 51st message groups behind the first disguised "final group" (and subsequently every 49th, 50th, and 51st group behind each additional disguised final group) are to be treated as follows:

From the 52nd group behind a disguised final group form the KETTENZAHL and subtract this from the 49th group after the final group; this gives--after deletion of the first digit (QUERSUMME)--the page number as the first HILFSZAHL. From the 49th group behind the same disguised final group form the KETTENZAHL and subtract this from the 50th group after this final group; this gives--after deletion

of the first digit (QUERSUMME)--the "repetition" of the page number or the second HILFSZAHL. From the 50th group behind the same final group form the KETTENZAHL and subtract it from the 51st group after this final group; this gives the next final group.

f. Example:

A telegram from which the disguise is to be removed: 10196 88840 39125 43316 64379 (followed by 47 secret text groups) 73215 37723 27967 22061 (followed by 10 secret text groups).

The KETTENZAHL of the fifth group, 64379, is 07065. The first group 10196 minus KETTENZAHL, 07065, gives the indicator 13131 (since the indicator is not "12345," the GRUNDVERFAHREN is used). The KETTENZAHL of the first group, 10196, is 11057. The second group, 88840, minus KETTENZAHL, 11057, gives 77893; after deletion of the first digit (QUERSUMME), the first HILFSZAHL = 7893. The KETTENZAHL of the second group, 888840, is 66248. The third group 39125, minus KETTENZAHL, 66248, gives 73987; after deletion of the first digit (QUERSUMME), the second HILFSZAHL = 3987. The KETTENZAHL of the third group, 39125, is 20378. The fourth group, 43316, minus KETTENZAHL, 20378, gives the final group 23048.

The KETTENZAHL of the 52nd group, 22061, after the above final group is 42673. The 49th group after the final group (73215) minus the KETTENZAHL, 42673, gives 31642; after deletion of the first digit (QUERSUMME), the first HILFSZAHL = 1642.

The KETTENZAHL of the 49th group after the final group (73215) if 05362. The 50th group after the final group (37723) minus the KETTENZAHL, 05362, gives 32461; after deletion of the first digit (QUERSUMME), the second HILFSZAHL = 2461.

The KETTENZAHL of the 50th group after the final group (37723) is 04956. The 51st group after the final group (27967) minus the KETTENZAHL, 04956, gives the final group 23011.

(End of the Appendix to Pers Z B 99, Secret Government Matter / 43.)

Confirmation requested.

AUSWAERTIG

SELCHOW

B. A message regulating the economy measures.

From: Berlin
To: Tokyo
6 September 1941
GEC (Keyword: UFINALOT)
Message No.: 3

Intercept Station: 1
Date Intercepted: 6 September 1941
Date Translated: 6 March 1943

Classified Matter C. For the purpose of stretching supplies and better use of BANDBLAETTER, in the future.

1. Of BANDBLAETTER, less than 4 lines of which were used in enciphering or deciphering, the lower half (5th to 8th lines) is to be preserved. The latter is to marked with the BLATTNUMMER of the whole BLATT, in addition to the appended word "ZWEI" as well as "Enciphering" or "Deciphering," corresponding to the original utilization purpose.

These lower halves of the BLATT are used again, always beginning with the first group, namely for enciphering the next telegram or deciphering a correspondingly marked incoming telegram, depending upon their original utilization-purpose. The lower BLATT halves should not be used for postal traffic.

As an indication for the decipherer that in the encipherment of a telegram the first group of the 5th line of a BANDBLATT was used first, the encipherer should place at the head the original number of the BANDBLATT with the clear word "ZWEI" which was written on the margin.

When using the SONDERFUNKWEG and VERSCHLEIERUNGSVERFAHREN [Special Radio Channels and Disguise Measures] the word "Zwei" is omitted. Berlin will operate in the same manner.

2. BANDBLAETTER of which more than four lines were used in the encipherment or decipherment are not to be preserved for further use.

3. Economy Measures go into effect immediately after sending confirmation of receipt of this decree.

Confirm receipt.

SELCHOW

C. A message setting up the security classifications.

From: Berlin		Date Intercepted:	18 November 1940
To: Circular		Date Received:	19 November 1940
13 November 1940		Date Translated:	22 February 1943
GEC (Keyword: ASOTOGBA)		Intercept Station:	1
Msg. No.: MULTEX 418			

Classified matter sent by enciphered post or telegram will in the future receive the following headings:

1. For Secret Government Matter:

a. "VERSCHLUSZSACHE A." This designation signifies: "For the Mission Chief or his representative in person. Secret Government Matter, to be deciphered personally. Strictly secret--Answer by courier or Secret cipher," or

b. "VERSCHLUSZSACHE B." This designation signifies "Secret Government Matter. Strictly secret. To be deciphered only by person authorized to decipher secret government matter. To be brought to immediate attention of Mission authorities. Answer by courier or secret cipher."

2. For all other classified matter: "VERSCHLUSZSACHE C." Secret. To be deciphered only by persons authorized to decipher "VERSCHLUSZSACHE." Answer by courier or secret cipher."

Please appoint special officials for decipherment of postal and telegraphic ciphers designated by 1 b or 2 and take care that other officials or employees have no access to such messages.

The code clerks are to be instructed to convert the short forms on messages into the long forms above when deciphering. Confirm receipt.

SELCHOW

BRP9103

SECTION II

Early Attempts at Solution

9. 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 five-digit coincidences theoretically expected at random occurred. At that time, the GEC system had not been broken into, and no information was available from its messages concerning GEE. 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, GEC, research began again on GEE. 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 GEC, GEZ, and GED 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 machine-cipher experience and with cryptanalytic experience on the GEC system were drafted to carry forward the solution and production of the GEE system. At the peak of production, the GEE unit included 123 persons working full 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 GEC 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 available additive, including the previously studied 1940 compromised material. This index of 380,000 cards was completed about the middle of November 1944.

10. 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 also 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.

11. Attempts to solve two-deep overlaps.--When personnel were made available for work on the GEE 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 GEE accumulated up to that time was studied. In the course of filing and logging traffic and of revieving 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 GEC system authorizing Buenos Aires to use pad sheets for two messages for a short period during which the new pad sheets which they needed would arrive from the Foreign Office and providing for a repagination of the sheets; (c) overlaps made possible by a message from Tarabya (Therapia) to Izmir on 30 July 1944 authorizing Izmir to use pad sheets for traffic with Tarabya which had already been used for other traffic with Ankara. 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) which differed in the several versions of the message, whereas, most of the text of the message was identical in all versions. These situations were, of course, tantalizing, representing only two-deep overlaps which could not have certain, unique solutions. But it seemed that attempts to solve these two-deep overlaps would possibly yield beginning and ending cribs. Two cases of the sort are shown below:

	Indicators		Group Count
BERLIN-ANKARA 7 Apr. 1943	04440 555 37713	/17 groups identical/ 02397 /00019	
	[No unique solution. Probable solution: some number]		Additive = 04335 Code = 08062 Plain = AUSWAERTIG
BERLIN-ISTANBUL 7 Apr 1943	04440 555 98814	/17 groups identical/ 04332 89491	
			Plain = 0007 PUNKT ABSATZ

The difference between the first two textual groups can be accounted for on the grounds that the Ankara and Istanbul number series were different. Moreover, all the code equivalents of numbers in the German code book (the Deutsches Satzbuch to underlie GLE) have the characteristic that the units digit of the sum of the digits is the same, 0; and when the same number (additive) is added to two numbers with such a property they still have the property, though the sums differ. 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 "00019" is a signature since the Germans put the signature meticulously at the end of the message; and since the most common final signature on GEC 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) GEC messages on lateral circuits often began or ended with an explanation to the receiving station that Berlin had been notified or informed of the information in the message; (b) in each of the two versions,

the station receiving the other version appeared; (c) the plain group 00007 usually appeared after the introduction of a message and before the text began; when this plain group is assumed for the top version, the code group for FUELLGRUPPE (filler group) results in the other exactly at the point where the identical text begins because of the necessity for making identical text in order to obviate an isolog where the text of the message is compromising.

b. The Buenos Aires overlaps.--In the second case, the following message was sent in the GEC system from Berlin to Buenos Aires on 29 September 1939, providing for the use of the same pad sheets for two purposes for an undefined period in the future. 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: GEC (Keyword- KEGAFUBA)
No message number

In answer to telegram of the 26th #479. In future use pages of the ROT volumes for both following purposes:

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, beginning with the 16th group, putting the first 15 groups at the end.

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 two purposes was indicated by the following message also read in the backlog:

From: Berlin
To: Buenos Aires
Date: 24 November, 1939
System: GEC (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 starting point in the use of the additive, 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., since one stereotyped beginning was displaced so that it did not overlap with another stereotyped beginning, the type of text which did occur as overlapped with a stereotyped beginning was not so reliable a check as another stereotyped beginning would have been.

c. The re-use by Izmir.--The third overlap situation was known as a result of another message read in GEC.

From: Therapia
To: Izmir
Date: 30 July 1944
Msg. No. 9 (NEBAAFON, Kenngruppe: 59971)
System: GEC (C. I. 966, translated 8/10/44)

The cipher material in THERAPIA used for cipher traffic between the THERAPIA Embassy and the consulate there, has been destroyed. Please, therefore, use there only the blocks used last month for other traffic with ANKARA.

Traffic between Tarabya and Izmir using blocks of additive already used for other traffic 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 stereotyped beginnings and endings of messages in GEE conforming to a great extent with the stereotyped beginnings and endings which we were thoroughly familiar with in GEC; 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 re-use so-called one-time additive with repagination, thinking that security would not be endangered thereby. The first of these discoveries was of the utmost importance to the actual solution.

12. The 380,000-card standard IBM index of all available additive.--In the attack on GEE, it was assumed that the only cryptanalytic method which might produce results was that of studying all available key. In studying the GEE additive two types of results were held possible; (a) the discovery of further duplication of additive, or re-use of the same additive, in which case the system would cease, technically to be a one-time pad system; (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 GEE 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 Germans' weakness in being systematically unsystematic. In material which is made apparently unsystematic or "random" in a systematic fashion, there is always a chance that the material may reveal in itself the nature of its generation.

Therefore, when the index of available additive was made, it took the form which would best reveal either re-use of additive with repagination 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 re-use of the additive in the special cases of two-deep overlaps were simply shifts to a different five-digit group, future shifts when additive was re-used would leave five-digit groups intact. The index, therefore, would reveal additive identity, even though the starting point were shifted. It was assumed also that the additive would be read from the pad sheets in the same normal fashion as in the first use. 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 hypothetical additive. It was noticed from a study of the logs of the GEE traffic that on 15 January 1942 there began to appear circulars, which were a series of isologs between the GEC system (which had been read almost completely) and the GEE system. The plain-code version of the GEC text of a circular could simply be subtracted from the cipher-text version of the GEE circular and additive was available for study since the same code book was known to be used for both systems and since the plain texts were apparently identical. This series of isologs continued from 15 January 1942 until approximately the middle of November 1944. Some 207,000 groups of hypothetical additive were thus accumulated. 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 real additive. Eventually, therefore, the index as finished contained approximately 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	35072	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	

a. Version--Originally a designation used to differentiate additive derived for the same pad-sheet number 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 machine which generated

the additive were also revealed. Then, some time in February, 1945, after the explanation of GEE had already got under way, a paper from British files showed that the idea for the machine used to generate GEE 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.

SECTION III

The Solution of the Generation Scheme in Compromised Material

13. Introductory.--With such extensive data at hand concerning the cryptography of GEE, as are given in Section I, the cryptanalytic problem was reduced to one of key reconstruction. Of the two routes to solution, the superimposition of messages and the discovery of a system of generation, the first had been found unrewarding, and the second remained to be investigated fully. The initial frequency abnormalities which made the solution of the system possible through the second method were discovered in the additive captured from Dr. Emil Wolff in 1940. The compromised material was marked SERIE 50 and involved pad sheets numbered from 5000 through 5499, 5900 through 6999, and 8000 through 9999. But the solution which yielded the necessary sequence to begin the reading of current traffic depended on

the hypothetical additive, recovered through cribbing. In the following discussion of this solution, an attempt has been made to discuss the steps in chronological order, but since many phases of the solution progressed simultaneously, a strictly chronological order has not been possible. Moreover, this solution was characterized by a long and laborious series of observations which, only shortly before the final steps, could be explained on the basis of any hypothesis, and finally, the complete solution of the principles of generation of the additive (discussed in this section) was accomplished before production of readable text from traffic.

14. Random five-digit coincidence in the key index.--In the examination of the complete additive index, it was first necessary to determine whether there were any exact repetitions of pages of additive and whether in the absence of such repetitions the index of coincidences of five-digit groups was what one would expect in absolutely random digit text.

In the first case, some repetitions were noticed, but all of them could be accounted for as duplicate derivations of additive from cribs. In the second case it was readily decided that, from the point of view of five-digit coincidences, the index was no higher than that to be expected from a chance distribution of these groups. That is, since the listing contained something like 380,000 entries, and since 10,000 five-digit numbers are possible, one would expect at random an average of about 3.8 occurrences of each possible five-digit number. Fifty sheets of the index were pulled at random from the 00000-09999 volume and were found to contain 3,796 listings involving 1,083 different numbers, with an average of 3.5 occurrences of each number listed. In addition, a thorough visual examination of the total index failed to reveal any abnormal violations of the expected distribution given by Poisson in his Exponential Binomial Limit. Therefore, for practical purposes the additive as listed in the complete additive index was considered from the point of view of five digit coincidence.

15. Abnormal single-digit coincidences in the compromised material.--Examination of the complete additive index, however, revealed several sheets on which the distribution of the digits in some positions in these consecutive additive groups was quite obviously not random. Since the average number of listings per sheet of the additive index is approximately 76, and the number of positions in which an additive group may occur on a sheet of the pad is 48, one would expect at random an average of about 1.58 occurrences of each of the 48 pad positions on any sheet of the index. But actually some positions appeared far more frequently than others. A typical sheet is shown in figure 11. A frequency count of the numbers identifying these positions on this sheet by group and line number showed considerable abnormality (circled). Below is the distribution:

Line No.	1						2						3					
Group No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Frequency	0	0	2	0	2	(10)	1	1	2	1	2	1	(6)	1	(6)	0	1	0

Line No.	4						5						6					
Group No.	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Frequency	1	1	3	0	0	(5)	0	2	0	3	2	0	2	0	0	0	2	1

Line No.	7						8					
Group No.	37	38	39	40	41	42	43	44	45	46	47	48
Frequency	2	0	2	1	3	1	1	0	3	2	1	0

Next, two lines of additive from one of these families revealed by the crests (e.g., line 1, group 6) were examined. At once a very high percentage of single-digit coincidence appeared; for example:

A[401 1 06 93773 52386 02249 47379 36735 21746 49757 28387
A[842 1 06 80770 60319 02263 67377 66635 20742 79757 28357

In such a situation one would expect at random an average of coincidence of about 4 digits out of the 40. In this situation we have 23 digits hitting. This was undeniably a nonrandom situation.

Line no.	Group no.									
B8680	1	06	53662	07641	02247	09015	60348	70369	10297	07530
A3399	4	19	52924	93302	02247	81079	99113	51592	53773	00107
A5569	8	46	54951	53930	02247 4	22386	10594			
B5469	8	47	98261	73455	02248	23709				
A0651	3	15	65078	50829	02248 2	32738	41843	26788	89803	41429
A8401	1	06	93773	52386	02249	47379	36735	21746	49757	28387
A9985	6	35	57575	41064	02249	56343	70239	59670	58047	40805
A0269	2	10	00799	96412	02249	85495	89910	48379	96134	09657
A9812	4	24	38085	41893	02249	85038	65484	33114	41210	65070
A5345	3	13	12872	90684	02249	72191	86672	90400	60822	82171
A5026	1	06	66507	70117	02249	69743	36623	83955	71750	58149
A6383	8	43	70954	72532	02249 7	20193	20404	57633	42428	75115
A7942	1	03	12047	72590	02250	17495	03947	69573	68220	37417
A7294	7	39	57098	64640	02250 2	00562	52952	50988	92504	70428
A0085	1	05	69205	79858	02251	60942				
A5182	3	15	26513	62086	02251 2	61864	30369	10678	34812	29963
A8804	7	40	22771	01086	02252	67079	00319	54716	50914	28583
B6438	7	41	36779	65284	02252	54004	88475	94355	58030	99564
A5452	6	36	75156	38710	02252	76534	93801	18585	59235	15672
A3818	2	09	85858	70070	02252	03208	46038	69408	95639	02909
A8654	6	31	87097	76585	02252 5	47860	67169	56763	91507	81909
A0075	1	05	94354	01725	02253	.....	74803	72902	35552	24126
A9619	3	13	90834	99086	02253	62115	68961	90716	53594	87331
B7248	2	12	12821	18366	02253	20713	38220	81145	59523	03646
A6845	5	29	60338	10964	02253 4	26473	59173	54640	61370	05091
A8830	8	45	09257	96136	02254	70325	32040	62560		
A5171	3	15	79887	62846	02254 2	69938	54396	47788	30377	98689
A2352	2	11	60297	22065	02255	53289	39731	76297	51951	60506
A9529	3	13	11871	65584	02255	91111	45562	77483	50827	67131
A5353	4	24	66111	07564	02255 3	84338	68464	63186	41484	66080
A9105	1	06	46969	83390	02256	55360	18685	70792	79745	28345
B5957	1	06	03745	50534	02256	94398	41222	86413	00603	32725
A3752	3	17	67453	36419	02256	61644	68534	40927	28293	03147
B6926	7	41	98799	31703	02256	24275	86612	76154	34538	59904
A9165	1	03	67135	33123	02256	70972	92825	70460	77589	14746
A5983	4	24	93282	45811	02256 6	56896	68824	61752	27417	89080
A9088	7	41	18244	91452	02257	70175	77597	99343	46974	33730
A7940	3	13	16491	33837	02257	75770	26385	25330	25250	28516
A6883	8	45	09056	56833	02257 3	00320	72346	72570		

Figure 11. A sheet from the index (continued on the next page).

Area no.	Group no.									
A5103	4	24	18083	41861	02258	15897	68214	29872	67485	14454
A5235	6	31	27817	71254	02258	85775	86232	30484	37618	79900
A6111	8	45	47769	40045	02258	71803	45087	75567		
A7094	5	28	35612	16310	02258	71950	91670	47777	29158	87650
					4					
A8689	7	37	20705	25893	02259	51489	08345	94350	19351	44135
B6699	3	14	60285	50963	02259	45819	92966	97948	41449	59783
A9916	1	06	72565	83375	02259	75365	68785	71796	49745	28355
A3559	4	20	06665	53784	02259	11344	98656	63385	94615	67844
A4126	5	28	60462	22460	02259	56745	91178	98677	24050	22677
A6287	3	13	96834	90086	02259	72111	47961	90706	53592	82331
					6					
A6411	7	42	29006	84429	02260	86166	48803	57423	97313	02030
A9346	4	21	11463	91040	02260	66394	60022	90515	43104	03281
A9164	5	29	52053	36812	02260	96387	50770			
A3697	8	46	44327	85999	02260	14220	91165			
					4					
A6542	2	09	55095	68440	02261	89946	93364	36056	82091	27153
B8067	3	15	30102	48083	02262	23274	80759	17509	88094	06779
A8842	1	06	80770	60319	02263	67377	66635	20742	79757	28357
A9113	1	06	16967	23385	02263	63395	31384	78794	69745	21431
					2					
B6739	1	06	13777	52391	02264	57370	76835	24617	14056	28877
A7665	3	13	07486	10114	02264	65533	84907	61258	92147	02932
					2					
A9659	3	15	26863	66028	02265	69819	20806	47812	10870	22033
B5969	1	06	85763	17508	02265	47490	39728	89322	39280	67871
A7579	7	37	44767	98908	02265	77707	95513	33150	46314	66580
A6843	2	11	15794	95889	02265	09641	29134	52898	96564	64981
					4					
B6945	5	28	19822	13329	02266	87929	90504	42402	58248	67270
A8048	4	21	52208	92231	02268	39344	77521	99167	96316	05381
B5470	6	35	67110	40652	02269	89551	98881	54330	92149	69495
A9604	3	15	33555	42216	02269	69433	54829	10537	74417	26244
B8405	5	26	64700	83007	02269	79578	74826	16694	38717	57322
A0826	2	08	86351	44135	02269	CC141	45260	53970	93621	71712
A9335	4	21	40489	96126	02269	13644	27521	86055	73316	67385
					5					
A1988	7	39	50616	25544	02270	68807	52061	44871	62824	31784
A9387	4	24	58983	03583	02270	59496	62894	93238	27180	83010
B8311	2	07	93015	06196	02270	66839	53378	59067	26236	63450
A8449	5	26	98426	44004	02270	96032	70801	05494	40580	79122
					4					

Figure 11. A sheet from the index (continued from previous page).

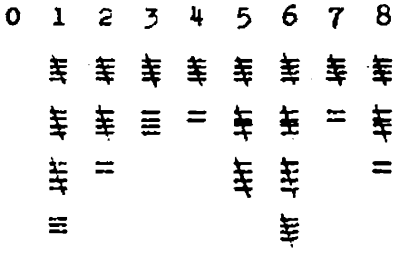
The two pad sheets involved in the two listings shown above were then juxtaposed in entirety to determine whether the high percentage of coincidence continued throughout the 48 groups. The two pad sheets are shown below overlapped group for group:

Pad Sheet	Line No.	1	2	3	4	5	6
8401	1	77104	29141	99136	93773	52386	02249
8842	1	72004	29640	84136	80770	60319	02263
8401	2	47379	36735	21746	49757	28387	90514
8842	2	67377	66635	20742	79757	28357	90532
8401	3	36509	13052	46531	71887	21362	17690
8842	3	06151	13018	86561	76883	51262	17647
8401	4	41853	27354	87608	24403	73563	31710
8842	4	61813	27134	57608	78623	77563	31610
8401	5	45907	84281	40658	95249	84560	12357
8842	5	75907	54281	40061	65229	64565	50287
8401	6	64412	68130	36822	51487	38017	74543
8842	6	64491	58133	55521	41116	78010	54343
8401	7	24413	27442	48886	01505	18479	24268
8842	7	74422	27694	11056	01000	11471	21568
8401	8	46757	58306	53218	27715	22878	97651
8842	8	46776	50303	53628	93110	32888	71651

The high percentage of single-digit coincidence continued throughout the 48 groups. In these two sheets there were hits in 129 out of the 240 positions; 53.75 percent of the digits on these two pad sheets are identical. Hoping to find a cyclic repetition of this phenomenon, we overlapped pad sheets 8402 and 8843, but the high percentage of digit

coincidences did not continue. We assumed, therefore, that the pad sheets 8401 and 8842 were related causally but that the relationship did not carry on into the following pad sheets. Still, after further examination we found more and more listings related in this fashion. We also noticed at this point that listings which showed abnormal percentage of coincidence were listings of additive compromised from Dr. Wolff in 1940. We continued our attempts to find a pattern whereby the positions showed coincidence, but with no success. But we did learn that the underlying cause of coincidences affected only single digits and not whole groups.

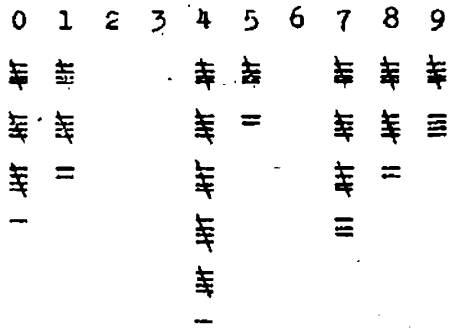
Next came a study of digits occurring in a single position throughout a volume of pad sheets; that is, the digits which occurred, for example, in the first position of the first group of each pad sheet in a book of 100 sheets were tabulated. Immediately after the distribution of the digits in the first position throughout a volume of pad sheets, a new interpretation of the abnormal amount of single-digit coincidences was reached; certain digits in certain positions were missing and certain digits occurred more frequently than others. The frequency distribution of the first digits in the first groups in the volume of pad sheets marked SERIE 50, SEITE 5000-5099 (Series 50, pages 5000-5099) was:



Since, in a distribution of 100 chosen at random, one would expect an average of 10 tallies for each of the ten digits, the likelihood that a digit would get no tally at all is extremely small. Therefore, that 0 and 9 did not occur at

all was immediately interpreted as fairly reliable evidence that 0 and 9 did not exist in the particular sequence from which the first digit of the first group of this volume of pad sheets had been generated.

Then, of course, the second digit of the first groups of the same volume of pad sheets was tabulated:



In this tabulation different digits are missing from those missing in the distribution of the first digit of group one, this time 2, 3, and 6.

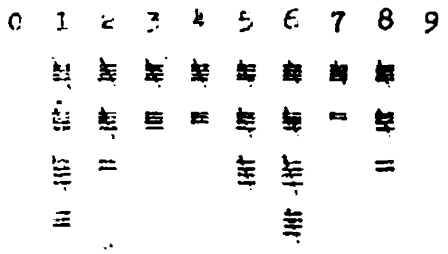
Nor was the distribution of the remaining digits in the two counts flat. In the distribution of the first digit the number of 1's and 6's is high. In the second digit distribution 4 is high. From these data it appeared that the elements which generated the first digit and second digit contained ten numbers, but that certain of the possible ten digits were not included and that certain others were doubled or even tripled in compensation.

Then, frequency counts were made for each of the 240 digit positions of the 5000's volume. In all but ten of these positions, digits were missing, and others were correspondingly increased in the frequency distributions. The ten positions which did not show missing and exaggerated

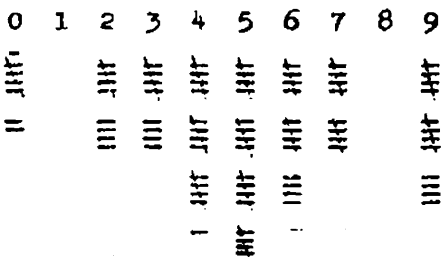
digits seemed to contain all ten digits, and the distribution was flat; thus it appeared that the elements which generated the sequence in these positions involved the ten different digits.

We then decided that distributions should be made on other volumes of captured material. When the first digit of the first group of the 5100's volume was tabulated, different digits were missing from those in the count of the first group in the 5000's volume. The distributions of the first digit of group one of the two volumes for comparison were:

5000's Volume



5100's Volume



When distributions were made of the first digit of group one for all of the rest of the volumes on hand it was found that, in all the volumes except the 5000's, 1 and 8 were missing and 4 and 5 seemed to be the correspondingly more frequent digits. It was assumed, therefore, that all of the

volumes of the captured material except the 5000's were homogeneous: all were generated with the same basic set-up of that which generated the additive. The 5000's were assumed to have been generated on a different basis.

16. Charts of missing and weighted digits.--In view of the fact that distributions on the basis of 100 sheets would reveal the missing digits, but often would not show clearly which digits received the counts which otherwise would have fallen to the missing digits, it was decided to make the 240 tabulations on four volumes instead of one. Therefore, tabulations were made on the 5100's, 5200's, and 5400's as well as on the 5000's in order to determine for all 240 positions which digits were missing and which digit could be proved to have received the so-called compensatory weights.

Charts were made showing the missing and weighted digits for all of the 240 positions in the 5000's and for the 240 positions of the 5100's. Examination of these charts revealed that the same 240 elements used in the 5000's were re-used for the volumes marked 5100 through 9999, but in a completely different order. For example, in the 5000's volume, group 23, position 4 had 0, 1, 2, 3, and 4 missing, a doubled frequency weight for 7. This same distribution appeared in the 5100's volume for group 48, position 1.

Five is the maximum number of digits missing in any distribution, as will be seen from the following summary of the missing digits in both the 5000's and the 5100's:

Number of digits missing	Number of distributions
0	10
1	49
2	72
3	74
4	29
5	6

Such information we added to our increasing store of curious, if still inexplicable data.

17. The clustering digits in the 5400's volume.--As distributions were being made of the 240 positions in the 5400's volume, we noticed that in one position out of the five of each five-digit group of the 48, digits seemed to cluster in an abnormal fashion as the distribution was made. Thus, in turning through the sheets of the volume, we noticed, for example, that the digit in the fifth position of the first group would be an 8 for as many as six or eight sheets running; then, the digit would change to a 2 and for five or six sheets would be a 2. This phenomenon persisted throughout the 5400's volume. One position out of each group of five showed this definite clustering.

The IBM listing in figure 12 shows the phenomenon clearly. This listing gives only the first line of each pad sheet of the 5400's in the order in which the sheets were bound. The positions in which the clustering was observed are marked with arrows. Following down the column of digits below the arrows, notice how often a single digit occurs consecutively. Notice also that the length of the repetition of any particular digit in each of the marked positions is the same at any given point; i.e., the change from one digit to another occurs simultaneously in all the marked positions (barring garbles and the repetition of a digit in the next set of repetitions).

Notice also that the fifth position of the first group, the first position of the second group, and one position out of each group of five showed this clustering. These positions were called the pattern V positions after the position in group one in which clustering was first observed. In figure 13, these positions which show clustering in all 48 groups are shown extracted from sheets of the 5400's volume and listed side by side.

		↓	↓	↓	↓	↓	↓
A5400	1	52824	73840	84417	19917	73075	51927
A5401	1	74914	75579	37537	32312	87097	01553
A5402	1	41074	77991	96197	11714	61021	91768
A5403	1	02044	77084	84257	62615	50070	41324
A5404	1	29924	74121	72217	70711	95045	71250
A5405	1	58082	90978	76754	16819	20491	44388
A5406	1	71022	99061	04414	61514	83484	04944
A5407	1	32912	91104	32114	76015	52475	94520
A5408	1	48172	98339	73294	95812	38446	84789
A5409	1	09170	16109	73321	76302	58595	47789
A5410	1	21888	10331	99201	95804	34526	77369
A5411	1	92220	19214	89111	03907	73578	47927
A5412	1	54010	15679	38731	49709	22540	47556
A5413	1	74935	47919	73317	60967	93284	46300
A5414	1	36165	49071	99437	79763	72275	16279
A5415	1	40885	41164	59577	92369	81296	46189
A5416	1	23184	77321	03207	90614	90086	71349
A5417	1	93824	79240	39117	09517	75078	41979
A5418	1	59214	71679	79737	46319	82090	41587
A5419	1	20035	23538	57246	35960	32307	72908
A5420	1	93065	25911	26116	13761	77331	42004
A5421	1	56975	26070	34796	66363	21354	42750
A5422	1	41828	88381	99275	92884	58926	88669
A5423	1	62238	83224	89345	00985	92978	78427
A5424	1	54068	84649	38415	43589	77940	58056
A5425	1	77678	86773	41595	86084	28929	08763
A5426	1	30848	88360	54105	21887	88971	98357
A5427	1	22085	66634	39239	42097	38270	75726
A5428	1	99685	60719	78379	80899	98299	45683
A5429	1	57823	67343	01449	29697	72281	45967
A5430	1	40915	64870	84519	12797	85255	15553
A5431	1	70965	29870	84766	16567	25375	02053
A5432	1	44085	21569	77436	31062	82397	92758
A5433	1	07085	28901	96376	16864	58321	42664
A5434	1	22935	23034	84246	65965	32374	72950
A5435	1	62671	56604	57302	81300	81869	73703

Figure 12. The listing of keys showing the repeated digits.(continued on next page)

A5436	1	54841	50739	36212	26801	50831	43607
A5437	1	53601	59777	31761	89982	73919	49273
A5438	1	39978	81868	77125	11089	82965	98783
A5439	1	01088	88503	96205	36887	58987	88368
A5440	1	99175	66019	79379	70741	94225	45189
A5441	1	46220	17267	49491	01702	81518	17757
A5442	1	08030	17608	58351	41805	50500	47406
A5443	1	23600	14731	21261	82501	53549	77043
A5444	1	33970	16093	22121	61307	68534	97700
A5445	1	46180	10187	33201	72803	54555	87379
A5446	1	68820	19328	69311	90509	93566	77909
A5447	1	51210	15243	09431	09307	72588	57547
A5448	1	73020	17677	88571	46303	81550	07776
A5449	1	03811	55307	49311	96383	57916	49579
A5450	1	20271	57232	69291	05780	31968	79707
A5451	1	93041	57613	28151	40881	70930	49306
A5452	1	53625	63747	48149	83692	72219	55973
A5453	1	79815	64372	61719	26790	27261	05587
A5454	1	31925	66863	24429	11397	88235	95743
A5455	1	31808	79373	08737	06712	22058	11969
A5456	1	43218	71290	31497	42015	81060	41557
A5457	1	68028	78688	64357	81812	64039	71746
A5458	1	56020	13643	48411	43604	73510	57956
A5459	1	78610	15772	61531	86705	27509	07503
A5460	1	33620	16361	24191	21301	88541	97707
A5461	1	94032	37549	32166	13917	77811	40384
A5462	1	57182	96377	93724	92312	88426	44169
A5463	1	42882	90292	89474	01815	64408	14629
A5464	1	04222	99683	79344	46912	53440	44957
A5465	1	82825	33310	31146	23673	72851	40473
A5466	1	74915	34878	74716	16779	27895	40087
A5467	1	41075	36561	07426	31374	88887	10743
A5468	1	02045	30900	86306	16877	54871	40328
A5469	1	29925	39039	74216	65572	33894	80984
A5470	1	97115	31113	02316	73374	73825	70040
A5471	1	58984	78542	77407	39810	74097	51603

Figure 12. The listing of keys showing the repeated digits (continued on next page).

A5472	1	53034	73973	06517	12917	82031	01948
A5473	1	43064	75090	34117	61317	67054	11074
A5474	1	08974	77188	62327	72719	51095	41700
A5475	1	39988	51098	62132	61009	62864	93180
A5476	1	43128	58183	03272	72807	58885	83649
A5477	1	63838	53320	39342	90907	92856	73479
A5478	1	59268	54248	79412	09709	77989	53087
A5479	1	59045	60582	62249	15641	32231	55654
A5480	1	47905	63943	03119	63542	77254	05950
A5481	1	00185	65070	89799	76040	21295	95509
A5482	1	23185	30133	22276	75877	34885	80600
A5483	1	93825	39310	43346	93973	73856	70459
A5484	1	59215	35278	69416	06379	22898	50009
A5485	1	20930	47882	84257	12645	50275	76903
A5486	1	64000	44523	37367	30741	95247	46008
A5487	1	56080	41947	46427	19042	78211	56154
A5488	1	43088	51962	24122	11001	82841	13104
A5489	1	06988	58003	42372	66802	58814	43650
A5490	1	20138	53132	53242	75900	32805	73909
A5491	1	93868	55313	29112	93701	77836	43009
A5492	1	56278	56277	39792	06303	21858	43757
A5493	1	36160	14193	93161	71702	65525	97059
A5494	1	40880	16382	59221	92300	58506	87759
A5495	1	64280	10221	29301	00801	94538	77657
A5496	1	96038	83617	48145	40682	72910	48456
A5497	1	58668	84772	61715	89585	75909	48003
A5498	1	43878	83171	24425	22081	52941	18707
A5499	1	43122	33171	29416	99514	77816	00449

Figure 12. The listing of keys showing the repeated digits (continued on next page).

Sheet No.	Line No. Group in Line Position in Group	1 123456	2 123456	3 123456	4 123456	5 123456	6 123456	7 123456	8 123456
		515432	341413	235343	313545	241525	134234	525434	241423
5400		477101	001890	211793	589247	578183	951509	614857	138666
5401		477101	001890	211793	589247	578183	951509	614857	138666
5402		477101	001890	211793	589247	578183	951509	614857	138666
5403		477101	001890	211793	589247	578183	951509	614857	138666
5404		477101	001890	211793	589247	578183	951509	614857	138666
5405		294144	230493	264086	643031	893879	086851	339523	791421
5406		294144	230493	275036	643031	893879	086851	339523	791421
5407		294144	230493	264086	643031	8938790086851		339523	791421
5408		294144	230493	264086	643031	893879	086851	339523	791421
5409		001057	944653	760039	137776	134444	434030	136481	885522
5410		011057	944653	760039	137776	134444	434030	136481	885522
5411		001057	944653	760039	137776	134444	434030	136481	885522
5412		011057	944653	760039	137776	134444	434030	136481	885522
5413		547626	007467	321403	425169	512560	900416	675118	358629
5414		547626	007467	321403	425169	512560	900416	675118	358629
5415		547626	007467	321403	425169	512560	900416	675118	358629
5416		477101	001890	211793	589247	578183	951509	614857	138666
5417		477101	001890	211793	589247	578183	951509	614857	138666
5418		477101	001890	211793	589247	578183	951509	614857	138666
5419		526632	387425	605808	825368	512540	612406	096116	382215
5420		526632	387425	605808	825368	512540	612406	096116	382215
5421		526632	387425	605808	825368	512540	612406	096116	382215
5422		885893	106527	158423	040599	583052	524543	216652	974881
5423		885893	106527	158423	040599	583052	524543	216652	974881
5424		885898	106527	158423	040599	583052	524543	216652	974881
5425		885898	106527	158423	040599	583052	524543	216652	974881
5426		885893	106527	158423	040599	583052	524543	216652	974881
5427		569925	323241	396965	257380	999031	948575	435363	443955
5428		569925	323241	396965	257380	999031	948575	435363	443955
5429		569925	323241	396965	257380	999031	948575	435363	443955
5430		569925	323241	396965	257380	999031	948575	435363	443955
5431		526632	387425	605808	825368	512540	612406	096116	382215
5432		526632	387425	605808	825368	512540	612406	096116	382215
5433		526632	387425	605808	825368	512540	612406	096116	382215
5434		526632	387425	605808	825368	512540	612406	096116	382215
5435		152083	304638	342733	497427	134474	073060	224480	824813
5436		152083	304638	342733	497427	134474	073060	224480	824813
5437		151899	146616	212421	351216	626792	715484	558509	402332
5438		885893	106527	158423	040599	583052	524543	216652	974881
5439		885898	106527	158423	040599	583052	524543	216652	974881
5440		569925	323241	396965	257380	999031	948575	435363	443955

Figure 13. Digits in pattern V positions, and extract from figure 1 (continued on next page).

5441	011057	944653	760039	137776	134444	434030	136481	885522
5442	011057	944653	760039	137776	134444	434030	136481	885522
5443	011057	944653	760039	137776	134444	434030	136481	885522
5444	011057	944653	760039	137776	134444	434030	136481	885522
5445	011057	944653	760039	137776	134444	434030	136481	885522
5446	011057	944653	760039	137776	134444	434030	136481	885522
5447	011057	944653	760039	137776	134444	434030	136481	885522
5448	011057	944653	760039	137776	134444	434030	136481	885522
5449	151899	146616	212421	351216	626792	715484	558509	402332
5450	151899	146616	212421	351216	626792	715484	558509	402332
5451	151899	146616	212421	351216	626792	715484	558509	402332
5452	569925	323421	396965	257380	999031	948575	435363	443955
5453	569925	323421	396965	257380	999031	948575	435363	443955
5454	569925	323421	396965	257380	999031	948575	435363	443955
5455	877101	040490	213789	583248	893889	551801	114527	735566
5456	877101	040490	213789	583248	893889	551801	114527	735566
5457	877101	040490	213789	583248	893889	551801	114527	735566
5458	011057	944653	760039	137776	134444	434030	136481	885522
5459	011057	944653	760039	137776	134444	434030	136481	885522
5460	011057	944653	760039	137776	134444	434030	136481	885522
5461	236180	571806	984997	399352	578124	167529	297852	111104
5462	294144	230493	264087	643031	893879	086851	339523	796421
5463	294144	230493	264087	643031	893879	086851	339523	796421
5464	294144	230493	264086	643031	893879	086851	339523	796421
5465	536780	542506	981960	396352	275227	567124	997042	610004
5466	536780	542506	981960	396352	275227	567124	997042	610004
5467	536780	542506	981960	396352	275227	567124	997042	610004
5468	536780	542506	981960	396352	275227	567124	997042	610004
5469	536780	542506	981960	396352	275227	567124	997042	610004
5470	536780	542506	981960	396352	275227	567124	997042	610004
5471	477101	001890	211793	589247	578183	951509	614857	138666
5472	477101	001890	211793	589247	578183	951509	614857	138666
5473	477101	001890	211793	589247	578183	951509	614857	138666
5474	477101	001890	211793	589247	578183	951509	614857	138666
5475	852083	378338	343767	492425	381975	173660	224190	221113
5476	852083	378338	343767	492425	381975	173660	224190	221113
5477	852083	378338	343767	492425	381975	173660	224190	221113
5478	852083	378338	343767	492425	381975	173660	224190	221113
5479	569425	344241	395920	259386	466435	548979	935533	740055
5480	569425	344241	395920	259386	466435	548979	935533	740055
5481	569425	344241	395920	259386	466435	548979	935533	740055
5482	536780	542506	981960	396352	275227	567124	997042	610004
5483	536780	542506	981960	396352	275227	567124	997042	610004
5484	536780	542506	981960	396352	275227	567124	997042	610004
5485	047426	044267	329425	429165	466465	300919	775538	755829

Figure 13. Digits in pattern V positions, and extract from figure 4 (continued).

Digits in Pattern V Positions

(Sheet) (No.) Line No.	1	2	3	4	5	6	7	8
Group in Line	123456	123456	123456	123456	123456	123456	123456	123456
Position in Group	515438	341413	235343	313545	241525	134234	525434	241423
5486	047426	044265	329425	429165	466465	300919	775538	755829
5487	047426	044267	329425	429165	466465	300919	775538	755829
5488	852083	378338	343767	492425	381975	173660	224190	221113
5489	852083	378338	343767	492425	381975	173660	224190	221113
5490	852083	378338	343767	492425	381975	173660	224190	221113
5491	852083	378338	343767	492425	381975	173660	224190	221113
5492	852083	378338	343767	492425	381975	173660	224190	221113
5493	011057	944653	760039	137776	134444	434030	136481	885522
5494	011057	944653	760039	137776	134444	434030	136481	885522
5495	011057	944653	760039	137776	134444	434030	136481	885522
5496	885898	106527	158423	040599	583052	524543	216652	974881
5497	885898	106527	158423	040599	583052	524543	216652	974881
5498	885898	106527	158423	040599	583052	524543	216652	974881
5499	236180	571806	084997	399355	578123	667529	297852	111104

Figure 13. Digits in Pattern V Positions, and extract from figure 4.

Figure 13 shows that each of the 48 elements which generated the digits listed had the same cycle; that is, when a "4" appears in the position of the first group which shows this clustering, it can be taken for granted that in most of the listings the clustering positions of the other 47 groups will have the digits 771010018902117935892475783595150961485713856 6. It seemed clear that this similarity in the 48 positions resulted from the fact that the elements involved all received the same motivation and thereby acted in parallel fashion, but we could still formulate no more explicit theory to account for all the phenomena thus far observed.

13. Methods of discovering the five pattern positions.-- It was immediately assumed that if one-fifth of the positions had the same cycle and acted in the same fashion so that the clustering phenomenon could be observed by eye, there were four other sets of pattern positions which would act in the same fashion. The problem then presented itself of locating the four other sets of pattern position

In earlier examination of the additive under study, we had noticed that, when there occurred a four-digit repetition between the additive of two different pad-sheets in the same group, the digit which did not repeat was almost always in the position five of the first group-- the Pattern V Position. That is, when the same four digits received in the first group of one pad-sheet and the first group of another pad-sheet, they would be found in positions 1, 2, 3, and 4; and position 5 (the Pattern V Position which was the one observed to show clustering) did not repeat. It had also been noticed that when such four-digit repetition occurred in the first four digits of group one, and when the fifth digit did not repeat, the same two digits were involved in the fifth position. Notice the example given below of four-digit repetitions between first groups of pad-sheets in the 5400's; and

notice also that the digits involved in the Pattern V Position are 4 and 5:

Pad-Sheet	First Group
5401	74914
5466	74915
5402	41074
5467	41075
5416	23184
5482	23185

At the same time, it was noticed that when three-digit repetitions occurred between two different pad-sheets, they occurred most frequently in digits 1, 2, and 4. Again, the Pattern V Position did not show a repetition, and the digits involved in the third position were almost always 0 and 9, thus:

Pad-Sheet	First Group
5405	58082
5471	58984
5485	20930
5419	20035
5311	56925
5350	56022

It was assumed that the third digit of the first group was the second most obvious, or easily discoverable, position; it acted in relation to the remaining digits as 5 had

acted in relation to 1, 2, 3, and 4. And so one position out of each of the remaining 47 groups ought to act in the same fashion also. Further, since four-digit repetitions seemed almost always to occur in positions 1, 2, 3, and 4 and in conjunction with the digits 4 and 5 in the Pattern V Position, it was assumed that there was a causal relationship between the digits 4 and 5 in position 5 and the four-digit repetition. Similarly the 0 and 9 in position 3 seemed related to the three-digit repetitions. The phenomenon was interpreted as the result of an interruption in the flow of the first four digits caused by the element which generated the fifth digit any time the digits 4 or 5 appeared and of an interruption in the flow of the digits in positions 1, 2, and 4 every time the 0 or 9 appeared in position 3.

Thus far the investigation had been one of observation of many phenomena; some relationships among them had been observed, but they had not been explained in any wholly satisfactory way. But about this time we began formulating a hypothesis about the nature of the additive generator. All the observed phenomena could be accounted for on the grounds that the machine was mechanical, not electrical (in its generation, that is, though it might well be electrically driven) and that the "elements" which produced the digits in the several positions were actually revolving wheels with 10 digits in mixed order embossed on their surfaces. The four-digit repetitions were immediately interpreted as being the results of notches or interrupter points on the Pattern V wheels. The four positions which showed the repetition in the first group, for example, were considered to depend on the fifth position: the fifth position was responsible for interruptions in the other four positions, and yet the cycle of the fifth position was apparently not disturbed by the first four (as in ordinary cyclometry, except that the wheels in this case were not in conventional order from

left to right or right to left and that they bore mixed sequences). Moreover the Pattern V digits throughout the 48 groups were produced by a single action; they were called the most obvious positions, or the first set of positions "in dependence order" and were also referred to as "the fast-wheel positions" (meaning the positions the cycles of which were never interrupted, or the wheels which turned one point on their rims with each movement of the additive generator.) Such principles are obvious in the light of the whole reconstruction, but at this stage of the investigation their formation represented a great step forward even though they seemed to explain less than what remained to be explained.

Though we were still working in the dark, we were no longer groping, and this method of studying repetitions led to the location of the five sets of pattern positions. But we also used a second method to great advantage with the help of IBM. We recalled that the fact which drew the first set of pattern positions to our attention was that digits clustered so obviously in those positions that the phenomenon could be noticed even by eye. Therefore, we assumed that if the first set of pattern positions were eliminated and if each of the remaining positions of group one were sorted one at a time, a clustering of digits in one position in each of the remaining 47 groups would result when the next most obvious pattern position (or the pattern position next in dependence order) of the first group were encountered. This process was performed by IBM, and when the sort on position three of the first group was examined, it was clear that a certain amount of clustering was more obvious in one position of each of the remaining 47 groups (see figure 14.) All the pad-sheets listed have a 6 in position three of the first group. The positions which show the most obvious clustering and which have the greatest limitation in number of different digits are marked with arrows.

Pad Sheet	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6
5124	2967-	-7339	3129-	257-2	31-41	7-753
5133	3963-	-7798	6116-	818-0	84-69	9-483
5134	0962-	-3308	6134-	269-9	52-61	4-983
5137	6962-	-8729	7829-	857-9	31-99	7-783
5146	6168-	-0721	0827-	858-7	38-89	7-646
5151	6764-	-0601	0414-	818-2	80-19	7-373
5175	6062-	-7604	5735-	817-0	88-99	7-783
5178	6764-	-7783	9731-	216-3	62-51	7-377
5179	9262-	-3680	3436-	819-5	63-09	7-453
5187	9464-	-0689	3721-	818-1	60-39	7-603
5191	5966-	-4638	7722-	667-2	57-49	4-253
5199	3266-	-9677	8772-	835-7	77-09	1-253
5200	7464-	-0619	3711-	858-1	30-39	4-603
5215	5268-	-1630	3429-	860-5	58-09	4-553
5232	3461-	-4678	3779-	837-2	72-39	1-703
5253	2867-	-6698	6447-	823-2	81-49	8-753
5239	4762-	-7643	6741-	809-2	93-19	0-453
5247	5062-	-7624	5420-	827-0	58-99	5-703
5304	3264-	-0790	8110-	818-3	88-59	9-323
5307	0160-	-9703	2131-	819-1	62-49	4-243
5335	4360-	-4783	3831-	865-1	53-49	4-206
5343	0366-	-4707	4136-	815-2	63-29	4-073
5347	2068-	-6732	8823-	820-5	52-79	8-156
5367	4666-	-5387	4121-	223-3	57-11	8-573
5370	4360-	-4383	2126-	227-7	55-31	8-043
5373	3162-	-3793	2114-	816-1	80-49	9-943
5425	7767-	-6773	4159-	860-4	28-29	0-763
5428	9968-	-0719	7837-	808-9	98-99	4-683
5435	6267-	-6604	5730-	813-0	81-69	7-703
5437	5360-	-9777	3176-	899-2	73-19	4-273
5443	2360-	-4731	2126-	825-1	53-49	7-043
5452	5362-	-3747	4814-	836-2	72-19	5-973
5459	7861-	-5772	6153-	867-5	27-09	0-503
5497	5866-	-4772	6171-	895-5	75-09	4-003

Figure 14. The sort used in determining Pattern Position III.

These positions were called Pattern III Positions after the position in the first group which showed the next most obvious clustering after Pattern V.

This method of discovering pattern positions would work definitely only on the first two most obvious sets of positions. For the third and fourth sets of positions, it was necessary to use the first method, the study of two-digit and one-digit repetitions, and the study of the digits which occurred in the previous pattern positions in connection with the repetitions.

The third and fourth sets of pattern positions had to be discovered a group at a time. For example, in the case of group one, only three positions were left to be identified after the Pattern V and the Pattern III position were eliminated. The remaining positions were 1, 2, and 4. In the work done in discovering the third set of pattern positions, it was necessary to observe the number of two-digit hits in positions 1 and 2, and 1 and 4, and 2 and 4. This study showed that the greatest number of two-digit hits occurred in positions 2 and 4 and that, at the same time, in position 1, the digits on the two pad-sheets which showed the two-digit hit would be 0 and 6. In this way, the position which belonged with the third set of pattern positions (Pattern Position I) could be discovered for each of the 48 groups.

Similarly, one-digit hits showed position 4 of the first group to be the position which belonged to the fourth set of pattern positions; and so on throughout the 48 groups, one position in each group could be discovered by this method to be the position which belonged to the fourth set of pattern positions. The last set of pattern positions (Pattern Position II) was naturally made up of the 48 digit positions which remained unidentified.

Now these patterns were believed to have arisen from the action of a generating machine and, since they could be extracted in order, to have been generated in order by a regular motion. This order would have to be recovered in the reconstruction of the method of generation. The term dependence order was used to describe the order in which these patterns were related.

The following is a list of the five sets of pattern positions showing which digit of each of the 48 groups was involved in each pattern position in the material compromised from Dr. Wolff in 1940:

Line	1	2	3	4	5	6	7	8
Group	123456	123456	123456	123456	123456	123456	123456	123456
Order								
1. Patt. V. Positions	515432	341413	235343	313545	241525	134234	525434	241423
2. Patt. III Positions	332155	132135	444514	131321	133111	553151	443322	423242
3. Patt. I Positions	143211	224551	123121	555412	452233	342522	214141	315154
4. Patt. IV Positions	424323	453322	512452	224154	325342	225345	331215	132335
5. Patt. II Positions	251544	515244	351235	442233	514454	411413	152553	554511

When our conventions were finally established, however, we decided to refer to the Pattern V Positions as the positions for fast wheels or for first wheels in dependence order; to refer to Pattern III positions as the positions for second wheels in dependence order; Pattern I positions as third in dependence order; Pattern IV Positions as fourth in dependence order; and Pattern II Positions as fifth in dependence order.

Then these data were rearranged into what was called the "dependence order" for the 48 groups of the compromised material (see figure 15 in which each digit is identified by its place in the dependence order). Notice that in group one, the fifth position is labeled first in dependence order; the third position is second in dependence order; the first digit is third in dependence order; the fourth digit is fourth; and the second digit is fifth. The resultant 35241 is the dependence pattern.

About this time we formulated another hypothesis about the generating machine--later proved correct--which explained the occurrence of these pattern positions: each group was generated by a separate machine, and the whole generator was a complex of 48 small five-digit machines. Hence the 48 fast wheels--one for each group.

19. The 10-100-1,000-10,000-100,000 relationship between sets of pattern positions.--After the five sets of pattern positions had been completely determined, it was possible to study the relationships among the different sets. From a close study of figure 13 there can be discovered twenty unique 48-digit numbers (i.e., sequences of 48 digits) generated by the fast wheels (those belonging to Pattern Position V). It will be noticed also that these twenty numbers fall into two sets of ten each and that the two sets are closely related to each other. These are listed in figure 16 and are labeled arbitrarily so that number 1 of the first set of 10 is related to number 1 of the second set of 10, etc. Notice that the similarity between number 1 of the first set and number 1 of the second set continues throughout the 48 digits, as can be seen when the two related lines are superimposed:

Group No.	1	2	3	4	5	6
Position.	12345	12345	12345	12345	12345	12345
Line 1	35241	14235	52341	23415	34152	31542
	7	8	9	10	11	12
Line 2	23145	53214	12435	25413	14253	34152
	13	14	15	16	17	18
Line 3	31524	43125	54321	35142	23514	34125
	19	20	21	22	23	24
Line 4	24153	14253	25143	45231	32514	23541
	25	26	27	28	29	30
Line 5	21435	54213	13254	23451	21345	24351
	31	32	33	34	35	36
Line 6	25341	54132	53214	21543	53142	23514
	37	38	39	40	41	42
Line 7	53421	31425	45231	34215	42135	32514
	43	44	45	46	47	48
Line 8	41325	32415	15243	32415	51423	52134

Figure 15. The complete dependence pattern based on the dependence order of the wheels of the 48 groups in the Wolff material.

FIRST SET

1	47710100188021179358924757318395150961485713866 6
2	29414423049326408664303189387908685133952379142 1
3	01105794465376003913777613144443403013648188552 2
4	04742604426732942542916546546530091977553875582 9
5	52663238742560680882536851254706124060961163822 15
6	88589810652715842304059958305252452321665297488 1
7	56992532324139696525738099903194857543536344395 5
8	85208337833834376749242538197517366024419022111 3
9	15189914661621242135121662679271548455850940233 2
0	53678054250698196039635227532756712499704261000 4

SECOND SET

1	87710104049021378958324889388955180111452773556 6
2	09404424839326006164203238197598665053919328232 1
3	81185792665376302513177162674213443443650147302 2
4	54762600746732140342516951256090041667511835862 9
5	42673233252560186682636027524731210439604663141 5
6	08599818322725946804759699905172454501636245228 1
7	56942534424139552025938646643554897993553374005 5
8	15208330463834273349742713447407306022448082481 3
9	55189914651521642535021558 09241550375855994683 2
0	23618057180603459739935557812366752929785211110 4

Figure 16. The two sets of ten 48-digit sequences generated by the fast wheels (based on figures 12 and 13.)

4771010018902117935892475781829515096148571386666
8771010404902137895832488938895518011145277355666

Notice also that number 2 of the first set and number 2 of the second set, are different in the same positions (with only two exceptions)[1] as number 1 of the first set and number 1 of the second:

2941442304932640866430318938790868513395237914 21
0940442483932600616420323819759866505391932823 21

This difference between the two lines superimposed in the two examples above and indeed between the two sets of ten, was accounted for as having been caused by some sort of change, e.g., hand resetting of the wheels which printed the digits in the fast-wheel positions. It was assumed that within any given setting of the "fast wheels," there would be a limitation of 10 and only 10 combinations of digits which could be generated by virtue of the fact that these "fast wheels," each with a cycle of 10, were always turning one step for each movement of the additive generating machine and being in step, produced such a cycle of ten 48-digit numbers.

In order to determine the relationship between the fast wheels (or first wheels in dependence order) and the second wheels in dependence order, it was thought logical to study the pad-sheets which showed the same one of the ten unique numbers generated by the fast wheels and the digits which appeared on these pad-sheets in the positions of the second wheels. In other words, it was decided to choose pad-sheets which had, for example, the fast-wheel positions yielding the number beginning 011057

[1] Later explained as arising from doubled digits within the sequence on the wheel.

and to list the digits which appeared on these pad-sheets in the positions for second wheels.

Figure 17 shows the pad-sheet number, the digits in fast-wheel positions for the first line of the pad-sheets, and the 48 digits which appeared in second-wheel positions. An X marks the first occurrence of each of the 48-digit numbers. Those not marked with an X are exactly the same as one of those already marked. From figure 17, it will be seen that, if the pad-sheets which have one of the ten numbers in fast-wheel positions are studied with a view to determining the relationship which exists between the fast-wheel positions and second-wheel positions, the relationship is again 1 to 10--that is, on the pad-sheets which show the same number in fast-wheel positions, the second wheels will generate 10 (and only 10) different numbers.

It was decided to study the second-wheel numbers on the sheets which showed the other nine unique fast-wheel numbers. As each unique fast-wheel number was studied, it was seen that 10 unique numbers resulted from second-wheel positions. In figure 18 are shown all pad-sheets which yielded the line 011057 for fast-wheel positions and the numbers yielded by second wheels. (In figures 17ff. the 48-digit numbers generated by sets of wheels in dependence order are represented by the six digits of the first line--that is, one digit from each of the six groups of the first line. The other seven lines are omitted for simplicity).

Once again a set of 10 and only 10 numbers was found. Figure 19 shows how these 10 figures are in turn followed by other sets of numbers, also limited to ten; it shows fast-wheel numbers for the first line and the second-wheel numbers for the first line. Again, those marked with an X are the basic 10 and all others are repetitions of one of these.

Pad Sheet	Pat. V First Line		Pattern III Line 1	Line 2	Line 3	Line 4	Line 5	Line 6	Line 7	Line 8
5409	011057	X	113759	405232	704329	343173	831527	308588	834183	535035
5410	011057	X	839969	842845	053740	148010	148463	811975	192344	637135
5411	011057	X	229087	560731	877232	412678	726615	866125	470802	770178
5412	011057	X	068406	657736	950654	720783	039814	235490	305216	784920
5441	011057		229087	560731	877232	412678	726615	866125	192482	632322
5442	011057		068406	657736	950654	720783	039814	235490	305216	787920
5443	011057	X	671893	295984	516323	105309	447795	247703	302551	782062
5444	011057	X	902640	771406	843876	333434	403921	452317	288480	161672
5445	011057		113759	405232	704329	343173	831527	308588	834183	535035
5446	011057		839969	842845	053740	148010	148463	811975	192344	637135
5447	011057		229087	560731	877232	412678	726615	866125	470802	402787
5448	011057		068406	657736	950654	720783	039814	235490	305216	784920
5458	011057		068406	657736	950654	720783	039814	235490	305216	784920
5459	011057		671893	295984	516323	105309	447795	247703	302551	780062
5460	011057	X	834217	638629	626911	690884	920109	094561	297020	936341
5493	011057		113759	405232	704329	343173	831527	308588	834183	535035
5494	011057		839969	842845	053740	148010	148463	811975	192344	637135
5495	011057		229087	560731	877232	412678	726615	866125	470802	402787
5310	011057	X	987153	884143	391164	594292	996302	160242	283183	509145
5320	011057	X	094114	306658	185458	080250	787286	759857	540974	090056
5328	011057		094114	306658	185458	080250	787286	759859	540974	090056
5337	011057		902640	771406	843876	333434	403921	752317	288480	161672
5343	011057		671893	295984	516323	105309	447795	247703	302551	780062
5352	011057	X	056378	513584	497037	461939	512838	503078	171093	692302
5355	011057		094114	306658	185458	080250	787286	759859	540974	090056
5359	011057		229087	560731	877232	412678	726615	866125	470802	402787
5360	011057		068406	657736	950654	720783	039814	235490	305216	784920

Figure 17. The analysis of the pattern III 48-digit figures.

Pad Sheet	Pattern V First Line	Pattern III First Line	Pad Sheet	Pattern V First Line	Pattern III First Line
9139	011057	902640	9859	011057	987153
9140	011057	113759	9881	011057	094114
9144	011057	229087	9885	011057	229087
9146	011057	068406	9892	011057	094114
9171	011057	068406	9907	011057	902640
9173	011057	671893	9919	011057	113759
9182	011057	902640	9938	011057	834217
9193	011057	834217	9940	011057	056378
9197	011057	056378	9946	011057	068406
9227	011057	902640	9951	011057	834217
9236	011057	229087	9953	011057	056378
			9961	011057	671893

Figure 18. The relationship of Pattern V numbers to Pattern III numbers.

Pad Sheet	First Line		Pattern III First Line
5121	011057	X	834217
5132	011057		834217
5133	011057	X	671893
5135	011057		834217
5310	011057	X	987153
5320	011057	X	094114
5328	011057		094114
5337	011057	X	902640
5343	011057		671893
5352	011057	X	056378
5355	011057		094114
5359	011057	X	229087
5360	011057	X	068406
5371	011057		987153
5372	011057		056378
5382	011057		902640
5409	011057	X	113759
5410	011057	X	839969
5411	011057		229087
5412	011057		068406
5441	011057		229087
5442	011057		068406
5443	011057		671893
5444	011057		902640
5445	011057		113759
5446	011057		839969
5447	011057		229087
5448	011057		068406
5458	011057		068406
5459	011057		671893
5460	011057		834217
5493	011057		113759
5494	011057		839969
5495	011057		229087
5973	011057		839969
5974	011057		229087
5975	011057		068406
5976	011057		671893
6066	011057		056378
6067	011057		094114
6068	011057		902640
6069	011057		113759
6117	011057		834267
6147	011057		987153
6182	011057		902640
6183	011057		113759
6184	011057		839969
6251	011057		068406
6267	011057		671893
6309	011057		094114
6324	011057		056378
6491	011057		834217
9129	011057		094114
9132	011057		987153
9133	011057		056378
9134	011057		056378
9242	011057		834216
9246	011057		094114
9247	011057		094114
9252	011057		839969
9255	011057		113759
9258	011057		671893
9261	011057		987153
9285	011057		056378
9287	011057		902640
9296	011057		834217
9302	011057		094114
9306	011057		229087
9313	011057		229087
9326	011057		839969
9328	011057		834217
9330	011057		056378
9337	011057		068406
9340	011057		113759
9386	011057		671893
9389	011057		987153
9396	011057		839969
9422	011057		839969
9426	011057		113759
9501	011057		902640
9505	011057		229087
9559	011057		839969
9574	011057		834217
9576	011057		094114
9580	011057		839969
9586	011057		834217
9605	011057		113759
9611	011057		671893
9614	011057		056378
9639	011057		671893
9641	011057		987153
9642	011057		113759
9652	011057		094114
9659	011057		068406
9689	011057		229087
9692	011057		902640
9693	011057		094114
9698	011057		902640
9713	011057		671893
9716	011057		094114
9726	011057		671893
9761	011057		229087
9776	011057		056378
9777	011057		094114
9784	011057		229087
9889	011057		113759
9791	011057		068406
9794	011057		987153
9811	011057		094114
9828	011057		068406
9843	011057		987153
9863	011057		671893

Figure 16. The relationship of Pattern V numbers to Pattern III numbers.

Unique Fast Wheel Numbers		Unique Second Wheel Numbers		Unique Fast Wheel Numbers		Unique Second Wheel Numbers	
		1	884157			1	904640
		2	269407			2	229087
		3	078896			3	062406
		4	829089			4	112759
1)	477101	5	631213	4)	047426	5	833969
		6	912750			6	096114
		7	133969			7	984153
		8	957373			8	057378
		9	096118			9	678893
		0	004644			0	831217
		1	133969			1	229087
		2	829089			2	833969
		3	631213			3	069406
		4	884157			4	678893
2)	294144	5	957373	5)	526632	5	831217
		6	269407			6	096114
		7	078896			7	904640
		8	096118			8	112759
		9	004644			9	057378
		0	912750			0	984153
		1	113759			1	902640
		2	839969			2	113759
		3	229087			3	056378
		4	068406			4	987153
3)	011057	5	671893	6)	885898	5	094114
		6	902640			6	229087
		7	834217			7	839969
		8	987153			8	060406
		9	094114			9	671893
		0	056378			0	834217
		1	112759			1	113759
		2	904640			2	902640
		3	068406			3	056378
		4	833969			4	094114
7)	569925	5	229087	9)	151899	5	987153
		6	831217			6	834217
		7	096114			7	839969
		8	057378			8	671893
		9	984153			9	229087
		0	678893			0	068406
		1	094114			1	833969
		2	056378			2	904644
		3	987153			3	112750
		4	068406			4	069407
8)	852083	5	671893	0)	536780	5	678896
		6	834217			6	984157
		7	839969			7	831213
		8	229087			8	229089
		9	902640			9	057373
		0	113759			0	096118

Figure 19. The discovery of the ten sets of digits generated by the second wheels.

From the list of second-wheel numbers all pad-sheets were pulled which had the second-wheel number 094114, etc., and the third-wheel numbers were listed for study. Again a 1-to-10 relationship was revealed--that is, pad-sheets which had the fast-wheel number 011057 and the second-wheel number 094114 yielded in third-wheel positions 10 numbers and only 10. Figure 20 shows the third-wheel numbers; again, the basic 10 are marked with an X and those not marked are repetitions. Since the amount of captured material available for study was limited, it was not possible to find all the unique sets of digits generated by the fourth and fifth sets of pattern positions, but it was assumed, since the fast wheels generated 10 numbers and no more, since the second wheels in dependence order generated 100 numbers, and since the third wheels in dependence order generated 1,000, that the fourth set of wheels would generate 10,000 and the fifth set of wheels would generate 100,000.

This 1-to-10 relationship among the different sets of pattern positions was assumed to arise from what came to be called a notch position on all wheels in every group. Because of the way the additives were mixed, we conceived of all the wheels of the machine advancing simultaneously except at the completion of the cycle of one of the wheels (of each set of five), when that wheel would cause the wheels dependend on it to stop. In the course of the cycle of the fast wheel, for example, one of the ten points on its rim would affect the cycles of the other four wheels in its group of five by causing them to stop one movement and print the same digits twice (the opposite of the true meter motion of a numbering machine); in the course of the cycle of the second wheel, there was one point on its rim which would in turn affect the cycles of the other three wheels in dependence order by causing them to stop one movement in their cycles and to print

Pad Sheet	Pattern V First Line	Pattern III First Line		Pattern I First Line
5320	011057	094114	X	774280
5328	011057	094114	X	575624
5355	011057	094114	X	547975
6067	011057	094114	X	461181
6309	011057	094114	X	393169
9129	011057	094114	X	482258
9246	011057	094114	X	233537
9247	011057	094114		575624
9302	011057	094114		482258
9576	011057	094114	X	914374
9652	011057	094114	X	002654
9693	011057	094114		393169
9716	011057	094114		002654
9777	011057	094114		547975
9811	011057	094114	X	621097
9881	011057	094114		774280
9892	011057	094114		461181

Figure 20. The ten unique numbers in Pattern Position I.

the same digits twice. The same phenomenon seemed to exist in the case of the third and fourth wheels in dependence order. The notch point of the third wheels would cause the fourth and fifth wheels in dependence order to stop once in their cycles and to print the same digits twice. The fourth wheel's notch affected only the cycle of the fifth wheel in dependence order.

20. Methods of determining order of digits in the 240 sequences.--Now that our theories concerning the essentials of the action of the mechanism generating the additive accounted fairly well for the observed phenomena, it became necessary to determine the actual order of the digits embossed on the rims of the 240 wheels involved in the additive generator. In this discussion it must be understood that the derivation of the sequences is a relative derivation and that the direction in which the digits actually appear on the wheels of the machine and the actual direction in which the machine turns the wheels may never be known. Our only concern in the derivation of sequences was consistency in derivation. As long as all sequences were derived and recorded on the basis of the same conventions, the actual direction of the digits on the wheels of the machine was immaterial. Method (a) makes use of four-digit repetitions. If such a repetition involves all the digits in a group save that generated by the fast wheel, then we can say that the repetition was caused by the notch action of the fast wheel and is possible only on adjacent pad-sheets--those generated one after or before the other. If such sheets are adjacent, then the digits of the columns were adjacent in the sequence of the wheels. Method (b) makes use of the effect of the notch action of a wheel on that next higher in dependence order. Since this action through causing a repetition in the sequence displaces the sequence one step on the rim of a wheel, where we can find evidence of such notch action, we can chain the

digits of the additive before and after the notch action to reconstruct the sequence. This evidence appears when we list for each of the ten numbers of a wheel the ten numbers of wheels next higher in dependence order (see paragraph 19). Third, method (c) makes use of two settings of the second wheels in dependence order. These can be detected in the lines (or numbers.) If we can rearrange the lines of the fast wheels in the order in which they were produced, we can recover the sequences on the wheels making up these lines. Finally, method (d) makes use of other phenomena arising from hand resettings of the wheels. Since the displacement of a wheel by resetting is uniform throughout the sequence, we can again chain the digits to recover a sequence or one of its decimations. Method (a) yields sequences for wheels second, third, fourth, and fifth in dependence order, other than those exhibiting the repetitions. Fast wheels cannot be completely derived by this method of solution alone. Method (b) will yield only the sequences displaced by the notches on the wheels higher in dependence order. Theoretically the sequences for second wheels in dependence order can be derived if enough material is available so that all the ten numbers generated by them can be obtained for study, but the data are never extensive enough for such complete recovery. In this method, it will be observed that when two fast-wheel notches turn up at the same time, no displacement will be shown in second wheels in dependence order. Method (c) gives only fast-wheel sequences, and only where there is evidence of resetting. By method (d), one can derive only the digits for sequences which show displacement through hand resetting; if for example, a third wheel in dependence order is reset, wheels three, four, and five can eventually be derived, but wheels one and two will show no displacement and therefore cannot be derived, since they have neither been reset, nor are

they affected by the resetting of the third wheel. Moreover, this method at best produced only one of four possible decimations of the real settings. As a result of these limitations, the four methods had to be used simultaneously.

Figure 21 is a list of pairs of pad-sheets which have been superimposed. Again, only the first line of the pad-sheets have been shown since they illustrate the entire process. These pad-sheets show 4-digit hits in the first group at the notch position of the fast wheel. The convention was established that the notch action occurs between the 4 and 5 on this fast wheel, so that the pad-sheet which shows the 4 is placed above and the one which shows the 5, below. The 5 is circled and arbitrarily called "the notch point". In the derivation of the sequences, this convention dictates the direction of the process.

The assumption in figure 21 is that since the two pad-sheets 5402 and 5467 show the four-digit hit 4107 with a 4 on one and a 5 on the other, the two pad-sheets were generated by chronologically adjacent movements of the additive generator. It can, therefore, be assumed that the digit 7 of pad-sheet 5402 in the first digit of the second group (also on a fast wheel) is adjacent on the rim of that wheel to the 3 below in pad-sheet 5467. But since all fast wheels are in phase with one another, the fast wheels of all the other groups will show only two digits which were in phase with the two digits of the first-group fast wheel. Since the fast-wheel pairs change (at pair no. 8), we assumed that there had been a hand resetting of the wheels at this point, and hence we derived two discrete pairs of digits within the sequence of the fast wheel of the second and following groups. Since only two pairs of digits can be given for these

	GROUP NUMBER	1	2	3	4	5	6
	DEPENDENCE ORDER	35241	14235	52341	23415	34152	31542
	PAD SHEET NUMBER						
1)	(5402	41074	77991	96197	11714	61021	91768
	(5467	41075	36561	07326	31974	88887	10743
2)	(5401	74914	75579	37537	32312	87097	01553
	(5466	74915	34878	74716	16779	27895	40087
3)	(5403	02044	77084	84257	62615	50074	41324
	(5468	02045	30900	56306	16877	54871	40328
4)	(5404	29924	74121	72217	70711	95045	71250
	(5469	29925	39039	74216	65572	33894	80984
5)	(5416	23184	77321	03207	90614	90086	71349
	(5482	23185	30133	22276	75877	30885	80600
6)	(5417	93824	79240	39117	09517	75078	41979
	(5483	93825	39510	43346	93973	73856	70459
7)	(5418	59214	71679	79737	46319	82090	41587
	(5484	59215	35278	69416	06379	22898	50009
8)	(5178	67644	27783	97316	21673	62351	72377
	(5151	67645	40601	04147	81862	80219	76373
9)	(5147	28084	26908	63175	61772	68334	72750
	(5183	28085	41592	52497	11362	81241	86154
10)	(5245	03064	24567	32526	12375	82301	42054
	(5248	03065	49873	30527	36767	22207	46058
11)	(5331	06064	75787	98367	86712	55029	41056
	(5312	06065	34603	09116	41574	55820	90267

	GROUP NUMBER	1	2	3	4	5	6
	DEPENDENCE ORDER	35241	14235	52341	23415	34152	31542
	PAD SHEET NUMBER						
12)	(5202	31924	27871	04716	39974	75317	92958
	(5200	31925	40349	26467	13667	73225	16463
13)	(5313	32264	75604	39167	41717	57070	91027
	(5385	32265	34290	49416	01777	65858	10279
14)	(5396	38034	73708	58157	81610	60009	91406
	(5384	38035	37692	59406	41875	60800	10357
15)	(5288	49074	27699	34406	82771	88389	82743
	(5159	49075	46269	21507	46361	88280	46706
16)	(5370	43604	74383	21267	22717	55031	81040
	(5335	43605	34783	38316	86571	53849	40206
17)	(5166	59944	20838	74216	32671	52337	52308
	(5296	59945	48382	66247	16862	50245	46653
18)	(5176	51024	29511	02316	10773	97351	42954
	(5195	51025	43823	04317	35562	35217	46958
19)	(5299	50804	29334	56236	12779	57395	52283
	(5169	50805	49754	87217	26560	55261	46907
20)	(5390	58124	78378	73477	96819	24046	51709
	(5129	58125	37142	62196	79770	78895	40750
21)	(5391	53814	71273	29437	06017	28088	51509
	($111	53815	35341	33116	99371	72836	40059
22)	(5106	63884	76820	34327	10317	98055	71177
	(5356	63885	31337	41236	25073	32811	70173

	GROUP NUMBER	1	2	3	4	5	6
	DEPENDENCE ORDER	35241	14235	52341	23415	34152	31542
	PAD SHEET NUMBER						
23)	(5389	63914	76114	32337	73017	78075	71570
	(5128	63915	31020	34536	60077	92854	70574
24)	(5198	73984	21811	24176	30374	91327	02668
	(5181	73985	45329	36397	15067	38285	46543
25)	(5392	71834	73261	09547	01914	82088	01449
	(5362	71835	37373	23756	92677	80836	40309
26)	(5117	94884	70811	24107	13812	74035	41657
	(5399	94885	38329	31376	20872	98841	70783
27)	(5174	93984	20033	29246	72672	52315	42669
	(5148	93985	48981	33357	66864	50224	76740
28)	(5286	93844	20381	26216	15574	52325	42363
	(5256	93845	40781	37347	22867	60281	76647

Sequences derived from these data

Notch Point						
0	5	36710	450	003 0	2 00	0 8
1		1627	677	950 5	7 78	2 3
2		5233	749	723 7	7 56	9 7
3	Fast Wheel	4381	412	667 3	5 15	4 3
4		9103	133	115 2	3 24	3 6
5		3091	821	319 4	5 81	6 7
6		7969	926	126 7	4 37	7 9
7		0578	931	268 1	6 45	7 9
8		9872	314	898 2	8 91	1 0
9		7344	245	437 9	8 69	5 4

Incomplete Fast Wheel

Figure 21. Deriving the notch points and sequences.

sequences they are marked incompletely derived in the listing of the derived sequence in figure 21. All that can be said about the sequence for the fast wheel of the second group is that 7 is adjacent to 3 and that 2 is adjacent to 4.

As for the derivation of the sequences of the other wheels, a good, simple example of the principles lies in the third digit of the second group in figure 21. Notice that this digit is the second in dependence order in the second group. From pairs of pad-sheets 1 and 9, 9 can be said to be adjacent to 5. Then, looking down the same column, we can make the following statements:

From pairs 2, 10, and 18.....5 is adjacent to 8.
" " 12, 17, 22, and 26.....8 " " " 3.
" " 16, 19, and 28.....3 " " " 7,

and 7 is the notch point for the sequence, since in all three pairs used, there was a 3-digit hit in the positions which printed wheels 3, 4, and 5 in dependence order. (The hits which yield the notch position in figure 21 have been underlined in both pad-sheets and the digit which is called the notch position is circled.) Continuing,

From pairs 8, 11, and 14.....7 is adjacent to 6.
" " 7, 13, and 15.....6 " " " 2.
" " 6, 21, and 25.....2 " " " 3.
" " 5, and 20.....3 " " " 1.
" " 4, and 23.....1 " " " 0.
And " 3, and 27.....0 " " " 9,

since 9 was the digit we started with, the sequence has been completely solved and reads: 7 6 2 3 1 0 9 5 8 3.

Some sequences are incomplete because the data are not complete; some notch points are unknown because they are on fifth wheels in dependence order, the notch points of which could not be discovered. In the actual derivation of sequences which have doubled digits, difficulties arise at some points because it cannot be determined immediately which of the doubled digits should be chosen. Method (a), then, allows us to reconstruct sequences through the assumption that the repetition in the first group reveals chronologically adjacent additives.

With method (b), second wheels in dependence order which show the effect of notch action by the fast wheels can be solved. Figure 22 (used in both method (b) and Method (c)) shows the two sets of fast-wheel numbers generated by two different settings of the additive generator and the two sets of ten second-wheel numbers which were discovered on the pad-sheets which showed each of the fast-wheel numbers. The ten numbers generated by second wheels on the pad-sheets showing the same fast-wheel number have been arranged arbitrarily, but each set of ten is in itself arranged consistently with every other set. (Reading down the like columns reveals this consistency.)

Notice that the blocks of ten second-wheel numbers have been arranged left to right on the basis of the degree of columnar difference shown from the first block of ten. Those with most differences are farthest from the left (chosen arbitrarily). The columns which show differences are marked. The columnar differences were assumed to have occurred as a result of the action of a notch position on the fast wheel which controls the

SETTING I

BLOCK NUMBER	1	2	3	4	5
FAST-WHEEL LINES	094044	877101	236180	426732	569425
	909656	909756	909756	909756	909756
	984178	984378	984378	984378	984378
	093140	093640	093640	093640	093649
SECOND	119769	119969	119969	119969	119969
WHEEL	836253	836153	836153	836157	836157
LINES	064493	064893	064893	064898	064898
	052314	052114	052114	052110	052110
	838989	838589	838089	838087	838087
	221007	221407	221407	221406	221406
	677817	677217	677217	677213	677213

BLOCK NUMBER	6	7	8	9	10
FAST-WHEEL LINES	547626	811857	551899	085998	152083
	109753	109753	109753	109753	109753
	084374	082374	082374	082374	082374
	993649	993649	993649	993649	993649
SECOND	818969	818969	818969	818969	818969
WHEEL	940157	940157	940157	940157	940157
LINES	667898	667898	667898	667898	667898
	053110	053110	053110	053110	053110
	251087	251087	251087	251087	251087
	024406	024406	024406	024406	024406
	876213	876213	876213	876213	876213

SETTING II

BLOCK NUMBER	1	2	3	4	5
FAST-WHEEL LINES	294144	477101	536780	526632	569925
	133969	133969	833969	833969	833969
	004644	004644	904644	904640	904640
	912750	912750	112750	112759	112759
SECOND	269407	269407	069407	069406	069406
WHEEL	078896	078896	678896	678893	678893
LINES	884157	884157	984157	984153	984153
	631213	631213	831213	831217	831217
	829089	829089	229089	229087	229087
	957373	957373	057373	057378	057378

SETTING II - Continued

BLOCK NUMBER	6	7	8	9	10
FAST-WHEEL LINES	047426	011057	151899	885898	852083
	839969	839969	839969	839969	839969
	902640	902640	902640	902640	902640
	113759	113759	113759	113759	113759
SECOND	068406	068406	068406	068406	068406
WHEEL	670893	670893	670893	670893	670893
LINES	987153	987153	987153	987153	987153
	858217	858217	858217	858217	858217
	229087	229087	229087	229087	229087
	056378	056378	056378	056378	056378
	091114	091114	091114	091114	091114

Figure 22. Deriving sequences from additives which show a hand resetting.

changed column.[2] That is, the digits in column 4 for instance, of block 2 reflect a displacement or movement of the wheels which produced the digits in column 4 of block 1 and are, therefore, assumed to be adjacent to the digits on the same line of block 1. Therefore, the sequence

[2]If that is the case, the way we formulated the arrangement of the blocks of ten by degree of columnar difference was the following: assume that block 1 is the point at which no notch actions have affected the second-wheel numbers; let line 1 of block 1 be represented, therefore, by six zeros, indicating that none of the six second wheels have been affected by fast-wheel notches; then compare line 1 of block 1 with the line 1 of block 2, and, since columnar changes are assumed to represent displacements of 1 step on the rims of second wheels by fast-wheel notches, put a 1 in positions where changes occur. If, then, line 1 of block 1 of setting I is compared with line 1 of all the other nine blocks, the following results:

SETTING I

Comparing	1	with	1	0	0	0	0	0
"	1	"	2	0	0	0	1	0	0
"	1	"	3	0	0	0	1	0	0
"	1	"	4	0	0	0	1	0	1
"	1	"	5	1	0	0	1	0	1
"	1	"	6	1	0	0	1	0	1
"	1	"	7	1	0	1	1	0	1
"	1	"	8	1	0	1	1	0	1
"	1	"	9	1	0	1	1	0	1
"	1	"	10	1	0	1	1	0	1

If the same type of comparison is made in the case of line 1's of the blocks in Setting II, the following countour results:

for the second wheel in dependence order for group 4 can be derived by chaining adjacent digits. If the fast-wheel notch has caused the second-wheel sequence to stop one in its cycle, then the changed column represents the digits ahead in the sequence--that is, we can say from lines 1 of block 1 and 2, that 7 is adjacent to and before a 6, and so on.

Note 2 (cont'd.).

SETTING II

Comparing	1 with	1	0 0 0 0 0 0
"	1 "	2	0 0 0 0 0 0
"	1 "	3	1 0 0 0 0 0
"	1 "	4	1 0 0 0 0 1
"	1 "	5	1 0 0 0 0 1
"	1 "	6	1 0 0 0 0 1
"	1 "	7	1 0 1 0 0 1
"	1 "	8	1 0 1 0 0 1
"	1 "	9	1 0 1 0 0 1
"	1 "	10	1 0 1 0 0 1

If, too, the line 2's of each block of ten for Setting I are compared in the same fashion, the same countour as shown above for Setting I results, and so on through comperisons of each of the 10 lines for the ten blocks. It will also be noticed that the columns 2 and 6 of the Setting I contour and columns 2, 4, and 5 of the Setting II contour shows zeros throughout; hence the notch positions on the fast wheels for groups 2 and 5 in the case of Setting I and 2, 4, and 5 for Setting II are set so that they act simultaneously. These contours, then, are representations of the action of the notches of the fast wheel.

From line	3	6	is adjacent	to	a	1
" "	7	1	" "	"	"	3
" "	2	3	" "	"	"	1
" "	5	1	" "	"	"	2
" "	10	2	" "	"	"	8
" "	6	8	" "	"	"	4
" "	9	4	" "	"	"	0
" "	8	0	" "	"	"	9
" "	4	9	" "	"	"	7

and 7 was the first digit of the sequence. The sequence as derived then reads: 7 6 1 3 1 2 8 4 0 9. This method of derivation, unfortunately, does not yield the notch position of the sequence derived.

Method (c) is the method whereby the sequence of the fast wheels can be derived from the ten possible fast-wheel lines by arranging the lines according to degree of difference using data from two different settings (or numbers). First, from figure 22, which shows the sets of ten second-wheel numbers listed under each fast-wheel line associated with them in the order of degree of difference from the first block, we can say that if the set of ten second-wheel numbers associated with the fast-wheel line reading 094044 is considered as a base for comparison, then there are two second-wheel sets which show the least amount of difference from the base--these are those associated with fast-wheel lines 877101 and 236180. Then it can be said that the set for the fast-wheel line 426732 shows the next least amount of difference from the base and so on for the others so that the order (with undeterminable members) of the fast-wheel lines for both settings is:

SETTING I			SETTING II		
Order		No. of column in fig. 22	Order		No. of column in fig. 22
1	0 9 4 0 4 4	1	1	(2 9 4 1 4 4)	1
2	(8 7 7 1 0 1)	2		(4 7 7 1 0 1)	2
	(2 3 6 1 8 0)	3	2	5 3 6 7 8 0	3
3	4 2 6 7 3 2	4		(5 2 6 6 3 2)	4
4	(5 6 9 4 2 5)	5		(5 6 9 9 2 5)	5
	(5 4 7 6 2 6)	6		(0 4 7 4 2 6)	6
	(8 1 1 8 5 7)	7	3	(0 1 1 0 5 7)	7
5	(5 5 1 8 9 9)	8		(1 5 1 8 9 9)	8
	(0 8 5 9 9 8)	9		(8 8 5 8 9 8)	9
	(1 5 2 0 8 3)	10		(8 5 2 0 8 3)	10

The exact positions of the fast-wheel lines are established in only three cases, and we have therefore only three lines placed relative to one another without ambiguity. The location of the bracketed lines is uncertain because of the fact that they came from sets of second-wheel numbers which showed the same degree of difference from the base. The following shows the three certain lines placed:

SETTING I	SETTING II
0 9 4 0 4 4	- - - - - -
- - - - - -	- - - - - -
- - - - - -	5 3 6 7 8 0
4 2 6 7 3 2	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -

Since in Setting I lines, through the principle of degree of difference, the 2 in the first position must precede the 4, (the location of which has been established exactly), and in Setting II lines, the 2 is adjacent to the 4 with no intervening 8, as in Setting I, we can establish the exact position of the lines 236180 and 877101 in Setting I thus:

SETTING I	SETTING II
0 9 4 0 4 4	2 9 2 1 4 4
8 7 7 1 0 1	4 7 7 1 0 1
2 3 6 1 8 0	5 3 6 7 8 0
4 2 6 7 3 2	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -

Now, since in column 2 of Setting I, the portion of the sequence established is 9732, we can assume that the sequence will read the same in column 2 of Setting II. If the complete list of Setting II lines is consulted, it will be found that there is a unique 2 in the second column sequence. Therefore, the line which has the unique 2 in the second position can be placed exactly. We have, then, up to this point established the lines thus:

SETTING I	SETTING II
0 9 4 0 4 4	2 9 4 1 4 4
8 7 7 1 0 1	4 7 7 1 0 1
2 3 6 1 8 0	5 3 6 7 8 0
4 2 6 7 3 2	5 2 6 6 3 2
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -
- - - - - -	- - - - - -

With fragments thus derived of all six sequences, the ten lines can be placed exactly, and all the fast-wheel sequences are established.

Method (d) yields only relatively correct sequences--that is, the order of digits which results from the solution is only one of four possible decimations of the actual sequence. This is true because of the fact that solution comes about as a result of the assumption that, in the case of hand resettings of the sequence, the resetting is not necessarily a displacement of one step on the rims of the wheels. The resetting may, actually, be a displacement of the sequence by three or four steps; yet, the assumption is that when a sequence has been displaced, the original position and the resetting position yield constant but relative positions of the digits in the sequence. In the two sets of 10 unique numbers generated by the fast wheels listed below, it will be noticed that columns 1 and 4 show a change which can be accounted for only as the result of a hand resetting. It is from this resetting that the sequences reset can be solved relatively:

	SETTING I							SETTING II						
	1*			4*				4*			1*			
1	8	7	7	1	0	1	1	4	7	7	1	0	1	
2	0	9	4	0	4	4	2	2	9	4	1	4	4	
3	8	1	1	8	5	7	3	0	1	1	0	5	7	
4	5	4	7	6	2	6	4	0	4	7	4	2	6	* Reset Wheels
5	4	2	6	7	3	2	5	5	2	6	6	3	2	
6	0	8	5	9	9	8	6	8	8	5	8	9	8	
7	5	6	9	4	2	5	7	5	6	9	9	2	5	
8	1	5	2	0	8	3	8	8	5	2	0	8	3	
9	5	5	1	8	9	9	9	1	5	1	8	9	9	
0	2	3	6	1	8	0	0	5	3	6	7	8	0	

From the illustration, we will derive the sequence for column 4. From line 1 of Setting I and line 1 and Setting II, we can say that "1" is a certain distance in the sequence from another "1", and so on the following statements can be made:

From	line	2	1	is	the	same	distance	from 0
"	"	8	0	"	"	"	"	another 0
"	"	3	0	"	"	"	"	8
"	"	9	8	"	"	"	"	another 8
"	"	6	8	"	"	"	"	9
"	"	7	9	"	"	"	"	4
"	"	4	9	"	"	"	"	6
"	"	5	6	"	"	"	"	7
"	"	10	7	"	"	"	"	1, and that

was the first digit derived. Now, all we can say is that the order of digits above is one of four possible decimations since we do not know how many steps there are between the digits which have been related above. We know in each case only that the digits related are the same number of steps apart.

If the constant distance between the digits related above is, for example, the interval 1, then the sequence would read as if the digits were adjacent, and the sequence would be 1 1 0 0 8 8 9 4 6 7. But if the interval were 3, the sequence would read 1 0 9 7 0 8 6 1 8 4. If the interval were 7, it would read 0 1 4 8 1 6 8 0 7 9. And, finally, if the interval were 9, the sequence would read 1 7 6 4 9 8 8 0 0 1. Any even interval would have given two chains of 5, and 5 would have given five chains of 2. Since the two digits between which the notch action occurs are adjacent in the original sequence, the proper decimation can be determined by finding the two digits and then choosing that decimation in which those two digits are actually adjacent.

By a continuation of these four methods the sequences were eventually all recovered.

21. Additive, key, development number, and delta relationships.--Since our hypotheses concerning the action of the additive generator not only accounted for all the observed data but also made possible the prediction of unknowns in the material, it was possible for us to duplicate this action. The example below shows successive movements of the machine and the additive generated by those movements in two of its 48 groups. The dependence order above the groups determines which wheel the notch positions affect. The nothhes on the wheels are circled and the repetitions caused by the notch actions are underlined:

	Group 1	Group 2
Dependence Order	3 5 2 4 1	1 4 2 3 5
	6 8 1 8 0	7 0 9 6 7
	3 7 0 7 2	8 0 0 9 7
	5 4 0 6 8	6 2 1 8 9
	5 4 1 6 6	4 3 5 7 1
	5 4 1 6 5	2 4 2 2 1
	5 3 2 2 5	5 2 7 0 2
	1 9 4 8 0	9 2 3 0 2
	4 7 0 3 5	5 5 4 1 8
	8 7 8 2 2	1 5 4 1 8
	6 6 2 2 9	3 6 8 4 6
	0 6 9 2 0	7 1 7 3 0
	7 1 1 4 2	8 7 9 3 3
	6 2 0 0 8	6 3 0 6 7
	3 0 0 8 6	4 3 1 9 7
	3 0 0 8 5	2 0 5 8 9
	3 0 1 8 5	5 2 2 7 7
	5 8 2 7 0	9 3 7 2 9
	5 7 4 6 5	5 3 3 2 9

Since such a complicated manipulation of sequences of digits as mixed as those in the illustration is not only cumbersome but conducive to considerable error, it was found convenient to establish a convention of referring all 240 sequences to the normal sequence from 0 through 9. It was decided to reorder all sequences in terms of the normal sequence, always speaking of the notch point as key 0. Thus the sequences in the illustration above can be arranged with all the notch positions parallel.

	Group 1				
Dependence Order	3	5	2	4	1
Key					
0	(0)	0	(1)	2	5
1	7	8	2	9	5
2	6	7	4	4	0
3	3	4	0	0	5
4	5	3	8	8	2
5	5	9	2	7	9
6	1	7	9	6	0
7	4	6	1	2	2
8	8	1	0	8	8
9	6	2	0	3	6

(The notch positions on the fifth wheels in dependence order are not circled because there is no wy of determining the notch since the fifth wheel does not affect any other wheels.) From this, the additives are translated into key terms thus:

	Group 1 Additive	Key Substitution
Dependence Order	3 5 2 4 1	3 5 2 4 1
	5 8 1 8 0	2 1 7 4 6
	3 7 0 7 2	3 2 8 5 7
	5 4 0 6 8	4 3 9 6 8
	5 4 ① 6 6	4 3 ⓪ 6 9
	5 4 ① 6 5	4 3 ⓪ 6 ⓪
	5 3 2 2 ⑤	5 4 1 7 1
	1 9 4 8 0	6 5 2 8 2
	4 7 0 3 5	7 6 3 9 3
	8 7 8 ② 2	8 6 4 ⓪ 4
	6 6 2 9 9	9 7 5 1 5
	⓪ 6 9 9 0	⓪ 7 6 1 6
	7 1 1 4 2	1 8 7 2 7
	6 2 0 0 8	2 9 8 3 8
	3 0 0 8 6	3 0 9 4 9
	3 0 0 8 ⑤	3 0 9 4 ⓪
	3 0 ① 8 5	3 0 ⓪ 4 1
	5 8 2 7 0	4 1 1 5 2
	5 7 4 6 5	5 2 2 6 3

Since the dependence order varies from group to group, it was necessary for general use to adopt the conventional dependence order 12345, because that is the order in which the wheels affect one another; hence the transposition:

	Group 1 Additive	Key Substitution
Dependence Order	1 2 3 4 5	1 2 3 4 5
	0 1 6 8 8	6 7 2 4 1
	2 0 3 7 7	7 8 3 5 2
	8 0 5 6 4	8 9 4 6 3
	6 (1) 5 6 4	9 (0) 4 6 3
	(5) (1) 5 6 4	(0) (0) 4 6 3
	5 2 5 2 3	1 1 5 7 4
	0 4 1 8 9	2 2 6 8 5
	5 0 4 3 7	3 3 7 9 6
	2 8 8 (2) 7	4 4 8 (0) 6
	9 2 6 9 6	5 5 9 1 7
	0 9 (0) 9 6	6 6 (0) 1 7
	2 1 7 4 1	7 7 1 2 8
	8 0 6 0 2	8 8 2 3 9
	6 0 3 8 0	9 9 3 4 0
	(5) 0 3 8 0	(0) 9 3 4 0
	5 (1) 3 8 0	1 (0) 3 4 0
	0 2 5 7 8	2 1 4 5 1
	5 4 5 6 7	3 2 5 6 2

It is still necessary, however, to be able to refer to the progressive action of the additive generator; conventionally, this was in terms of the series of numbers from 1 through 100,000 in order. In other words, we numbered each page of additive in the order in which it was generated by the additive generator. This serial designation we referred to as the "development number." But in order for us to number the five-digit additives generated by each of the 48 sets of five wheels, we had to adopt a consistent convention concerning the point where the numbering process began. We decided to adopt the convention of giving all additives in every group a development number designation on the basis of the

assumption that all five wheels had been set at their notch points (key 0).

If, therefore, a five-wheel machine had all its wheels set at their notch positions, the key for the additive which the machine would produce at that point would be 00000 and the development would also be 00000. The next printing of the machines would cause the wheels of the machine to be in the key positions 11111, and the development number designation would be 00001. The example below shows the relationships among development number, key, and additive, the additive equivalents (from given sequences) for key digits, and the additive as it would be printed by the machine in the 35241 dependence order for group 1.

Development Number	Key	Additive Equivalent for Key	Additive Transposed into Dependence Order for Group 1 (35241)
0 0 0 0 0	(0)(0)(0)(0) 0	(5)(1) 0 (2) 0	(0) 0 (1)(2)(5)
0 0 0 0 1	1 1 1 1 1	5 2 7 9 8	7 8 2 9 5
0 0 0 0 2	2 2 2 2 2	0 4 6 4 7	6 7 4 4 0
0 0 0 0 3	3 3 3 3 3	5 0 3 0 4	3 4 0 0 5
0 0 0 0 4	4 4 4 4 4	2 8 5 8 3	5 3 8 8 2
0 0 0 0 5	5 5 5 5 5	9 2 5 7 9	5 9 2 7 9
0 0 0 0 6	6 6 6 6 6	0 9 1 6 7	1 7 9 6 0
0 0 0 0 7	7 7 7 7 7	2 1 4 2 6	4 6 1 2 2
0 0 0 0 8	8 8 8 8 8	8 0 8 8 1	8 1 0 8 8
0 0 0 0 9	9 9 9 9 9	6 0 6 3 2	6 2 0 3 6
0 0 0 1 0	(0) 9 9 9 9	(5) 0 6 3 2	6 2 0 3 (5)
0 0 0 1 1	1 (0) 9 9 9	5 (1) 6 3 2	6 2 1 3 5
0 0 0 1 2	2 1 (0) 9 9	0 2 (0) 3 2	(0) 2 2 3 0
0 0 0 1 3	3 2 1 (0) 9	5 4 7 (2) 2	7 2 4 (2) 5
0 0 0 1 4	4 3 2 1 0	2 0 6 9 0	6 0 0 9 2
0 0 0 1 5	5 4 3 2 1	9 8 3 4 8	3 8 8 4 9
0 0 0 1 6	6 5 4 3 2	0 2 5 0 7	5 7 2 0 0
0 0 0 1 7	7 6 5 4 3	8 9 5 8 4	5 4 9 8 8
0 0 0 1 8	8 7 6 5 4	2 1 1 7 3	1 3 1 7 2
0 0 0 1 9	9 8 7 6 5	6 0 4 6 9	4 9 0 6 6
0 0 0 2 0	0 8 7 6 5	(5) 0 4 6 9	4 9 0 6 (5)
0 0 0 2 1	1 9 8 7 6	5 0 8 2 7	8 7 0 2 5
0 0 0 2 2	2 0 8 7 6	0 (1) 8 2 7	8 7 (1) 2 0
0 0 0 2 3	3 1 9 8 7	5 2 6 8 6	6 6 2 8 5
0 0 0 2 4	4 2 0 8 7	2 4 (6) 8 6	0 6 (4) 8 2
0 0 0 2 5	5 3 1 9 8	9 0 7 3 1	7 1 0 3 9
0 0 0 2 6	6 4 2 0 8	0 8 6 (2) 1	6 1 8 (2) 0

The relationship between key and development number could be easily found by means of IBM listings which

showed development number and the key which by definition is associated with it. For purposes of finding a development number if the key is known, the IBM lists were sorted according to key so that all possible keys could be found in numerical order with the development number shown beside it. For purposes of finding the key associated with any possible development number, the IBM lists were sorted according to development number and showed the key associated with it. These runs have been referred to as "Standard Cyclometers" (see paragraph 40). Another method of obtaining a key from a development number without the use of a cyclometer involves calculation. The first digit of key represents the fast wheel, which, in the development number, is the last digit. The second wheel in dependence order is represented by the second digit of key but is the next-to-last digit of the development number. And so on, until the last digit of the key, which represents the slowest wheel or the fifth wheel in dependence order, which, in turn, is represented by the first digit of the development number. This set of conventions is such, therefore, that the first digit of key is always exactly the same digit as the last digit of development, and the last digit of development number, therefore, represents the key position of the fast wheel, and the five-digit development number gives the total number of steps the fast wheel will have had to take from the arbitrary starting point of development number 00000. Take for example, the key for development number 23709; the fast wheel must have taken 23,709 steps on its rim from development number 00000 in order to produce the additive generated at development number 23709. The first digit of key for development number 23709 is 9 since the last digit of development number is the key position for the fast wheel and the first digit of key is the key position for the fast wheel.

But, in order to get the key position for the second wheel in dependence order, one must subtract from the total steps of the fast wheel, the number of times the fast wheel has caused the second wheel to stop in its cycle and print the same digit twice. The number of notch actions of the fast wheel will have been one-tenth of the total number of steps it took, and is, therefore, 2,370. The result of the subtraction is 21,339, which represents the total number of steps taken by the second wheel in dependence order in the course of producing development number 23709. Therefore, the key position for the second wheel in dependence order is 9. Now since the effect of the notch action of the fast wheel on all other wheels has been discounted, it is necessary to discount the retarding action of each of the other wheels, so that each time another digit of key for the development number is produced, until all the notch effects of wheels 1, 2, 3, and 4 have been discounted. The complete calculation is given below:

23709 = dev. no. of fast-wheel steps - first digit of key = 9
2370 = fast-wheel notch actions
21339 = number of second-wheel steps -second digit of key = 9
2133 = second-wheel notch actions
19206 = number of third-wheel steps - third digit of key = 6
1920 = third-wheel notch actions
17286 = number of fourth-wheel steps -fourth digit of key = 6
1728 = fourth-wheel notch actions
15558 = number of fifth-wheel steps - fifth digit of key = 8

The key corresponding to development number 23709 is thus found to be 99668. Clearly, this process may be reversed to obtain the development number for a given key. For example, given the key 99668, we may proceed as follows:

Step 1	Step 2	Step 3	Step 4	Step 5
9	9	09	09	709
X	X = 0	0	70	70
9	9	39	39	339
X	X = 3	3	33	33
6	6	06	06	206
X	X = 0	0	20	20
6	6	86	86	86
X	X = 8	8	8	8
8	8	8	8	8

Step 6	Step 7	Step 8	Step 9	Step 10
709	3709	3709	23709	23709
370	370	2370	2370	2370
339	1339	1339	1339	21339
133	133	133	133	2133
206	206	206	206	19206
20	20	20	20	1920
86	86	86	86	17286
8	8	8	8	1728
8	8	8	8	15558

In step 9, the development number is found to be 23709; step 10 need be taken only if it is desired to determine the number of steps for each wheel.

Up to this time, calculations have been illustrated for one machine only, that which generated the first group; the conventions were so set up that these same calculations might be made on any one of the 48 machines alike. Therefore, there arose the problem of what relationships existed among the different machines. This relationship was represented by what we called delta. This delta is only the constant lateral difference between any two given machines as long as neither of the machines

has been reset. Assume, for example, that two different pad-sheets have been covered and from the additive in each of the first six groups of the two pad-sheets, development numbers have been computed. Notice that the difference between the two development numbers of additive produced by the same machine is always the same from group to group:

Development numbers	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6
Pad-sheet						
5382	26385	99904	73244	29116	32880	59174
5428	26511	00030	73370	29242	33006	59300
	126	126	126	126	126	126

Notice, also, that if the development number for group 1 of pad-sheet 5382 were subtracted from the development number of group 2 for the same pad sheet, the same difference would exist as between the same two groups of pad-sheet 5428; the same relationship exists also between any two given groups of two different pad-sheets in the same setting series.

Develop-ment nos.	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6
Pad-sheet						
5382						
Lateral	26385	99904	73244	29116	32880	59174
differences	$\Delta_{1,1}$ 73519	$\Delta_{2,2}$ 73340	$\Delta_{3,3}$ 45872	$\Delta_{4,4}$ 03764	$\Delta_{5,5}$ 26294	
5428						
Lateral	26511	00030	73370	29242	33006	59300
differences	$\Delta_{1,1}$ 73519	$\Delta_{2,2}$ 73340	$\Delta_{3,3}$ 45872	$\Delta_{4,4}$ 03764	$\Delta_{5,5}$ 26294	

These delta relationships were most useful in the process of deciphering messages which were readable through an interpretation of development numbers within the limits of a setting series for which the wheel settings had been determined by the solution of an overlap. (See section IV for a discussion of the function of overlapping in determining the wheel settings.)

22. Determining the nature of the additive generator.-- The specific nature of the machines which generated the pages of additive used by the Germans for the one-time pad system was, particularly during the early period of solution, a matter of great concern. Gradually it became possible, from a series of inferences, to determine with a fair degree of certainty the exact principles involved in the machine.

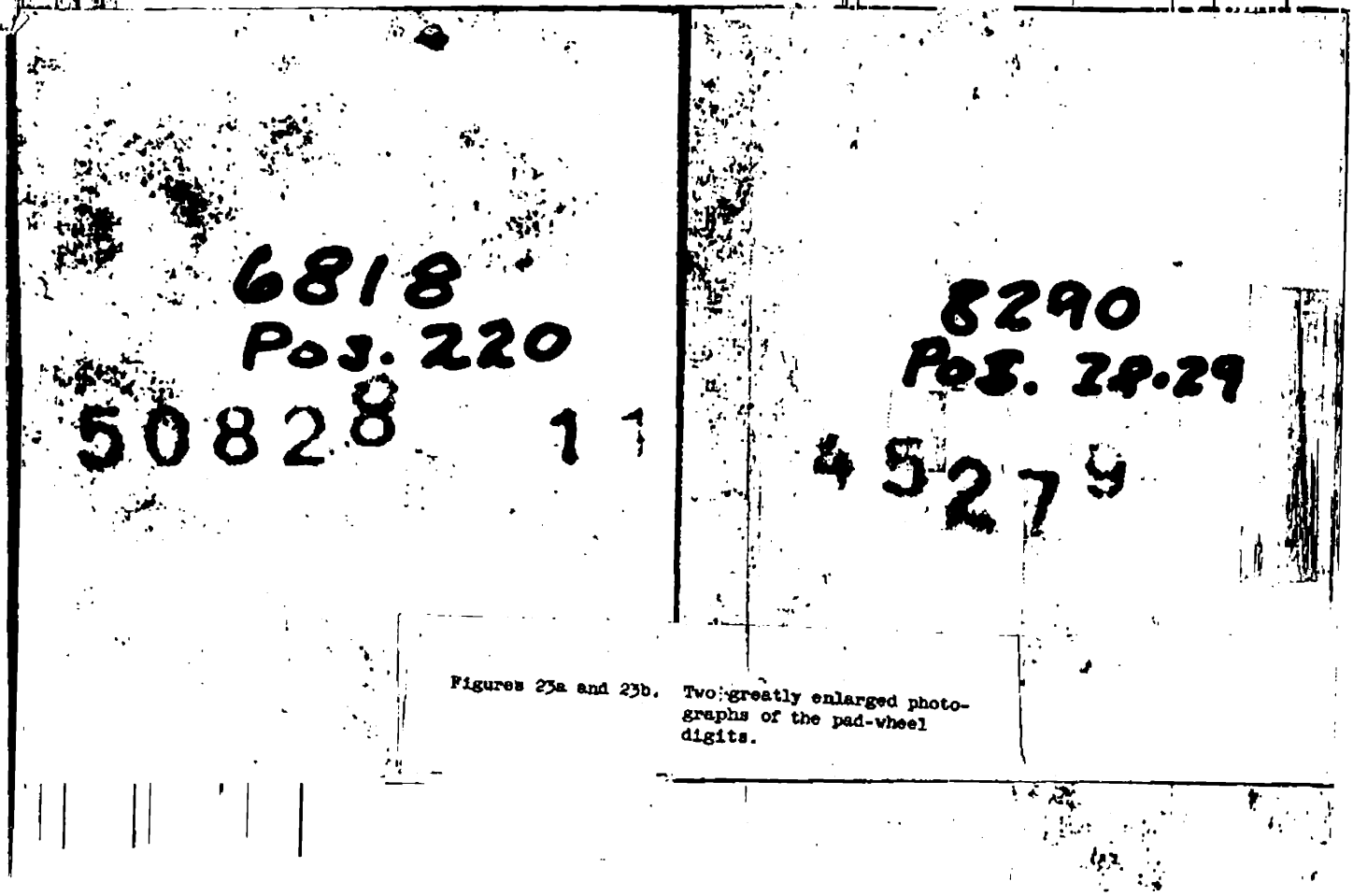
In the very beginning of solution, after the frequency distributions had been made on the 240 positions of the books of compromised pad-sheets, it was obvious that the elements of the machine which generated the digits on the pad-sheets involved 10 units; that is, when a hundred distributions were made on a given position throughout a volume of sheets and when that position showed a missing digit, there was always a compensation of frequency weight on another digit of those remaining and not an equal distribution of tallies on the remaining.

A close study by IBM experts of the actual photographs of the pad-sheets captured from Dr. Wolff revealed the fact that the elements of the machine must be wheels or turning disks with digits embossed on the surfaces of their rims. IBM experts were asked to inspect the actual photographs in order to determine whether or not the sheets had been produced by IBM scramblers or printed by IBM tabulators. In the course of the investigation, several aberrations or distortions

of digits were noticed. The greatly enlarged photographs presented in figures 23a and b show that the elements are disks or wheels when one considers the fact that the 8 in position 220 of pad-sheet 6818 (figure 23a) can have been both raised and only partially printed (and therefore penciled in later) only if the particular element which printed it were circular. The same observation can be made about the 2 and the 7 in position 28 and 29 of pad-sheet 8290 in figure 23b.

At the same time, one case of damaged digits in the same position was found. It will be noticed that the second digit of each of the five-digit numbers in figure 24 is damaged or broken in certain spots. Apparently, the machine which printed the additive was of the type of printing apparatus called a flat-bed press. Some metal particle may well have fallen into the bed; and when the machine was started, the wheel (in position 52) took three steps in its cycle without paper in place to cushion the wheels before the metal was removed or pushed out of place by the paper, thus the three digits were damaged by the particle of metal. When the sequence of digits embossed on the rim of the wheel in position 52 was derived, it was found to be 3628170547; the damaged digits 2, 8 and 1 are adjacent in the sequence. Probably, the same thing which damaged one digit damaged the others.

218



Figures 23a and 23b. Two greatly enlarged photographs of the pad-wheel digits.

Figure 24a. The defective 1.

DOCID: 4325626

8259
Pos.52
92802

8217
Pos.52
98305

Figs. 2a, 2b and 2c. The defective ? and 8.

The fact that the 8 did not break in the middle, even though the obstacle may have struck it there, can be explained by the fact that the 8 has a double thickness of metal in the center where the two oval halves meet.

The machine which generated the German additive was, then, an apparatus with 240 wheels or disks which had 10 digits in mixed sequence embossed on each of their rims. The 240 wheels were arranged in 48 groups of 5. Each group of five wheels operated as a separate machine and moved in step with all the others; the wheels seem to have received motivation simultaneously from the same or a similar source. The apparatus printed the digits on the pad-sheets directly from the wheels 240 at a time and can be said to have been analogous to a numbering machine in method of operation.

As confirmation of the inferences made about the nature of the additive generator, there came from GCCS by bag in February, 1945, a nontechnical description of a cipher machine sold to the German Government, which was essentially a description of the type of machine the Germans used to generate the additive for the one-time pad system:

> This morning Mr. Lorant of the firm of Loranco Ltd. Engineers, 42 Newlands Park, S.E. 26, was interviewed at the Foreign Office by Mr. Eastward, Commander Travis and Mr. Foss. He explained a printing device that his firm had supplied to the German Government in 1925. It had proved successful and there had been a repeat order in 1928 and another this year [1932]. The German Government had apparently never made any proviso that its nature should be kept secret and his firm was accordingly trying to sell one to His Majesty's Government also.

Mr. Lorant appeared to believe that it was a device for printing a given number of copies of a cypher telegram and then automatically distributing the type so that no unauthorised copies could be made afterwards. It became clear, however, that the real use of the device was for printing a given number of copies of a page of an adder or subtractor recyphering table and then automatically altering all the figures to print the next page. It was far easier to manage and quicker to change than ordinary moveable type.

The device, of which he showed a photograph, consisted of printed pages of 48 five-figure groups; eight lines with six groups in each line. Each five-figure group was printed by a quintet of wheels. (See Fig. 2[5] here the quintet is in position for printing the group 15437). The wheels had ten or more figures engraved on them (Mr. Lorant said up to thirteen) in an arbitrary order and every figure from "0" to "9" was represented at least once. The wheel could be turned by hand so that any figures could be printed. (The figures of the cypher telegram according to Mr. Lorant). Then, when a specified number of copies had been made, the wheels were all moved by cams through one or sometimes two units to be in position for printing the corresponding group on the next page. (Mr. Lorant said that this shift was to distribute the type and prevent unauthorized copies being made.) Contiguous wheels did not necessarily have the same number of units on their edges. Thus a quintet might contain two wheels with 11 units, two with 12 and one with 13. In the

first models, apparently, all wheels moved through one unit at each shift but they were now provided with extra cams so that they would sometimes move two units. The wheels, which were all numbered, could be taken out of their places and rearranged. The German Government had also 240 spare wheels to choose from.

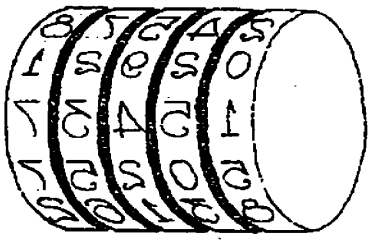


Figure 2 [5].

It will be seen that this device provides a means of printing a large number of different pages of figures in a short time, and that one page would be very difficult, if not impossible to deduce from the previous one. There was no device for numbering the pages, so presumably they need not be bound together in the order of printing. Mr. Lorant said that the German Government had printed two million pages of figures (cypher telegrams according to Mr. Lorant) without a breakdown.

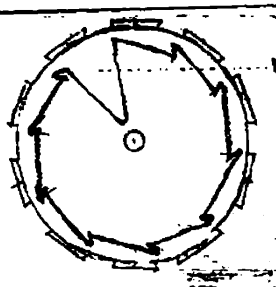
Mr. Lorant was asked to inform the Foreign Office of the cost of the machine.

14th June, 1932.

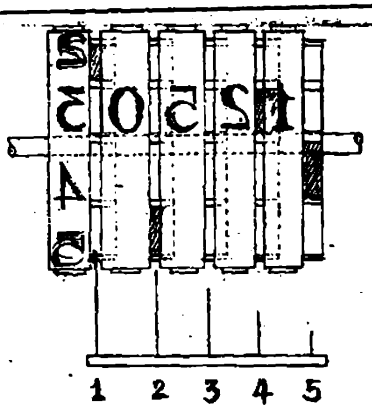
Later, TICOM material captured in Germany contained the bills of sale, receipts of payment, and requests for repairs. All the details in these papers conformed to those of the machine as it had been reconstructed.

23. The machine reconstructed.--The machine for generating a metrical series of numbers has wheels or disks with the normal series of numbers from 0 through 9 embossed in reverse on their rims; a notch position on all wheels in the form of a depression in a flange on the side of the wheel where the motivating finger grips the wheel to turn it in its cycle; nine nonnotch positions in the form of ledges on the flange on the side of the wheels, and the motivating fingers, each systematically shorter than the other in 12345 order with the largest finger opposite the fast wheel. In figure 26 the metrical numbering machine is at the position to print the number 12503. The tallest (or 1) finger motivates the units wheel (fast wheel). Notice that the notch position appears in the cross section of the "units" or fast wheel as a depression.

The German additive manufacturing machine, on the other hand, is in some senses the inverse of the metric numbering machine. Its principal items are wheels or disks with mixed sequences of ten numbers (which may or may not include all the possible 10 digits) embossed in reverse on their rims; a notch position on all the wheels in the form of a ledge in the flange on the side of the wheel where the motivating finger grips the wheel to turn it in its cycle; nine nonnotch positions, in the form of depressions in the flange on the



CROSS-SECTION OF WHEEL OF METRICAL NUMBERING MACHINE



FRONT VIEW OF FIVE-WHEEL METRICAL NUMBERING MACHINE

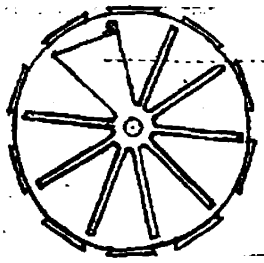
Figure 26.

side of the wheels; the motivating fingers, still with five different lengths but in a mixed order (see figure 27).

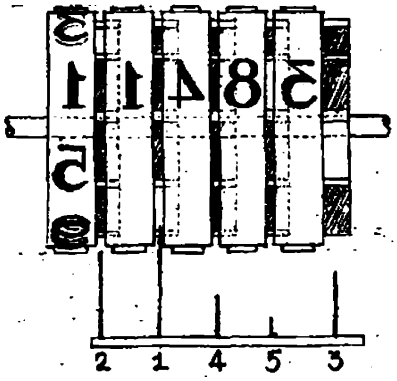
The two machines perform almost invesse tasks. The metrical numbering machine changes one digit at a time in the normal sequence of its fast wheel except when the notch point of the fast wheel comes up; then the fingers make it possible for the next wheel in order to turn one point in its cycle. The German Additive Manufacturing Machine, on the other hand, changes (by virtue of the fact that the fingers can plunge into depressions of all five wheels) the digits of all five wheels with each movement of the machine except when any one of the five wheels has a notch point in position, at which time the wheels which are motivated by shorter fingers than the wheel with the notch point in position do not turn in their cycles.

Despite the fact that the machines perform almost inverse tasks, both have a period of 100,000. If both machines had the same sequences embossed on their wheels, both machines would, in the course of 100,000 movements, generate exactly the same set of numbers, but in a different order.

24. The shuffling of pad-sheets after generation.-- In view of the systematic motion of the German Additive Manufacturing Machine and in view of its cyclic characteristics, the German cryptographers apparently realized the necessity of destroying the order in which the sheets were generated by shuffling the sheets thoroughly. In the course of reading a great number of messages enciphered with pad-sheets generated by this machine, we discovered two, more or less, systematic methods of shuffling the pad-sheets. These methods of shuffling were apparently never followed consistently nor to any great extent, but there was an observable tendency to



CROSS-SECTION OF WHEEL OF GERMAN ADDITIVE MANUFACTURING MACHINE



FRONT VIEW OF ONE OF FORTY-EIGHT CYCLOMETRIC MACHINES IN GERMAN ADDITIVE MANUFACTURING MACHINE

Figure 27.

follow simple psychological patterns in executing the two different methods of shuffling.

In the first method, as the pad-sheets came off the machine, they were stacked in handy piles of various sizes. When a great number of piles of pad-sheets had been generated, the sheets were shuffled by a process of gathering them one, two, or three at a time from the tops of the piles of sheets. After a hundred pad-sheets had been gathered from the tops of the piles, they were given serial pad-sheet numbers and were then bound into a volume. This method of shuffling, particularly when the operator doing the shuffling simplified his task by following a regular pattern of gathering, resulted often in a constant interval between pad-sheet numbers which were put on sheets generated in sequence (sheets with adjacent development numbers). If, for example, it were known that pad-sheet 2188 had been generated immediately preceding pad-sheet 5624, the chances were good that pad-sheet 2189 would immediately precede pad-sheet 5625 in generation order.

This first method of shuffling was used in the case of pad-sheets which had only one number on them--the serial page number. For traffic enciphered with pad-sheets of this type, the pad-sheets were used in serial order of pad-sheet number and the indicators on this traffic, therefore, were in serial order.

The second method, however, was used in connection with pad-sheets which had two numbers--the red serial page number, and a black number which was used as the indicator. The black numbers were not serial, but seemed to be in a completely mixed order. In the second method, as the pad-sheets came off the machine, they were stacked, as in the first method in handy piles of various sizes. But, in this case the stacks were produced from several different machines which were apparently printing other

sheets of additive at the same time. The stacks then were mildly shuffled within themselves by a simple process of changing positions of portions of the stacks. Then, the black indicator numbers were put on all the pad-sheets serially. After this process, all of the stacks were thoroughly shuffled together and were then gathered into lots of a hundred, numbered again serially with red page numbers and bound into volumes. Since the black indicator numbers were used on the traffic, the development number order of portions of the original stacks could be obtained by sorting the traffic on the black indicator number.

Thus, from the original additive compromised in 1940 from Dr. Wolff, almost the complete generation scheme of the German Additive Manufacturing Machine was brought to light and was largely understood before we tried to solve the generation scheme of the additive used on current traffic. Next came the problem of analyzing the hypothetical additive derived from isologs and the solution of completely new settings of the additive generator from cipher text.

SECTION IV

Cryptanalytic Development

25. The unknowns.--The preceding sections present the data known before messages were solved: the mechanics of the cryptography, the findings of the first attempts at solution, and the nature of the machine which generated the German additive. Some of the keying elements were still not understood, but we knew what they were. The unknowns involved in the solution were:

a. the dependence pattern (or the order of the motivating fingers) for each of the five-wheel machines in the frame;

b. the particular set of 240 wheels used in the machine at a given time;

c. the order or arrangement of the 240 wheels;

d. the settings of each of the 240 wheels in the frame when the machine began generating additive; and

e. the exact number of movements of the machines from the given starting point at which a a specific sheet of additive was produced.

The first three of these elements we called the setup; the first four, the setting series; the first five, the placement. When the setting series and one additive were known for it, all additives possible could be predicted. Each pad was in turn identified by a development number; and this development number was a short cut to the additive of a pad-sheet once all other elements were known.

26. The solution of the generation scheme of hypothetical additive.--The problem to be attacked first was the hypothetical additive--the great bank of additive recovered by the assumption of cribs for a large body of material. With the possibility of solution proved, the solution of the generation scheme was a simpler matter than the original entry. To be sure, it was complicated by new factors but in essence it involved the same procedure. The hypothetical additive was derived from several circuits, and, therefore, involved additive generated from something like at least ten different setups of the additive manufacturing machine. Consequently an additional problem of isolating homogeneous material was involved. Moreover, the additive was at times corrupt; naturally, the cribs were not infallible, and the transmitted cipher text was subject to garbles so that the additive text was far less reliable than that for which pad-sheets had been captured. The paragraphs below follow roughly the chronology of the several problems, but within them are discussed techniques of recovery developed at different stages of the investigation and in general arranged in order of an increasing number of unknowns.

27. Discovering the dependence pattern.--Three basic methods of solving the dependence pattern determine which of several already solved setups of the additive manufacturing machine might have been used to generate the additive to disguise the plain code in any given cipher text. First, is the method of assuming at least a two-group stereotyped beginning for several cipher messages

and looking for fast-wheel hits in each group; i.e., looking for a high percentage of single digit hits in the same position in group one, at the same time as a high percentage of hits in a single position of the second of any other group. By this approach the dependence pattern can be discovered. The next step in this method is to recover for each message as much additive as the cribs permit and compute development numbers for each possible setup so far recovered with that dependence pattern until a cluster of development numbers appear. The German habits of assembling pad-sheets led to this clustering in development numbers of consecutive pad-sheets (see paragraphs 23 and 24). In the absence of a reliable crib, cipher text can be aligned in development number order with the help of four-digit hits, caused by the encipherment of the same plain code by four-digit repetitions in the additive brought about by the notch position of the fast wheel. When this has been done, relative wheel sequences can be derived. From differences between the cipher digits in the sequence, the actual sequence can be determined, since the differences can be matched with the differences in the recovered plain sequence. If the sequence is in the same position as it was in an already solved set of 240, then the whole set of sequences together with the wheel order has been determined.

The second method of working from cipher text involves looking for four-digit cipher hits which, by the frequency of their occurrence and by the difference between the two digits which do not hit, can be determined to be the repetitions caused by repeated plaincode enciphered by additive containing a repetition caused by the fast-wheel notch. In this way, the fast-wheel position of one group can be found. With luck, the exact sequence of the fast wheel can also be derived from the cribs, and the arrangement of sequences and dependence pattern will have been determined also. At some point in the use of this method, however, it is necessary to assume the exact stereotype

unless the one-group stereotype is so certain that enough cases of four-digit repetitions occur for the sequences of the second, third, fourth, and fifth wheels in dependence order to be derived.

The third method involves the recovery of additive through the application of all known stereotyped beginnings for the given circuit and looking for four-digit repetitions in the additive in order to determine the dependence order and the arrangement of the set of sequences if that set of sequences is known. In this case, only one of the resultant additive sequences is good and therefore, computations must be made on many additives not actually used. The matter of determining what kind of clustering of development numbers actually reflects the original composition is a difficult one. But, when the proper setup of the machine has been assumed and development numbers have been computed on the hypothetical additives, the proper setup should show a more distinct pattern of clustering than in the other setups. In actual solution the three methods described above were seldom used singly or as simply as described, but were used in conjunction with one another at various times and with variations in procedure.

28. Sequence solution.-- after the dependence pattern has been found--or at least the fast-wheel position for one group--the problem is to determine the digits and their order on the rims of each of the 240 wheels. In the beginning, it is necessary to find as many cases as possible of pad-sheets which can be said to be adjacent by virtue of four-, three-, two- and one-digit repetitions caused by the same placode enciphered by additive with similar repetitions brought about by notch actions on the various wheels in dependence order. When this had been done and when the proper stereotype has been assumed, digits

which must be adjacent to one another in the sequence can be determined. Then, all ten digits can be chained. When the sequences have been solved, of course, development numbers can be computed, and the pad sheets can be placed in exact development number order. With the second group and all other groups throughout the remaining 37, the method of procedure is basically the probable-word method, requiring the assumption of the plain text of the messages in order to reconstruct the sequences from the hypothetical additive thus derived. The problem of identifying sequences with those already recovered is in essence the same, except that complete sequences need not be derived. With as few as four digits placed in order, the known portion of the sequence can be looked up in an index and the remainder of the ten digits placed.

29. Pad-sheet placement techniques.--With the dependence order and the sequences recovered, it remains to determine the exact points at which the 240 wheels are set when the additive manufacturing machine began to generate the additive of a given setting series. To this end, overlaps must be set up so that the exact text of the messages will yield the additive generated at one point in the course of the total movement of the machine. Before this process can be undertaken, the cryptanalyst must know the relationship among the pad-sheets in the setting series as regards generation so that the distances between them can be established and so act as a control of the overlapping process. The development numbers are an index to these relationships.

The various techniques of such placement of pad-sheets are almost all related to the fact that the Germans worked on a definite, regular plan of beginning and ending stereotypes. Accordingly, the problem of placement progresses in direct proportion to the ease

with which such stereotypes can be predicted within the texts. This process, however, applies only to initial pad-sheets in messages; pad-sheets which are not initial in messages do not have predictable beginning stereotypes and so must be reconstructed with the probable words revealed by the context of the initial and final pad-sheets when they have been recovered.

With some circuits, the number of stereotypes is sufficiently limited so that a great number of overlaps can be set up on the basis of a few highly probable stereotypes. But in others the variety is so great that the process is delayed by time-consuming trial and error. When beginning and ending stereotypes fail to produce results, punctuation groups of high frequency can be assumed in all 48 positions of the pad-sheets in order to reconstruct additive which will lead to the placement of the pad-sheet relative to the others and so to the prediction of the additives used to encipher the messages.

30. Overlap techniques.--The GEE overlap is not an overlap in the ordinary sense; to be sure, messages are superimposed on it to be used in additive recovery, but each message does not use the same additive but an entirely different set of additive digits. The GEE overlap is made up of messages which can be determined to use additive generated with the same original setting of the 240 wheels in the additive manufacturing machine, the same setting series. Even though two messages on an overlap may read on additive generated hundreds of thousands of steps of the machine apart from each other, they can be superimposed provided that there has been no resetting of the wheels of the machine between the time the first sheet was generated and the time the second sheet was generated. For when Θ_k had been recovered for one digit of a column of an overlap, if the relationship of the other messages to

it as regards the progression of the additive generating machine is known (through the development number, e.g.), then e_c can be predicted. Thus the technique of solution of a GEE overlap is similar to that with an ordinary overlap in the use of probable words to carry the text of the messages laterally but differs markedly in the fact that after such an assumption has been made, the hypothetical additive derived cannot be used in the same column without conversion to the terms of the progression of the additive generating machine. Additive for each message in the overlap must be generated by hand or by the use of catalogues prepared for the purpose.

31. Hand and machine decrypting.--After an overlap has been solved for 48 groups, any message which has been enciphered with a sheet of additive generated in the same setting series of the machine can be deciphered. It was the practice in the GEE section to decrypt a great number of pad-sheets (at least a hundred) at one time by machine. To be sure, any pad-sheet can be immediately deciphered by hand from the overlap to which it belongs, but at a certain stage in the development recovery became much more rapid than exploitation, and machine methods came into use. The procedure was to compute development numbers for the 48 groups of a single pad-sheet on the overlap. This was called the decode base pad. This pad-sheet could be one for which all 48 groups had been recovered and which was reasonably free of garbles. With this as an arbitrary base, any pad-sheet could be deciphered in three steps:

a. the addition to each of the remaining 47 groups of the difference between the development number of its first group and the development number of the first group of the base pad-sheet;

b. the computation of the additive for the new development number;

c. the addition of that additive to the cipher text of the pad-sheet to be deciphered.

Machine decoding, already an established practice with GBC, was also used in the exploiting of CBE. For discussion of the process, see paragraph 38.

32. Conspectus of recovery.--The unknowns differed in the several families of material isolated. To identify these families, we set up some conventions based on the unknowns; a trigraph designated the family, and its three letters stood in turn for the first three elements of the unknowns--the dependence pattern, the set of 240 wheels, and the wheel order. (The remaining elements are in a sense specific keying elements.) In the first two letters of these trigraphs, C identified the compromised material H, the hypothetical additive, and S material from the cipher text out of Shanghai. The third letter was simply an arbitrary alphabetical identification in order of recovery of the wheel orders. Thus, CCA and CCB identified the dependence patterns, a set of 240 wheels, and two wheel orders recovered from Wolff's material. In all, 26 such families or setups or keys are known. They were identified as follows:

CCA	HHC	HHG	HHL	HSA	JJV
CCB	HHD	HHH	HHM	HSB	JJW
CCC	HHE	HHI	HHN	JJT	JJX
HHB	HHF	HHJ	HHO	JJU	JJY
HHC					JJZ

The work done on these setups is summarized in the paragraphs which follow:

a. Compromised material.--The material compromised from Wolff was called CCA and CCB. Cryptanalysis of another body of cipher text revealed another member of this family: Washington-Berlin traffic for 1940. This material was found to use the same dependence patterns and set of wheels as the compromised material, but the wheels were arranged in a different order; hence the designation CCC. In the cryptanalysis, the problem was one of sequence identification, and the work was considerably hastened by the fact that traffic consistently used beginning stereotypes which extended sometimes as far as ten groups.

b. Hypothetical material.--The families which yielded hypothetical additive which was used in the prediction of additive to read messages included HHB, HHC, HHD, and HHE. These were based on cribs from MILON and LUCIE (military attache and air attache) circulars also sent in GEC. Cryptanalysis yielding hypothetical additive derived from isologs yielded six setups involving two sets of dependence patterns and two sets of 240 wheels (HH and JJ). The traffic yielding these keys was as follows:

Setup	Source
HHB	MILON and LUCIE Circular traffic, circa July 1944.
HHC	MILON and LUCIE Circular, December 1943 through May 1944.
HHD	MILON and LUCIE Circular, February through September 1943.
HHE	MILON and LUCIE Circular, December 1943.
JJY	MILON and LUCIE Circular, Date (?)
JJZ	MILON and LUCIE Circular, Date (?)

Other traffic belonged to these and to related families, but it did not yield hypothetical additive to be analyzed in a body. Rather the problem was that of identifying in it already recovered keying materials, for the cribs were not always reliable. This included:

Setup	Source
HHB	Circular 17111, November 1943 - March 1944
	" 00822, January-March 1945
	" 46444, July-August 1944
	" 62282, July-August 1944
HHC	" 28200, April-May 1944
	" 33735, May-November 1944
HHD	" 35599, May-July 1944
HHF	" 59999, September-November 1944
	" 62400, November-December 1944
HHH	" 00822, January-May 1945
HHI	MILON and LUCIE Circular, December 1942 and January 1943
HHI	Circular, Kenngruppe 62400 - December 1944-February 1945
HHJ	Circular, Kenngruppe 77377 - February 1945

c. Shanghai cipher text.--Three other families were involved in Shanghai-Berlin traffic. This problem was one of the most demanding in sequence solution; the sequences for some ten groups had been recovered when captured material made possible further solution. American work on this material ceased, and it was turned over to GCCS, who analyzed the captured additives to reconstruct the remaining sequences.

Setup	Source
HSA	Shanghai-to-Berlin traffic, late 1943-July 1944
JJX	Shanghai-to-Berlin traffic, August 1944
JJY	Berlin-Shanghai, January 1944 Shanghai-Berlin, after February 1945

d. Madrid cipher text.--The "black" nonserial pad-sheet indicators were first broken into in the exploratory work done on Berlin-to-Madrid and Madrid-to-Berlin traffic. This traffic presented the first cases in which several setups of the additive manufacturing machine were used in the same volumes of additive. This situation of mixed setups posed a very difficult problem of isolating homogeneous material for research. The HHF and HHG setups of the machine were solved completely as problems of sequence identification from the Berlin-to-Madrid and Madrid-to-Berlin traffic. The sources of the material were:

Setup	Source
HHB	Berlin to Madrid, November 1944-February 1945. Madrid to Berlin, late July-October 1944; after February 1945
HHC	Berlin to Madrid, after February 1945
HHF	Madrid to Berlin, October 1944-March 1945; September 1944
HHG	Berlin to Madrid, February-April 1945; October-November 1944

e. Other European circuits.--It was discovered in the Lisbon research that Madrid, Lisbon, and the other European circuits solved were using the same setups of the machine at various times. Often, therefore, work on the setups involved was done on more than one circuit

simultaneously and even in the same overlaps or setting series. This work showed that at certain times the exact development-number order of the pad-sheets could be obtained for long stretches by simply using the black nonserial pad-sheet indicator. In view of the fact that the work done on the European circuits other than Madrid by Arlington Hall was negligible in comparison with the amount of work done on the Tokyo circuits, the information on the European circuits is listed all together below:

Setups	Sources
HHB	Berlin-Lisbon - July-October 1944
	Lisbon-Berlin - June-July 1944;
	September-October 1944
	Berlin-Belgrade - September-October 1944
HHC	Berlin-Belgrade - September-October 1944
HHF	Berlin-Lisbon - October-November 1944
	Lisbon-Berlin - July-October 1944; February 1945
	Berlin-Belgrade - September-November 1944
HHI	Berlin-Lisbon - April 1945
	Lisbon-Berlin - October-November 1944
	Berlin-Bern - January-February 1945
HHK	Lisbon-Berlin - February 1945
	Berlin-Bern - March 1945
	Bern-Berlin - April 1945
	Berlin-Locarno - April 1945
HHL	Berlin-Lisbon - November-December 1944
	Lisbon-Berlin - October 1944-January 1945

f. Tokyo cipher text.--About the end of February, 1945, on G-2's instructions, the complete GEE unit began to work full time on the Berlin-to-Tokyo and Tokyo-to-Berlin circuits in order to produce as much intelligence of operational value as possible. At the

same time, LSIC agreed to take over the work on European circuits. For a while Arlington Hall continued with the Shanghai circuit. But this was abandoned because of the tremendous bulk of traffic in the Tokyo circuits and because of the complications in its solution.

The date period specified by G-2 as of importance in Tokyo traffic was from January 1944 with particular emphasis on the period after 1 July 1944. In this period, traffic for Tokyo amounted to 22,427 pad-sheets of cipher text, of which 11,060 sheets had been placed and decoded when work on the Tokyo circuits was discontinued in the beginning of February, 1946.

The work on Tokyo was particularly difficult because seven different setups of the machine were used in the course of the two years' traffic and were mixed thoroughly throughout the whole period. The following setups were used: HSA, JJU, JJV, JJW, JJX, JJY, and JJZ. In the course of the work on these setups of the machine, there were discovered and solved 204 different setting series. That is, 204 different overlaps had to be solved by the probable-word method in order to make possible the deciphering of the 11,060 pad-sheets which were placed.

g. Buenos Aires and Tangier cipher text.--In February, 1946, work was concentrated on Berlin-to-Buenos Aires, Buenos Aires-to-Berlin, Tangier-to-Berlin, and Berlin-to-Tangier circuits. Berlin-to-Buenos Aires for 1942 reads on HSA and HSB setups, and Tangier-to-Berlin reads on HHG. Buenos Aires-to-Berlin and Berlin-to-Tangier have not been broken into.

h. Captured material.--In the course of deriving the known setups of the machine, captured pads

yielded the following setups: HHG (checked), HHL, HHM, HHN, HSA (remainder), HSB, JJY, JJW, and JJX (checked).

SECTION V

Machine Processes

33. Introductory.--The following discussion of machine processes involved in the GEE problem does not pretend to be exhaustive technical information but attempts to show only the relationship of IBM to the work on the German one-time pad system and the function in that work. As such it does not do justice to the tremendous industry and ingenuity of the IBM specialists whose contribution to the success of the project cannot be measured.

34. Machine work in connection with research.--In the beginning of research, of course, it was the task of the IBM to make all the preparations for the complete additive index. Almost all of the derivation of the hypothetical additive from cribs was done by IBM. This process of derivation of additive was a matter of subtracting the cipher text of the GEE version from the code text of the

GEC version.[1] In this process, the resulting additive was summary punched into cards simultaneously with the process of subtraction. After all additive was derived, the complete standard index of additive was made using all the material available, including the compromised additive. In order to index all groups of additive, it was necessary to punch a separate card for each group of additive and two groups preceding and five groups following; this was done by offsetting. Then the material was sorted on all five digits of the group being indexed. Along with this job, IBM furnished a complete print of all pages of additive involved in the index.

After the initial discovery of abnormal single-digit frequencies within columns of the compromised additive, IBM was called on to produce a great number of tabulations. First, the machines selected all sheets of compromised additive from the complete additive index and made runs for a study of pattern positions and for sequence derivation. Moreover, all digits in positions discovered to belong to certain pattern positions were selected, sorted, and listed in various ways for a study of other pattern positions. For example, all sheets were selected which showed a certain set of Pattern V digits, and the digits in the Pattern III positions were selected, sorted, and listed to determine the relationship between the Pattern V and the Pattern III positions. Further, the relationships between the different sets of pattern positions were discovered with the aid of several different types of runs.

For the purpose of deriving the sequences of digits on the rims of the 240 wheels of the machine, IBM had to

---

[1] This gave the key in complementary form, the form in which we worked with it throughout the problem. In GLC the Germans had used the complementary form for deciphering so that both enciphering and deciphering processes used addition. In GEE the cryptographers were provided with only the version for human use because of the nature of the machine.

make several different types of runs. For example, digits of the additive groups had to be transposed and the groups sorted in reverse order; and the end of each group of repetitions in second, third, fourth, and fifth positions in dependence order had to be recognized. With this type of run, it was possible to chain the digits in the sequences on the wheels. With the aid of these types of machine runs the two wheel orders in the compromised material were derived.

At this point in the research, the concepts of the relationships between additive, key, and development number were formed, and IBM developed an index whereby one could, by knowing development number, find key and additive. This involved substituting actual additive digits for the key digits of the normal key sequence. The first attempt was made with groups 1 through 5 of the CCB setup. Later, this type of run was developed into what we called the standard cyclometer sorted on key and sorted on development number and the additive catalogue sorted on additive and sorted on development number.

Then, when the study of the hypothetical material got under way, runs similar to those requested for the research on compromised material were made by IBM, and from these we reconstructed six of the setups of the additive generating machine. To eliminate pad-sheets in the hypothetical material which had been generated on known setups of the machine, IBM computed development numbers for all 48 groups of all remaining pad-sheets, making one at a time the assumptions that the material had been generated on one of the four "HH" setups known up to that time. This type was called "Wheel Setting Determination."

For the cryptanalysis of Shanghai traffic, which yielded the discovery of the HSA and JJX setups of the

additive generator, IBM prepared an abridgment of the code book, sorted on all possible dinomial positions,[2] and prepared the first set of slide-run decks and produced positive results with the actual slide-run process by placing Shanghai pad-sheets.

At this time attempts were being made to break into Washington, Tokyo, Madrid, Lisbon, and several other circuits. IBM played its role in this part of the research by preparing message prints for these circuits, sorting the first-line cipher digits in increasing and decreasing dependence order to show the repetition at fast-wheel notch positions in the event of stereotyping in successive pages in development-number order.

With the Washington-to-Berlin circuit, these runs produced startling results since the Washington traffic almost always began with a neat stereotype which extended in some instances for as many as ten groups. From the Washington traffic, a new wheel order in the C material was discovered, but, because research on that particular date period was discontinued, the CCC setup was never completely derived.

In connection with attempts to enter the setups used in circuits not already exploited, a so-called crib slide run was made on a von Ribbentrop circular message of extreme length. This run was necessary because the GEE cipher version of the crib was not the same length as the GEC code version. Therefore, we tried through it to discover the setup of the additive generating machine by assuming an already known setup of the machine, placing the crib version in one juxtaposition, removing

---

[2] That is, on digits 1 and 2, 1 and 3,....1 and 5, 2 and 3, 2 and 4,.....4 and 5, and 5 and 1 for good measure.

the additive, computing development numbers, and inspecting the development numbers of the different pad-sheets to see whether the message used two pad-sheets with a constant difference and then, in the face of negative results, to perform the same process with another juxtaposition of the code and cipher versions. The additive derived from the juxtapositions of the crib versions was also studied to see if new setups of the machine could be discovered from fast-wheel hits. The run, however, proved unsuccessful.

Another type of run which helped tremendously in the task of placing pad-sheets and of discovering new setting series of the machine was the crib run. The crib run was of various types: (a) the single-group assumption which was a matter of subtracting an assumed five-digit code group from the proper cipher group, and, on the basis of the additive derived, computing development numbers, sorting the development numbers, and inspecting them for a clustering of pad-sheet numbers which would reflect the progression of the original generation; (b) the crib run which assumed a two-group crib, computed development numbers, derived deltas, sorted on deltas, with break-in control on any change in delta digits; (c) miscellaneous types of special runs involving two digits of delta and three digits of hypothetical cipher text produced by the encipherment of frequent code groups by additive assumed to have been produced by the German machine.

In connection with research to determine unknown setups of the additive generating machine which could be obtained from the captured additive, the IBM made the following types of runs on the first 12 groups of each pad-sheet:

a. sorts on red and black pad-sheet numbers;

b. sorts on the 12 fast wheels for purposes of identifying the setup to which they belonged;

c. computation of development numbers for certain groups out of the twelve which did not have doubled digits in the sequences;

d. sorts on the development numbers, for the purposes, in various situations, of eliminating pad-sheets not on the assumed setups, of checking inaccurately derived sequences, of ascertaining the extension of setting series, and of getting a pad-sheet to be used as the basis for generating all possible additive of a given setting series (called the base pad-sheet) for which overlaps had not yet been solved.

35. Traffic study by machine.--In the beginning of research on GEE, the problem of studying traffic was tremendous, and it was decided to let IBM assume as much of the burden as possible. Their work consisted, in general, of the following main functions:

a. punching traffic cards which contained all pertinent information for each separate sheet of cipher text in every message in circuits which were being worked on;

b. sorting all traffic cards on pad-sheet number, showing all other information;

c. sorting all traffic cards by circuit, date, worksheet number, and first two groups of cipher text;

d. making total digit counts, and digit counts according to months and other specified time intervals;

e. selecting cipher text needed for delta runs.

36. The slide-run process.--The slide-run is an IBM process of placing pad-sheets in relation to the total body of additive, especially those pad-sheets which do not occur at the beginnings of messages. The slide-run process depended upon a number of studies to determine precisely the plain-code groups with the highest frequency in the known usage of the Deutsches Satzbuch. These were made from the already solved GEC messages, which used the same code book. The original attempt at the slide-run process was made with a machine which could test only four of the five digits in a group and only five such groups. It was necessary, therefore, for the testing to be done on series of groups in which the fifth wheel in dependence order was also the fifth wheel in printing position.

The four-digit slide-run process was used to place pad-sheets in the Madrid and Shanghai traffic; in the course of this work the HHG, HBA, and JJX slide-run decks were made up. The success met with in this first attempt at slide-runs was such that there was no question as to the advisability of developing the technique. Accordingly, it was decided to construct a machine to test all five digits of eight groups of cipher text simultaneously.

The five-digit machine was used in various ways at various times. Certain cipher texts were selected as having the best probability of success. These were run singly against all additive cards in all of the decks which had been chosen as containing the likely additive. For some, it was impossible to predict the general area in which the sheets could be placed. It was necessary, therefore, to run these sheets singly against all decks on hand.

The most efficient method of testing used in the course of developing the slide-run process was what we called the "preselection run." This run was most efficient

when at least 100 pad-sheets could be gathered for testing at one time. The process involved, first, the subtraction of the 100 most frequent code groups (taken from the frequency study of Madrid traffic) from the first group of cipher text. The resulting artificial or hypothetical additive was sorted. All additive believed possible on the basis of recovered additive up to the time of the test was recorded on cards; these were sorted on the first group. Then the two decks were collated, and those which matched were put into the slide-run machine for testing on eight groups on the theory that the process of preselecting would lead in a very high percentage of cases to the cards which would yield good hits. The code groups, which were wired into the testing board of the slide-run machine, were changed several times, once on the basis of a frequency study of the plain code used in Madrid traffic and again on the basis of a frequency study of the plain code used in Tokyo traffic.

One other type of slide run was made in the course of the work in placing Tokyo pad-sheets. It was a slide run specifically designed for placing initial pad-sheets of messages. The methods used for this special run were the same as those described above, but a completely different recognition board was used which contained only those groups which could occur in the first four groups of initial pad-sheets.

Related to slide runs was the work done in preparing sorts on various productive slide-run decks on separate additive groups for the purpose of trying beginning cribs by hand. Then, also, in connection with key recovery of Tokyo traffic, IBM made for the purpose of hand placement of pad-sheets extensive sorts of the slide-run decks, which contained all additive assumed to have been produced by the German machine.

37. Message prints.--For the most efficient decrypting it was decided that before the cryptanalytic development of a circuit was undertaken, the whole block of traffic in process of recovery should be recorded on a message print; since the process of decrypting by machine involved the punching of cipher text on cards anyway, messages were recorded on cards for a whole circuit so that later when a message or single pad-sheet was placed for decrypting, the cipher text could be supplied by simply selecting the desired cards from the message-print deck.

Therefore, before the policy of concentrating on the Tokyo circuits was instituted, a great deal of message printing was done wholesale. For example, before work was discontinued on the European circuits, all the relevant traffic on the Madrid and Lisbon circuits (the two largest European stations) as well as a good number of miscellaneous European circuits later taken over by GCCS had been printed. Then, when it was decided that the Arlington Hall force should concentrate on the production of the Tokyo circuits, the complete 1944 and 1945 traffic in Tokyo was printed. These message prints were filed by pad-sheet number, and when a pad-sheet had been placed for decrypting, the copy of the message print was sent with the placement development number to IBM to be kept as a record until a sufficient number of pad-sheets had been placed to justify setting into motion the process of decrypting. Usually, the Machine Branch preferred to work on lots of pad-sheets amounting to at least 100 sheets.

With Far Eastern circuits the traffic of many stations of significance was generally printed for relevant date periods. Our priority directives from G-2 dictated which circuits should be printed and in what order they

should be processed as soon as the work of producing the Tokyo circuits had been accomplished.

38. Machine decrypting.--For the process of decrypting it was necessary to prepare an abridged code book, one which would decode approximately 90 per cent of the groups occurring in GEE traffic. In addition, message prints of cipher text and decode base pad-sheets, which gave the point of reference in the process of deriving readable text, were needed. In order to obtain significant information about the frequency of code groups used in German traffic, it was necessary in the first place to make frequency studies on material available at the time. The first frequency study, accordingly, was made on the GHC code version of the MILON and LUCIE (the discriminants of military and air attaches) circular reports which had been found to be isologs of GEE circulars. Such a study was not expected to yield reliable results for other circuits in the GEE system, but no other material was immediately available for the purpose until enough actual GEE traffic could be read to make revision worthwhile. These data obtained from the MILON and LUCIE study were used for decrypting purposes at first for Madrid and Lisbon and for a while, Tokyo, but after enough of this traffic was read, a new frequency study made possible the revision of the abridged code book.

In order to increase decrypting speed, it was necessary that we continually revise the decode base pad-sheets and add more decode base pad-sheets to the list. Actually, the policy was finally established that a decode base pad-sheet would be sent to IBM for every setting series of the German additive generating machine encountered in the process of setting up overlaps. In the process of overlapping, however, we discovered that in many cases in the same setting series of the machine certain groups had aberrations: they had reset themselves by an irregularity in their motion. In these cases, it was decided to send a new base pad-sheet for

each aberration also, so that when pad-sheets were decrypted in the vicinity of the aberration, the groups involved would be decrypted exactly, and thus obviate the necessity of special handling.

For the purpose of hand placement, IBM made up decode base pad lists showing the 48 development numbers and the 47 deltas. These were sorted on development number for each group and on delta in each of the 47 places. The form of the machine decryptment can be seen in figure 28.

39. Sequence lists and indexes.--In order to be able to recover other wheel orders of known sets of wheels of the German machine, it was necessary to have indexes made on all the different sets of 240 sequences known. These IBM provided as well as indexes of the differences of the digits in order in all the sequences. In the course of solution--particularly of overlaps which involved setups of the German machine for which additive catalogues were not available--IBM made up lists of sequences showing their location in all scrambles known. These lists were sorted by position within each separate setup to give a listing in the order in which the wheels were arranged on the additive generating machine. These lists were continually revised and enlarged as the solution progressed.

4. Cyclometers.--Probably the most useful instruments for facilitating hand processes involved in producing GEE were the cyclometers and additive catalogues. They were of four types:

a. sorts by development number showing four groups of additive in a single book, with 10,000 listings and the 10 possibilities for the slow wheel;

...EXT	GERMAN EQUIVALENT	GROUP NO.	CIPHER TEXT	ADDITIVE	WHEEL POSITION
05942	26	01	20034	85918	2
07127	39	02	91319	16118	1
07427	39	03	11061	96466	5
62183	6 NOVEMBER	04	22002	40181	2
50330	MOHR	05	01549	59891	1
31145	VERSCHLUSSSACHE	06	59402	32743	4
13976	C.	07	29601	94375	4
11552	(UNDECIPHERABLE)	08	92897	39765	3
19882	WA	09	16426	23462	5
04002	FUNKT	10	70433	30678	4
01302	A.	11	61203	40108	1
00012	MITTEIL ::	12	85788	75334	3
12360	ZU DORTIGEM TELEGRAMM NUMMER	13	25149	77721	1
13628	95	14	58622	65006	4
03284	12. MAI	15	03594	49790	1
26048	44	16	52474	56674	2
23474	ZIFFER	17	23273	79201	4
03214	2	18	31990	72324	3
00016	COLON ABSATZ	19	77026	33090	1
09834	ZU	20	98139	04705	2
14853	2.)	21	34955	70908	1
19352	GESCHUETZ	22	05597	24866	4
12081	PUNKT	23	27642	45249	1
12637	TEILEN	24	10036	62601	5
00094	ZIFFER KLARTEXT VORSTEHENDE 3 GRUPPEN.	25	60986	40118	1
18000	KOMMA DIE	26	19709	09301	5
07189	SICH	27	26458	41731	2
35572	IM LAUFE	28	97899	48783	3
17137	DER	29	59651	68586	5
55342	WAEHRE	30	54672	31770	4
09509	BEHANDLUNG	31	03576	06133	3
00092	ZIFFER KLARTEXT VORSTEHENDE 2 GRUPPEN.	32	02558	08545	5
19080	VER--	33	68531	11559	1
52661	ZOG	34	35092	67679	3
21454	--EN	35	97415	34049	3
31190	HABEN	36	21609	10591	4
07060	WERDEN	37	82498	05672	1
82168	ENTWEDER	38	07931	25237	5
39151	KALT	39	27590	12661	2
62631	GERICHTET	40	49864	23877	2
76500	UND	41	24095	52515	1
04704	ANSCHLUSS ::	42	12522	92232	4
09383	BEI	43	08996	01797	3
72781	TEMPERATUR	44	14007	68784	2
83022	VON	45	14869	79263	5
53488	RUND	46	69857	04631	1
36317	300	47	47660	99757	4
30242	GRAD	48	06128	34124	2

28 0010 000342 4751 2 4410273
DECK IDENTIFICATION PAD SHEET WORKSHEET NUMBER

Figure 28a. A machine decryptment.

CALL SIGNS	KILOCYCLES
DFV DE PLV	(MISSING)
EOA2 DE PLK2	(MISSING)
EOA4 DE PLK1	(MISSING)
PMA DE DFB	17520

FROM: BERLIN SIGNATURE: AUSWAERTIG
TO: TOKYO ADDRESSEE: DIPLOGERMA
DATE: 6 NOVEMBER 1944 DATE INTER.: 7 NOVEMBER 1944
GOVERNMENT: GERMAN DATE REC'D: 7 NOV. 44 DATE TRANS.: 28 JULY 45
SYSTEM: GFE MSG. NO.: 2639 STATIONS: 98, 92, 1 TRANSLATOR: 16181

(Part 1 of 4 Parts)

MOHR.
Classified Matter C.
Army Ordnance Branch reports to your telegram No. 95, 12 May 1944, paragraph 2:
To 2.) Gun tube parts [GESCHUETZROHRTEILE] which have become warped in the course of the heat treatment are either straightened cold and then annealed at a temperature of approximately 300 degrees . . . .

H-182416 W.S. No.: 4410273 (4751)

Figure 28b. The translation.

b. sorts by additive, showing key and development number and the ten possibilities for the slow wheel for a single group in one listing;

c. the standard cyclometer showing key and development number, sorted by key and sorted by development number, a run which later was set up as a "double cyclometer" showing the sort by key and the sort by development number listed side by side on a single page of the listing; and

d. the positional key index, which could be used for any setup of the machine on a given dependence pattern and involved strips with the sequences for each wheel in the different five-wheel machines listed laterally.

4. New developments in IBM technique.--In the first place, the GEE problem was the problem which gave immediate justification for the construction of a five-digit slide-run machine which would test eight groups of cipher text simultaneously.

Later in the production of GEE, it became evident that the slide-run process would be far more efficient if the code groups which the machine was wired to recognize were given log weights so that the value of a good hit in the testing process might be generally evaluated by the machine itself and the problem of hand-checking the hits reduced to a minimum. After a great deal of work in attempting to set up the mechanism so that code values could be weighted, the technique was perfected so that any future slide run will be considerably facilitated by the exploration of the GEE problem.

GEE was the first problem on which the "presensing punch" made possible the substitution of additive digits

for key digits, five digits simultaneously--a fact which reduced the amount of work necessary to reduce the additive catalogues and additive cyclometers to about one-fourth of their original size. The "presensing punch" also made possible the processes of substitution and transposition simultaneously. This process involved substituting additive for key digits and at the same time transposing the order of the digits from 1-2-3-4-5 dependence order to the order in which the German additive manufacturing machine printed the digits on the sheet of additive.

Another result of the demands of the GKE problem was the introduction of a "relay gate" for the reproducer. The "relay gate" was built for the purpose of substituting sequences for the key digits four groups at a time. This process was used primarily in catalogues of additive which were sorted by development number showing four groups at a time.

42. The M-1005 machine.--Early in the cryptanalytic development of GKE, it became apparent that, when solving sequences, identifying sequences, or breaking into new overlap areas, a great deal of hand generation of additive would be necessary. This was a cumbersome and time-consuming process, particularly before the standard cyclometers and additive catalogues were prepared by IBM. Therefore, Equipment Branch built a machine for generating additive for any specified stretch of development numbers on any setup of the additive manufacturing machine. The big problem involved in such a machine was that of accomplishing the transitions from development number to key in 1-2-3-4-5 order to additive transposed into printing order.

These problems were solved by the M-1005 machine. It played a well-defined and unique role in solution from the

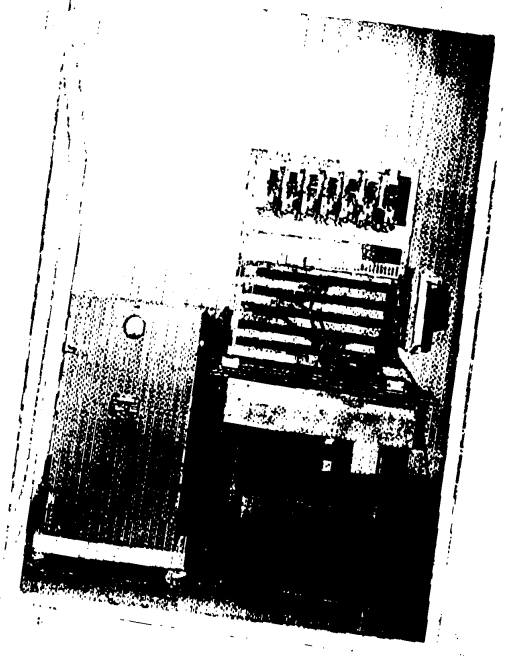
time it was constructed until the very last circuits were entered. The machine had the following components: seven rotary switches, five multiple-prong plugs, sequence plugboards for each group of additive, a key-setting board, and an Electromatic typewriter. See figure 28.

The seven rotary switches reproduced the exact motion of the wheels in the German additive manufacturing machine. Four of the five rotary switches had one dead point which reproduced the effect of the notch point. They were arranged so that the rotary switch for the fast wheel, or first wheel in dependance order, controlled the action of the four others when the dead point came up so that the four other switches remained motionless. The same principle was employed with the other three wheels with effective notch points. The sixth rotary switch controlled the carriage return of the typewriter; when the typewriter had printed five digits for a group, the carriage return would act. The seventh rotary switch stopped the machine after 20 groups of additive had been printed. The sixth and seventh rotary switches were always set at key 1 when a run was begun. The five rotary switches representing the five wheels were set, at the beginning of a run, at the key digits for the first additive group to be generated by the five wheels. Thereafter, the movement of the rotary switches duplicated the action of the wheels of the German additive manufacturing machine.

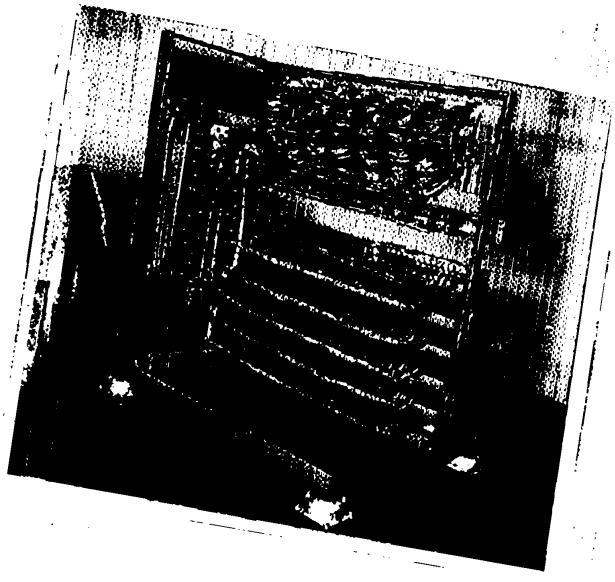
The sequence plugboard was a small, regular IBM plugboard into which five sequences of 10 digits could be wired to the normal key sequence so that five digits of additive could be substituted for key digits at once. The sequences of any group of any setup of the German machine could be wired into the plugboards. The multiple-prong plugs were used for replugging any possible dependence order.

When a stretch of additive was to be generated, the key for the first group of additive to be generated was

Figure 20a. The M-1005 machine. Front view showing control panel and robot head.



View from the apparatus side, showing relay-selector unit, rectifier, and rectifier mounting.



View of the relay-selector unit showing the wiring.

Figure 28 b. The M-1005 machine.

obtained by hand. The sequence board was wired with the five sequences of the particular group being generated; the plugs were plugged to duplicate the printing order of the group being generated; the key digits were used to set the five rotary switches at their beginning points; and the machine was ready to generate additive.

SECTION VI

Chronology of Solution

July 1940	Emil Wolff apprehended; 36 pads photographed and returned.
September 1943	Cryptanalytic research resumed.
31 August 1944	49,000 lines of hypothetical additive derived by machine.
November 1944	The 380,000 card index completed.
November 1944	Discovery of possibility of solution.
January 1945	First entry: reading of a message through prediction of the additive.
5 February 1945	Two reports on developments (including that of Major Cheadle.)
15 February 1945	First overlap set
25 February 1945	Plans drawn up for additive generating machine.
1 March 1945	First translations of five GEE messages.
18 April 1945	Messages translated directly from overlaps.
20 April 1945	First 16 pad-sheets, Tokyo to Berlin for October-December 1944, recovered and messages translated.

23 April 1945	All JJU and JJV sequences identified. Six pad-sheets of cipher text placed by Boston Item Cribs.
25 April 1945	The new M-1005 machine for generating additive completed.
27 April 1945	Thirteen of the last fourteen pieces of German diplomatic traffic (received at ASA) transmitted directly to Berlin were in GEE.
3 May 1945	Studies of development numbers and prediction of resettings of the additive manufacturing machine in GEE made to such an extent that the regulations for resetting of the machine were recovered and solved as overlaps.
16 May 1945	Part of a message read concerning uranium and discovery of pitchblende in Korea; MIS requested more information.
17 May 1945	Additive manufacturing machine used for decoding; 100 pad-sheets ready.
18 May 1945	1945 traffic: Berlin-Tokyo - 573 messages with 1,966 pad-sheets placed. Tokyo-Berlin - 655 messages with 3,049 pad-sheets placed.
18 May 1945	Presenser for new decoding machine cut in half the time necessary for decoding.
23 June 1945	New slide-run procedure and new recognition board for placing pad-sheets.

28 June 1945	260 books of captured pad-sheets received from GCCS; studies made of them to predict key of the same series.
10 July 1945	Ninety volumes of captured pad material of definitely predictable value processed by IBM.
31 July 1945	Of the 756 "A" priority pad-sheets, 557 (73 per cent) placed. Of the 584 "B" priority pad-sheets, 408 (70 per cent) placed.
2 August 1945	8,029 pad-sheets placed: 2,295 Berlin-Tokyo and 5,734 Tokyo-Berlin.
17 August 1945	8,964 pad-sheets placed: 2,637 Berlin-Tokyo and 6,327 Tokyo-Berlin. Of 191 overlaps set up, 179 solved. 276 volumes of captured pad-sheets received from GCCS.
16 October 1945	10,593 pad-sheets placed: 7,326 Berlin-Tokyo and 3,267 Tokyo-Berlin.
1 November 1945	10,500 pad-sheets placed: 3,239 Berlin-Tokyo and 7,261 Tokyo-Berlin.
15 November 1945	9,315 Berlin-Tokyo messages involving 23,280 pad-sheets, and 10,566 Tokyo-Berlin messages involving 31,167 pad-sheets received. Since 1934, 156,065 messages using 357,602 sheets received. 96 per cent "A" priority pad-sheets placed, 87 per cent "B" priority pad-sheets placed, 65 per cent "C" priority pad-sheets placed, 1,200 messages from July 1944 remain unplaced.

30 November 1945	10,644 pad-sheets placed: 7,336 Tokyo-Berlin and 3,328 Berlin-Tokyo. 98 per cent "A" priority pad-sheets placed, 88 per cent "B" priority pad-sheets placed, 64 per cent "C" priority pad-sheets placed.
21 December 1945	10,738 pad-sheets placed: 7,312 Tokyo-Berlin and 3,426 Berlin-Tokyo. Almost 100 per cent "A" priority pad-sheets placed. About 90 per cent "B" priority pad-sheets placed. About 66 per cent "C" priority pad-sheets placed.
2 January 1946	10,774 sheets placed. 7,328 Tokyo-Berlin and 3,446 Berlin-Tokyo. 99.6 per cent "A" priority pad sheets placed, 90.4 per cent "B" priority pad sheets placed, 67.5 per cent "C" priority pad sheets placed.
18 January 1946	10,882 pad-sheets placed: 7,408 Tokyo-Berlin and 3,474 Berlin-Tokyo. 99.6 per cent "A" priority pad-sheets placed. 91.4 per cent "B" priority pad-sheets placed. 68 per cent "C" priority pad-sheets placed.
1 February 1946	Work on Tokyo-Berlin circuit ended. (MIS no longer interested); one-fourth total traffic translated. Work continuing on Tangier-Berlin and Buenos Aires-Berlin circuits.
4 February 1946	10,997 pad-sheets placed: 7,476 Tokyo-Berlin and 3,521 Berlin-Tokyo. 99.6 per cent "A" priority pad-sheets placed. 94 per cent "B" priority pad-sheets placed. 69.1 per cent "C" priority pad-sheets placed. Tangier-Berlin circuit (1943) entered, Berlin-Buenos Aires circuit (March 1942) entered.

18 February 1946	11,060 pad-sheets placed: 7,509 Tokyo-Berlin and 3,551 Berlin-Tokyo. 25 pad-sheets placed Buenos Aires-Berlin. 127 pad-sheets placed Tangier-Berlin.
1 March 1946	212 placements) 1943-44 Tangier-Berlin traffic. 11 overlaps) MIS interested in traffic of April-May 1944, the last two months of heavy traffic. 9 placements) Buenos Aires-Berlin 1942 1 overlap) traffic.
19 March 1946	242 placements in 1943 Tangier-Berlin traffic, 3 overlaps in Buenos Aires-Berlin traffic.
17 May 1946	157 pad-sheets placed: Berlin-Buenos Aires. 295 pad-sheets placed: Tangier-Berlin. Pad placements on Tangier-Berlin traffic discontinued.
3 June 1946	207 Berlin-Buenos Aires pad-sheets placed.
17 June 1946	313 Berlin-Buenos Aires pad-sheets placed. 44 Buenos Aires-Berlin pad-sheets placed.
8 July 1946	349 Berlin-Buenos Aires pad-sheets placed. 74 Buenos Aires-Berlin pad-sheets placed.
16 July 1946	378 Berlin-Buenos Aires pad-sheets (1942) placed. 89 Buenos Aires-Berlin (2 December 1941-10 February 1942) pad-sheets placed.

2 August 1946	405 Berlin-Buenos Aires (1942) pad-sheets placed. 108 Buenos Aires-Berlin (1942) pad-sheets placed.
16 August 1946	455 Berlin-Buenos Aires (January-May 1942) pad-sheets placed. 136 Buenos Aires-Berlin (January-May 1942) pad-sheets placed.
26 August 1946	Cryptanalytic study stopped.
30 August 1946	Final score: 461 Berlin-Buenos Aires pad-sheets placed. 175 Buenos Aires-Berlin pad-sheets placed.

SECTION VII

Weaknesses in German Security

43. TICOM and the German attitude towards the additive generator.--In general, almost all responsibility for weaknesses in German security lies on the shoulders of the Foreign Office. Little or no progress was made in the solution of GEE from errors made by cryptographic clerks. The possibility of solution of GEE lay in the basic assumptions and misconceptions of the cryptographers in the Foreign Office (das Auswaertige Amt) in Berlin. From the TICOM material received on German cryptography, it is quite evident that the German office of cryptography was perfectly well aware of the mathematical limits, phases, cycles, and periods of all the elements of the additive generator which would be "unknown factors" to foreign cryptanalysts. In fact, many of the terms and conventions used by Herr Schauffler, the co-head of the cryptanalytic section of the German Foreign Office, were used by those working on the system during solution. One of his studies[1] makes clear not only that the limitations of the

[1] TICOM Document No. 3280: "Theorie eines Chiffrier-Numerierwerkes," Berlin, 3 December 1928, Section I.

machine were well known, but that the machine was also trusted, in spite of its systematic nature, as giving sufficient security for the system. Part of this study, translated, reads:

1. Description of the mechanism and statements of the problems.

On an axle which goes from right to left, there are r wheels arranged so that they can turn. The smallest number of wheels possible is 2; in practice up to now r has been 5. The wheel farthest to the right is called wheel number 1. Around the outside of each wheel, 10 printing surfaces are embossed, i.e., the 10 digits in mixed order; the sequences may be different ones on different wheels. When a wheel turns, each digit comes in turn to 10 positions; one of the 10 positions is the "printing position," the position in which the digit is printed by the numbering machine. The change-over from one position to the next is called "step." On each of the wheel numbers 2 to r, one of the 10 digits has special properties and is called the "influence digit." The mechanism is so constructed that all r wheels turn step by step in a specified direction, and after each step, the digits which are in printing position are printed. Only when the "influence digit" of one of the wheel numbers 2 to r is in printing position does it happen that all wheels which are to the right of the digit under consideration stand still for the duration of one step. Thus the result is that only wheel number r turns uninterruptedly and uninfluenced with a period of 10, while all other wheels are brought to a stop at certain positions, thus printing the same digit two or more times in succession.

This will be explained by means of an example. Figure 1 shows the sequences on the five wheels, i.e., the order of digits for each wheel as they come to printing position in uninfluenced succession. The influence digits are circled in black.

Figure 1

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

WHEEL NUMBERS

Figure 2

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

Figure 2 shows the five-digit groups in the order in which they are printed if the starting group is 50066. The repetitions which are caused by the "influence digits" are circled in red [here underlined].

The cipher numbering machine, then, has to some extent the inverse action of an ordinary numbering machine whose wheel number r also turns regularly with a period of 10, while one of its wheels, number to r-1, however, can step once only when all of the wheels to the left have the "influence digit" 9 in printing position.

The ordinary numbering machine has a period of 10 (for a five-wheel machine, the period 100,000).

We shall now prove that the cipher numbering machine has the same period and compute the periods which the individual wheels receive under the influence of the other wheels. For this purpose, in the next section, we will set up a formula which applies to the ordinary numbering machine, the cipher numbering machine we are describing and many similar mechanisms. In the third section, we will apply the derived formula to numbering machines and solve the problem just proposed. The last section will discuss the cipher numbering machine frame.

This extract shows how clearly the limits of the additive machine were understood by the Foreign Office. The conclusions drawn concerning the security of the machine were put in terms of a statistical comparison with the Enigma machine: A translation of Section IV of Herr Schauffler's paper follows:

IV. Cipher Numbering Machine Frame

n cipher numbering machines, all of which have the same number of wheels, r, and all of which run in phase are put into a printing frame. A practical example, to which we will return several times, is n = 48 machines, each with r = 5 wheels. These machines print variations of the numbers 0, 1.....9 to the (n.r) power; the number of different variations possible is:

$$V = 10^{240}$$

In the example at hand, therefore, the number of different variations which can be printed is:

$$V = 10^{240}$$

That is, the number which, written in the usual manner, is 1 followed by 240 zeros.

Since the separate cipher numbering machines in the frame all have the same period, Q, the frame, too, has the period:

$$Q = 10^r$$

Therefore, in the practical example, the period Q = 100,000, i.e., after 100,000 sheets have had 240 digits printed on them, the numerical variations will start to repeat.

Each of our variations to the (n.r)th power belongs to a "period series," i.e., to a series of Q variations which result from the moving ahead of the machines. There are, therefore,

$$S = \frac{V}{Q} = 10^{(n-1)r}$$

different period series which have no variations in common. In the example $S = 10^{235}$.

To compare the possibilities of combination, the Enigma may be referred to (see Patent Document DRP No. 429122). We ask: How many keys 240 digits long will the Enigma produce? The answer for the performance of the Enigma in the Patent Document mentioned is:

$$V = 11 \times 15 \times 17 \times 19 \times 26 = 24,350,000,000$$

therefore, an eleven-digit number, while the corresponding number for our present example of the cipher numbering machine frame is a 240-digit number.

Thus, with rather arrogant confidence, Herr Schauffler convinced himself and the Foreign Office of the security

of the one-time pad system. But he was thinking of security in terms of pure statistics rather than in terms of foiling completely the enemy cryptanalysts.

44. Error in over-simplified cyclical machine.-- In any one-time system, there is always danger in attempting to produce an extremely large amount of additive in an economical, systematic fashion. In the production of secure random mixed sequences, economy and systematic generation cannot safely be allowed to control completely the process of key generation.

In the case of the German additive generating device, the German cryptographers committed the error of supposing that the mere fact of no repetition of exact additive sheets was sufficient security to prevent the solution of the generation scheme of the additive. In reality, however, it can be said that the method of generation used in the German additive involved two basic weaknesses:

a. The unvarying period of 10 in the cycle of the fast wheel of each five-wheel machine and the repetition caused at an unvarying interval of 10 by the notch position on the fast wheel.

b. The fact that each of the 48 five-wheel machines was always in phase with all the other five-wheel machines in the frame, yielding a constant lateral relationship between the five-wheel machines in the frame.

The absolute period of 10 in the cycle of the fast wheel, taken together with the constant lateral relationship between the 48 different five-wheel machines, made it possible to observe (by looking at the fast-wheel positions of two or more groups of sheets generated in the same setting series) the fact that each group was

generated by a machine always in phase with the other machines. That the Germans not only used stereotypes at the beginnings and at the ends of messages but made a strict policy of stereotyping made it possible to observe this period of 10 in the cycle of the fast wheel in cipher text. And the lateral relationship between the different machines was particularly valuable in the solution of overlaps or wheel settings since it was necessary to use probable words to derive wheel settings from internal message text after the stereotyped beginnings.

45. Use of wheels and dependence patterns.--Even though the sets of fingers which motivated the wheels were removable and could, therefore, be changed and rearranged in a fantastically large number of ways and even though the sets of 240 wheels could be placed on the axles of the frame in an even greater number of ways and could even be mixed with other sets of 240 wheels, the Germans made meticulously certain that the sets of fingers (dependence patterns) were never changed on any of the machines; made certain that all wheels of a set of 240 were always used at the same time and that they were never mixed with other sets of 240 wheels, and in almost all cases, left the wheels in the same order and set at the same points for far too long a time for security purposes. By the proper manipulation of sets of wheels and motivating fingers, the Germans could easily have made solution from cipher text impossible. In many cases, the operators of the additive generating machine allowed the machine to produce as many as 10, 12, 15, and 30 thousand pad-sheets without changing anything about the basic setup of the machine. For purposes of solution, therefore, there was ample homogeneous material to use in most cases.

46. Systematic shuffling of sheets and their relationship to the indicators.--The Germans were apparently

aware of the necessity (from the point of view of security) of destroying the order in which the sheets of additive were generated. Therefore, the rule of shuffling the pad-sheets after they were generated was strictly followed.

But the operators made two errors in the shuffling processes:

a. the shuffling processes used were too simple and too systematic and not thorough enough, and

b. the shuffling processes were, in many cases, performed on and within material which, for solution purposes, was homogeneous and, therefore, could be used without question and in order of its use in transmission for entering into new circuits and for discovering new setting series.

The simple systematic methods of shuffling proved quite useful in the placement of pad-sheets in the order in which they were generated by the machine, that is, in relation to the development number which would yield readable text. As far back as late 1943, the Germans began using an indicator system for traffic in several large stations which did not show a clear series in the pad-sheets. The indicators seemed to follow one another in an unpredictable sequence. When this traffic was read, however, it became clear that the placement of pad-sheets in development number order could be facilitated by a study of the relationship between the indicators and the development numbers of the pad-sheets. Often it was possible to place as many as 30 or 40 pad-sheets in development number relationship with reference to one another by simply sorting on the "black" or nonserial indicators. This method of placing pad-sheets played a large part in the analysis of the Tokyo circuit.

47. The policy of stereotyping.--It is understandable that in such a large system as GKK a certain amount of stereotyping at beginnings and endings of messages could not be avoided. But the German Foreign Office insisted, as a matter of policy, that absolutely stereotyped beginnings and endings be used without any consideration for the point of beginning or ending in encipherment. This systematization of policy has long been recognized as one of the characteristics of the "German mind" and has been used to great profit in almost all work done on German systems.

48. The use of the same code book for two large systems.--Because of the fact that the Foreign Office placed so much confidence for security purposes in their encipherment, they did not hesitate to use the same code book for the two largest systems. This fact simplified the whole task of solution to a great extent and must be considered one of the basic errors of German cryptographers.

49. Isologs.--The Germans seemed to have equal confidence in the insolubility of GEC and GKK, the two large systems, and, therefore, began late in the use of both systems, to send exactly the same encodement of the same circular message in both of the systems. This fact made it possible for us to obtain a great amount of hypothetical additive for study in the early cryptanalytic research on GKK. This hypothetical additive was extremely valuable in solving setups of the German additive manufacturing machine in later research which might never have been solved otherwise. Finally, they failed to realize the importance of the compromise of the 3,500 sheets of additive in destroying the security of their systems.

In summing up the errors made by German cryptographers, we may say that the most important factor in the

weaknesses in German security was the uncritical confidence they placed in statistical proofs of the insolubility of the systems.

SECTION VIII

Conclusion - Lessons in Cryptanalytic Principles

The success met with in the cryptanalytic research done on the GEE system yielded, in terms of experience, two rather strong feelings which, in the future of cryptology, may have considerable value: --

a. that a one-time system need not be looked upon as hopelessly insoluble

b. That a consideration of elements position by position probably will play a more important role in the future when considering whether or not any given additive text is 'random.'

In view of the fact that GEE is the first case known in which a legitimate one-time pad system was solved, the general attitude toward such systems should undergo some change from the attitude commonly held before the solution of GEE. It should be assumed, that despite the probability that many cases of one-time systems, even where key text is available, will remain forever unsolved, any one-time key is susceptible of eventual solution, provided there is key text available.

In the future, also, the consideration of elements position by position in determining whether or not any key text is random has become a sine qua non of the text, thus instead of calling any given key text random simply by virtue of the distribution of the digits involved, we must decide on the basis of identity of digits plus the position it occupies.